

ID: 655326
Sample Name: office365 Validation.html
Cookbook: default.jbs
Time: 23:09:36
Date: 30/06/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report office365 Validation.html 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Process Tree 5
Malware Configuration 5
Yara Signatures 5
Initial Sample 5
HTML 5
Sigma Signatures 6
Snort Signatures 6
Joe Sandbox Signatures 6
Phishing 6
System Summary 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 10
Public IPs 10
Private 11
General Information 11
Warnings 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic 12
C:\Users\user\AppData\Local\Google\Chrome\User Data\253928f3-17c6-48cf-b231-2d628346fe0a.tmp 12
C:\Users\user\AppData\Local\Google\Chrome\User Data\298a0a15-b5e9-4871-82f4-99c12566f0e2.tmp 13
C:\Users\user\AppData\Local\Google\Chrome\User Data\3b475dfe-4be6-4691-b93e-a3b147eba555.tmp 13
C:\Users\user\AppData\Local\Google\Chrome\User Data\740d1272-9686-4f89-a592-5203cd65ca81.tmp 13
C:\Users\user\AppData\Local\Google\Chrome\User Data\8007631f-3e0e-4574-b8d1-6dc6700b6143.tmp 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\887fa3d8-04dd-407a-8391-7163efc10350.tmp 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3c084803-dc84-49cd-9d0f-24465b2ea809.tmp 15
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4ef8fddd-7c36-4075-a355-f0dba4be53be.tmp 15
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\539b84f3-4feb-4d02-b707-89020068be86.tmp 15
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\566fec97-48f9-46b2-a073-efe0e628cdd0.tmp 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5c781412-7eec-468b-bc04-58f62f911d34.tmp 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7f517936-9ccb-4598-bded-8d34ddae261a.tmp 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\830b2dfe-c5b2-4a8c-bd2f-6e12646f6da5.tmp 17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\84064e56-577a-4560-ac9a-e992f0f65129.tmp 17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json 17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy) 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy) 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy) 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy) 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\7da08f8a-dadd-45b7-9551-c4661cd51be9.tmp 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State

(copy) 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\190c4c6d-14a3-4c53-8082-9ee234662c1e.tmp 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Network Persistent State (copy) 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a353eaae-12d3-48a3-98fe-04ddeb2cfbf1.tmp 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a6d66304-18f2-4158-b7cf-2572974c5646.tmp 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ac9c4078-e4fe-45c3-99b4-7b0256074620.tmp 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\beb7615e-6f01-4819-a0a9-d6e7d55ad463.tmp 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bee1c790-598b-46ba-87e7-b0c9741604a7.tmp 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c94898ba-aa6a-4201-86a9-5e5a0636bdd7.tmp 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cf9cd8be-a809-459c-9b27-079ca4e1861f.tmp 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d32650d4-420c-4d7e-a10f-e5e36d71df04.tmp 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy) 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e28b655b-9ac8-4011-884b-eda5321cd29a.tmp 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy) 26
C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy) 26
C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir6304_1087354267\Ruleset Data 26
C:\Users\user\AppData\Local\Google\Chrome\User Data\a82d342c-fe02-477b-a699-9a3b0ef04c2b.tmp 27
C:\Users\user\AppData\Local\Google\Chrome\User Data\abc62dfa-9aca-4e7a-8c08-73583ae6653e.tmp 27
C:\Users\user\AppData\Local\Google\Chrome\User Data\ad71061a-ba54-4486-a33a-afc263ce1c10.tmp 27
C:\Users\user\AppData\Local\Google\Chrome\User Data\c2621fca-4d40-46a2-944a-d39715a9da4c.tmp 28
C:\Users\user\AppData\Local\Google\Chrome\User Data\c27aceda-310b-416d-9485-c36fda0b03fa.tmp 28
C:\Users\user\AppData\Local\Google\Chrome\User Data\d48bf9d3-ab13-4e92-b163-c8106af1aee1.tmp 28
C:\Users\user\AppData\Local\Google\Chrome\User Data\eb1e3843-b299-4531-bbb2-c8c0f9ef648e.tmp 29
C:\Users\user\AppData\Local\Google\Chrome\User Data\ec96d661-b31f-4e9a-b125-d48d98660367.tmp 29
C:\Users\user\AppData\Local\Temp\201465c9-d45e-4764-9cc5-184c46c51ed9.tmp 29
C:\Users\user\AppData\Local\Temp\6304_1644556325\LICENSE 30
C:\Users\user\AppData\Local\Temp\6304_1644556325_metadata\verified_contents.json 30
C:\Users\user\AppData\Local\Temp\6304_1644556325\crl-set 30
C:\Users\user\AppData\Local\Temp\6304_1644556325\manifest.fingerprint 31
C:\Users\user\AppData\Local\Temp\6304_1644556325\manifest.json 31
C:\Users\user\AppData\Local\Temp\6304_2066690316\Filtering Rules 31
C:\Users\user\AppData\Local\Temp\6304_2066690316\LICENSE.txt 31
C:\Users\user\AppData\Local\Temp\6304_2066690316_metadata\verified_contents.json 32
C:\Users\user\AppData\Local\Temp\6304_2066690316\manifest.fingerprint 32
C:\Users\user\AppData\Local\Temp\6304_2066690316\manifest.json 32
C:\Users\user\AppData\Local\Temp\6304_848482870\Recovery.crx3 33
C:\Users\user\AppData\Local\Temp\6304_848482870_metadata\verified_contents.json 33
C:\Users\user\AppData\Local\Temp\6304_848482870\manifest.fingerprint 33
C:\Users\user\AppData\Local\Temp\6304_848482870\manifest.json 34
C:\Users\user\AppData\Local\Temp\6304_91553969_metadata\verified_contents.json 34
C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_pnacl_json 34
C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_for_eh_o 35
C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_o 35
C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_crtend_o 35
C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe 35
C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_libcrt_platform_a 36
C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_libgcc_a 36
C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_a 36
C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_dummy_a 37
C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe 37
C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe 37
C:\Users\user\AppData\Local\Temp\6304_91553969\manifest.fingerprint 38
C:\Users\user\AppData\Local\Temp\6304_91553969\manifest.json 38
C:\Users\user\AppData\Local\Temp\eced9d10-a2e5-4d97-8392-cfa9e1143505.tmp 38
C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\201465c9-d45e-4764-9cc5-184c46c51ed9.tmp 39
C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\bg\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\ca\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\cs\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\da\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\de\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\el\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\en\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\en_GB\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\es\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\es_419\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\et\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\fi\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\fil\messages.json 43
C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\fr\messages.json 43
C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\hi\messages.json 43
Static File Info 44
General 44
File Icon 44
Network Behavior 44
Network Port Distribution 44

TCP Packets 44
UDP Packets 46
DNS Queries 47
DNS Answers 47
HTTP Request Dependency Graph 47
HTTPS Proxied Packets 47
Statistics 56
Behavior 56
System Behavior 56
Analysis Process: chrome.exePID: 6304, Parent PID: 1468 56
General 56
File Activities 57
Registry Activities 57
Key Value Modified 57
Analysis Process: chrome.exePID: 6572, Parent PID: 6304 57
General 57
File Activities 57
Disassembly 58

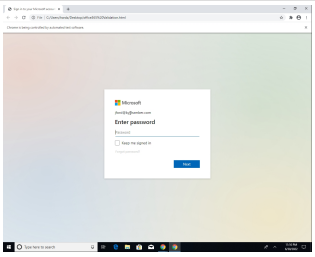
Windows Analysis Report

office365 Validation.html

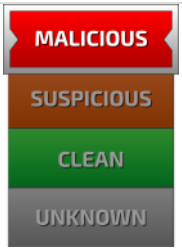
Overview

General Information

Sample Name:	office365 Validation.html
Analysis ID:	655326
MD5:	d093787907af46..
SHA1:	8b55805d15db65.
SHA256:	bffffe8e717d7e8…
Infos:	



Detection



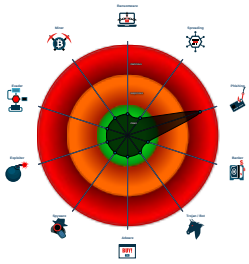
HTMLPhisher

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish44
- Yara detected HtmlPhish10
- HTML document with suspicious title
- Phishing site detected (based on log…
- HTML body contains low number of …
- IP address seen in connection with …
- None HTTPS page querying sensitiv…
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6304 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "C:\Users\user\Desktop\office365 Validation.html MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6572 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1560,1595704125475944836,7329412530459423612,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1956 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
office365 Validation.html	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	

HTML

Source	Rule	Description	Author	Strings
89955.0.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Copyright Joe Security LLC 2022

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Phishing



Yara detected HtmlPhish44

Yara detected HtmlPhish10

Phishing site detected (based on logo template match)

System Summary

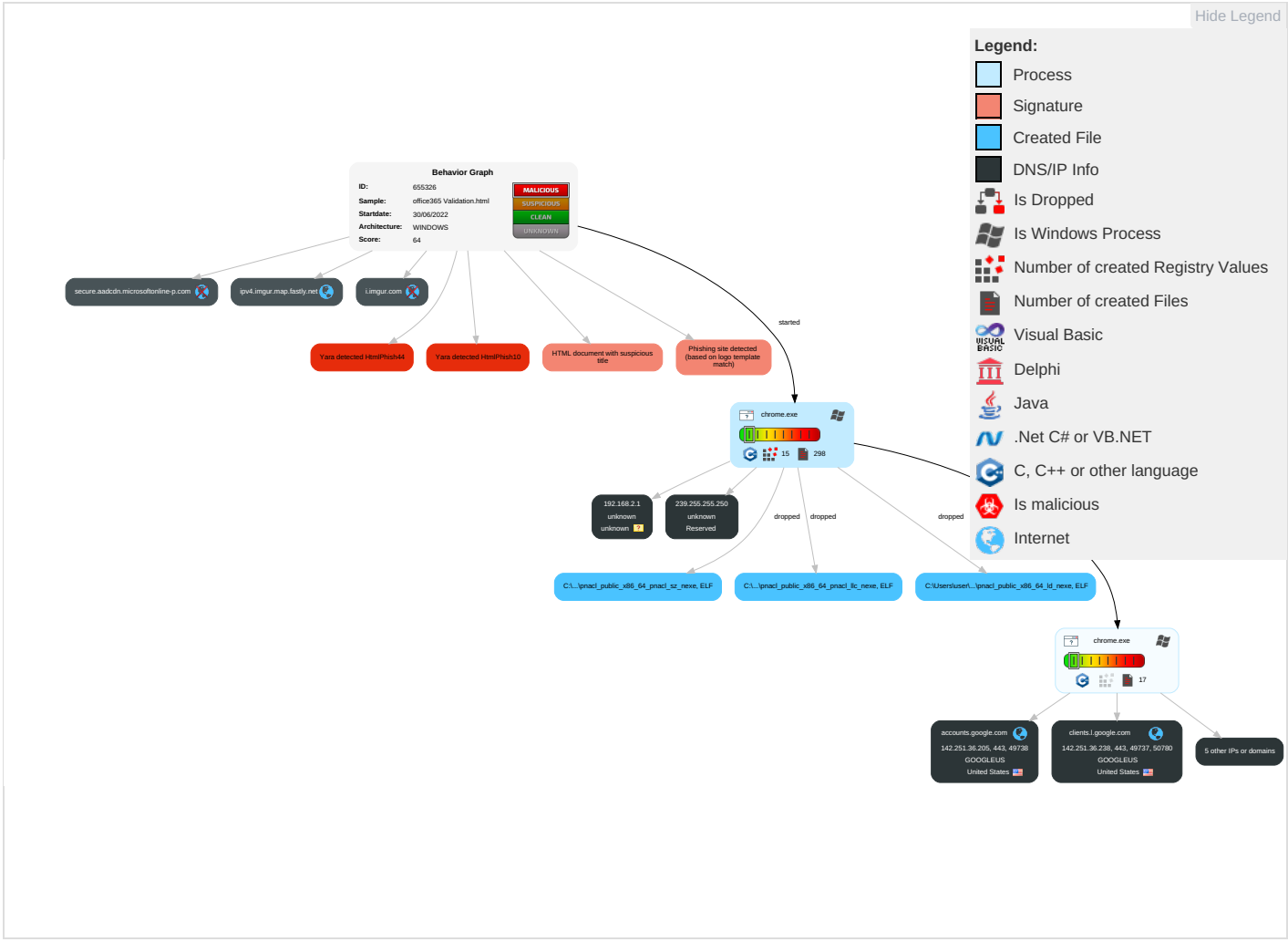


HTML document with suspicious title

Mitre Att&ck Matrix

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

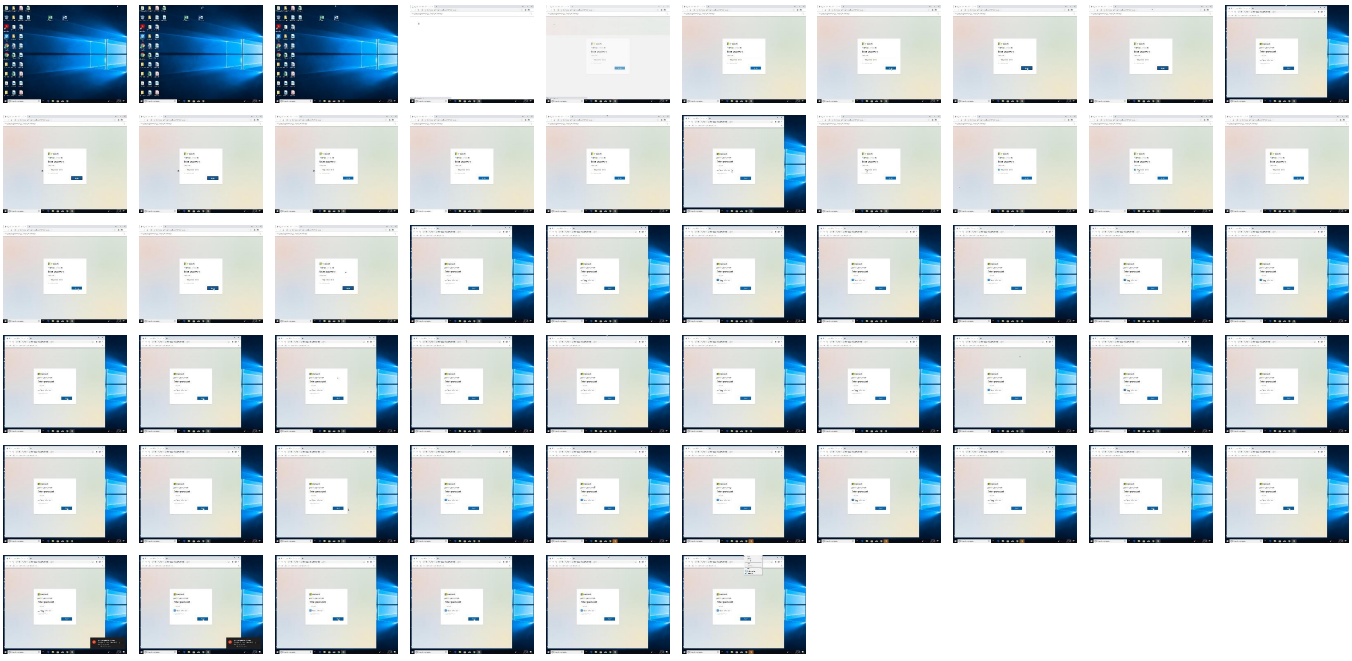
Behavior Graph

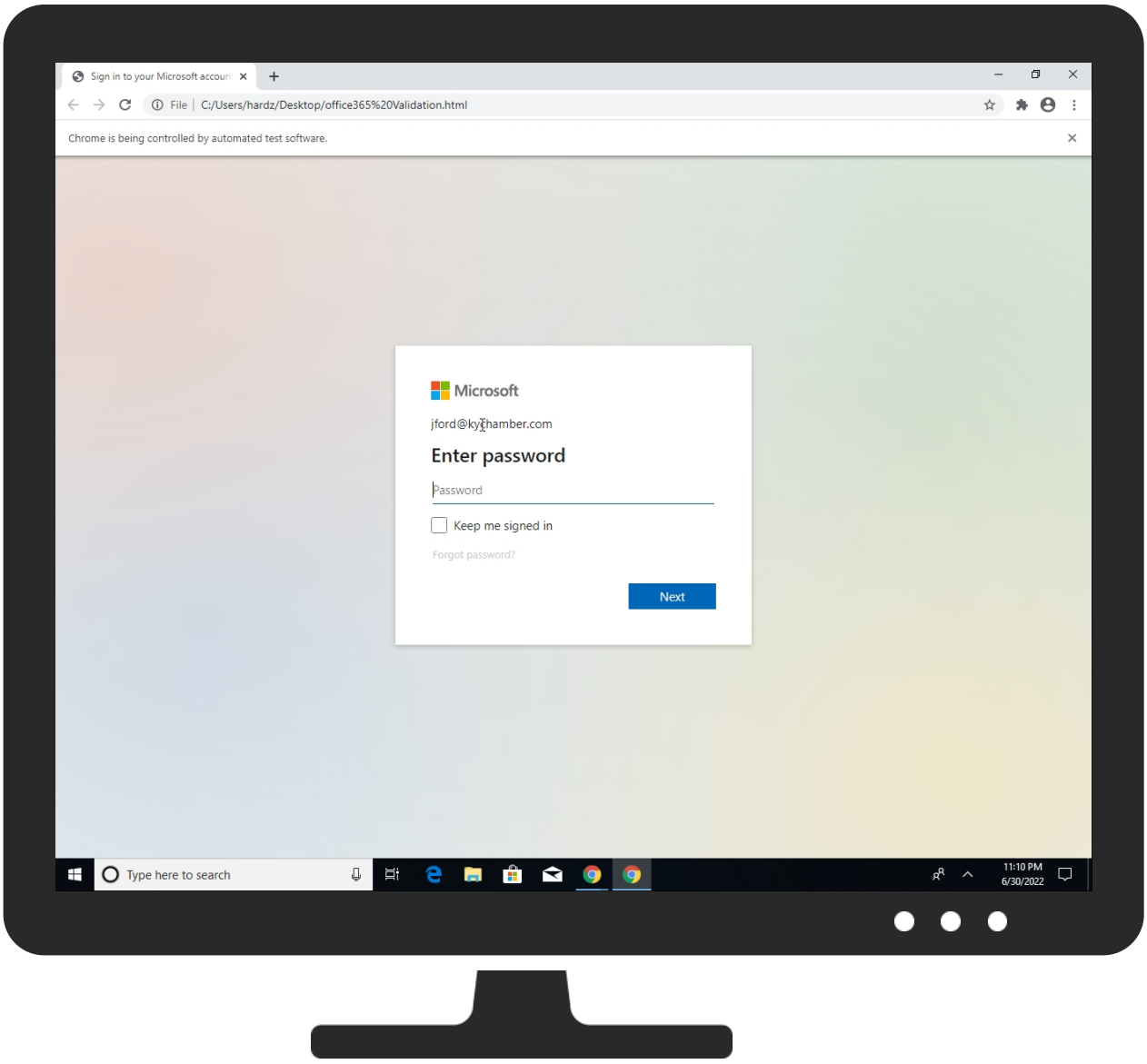


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Copyright Joe Security LLC 2022

Domains

Source	Detection	Scanner	Label	Link
ipv4.imgur.map.fastly.net	0%	Virustotal		Browse
secure.aadcdn.microsoftonline-p.com	0%	Virustotal		Browse

URLs

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

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.251.36.205	true	false		high
clients.l.google.com	142.251.36.238	true	false		high
ipv4.imgur.map.fastly.net	151.101.112.193	true	false	• 0%, Virustotal, Browse	unknown
clients2.google.com	unknown	unknown	false		high
secure.aadcdn.microsoftonline-p.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
i.imgur.com	unknown	unknown	false		high

Contacted URLs

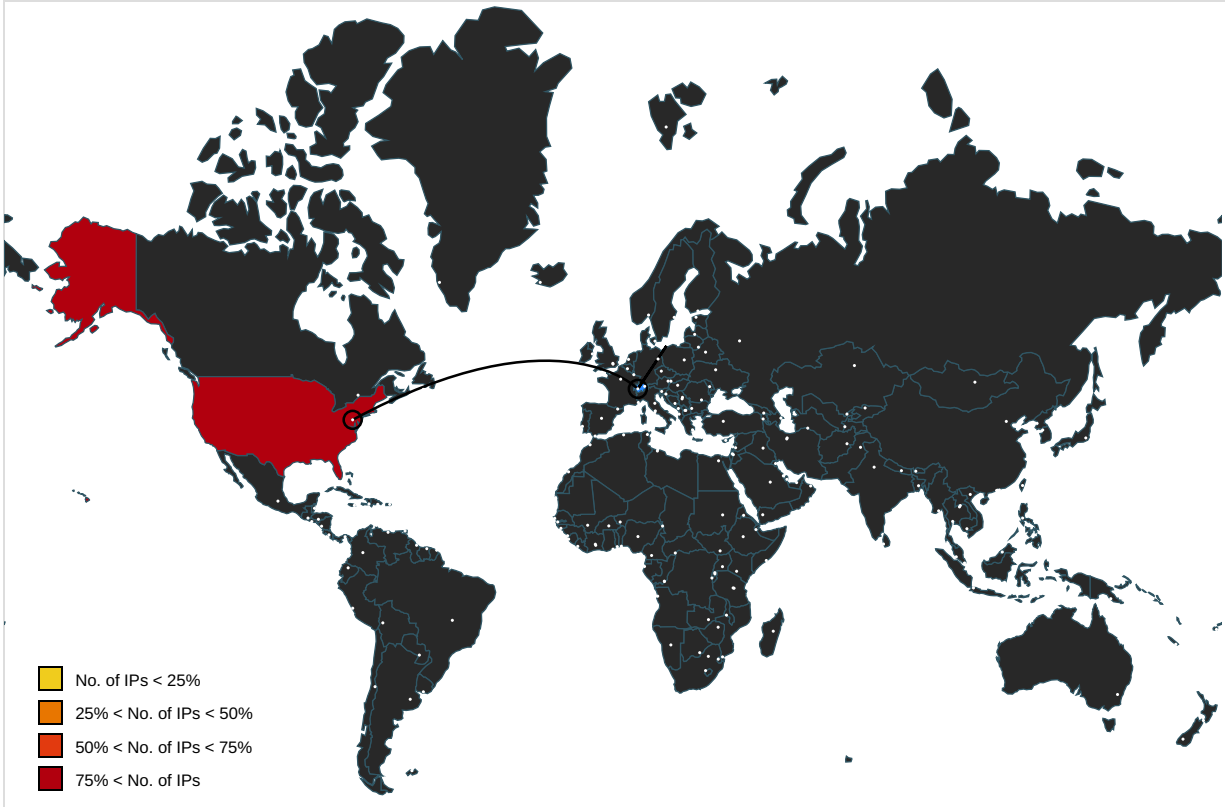
Name	Malicious	Antivirus Detection	Reputation
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
file:///C:/Users/user/Desktop/office365%20Validation.html	true		low
http://https://i.imgur.com/UeUQRKC.png	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	7da08f8a-dadd-45b7-9551-c4661cd51be9.tmp.1.dr, 7f517936-9ccb-4598-bded-8d34ddae261a.tmp.1.dr, bee1c790-598b-46ba-87e7-b0c9741604a7.tmp.1.dr, 190c4c6d-14a3-4c53-8082-9ee234662c1e.tmp.1.dr	false	• URL Reputation: safe	unknown
http://https://github.com/google/closure-library/wiki/goog.module:-an-ES6-module-like-alternative-to-goog.p	craw_window.js.0.dr, craw_background.js.0.dr	false		high
http://https://www.google.com/intl/en-US/chrome/blank.html	craw_background.js.0.dr	false		high
http://https://ogs.google.com	7f517936-9ccb-4598-bded-8d34ddae261a.tmp.1.dr, bee1c790-598b-46ba-87e7-b0c9741604a7.tmp.1.dr	false		high
http://https://www.google.com/images/cleardot.gif	craw_window.js.0.dr	false		high
http://https://play.google.com	7f517936-9ccb-4598-bded-8d34ddae261a.tmp.1.dr, bee1c790-598b-46ba-87e7-b0c9741604a7.tmp.1.dr	false		high
http://https://payments.google.com/payments/v4/js/integrator.js	craw_window.js.0.dr, manifest.json.0.dr	false		high
http://https://chromium.googlesource.com/a/native_client/pnacl-llvm.git	pnacl_public_x86_64_libpnacl_irt_shim_dummy_a.0.dr	false		high
http://https://easylist.to/)	LICENSE.txt.0.dr	false		high
http://https://sandbox.google.com/payments/v4/js/integrator.js	craw_window.js.0.dr, manifest.json.0.dr	false		high
http://https://www.google.com/images/x2.gif	craw_window.js.0.dr	false		high
http://https://accounts.google.com/MergeSession	craw_window.js.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://llvm.org/):	pnacl_public_x86_64_pnacl_sz_nexe.0.dr, pnacl_public_x86_64_pnacl_llc_nexe.0.dr	false		high
http://https://creativecommons.org/compatiblelicenses	LICENSE.txt.0.dr	false		high
http://https://www.google.com	7f517936-9ccb-4598-bded-8d34ddae261a.tmp.1.dr, bee1c790-598b-46ba-87e7-b0c9741604a7.tmp.1.dr	false		high
http://https://www.google.com/images/dot2.gif	craw_window.js.0.dr	false		high
http://https://github.com/easylist)	LICENSE.txt.0.dr	false		high
http://https://creativecommons.org/.	LICENSE.txt.0.dr	false		high
http://https://code.google.com/p/nativeclient/issues/entry%s:	pnacl_public_x86_64_ld_nexe.0.dr	false		high
http://https://code.google.com/p/nativeclient/issues/entry	pnacl_public_x86_64_ld_nexe.0.dr	false		high
http://https://accounts.google.com	7f517936-9ccb-4598-bded-8d34ddae261a.tmp.1.dr, bee1c790-598b-46ba-87e7-b0c9741604a7.tmp.1.dr	false		high
http://https://clients2.googleusercontent.com	7f517936-9ccb-4598-bded-8d34ddae261a.tmp.1.dr, bee1c790-598b-46ba-87e7-b0c9741604a7.tmp.1.dr	false		high
http://https://apis.google.com	7f517936-9ccb-4598-bded-8d34ddae261a.tmp.1.dr, bee1c790-598b-46ba-87e7-b0c9741604a7.tmp.1.dr	false		high
http://https://www.google.com/accounts/OAuthLogin?issueuberauth=1	craw_window.js.0.dr	false		high
http://https://www.google.com/	manifest.json.0.dr	false		high
http://https://www-googleapis-staging.sandbox.google.com	craw_window.js.0.dr, craw_background.js.0.dr	false		high
http://https://chromium.googlesource.com/a/native_client/pnacl-clang.git	pnacl_public_x86_64_libpnacl_irt_shim_dummy_a.0.dr	false		high
http://https://clients2.google.com	7f517936-9ccb-4598-bded-8d34ddae261a.tmp.1.dr, bee1c790-598b-46ba-87e7-b0c9741604a7.tmp.1.dr	false		high
http://https://clients2.google.com/service/update2/crx	manifest.json1.0.dr, manifest.json.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.251.36.238	clients.l.google.com	United States		15169	GOOGLEUS	false
142.251.36.205	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
151.101.112.193	ipv4.imgur.map.fastly.net	United States		54113	FASTLYUS	false

Copyright Joe Security LLC 2022

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	655326
Start date and time: 30/06/202223:09:36	2022-06-30 23:09:36 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	office365 Validation.html
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
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 • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.phis.winHTML@30/139@6/6
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .html • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.251.36.206, 142.251.36.170, 2.20.16.227, 142.251.36.195, 74.125.104.71, 34.104.35.123
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ajax.googleapis.com, secure.aadcdn.microsoftonline-p.com.edgekey.net, settings-win.data.microsoft.com, ctldl.windowsupdate.com, clientservices.googleapis.com, arc.msn.com, ris.api.iris.microsoft.com, r2.sn-4g5lznlz.gvt1.com, redirector.gvt1.com, edgedl.me.gvt1.com, store-images.s-microsoft.com, login.live.com, r2---sn-4g5lznlz.gvt1.com, sls.update.microsoft.com, e13761.dscg.akamaiedge.net, update.googleapis.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, www.gstatic.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\253928f3-17c6-48cf-b231-2d628346fe0a.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	205538
Entropy (8bit):	6.041900702341169
Encrypted:	false
SSDEEP:	6144:XYSeqcBrQFL5X5phQl3Zkq+lnVA1yo+aqfllUOoSiuRx:XYSPcBMFPQl3mz8yotoy
MD5:	27B2C033419CBACA4219E5B0FB1849BD

SHA1:	89B5F17E132B01477F4A9822A42C99AC4F6DDD52
SHA-256:	6B1585F2AD3FDBA2542B6749670576A982AFA2E35AD391615781591D209953A8
SHA-512:	7A14C0DBE5D2B9DD42D2296A4015019E9B45810B28DD3D31B03A7EE65EBFCA737F4B776842BB76CE9652C5D0FDFCCD8DFDE3959632770F1C3C018D811EF42F9
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.656655848161272e+12,"network":1.65662345e+12,"ticks":125155003.0,"uncertainty":4118664.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639031191"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\298a0a15-b5e9-4871-82f4-99c12566f0e2.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	206196
Entropy (8bit):	6.043871744815839
Encrypted:	false
SSDEEP:	6144:PSeqcBrQFL5X5phQl3Zkq+lnVA1yo+aqfIlUOoSiuRx:PSPcBMFPQl3mz8yotoy
MD5:	AE0BD2BFFFEB1864A7F735588DFFB49A
SHA1:	2BAEB795DB91BE3518E04E32B98DF6F355481DE9
SHA-256:	01C02B375A5C8BF3C6203DA7040B9BF535D7FD2E71F5400A2B1E4290D06F33FD
SHA-512:	2EA322AD5B377AE5B40DD95A188343C3EEF74DFA421A47F732B2925C53D2CB567B9A81C5F571A037E5FF4987AA8B800A136EB34F5B07A1CEC34A440C5ABF16DF
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.656655848161272e+12,"network":1.65662345e+12,"ticks":125155003.0,"uncertainty":4118664.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639031191"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\3b475dfe-4be6-4691-b93e-a3b147eba555.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7514498783381622
Encrypted:	false
SSDEEP:	384:vzGBRPkqnTMNINFrmvJD3KtP6HbyGG5rE35ZxaT/3erc1mc/0TdBt2OXXJN011cM:Wq1NerO6Aez1fTsv76PK9jhlY
MD5:	163167776194CD7CDA675015F2A85947
SHA1:	9C97CDA624C21541CEE091B07955D4321FCB2371
SHA-256:	DCB472C196010C67E19226A26020D33B52B09965B5671A8CEA36AAB568462CAA
SHA-512:	4D43D8AFCB89E9D708437F7C62C65A1D83BE6B11C46BE01F976330B0F3E62D143B144D0ADC8FE5180066789935B0EC2B2A68B90C1DC66614E64649A0A946C8E3
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....`8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\740d1272-9686-4f89-a592-5203cd65ca81.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	206007
Entropy (8bit):	6.043457551068367

Encrypted:	false
SSDEEP:	6144:GSeqcBrQFL5X5phQl3Zkq+lnVA1yo+aqfIlUOoSiuRx:GSPcBMFPQl3mz8yotoy
MD5:	065FA6CB946AE9A039A59034ADEA5B4D
SHA1:	6685A8CF160B5913F1E0B7BE5D947AC4ADAB9FAD
SHA-256:	1EFA64963E0DC4CF7C2EECDC055CF6725DB2FEF576E5DAB304F1140A352E1B2B
SHA-512:	56B04CFE58824CCF81E953CD7C949F08C3BFEC92434200A3C194B314F740BD01B88C7EA87A30231FEEF45AB864427A58254EAF0A4F5B7216FC420088CF21889
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.656655848161272e+12,"network":1.65662345e+12,"ticks":125155003.0,"uncertainty":4118664.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAADDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639031191"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\8007631f-3e0e-4574-b8d1-6dc6700b6143.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	214262
Entropy (8bit):	6.0708605267196765
Encrypted:	false
SSDEEP:	6144:NYSeqcBrQFL5X5phQl3Zkq+lnVA1yo+aqfIlUOoSiuRx:NYSPcBMFPQl3mz8yotoy
MD5:	0D47ACA787DAD249482096FC8F1F6681
SHA1:	FCBBB0B894B41102F4874ADDA42276715D2FC144
SHA-256:	BEB7E9E7483A5D08C3DFA79AA88596EC57A556DBFE986810C42E2AB26ACBCE20
SHA-512:	A30ACD1BE098D8AB01EA84461B8113ADB622459360EFEB68F2ED47168CC2E693C1BDE2063BAEF6E0580AC0C977C34E35CBFE28C2B9D3D30C931CA5EAD01F D0B
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.656655848161272e+12,"network":1.65662345e+12,"ticks":125155003.0,"uncertainty":4118664.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAADDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\887fa3d8-04dd-407a-8391-7163efc10350.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	205821
Entropy (8bit):	6.042966268754943
Encrypted:	false
SSDEEP:	6144:ZSeqcBrQFL5X5phQl3Zkq+lnVA1yo+aqfIlUOoSiuRx:ZSPcBMFPQl3mz8yotoy
MD5:	43BDD78E5F3806D036DFF9B836FD8746
SHA1:	084AFF7870BB5C0755EEA4E6DD62C4174D4A6C0E
SHA-256:	4DAD508672903D2E100BC5562A8D0048544A02E7396DEC7D6E51EA44FAA37D99
SHA-512:	C75E35408A67F8C090EBF0482C1A175F5EEEAD35B32F8F4C89A644F054754195087FB2A098BDB4814919F7A7B4BBC1D2ECCFB86F737E024CF36A86515630E69
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.656655848161272e+12,"network":1.65662345e+12,"ticks":125155003.0,"uncertainty":4118664.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAADDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639031191"},"plugins":{"metadata":{"adobe-flash-player":{"displ

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

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

Size (bytes):	40
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1n:+ftlE1n
MD5:	BD4642AD6C750A12D912B20BCB92E14D
SHA1:	C549F0F48FDD4FBC62E51AC26D7E185160CE2123
SHA-256:	4FD71FE78DFE203137C89C9FB0734358FF432F2BC83338112DC7B830F9B30F2C
SHA-512:	04410D12EF327614C3AF1251C9906BFEB2977211A7F53CBB08A8C01F9465A382CD001E51AB936A0D196D359F1DECDDAEAF5E7D1DBD49CE5F4FF91BF5C332B6CF
Malicious:	false
Reputation:	high, very likely benign file
Preview:	sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3c084803-dc84-49cd-9d0f-24465b2ea809.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17703
Entropy (8bit):	5.576739187463595
Encrypted:	false
SSDEEP:	384:LYQtkLliJX01kXqKf/pUZNCgVLH2HfDvrUIQbsfv4i:YLli01kXqKf/pUZNCgVLH2HfrrUaHR
MD5:	70A383AAF298CB9D1F5F32A5C9EB0ACE
SHA1:	3CF8A727C2C35CA87991FA6322033C5DD1FCF80C
SHA-256:	486B6D8F60968A85840EFCAFA52530BBF5230B6BFCD999E6AE4C13AD20EEBD9A
SHA-512:	96C8C744220DA701FB1AD18E082A54DDB0B2011E398030DC63AA55AE2A18D7ACAD92A0E518E6AA0A9497B91123DCEC7F718595C73F61EE7B7214D2BFF8E142FA
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13301129445060910","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4ef8fddd-7c36-4075-a355-f0dba4be53be.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19792
Entropy (8bit):	5.564076748001643
Encrypted:	false
SSDEEP:	384:LYQtkLliJX01kXqKf/pUZNCgVLH2HfDvrUBHGgQzwsfv4v:YLli01kXqKf/pUZNCgVLH2HfrrU1GRzw
MD5:	AC854F69E68FD72B8F9EF0A3EA6F444D
SHA1:	1C2B4677577C06F78C1717F7E271F4C72894350E
SHA-256:	BF02D116B80F30C53E16499DF8A80F98D57C0094469B72B1ED80AFB7C95A9E6E
SHA-512:	21DB7AE60447B809D9F73FF4BD2D529193E9BBB75CD522617A0CCA2BF210B01BA3D45E335101BAFF19F87867A0D62FD9C4F8FB840919DDB45D611ECAFB4624F7
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13301129445060910","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\539b84f3-4feb-4d02-b707-89020068be86.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4873
Entropy (8bit):	4.955364285621537

Encrypted:	false
SSDEEP:	48:YczUklSLklwHjlc9qA8iqTlYqlQKHoTw0X3TH3CH3G/s8C1Nfct/9BhUJo3Khme2:njC4MX1pcKIZpok0JCKL8VbOTQVuwn
MD5:	971502139E169B7468CC53056266D977
SHA1:	38C71B9668C90EDAB18CCB2E8062042C42EAB394
SHA-256:	BE8D541E096274CAD2B90CEB1D606E1026FB0D4F7BC981C3A2BE549934A0D1FC
SHA-512:	4C7753A5062D1AC38460213B1D6B41DB1DF0E171C6CFC5898E459EB225846CC8C2A81ED060CDA27B27704104B6BDA8705E8ED0E7D438B77B34B4ECF05891BE 2E
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301129446648478","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\566fec97-48f9-46b2-a073-efe0e628cdd0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19793
Entropy (8bit):	5.563971684768955
Encrypted:	false
SSDEEP:	384:LYQtkLliJX01kXqKf/pUZNCgVLH2HfDvrUBHGbQasfv4Le:YLli01kXqKf/pUZNCgVLH2HfrrU1GWHp
MD5:	CE19623F3E08CF964B21E5CAFCB41C18
SHA1:	DD92C8A72C66F6C0F74C96688CDAE0D56481EBD3
SHA-256:	862B415BF84868180E9A56FFE28FAFDCC94C8DFCDD980D68D72A07ADE2BFA672
SHA-512:	D0E3215DA48E7B86F612534A0D2815CBF83F672701ADEB0366B46C16A7CC7C3DEB7769D91DD05DE39745E9334D93F5D7976355753297813775501D4AF167E36C
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13301129445060910","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5c781412-7eec-468b-bc04-58f62f911d34.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4901
Entropy (8bit):	4.959518441222536
Encrypted:	false
SSDEEP:	48:YczUklSLkSwHjlcebZqAiiqTlYqlQKHoTw0X3TH3CH3G/s8C1Nfct/9BhUJo3KhS:njCz9t1pcKIZpok0JCKL8nbOTQVuwn
MD5:	B60747A1EB28520407642B8519E428AE
SHA1:	25A63762D1C6741CB79E12CACACEC849A33EC709
SHA-256:	5AF2995055CE0770EE1F140A811AD1B3A0F18727DD9795F04FDE0ABA4B1456E3
SHA-512:	C76FD753275B8AF450032CE74FC925D4C91C48A58754580C61C8687EA1A741E6AC9068DD6E958748DDAA843E9A9D5738D029E21A2D2FF6D0B6FB84CFB87D66 9
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301129446648478","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7f517936-9ccb-4598-bded-8d34ddae261a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1989
Entropy (8bit):	4.899927480639872
Encrypted:	false

SSDEEP:	48:Y2TntwCXGDH3qyvz5sVRsHKGsTRLssptasmsMHKSOYhbD:JTnOCXGDHa+z+gK5PwsGKSjhH
MD5:	1C767B87EF457B2969F52BADD2D21E12
SHA1:	95EC0FC68856E889EC6473233049FCD43DAD589D
SHA-256:	1CA286FC5A4CA26ECEB3507A0C85C27EF31CACFE629F9CB5135AB17870C2B0ED
SHA-512:	F77B2A529A4F0A903481FFB0AF6E9A9A3BA1E6D52253BED3BF2B20E2A4E09D97102AAB1BEC9D72D2947B1E1C3CA50D2A9D4A9892B17B1DC8CB1068CC8A878CD2
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13303721449602933","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ajax.googleapis.com"},{"alternative_service":[{"advertised_

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\830b2dfe-c5b2-4a8c-bd2f-6e12646f6da5.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4901
Entropy (8bit):	4.959779636735257
Encrypted:	false
SSDEEP:	48:YczUklSLkSwHjlcebaqAiiqTlYqlQKHoTw0X3TH3CH3G/s8C1Nfct/9BhUJo3KhS:njCzit1pcKIZpok0JCKL8nbOTQVuwn
MD5:	B7AE4437629D08EC72CBCF44D188B565
SHA1:	A4B539CCCCF104FB5FFFE35356EFD2743833970E
SHA-256:	8A400EB0DA10447D14A50C320B39A6BE8B3E2DC1023B0D48B04E4989896543CE
SHA-512:	7AB5C1C9261E81E57DE7516A1F08B8E8741483AABC1D966B88FE47E7348441AC33AF66E44F61FCBE031EEEC673BC9F4484F3BEB78B3B9BCB00E972C7582EE965
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301129446648478","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\84064e56-577a-4560-ac9a-e992f0f65129.tmp

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

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF

SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvuI11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUscllJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlXNQxlX:qTCT
MD5:	51A2CBB807F5085530DEC18E45CB8569
SHA1:	7AD88CD3DE5844C7FC269C4500228A630016AB5B
SHA-256:	1C43A1BDA1E458863C46DFAE7FB43BFB3E27802169F37320399B1DD799A819AC
SHA-512:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985DE
Malicious:	false
Preview:	.f.5.....f.5.....

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.27793481405139
Encrypted:	false
SSDEEP:	6:H9q2PWXp+N23iKKdK25+Xqx8chI+IFUtqVCqZZmwYVCHkwOWXp+N23iKKdK25+Xc:dva5KkTXfchI3FUt8/P5f5KkTXfch1J
MD5:	FB9A58E43CD57646C329EF315BEA070E
SHA1:	0ABD46629C035EDC24ECEB127145CECE537B2883
SHA-256:	7E2FBC6936F425D84AB478FED87D056899DB7A969BCD023210940533D3D6D466
SHA-512:	05A07A025C23EE3E062E0B11685BFCC9BCDB3DC425F990B04677B0E1D1E455A8040DC50C92B5547D8F9CC6A6E1BD2A4EAA9D01729D6272BAE3EC9034EAFAE6B4
Malicious:	false
Preview:	2022/06/30-23:11:02.216 1754 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/06/30-23:11:02.258 1754 Recovering log #3.2022/06/30-23:11:02.259 1754 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.27793481405139
Encrypted:	false
SSDEEP:	6:H9q2PWXp+N23iKKdK25+Xqx8chI+IFUtqVCqZZmwYVCHkwOWXp+N23iKKdK25+Xc:dva5KkTXfchI3FUt8/P5f5KkTXfch1J
MD5:	FB9A58E43CD57646C329EF315BEA070E
SHA1:	0ABD46629C035EDC24ECEB127145CECE537B2883
SHA-256:	7E2FBC6936F425D84AB478FED87D056899DB7A969BCD023210940533D3D6D466
SHA-512:	05A07A025C23EE3E062E0B11685BFCC9BCDB3DC425F990B04677B0E1D1E455A8040DC50C92B5547D8F9CC6A6E1BD2A4EAA9D01729D6272BAE3EC9034EAFAE6B4
Malicious:	false
Preview:	2022/06/30-23:11:02.216 1754 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/06/30-23:11:02.258 1754 Recovering log #3.2022/06/30-23:11:02.259 1754 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	835
Entropy (8bit):	5.3195133462962625
Encrypted:	false
SSDEEP:	24:uPKcZjENR3cxwls97iJvY78BJgskfa9yBDOxoq+vAEMzPAW1:HcCbMZliJbUsrPAs
MD5:	45ABEC05686D01BD8E38543E1E3D3330
SHA1:	F51F518540C1B334F607187B68058FB32D833634
SHA-256:	73BC2735D663B8FAC2FC58C9C65DF6D91417B346D5E7A05208076A1A772752FE
SHA-512:	7848F8205BFEC4AB56C36C20D8222F86A1F60E0879482F0606EEBC443C061045D5BB3303284EE8403E61DCB82003D78A6DD1C28666C81A26EB780BD760613DE
Malicious:	false
Preview:	............"g....account..c..desktop..file..user..html..in..microsoft..office365..sign..to..users..validation..your*........account......c......desktop......file......user......html......in......microsoft......office365......sign......to......users......validation......your..2.........3........5........6........a..........c...........d..........e...........f..........g........h.........i............k........l..........m.........n...........o.............p........r...........s..........t............u..........v........y........z...:...B........... ....*:file:///C:/Users/user/Desktop/office365%20Validation.html2!Sign in to your Microsoft account:...............J...............)4........

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1989
Entropy (8bit):	4.899927480639872
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDH3qyvz5sVRsHKGsTRLssptasmsMHKSOYhbD:JTnOCXGDHa+z+gK5PwsGKSjhH
MD5:	1C767B87EF457B2969F52BADD2D21E12
SHA1:	95EC0FC68856E889EC6473233049FCD43DAD589D
SHA-256:	1CA286FC5A4CA26ECEB3507A0C85C27EF31CACFE629F9CB5135AB17870C2B0ED
SHA-512:	F77B2A529A4F0A903481FFB0AF6E9A9A3BA1E6D52253BED3BF2B20E2A4E09D97102AAB1BEC9D72D2947B1E1C3CA50D2A9D4A9892B17B1DC8CB1068CC8A878CD2
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13303721449602933","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ajax.googleapis.com"},{"alternative_service":[{"advertised_

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4901
Entropy (8bit):	4.959779636735257
Encrypted:	false
SSDEEP:	48:YczUklSLkSwHjlcebaqAiiqTlYqlQKHoTw0X3TH3CH3G/s8C1Nfct/9BhUJo3KhS:njCzit1pcKIZpok0JCKL8nbOTQVuwn
MD5:	B7AE4437629D08EC72CBCF44D188B565
SHA1:	A4B539CCCCF104FB5FFFE35356EFD2743833970E
SHA-256:	8A400EB0DA10447D14A50C320B39A6BE8B3E2DC1023B0D48B04E4989896543CE
SHA-512:	7AB5C1C9261E81E57DE7516A1F08B8E8741483AABC1D966B88FE47E7348441AC33AF66E44F61FCBE031EEEC673BC9F4484F3BEB78B3B9BCB00E972C7582EE965
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301129446648478","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators

Category:	dropped
Size (bytes):	19793
Entropy (8bit):	5.563971684768955
Encrypted:	false
SSDEEP:	384:LYQtkLliJX01kXqKf/pUZNCgVLH2HfDvrUBHGbQasfv4Le:YLli01kXqKf/pUZNCgVLH2HfrrU1GWHp
MD5:	CE19623F3E08CF964B21E5CAFCB41C18
SHA1:	DD92C8A72C66F6C0F74C96688CDAE0D56481EBD3
SHA-256:	862B415BF84868180E9A56FFE28FAFDCC94C8DFCDD980D68D72A07ADE2BFA672
SHA-512:	D0E3215DA48E7B86F612534A0D2815CBF83F672701ADEB0366B46C16A7CC7C3DEB7769D91DD05DE39745E9334D93F5D797635575329781377550 1D4AF167E360
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13301129445060910","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\7da08f8a-dadd-45b7-9551-c4661cd51be9.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

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

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420

Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\190c4c6d-14a3-4c53-8082-9ee234662c1e.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071B
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898 D58
Malicious:	false
Preview:	....

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D

SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BI
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a353eaae-12d3-48a3-98fe-04ddeb2cfbf1.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4874
Entropy (8bit):	4.954866231414159
Encrypted:	false
SSDEEP:	48:YczUklSLkSwHjlcOqAiiqTlYqlQKHoTw0X3TH3CH3G/s8C1Nfct/9BhUJo3Khme2:njCzft1pcKIZpok0JCKL8VbOTQVuwn
MD5:	82906225A63416DCCD679D4F921C414D
SHA1:	267AE1D6CFEB392C22CE06EE5F41924EA5A3EC8B
SHA-256:	C4B3F8DDB997DE582D43E9245E489FD008A97A08FC4E336145047BA3CF503A28
SHA-512:	29D8FD80E78ADF5DAA686F00FB81C7154C368B439E8A7EDC42775F4962784F72B5669C3E26A985479B2C1A952EE558307194DFB5BB5DAC651E6A393799A1792
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301129446648478","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a6d66304-18f2-4158-b7cf-2572974c5646.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4901
Entropy (8bit):	4.959905476280507
Encrypted:	false
SSDEEP:	48:YczUklSLkSwHjlcebNqAiiqTlYqlQKHoTw0X3TH3CH3G/s8C1Nfct/9BhUJo3KhS:njCzNt1pcKIZpok0JCKL8nbOTQVuwn
MD5:	E0D472058CD57D9ADFC5A350594A8BD4
SHA1:	F22A59EE3BED6EC7AEF93D829F9168E48E2162F3
SHA-256:	D3A97BE5203FD1B932AFC7343E4494FD334871C247D62D1D3AC32D23F59F067A
SHA-512:	09CC5E034A2C8A71F3538934A6104670BDF2E01764A29BD62A65E530D79945B5071C5EF570BFCD73ADF027C407B0216E44E090D5158FE6906E84D4D9EC309A7
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301129446648478","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ac9c4078-e4fe-45c3-99b4-7b0256074620.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4873
Entropy (8bit):	4.954686933624682
Encrypted:	false
SSDEEP:	48:YczUklSLklwHjlcOqAiiqTlYqlQKHoTw0X3TH3CH3G/s8C1Nfct/9BhUJo3Khme2:njC4ft1pcKIZpok0JCKL8VbOTQVuwn
MD5:	1B5815108D6A5CFBE4A5A9BB9AF32AD4
SHA1:	E3E9B822CEF5622FE112868EB1FD008AA519090C
SHA-256:	FADD532966D64B1A9AC34E86DCD063570367ACB71948ED7249F8E446C6FFD74D
SHA-512:	B80EA578AE9BEFBAA1997C6DEBEEB151E5FA7D60ABA54CD1ACE569AF61A093AE66C023E2EA7C407C5531863CFB15FCAD7349876E0047F4837083A4C99EFCB248
Malicious:	false

Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301129446648478","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\beb7615e-6f01-4819-a0a9-d6e7d55ad463.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17529
Entropy (8bit):	5.573986923383048
Encrypted:	false
SSDEEP:	384:LYQtNLliJX01kXqKf/pUZNCgVLH2HfDvrUCDQMsfv4od:ZLli01kXqKf/pUZNCgVLH2HfrrUCYH7d
MD5:	B830E95D8E92325D7C9858748E086516
SHA1:	FFE13B82732B72CFFF690D548060307858639D52
SHA-256:	24E0FC31699EFC61ABB6B95C0C49E206992AFA7B34550BCD8C140FBFABBD193E
SHA-512:	42DE28ED58AC5C868A407D74F93C14D81F580FC29B2F93CC38FE50ED39AA3C4FF0D8531B3B1B2D014304829622445F9B229A37C2C4E54D61D5CDE2A1B702EEA
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13301129445060910","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bee1c790-598b-46ba-87e7-b0c9741604a7.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD160
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c94898ba-aa6a-4201-86a9-5e5a0636bdd7.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4901
Entropy (8bit):	4.959905476280507
Encrypted:	false
SSDEEP:	48:YczUklSLkSwHjlcebNqAiiqTlYqlQKHoTw0X3TH3CH3G/s8C1Nfct/9BhUJo3KhS:njCzNt1pcKIZpok0JCKL8nbOTQVuwn
MD5:	E0D472058CD57D9ADFC5A350594A8BD4
SHA1:	F22A59EE3BED6EC7AEF93D829F9168E48E2162F3
SHA-256:	D3A97BE5203FD1B932AFC7343E4494FD334871C247D62D1D3AC32D23F59F067A
SHA-512:	09CC5E034A2C8A71F3538934A6104670BDF2E01764A29BD62A65E530D79945B5071C5EF570BFCD73ADF027C407B0216E44E090D5158FE6906E84D4D9EC309A7
Malicious:	false

Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301129446648478","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cf9cd8be-a809-459c-9b27-079ca4e1861f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4901
Entropy (8bit):	4.959518441222536
Encrypted:	false
SSDEEP:	48:YczUklSLkSwHjlcebZqAiiqTlYqlQKHoTw0X3TH3CH3G/s8C1Nfct/9BhUJo3KhS:njCz9t1pcKIZpok0JCKL8nbOTQVuwn
MD5:	B60747A1EB28520407642B8519E428AE
SHA1:	25A63762D1C6741CB79E12CACACEC849A33EC709
SHA-256:	5AF2995055CE0770EE1F140A811AD1B3A0F18727DD9795F04FDE0ABA4B1456E3
SHA-512:	C76FD753275B8AF450032CE74FC925D4C91C48A58754580C61C8687EA1A741E6AC9068DD6E958748DDAA843E9A9D5738D029E21A2D2FF6D0B6FB84CFB87D669
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301129446648478","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d32650d4-420c-4d7e-a10f-e5e36d71df04.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4873
Entropy (8bit):	4.954686933624682
Encrypted:	false
SSDEEP:	48:YczUklSLklwHjlcOqAiiqTlYqlQKHoTw0X3TH3CH3G/s8C1Nfct/9BhUJo3Khme2:njC4ft1pcKIZpok0JCKL8VbOTQVuwn
MD5:	1B5815108D6A5CFBE4A5A9BB9AF32AD4
SHA1:	E3E9B822CEF5622FE112868EB1FD008AA519090C
SHA-256:	FADD532966D64B1A9AC34E86DCD063570367ACB71948ED7249F8E446C6FFD74D
SHA-512:	B80EA578AE9BEFBAA1997C6DEBEEB151E5FA7D60ABA54CD1ACE569AF61A093AE66C023E2EA7C407C5531863CFB15FCAD7349876E0047F4837083A4C99EFCB248
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301129446648478","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E089
Malicious:	false
Preview:	MANIFEST-000004.

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e28b655b-9ac8-4011-884b-eda5321cd29a.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4901
Entropy (8bit):	4.959518441222536
Encrypted:	false
SSDEEP:	48:YczUklSLkSwHjlcebZqAiiqTlYqlQKHoTw0X3TH3CH3G/s8C1Nfct/9BhUJo3KhS:njCz9t1pcKIZpok0JCKL8nbOTQVuwn
MD5:	B60747A1EB28520407642B8519E428AE
SHA1:	25A63762D1C6741CB79E12CACACEC849A33EC709
SHA-256:	5AF2995055CE0770EE1F140A811AD1B3A0F18727DD9795F04FDE0ABA4B1456E3
SHA-512:	C76FD753275B8AF450032CE74FC925D4C91C48A58754580C61C8687EA1A741E6AC9068DD6E958748DDAA843E9A9D5738D029E21A2D2FF6D0B6FB84CFB87D66 9
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301129446648478","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691 724
Malicious:	false
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.8150724101159437
Encrypted:	false

SSDEEP:	3:Yx7:4
MD5:	C422F72BA41F662A919ED0B70E5C3289
SHA1:	AAD27C14B27F56B6E7C744A8EC5B1A7D767D7632
SHA-256:	02E71EB4C587FEB7EE00CE8600F97411C2774C2FC34CB95B92D5538E7F30DA59
SHA-512:	86010ED2B2EEBDCC5A8A076B37703669C294C6D1BFAAEA963E26A9C94B81B4C53EC765D9425E5B616159C43923F800A891F9B903659575DF02F8845521F8DC4
Malicious:	false
Preview:	85.0.4183.121

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	206196
Entropy (8bit):	6.043871744815839
Encrypted:	false
SSDEEP:	6144:PSeqcBrQFL5X5phQl3Zkq+lnVA1yo+aqfIlUOoSiuRx:PSPcBMFPQl3mz8yotoy
MD5:	AE0BD2BFFFEB1864A7F735588DFFB49A
SHA1:	2BAEB795DB91BE3518E04E32B98DF6F355481DE9
SHA-256:	01C02B375A5C8BF3C6203DA7040B9BF535D7FD2E71F5400A2B1E4290D06F33FD
SHA-512:	2EA322AD5B377AE5B40DD95A188343C3EEF74DFA421A47F732B2925C53D2CB567B9A81C5F571A037E5FF4987AA8B800A136EB34F5B07A1CEC34A440C5ABF16DF
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.656655848161272e+12,"network":1.65662345e+12,"ticks":125155003.0,"uncertainty":4118664.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639031191"},"plugins":{"metadata":{"adobe-flash-player":{"displ

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7516195581617966
Encrypted:	false
SSDEEP:	384:JzGBRPkq70TLVgmNINFrmvJD3KtP6HbyGG5rE35ZxaT/3erc1mcIe0TdBt2OXXJB:hGq1Nero6Aez1fTsv76PK9jhl3
MD5:	913B4EB2DE099B0422D9F5FFE61DDED6
SHA1:	E750B532C3C3F86C1A3D4E9A451DFDDEFED6F642
SHA-256:	13C3D115E11540D27D247AB94A01C71D87B9E90DFC78ED0A5AC46258E50F39E3
SHA-512:	CB6412D1A0174B31A573D837313D9EFD0CD5770CA36026DBEB7CBF2F21738865E299776667EC4E0C98202F1D1571A47EA99F77FD041270C363F62F77A9E5F4A3
Malicious:	false
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....`8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir6304_1087354267\Ruleset Data

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	150056
Entropy (8bit):	4.8588214550289095
Encrypted:	false
SSDEEP:	3072:P8C4uHgjBz+BZKEZZ3F0Sl03PzpDL7UI09QEwNyfe:P8C5go1U6IYeH
MD5:	C56FF16BF9B9FC0002C0128DD0BD763D
SHA1:	5048CFDBAC5D7AAAD345BAE08E66E8C4E803CA02
SHA-256:	404AA48D274C3A8FEC3145858E00279D01E0C37A5304218E191C0156E4DE00FF
SHA-512:	D993A324F5D9A1FC4FB3131252F48679750081D996295C994E2DCA4E84F2DECF7E90AF6766EFEDC2CEFC6B66194FFF38181C9E9CE45346BEEB8B3A09CE66BB73

Malicious:	false
Preview:	.....[..... ...X...I...h...d...0.....X...T...P...L...H.....@...<.....4...0...,.....|...`...D..... .....'.....ozama.....*...'.....g.bat.....&.. .'.....onwod.....`....'.....ennab.....'.....nozam.....(.....geips.....P...((.....rekoj.....@(.....lgoog.....X(.....uotpo.....+..p(.....lreko.....d...h(.....Y..... .....Y...Y..pY..TY..8Y...Y...Y...Y...Y...Y...X...Y...Y...Y...Y...X...|Y..xY...X..pY..xX..hY..XX..`Y..\Y..4X..TY..PY..LY..HY..DY..@Y...X..8Y...W..0Y...W..(Y...W.. Y...Y...Y.. .Y...Y...Y...Y...Y...X...X...X...X..PW..4W...X...X...X...X...W...X...X...X...X...V...X...V...V...X...X...X..xV...X...X...X...X...X...X...X...X...X..|X..4V..tX..pX..lX..hX..dX...V...U..XX ...U..PX..LX...U..DX..@X..<X..8X..xU..\U..@U..(X..$X.. X...X...X...X...U...X...X...X...X...T...T...T...T...W...W...W...W...W...W...W...W..LT...W...W...W...W.. T...W..

C:\Users\user\AppData\Local\Google\Chrome\User Data\a82d342c-fe02-477b-a699-9a3b0ef04c2b.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.751664062843559
Encrypted:	false
SSDEEP:	384:ZzGBRPkq70TLVgmNINFrmvJD3KtP6HbyGG5rE35ZxaT/3erc1mc/0TdBt2OXXJNG:RGq1NerO6Aez1fTsv76PK9jhlS
MD5:	F584E4ED15822A8BFB729C6D7D7E41A3
SHA1:	DC854CF22E039A071718306A251A8E5814C5A488
SHA-256:	46F08974A4251E186AD036EF17B542B89BDB517FDA1432B0C427ECA529E6090E
SHA-512:	3BE1E1F25D33A9377BBA38FC3594A8964A56D88DDAD778848C07F5D2F9B6232FFE8D47F0D4C38D16DCB17C704E8F050271037C8A433F897C35DB31B2D5F9C7D
Malicious:	false
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....`8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\abc62dfa-9aca-4e7a-8c08-73583ae6653e.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	214262
Entropy (8bit):	6.070859139193122
Encrypted:	false
SSDEEP:	6144:NYSeqcBrQFL5X5phQl3Zkq+lnVA1yo+aqfIlUOoSiuRx:NYSPcBMFPQl3mz8yotoy
MD5:	3BE6C41F4D3A83E83038EA7B116B79C7
SHA1:	B394DDEFA104968994BDD598E01DAA4FF7CF7747
SHA-256:	A2BEA74DB175C96C5BE24686B545171C3D1CC7F6C05DD9B8C44D9226B17F2EAE
SHA-512:	1B91A6D62359C0381EB6E89CC113389976E7235DB98D7A68F2A60197D3CC341A2740F46B94E006E789C69608ACBB477672F81A214F47F47A30CB1D046B4FEE02
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.656655848161272e+12,"network":1.65662345e+12,"ticks":125155003.0,"uncertainty":4118664.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639031191"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\ad71061a-ba54-4486-a33a-afc263ce1c10.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	205913
Entropy (8bit):	6.0432145335290715
Encrypted:	false
SSDEEP:	6144:uSeqcBrQFL5X5phQl3Zkq+lnVA1yo+aqfIlUOoSiuRx:uSPcBMFPQl3mz8yotoy
MD5:	491AD4C5558AAA7300852BBAC7DBC7AF
SHA1:	18514C2729CA10733B3817496ED0FE4BBFDAD7ED
SHA-256:	B4996ACAAB0066E7945C550B509D8FAAD5CC9096F3A864882368DF81A0A0B3D9
SHA-512:	458E77BC1709DA7FA96B7224F61AEA9708686134FB2892CBB285042F1796326BAF36AB4F3AD3033B7B969F824EA885546398A9536EC42A5C692B736854A0F864
Malicious:	false

Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.656655848161272e+12,"network":1.65662345e+12,"ticks":125155003.0,"uncertainty":4118664.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639031191"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\c2621fca-4d40-46a2-944a-d39715a9da4c.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7516195581617966
Encrypted:	false
SSDEEP:	384:JzGBRPkq70TLVgmNINFrmvJD3KtP6HbyGG5rE35ZxaT/3erc1mcIe0TdBt2OXXJB:hGq1Nero6Aez1fTsv76PK9jhl3
MD5:	913B4EB2DE099B0422D9F5FFE61DDED6
SHA1:	E750B532C3C3F86C1A3D4E9A451DFDDEFED6F642
SHA-256:	13C3D115E11540D27D247AB94A01C71D87B9E90DFC78ED0A5AC46258E50F39E3
SHA-512:	CB6412D1A0174B31A573D837313D9EFD0CD5770CA36026DBEB7CBF2F21738865E299776667EC4E0C98202F1D1571A47EA99F77FD041270C363F62F77A9E5F4A3
Malicious:	false
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....`8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\c27aceda-310b-416d-9485-c36fda0b03fa.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	206110
Entropy (8bit):	6.043721839612979
Encrypted:	false
SSDEEP:	6144:WSeqcBrQFL5X5phQl3Zkq+lnVA1yo+aqfIlUOoSiuRx:WSPcBMFPQl3mz8yotoy
MD5:	6B03D1DE1DEC53715B5A4C646DC7FD3C
SHA1:	B1288F19F670D9A8344AAB142DDFD74C79314677
SHA-256:	A7C806523FBE0065631A5A29E6F62F891B228DE4992923561B6ED883A2280902
SHA-512:	B9D7A0A84121DAAF2D2316D5A4CA008F86DA4BF1754C5C7D12037BDA16BC66EFEA76A0A850E8A0B2C0F3919730BCA326D542A0E49EE9FA34D002236626A73B27
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.656655848161272e+12,"network":1.65662345e+12,"ticks":125155003.0,"uncertainty":4118664.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639031191"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\d48bf9d3-ab13-4e92-b163-c8106af1aee1.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	205913
Entropy (8bit):	6.0432145335290715
Encrypted:	false
SSDEEP:	6144:uSeqcBrQFL5X5phQl3Zkq+lnVA1yo+aqfIlUOoSiuRx:uSPcBMFPQl3mz8yotoy
MD5:	491AD4C5558AAA7300852BBAC7DBC7AF
SHA1:	18514C2729CA10733B3817496ED0FE4BBFDAD7ED
SHA-256:	B4996ACAAB0066E7945C550B509D8FAAD5CC9096F3A864882368DF81A0A0B3D9
SHA-512:	458E77BC1709DA7FA96B7224F61AEA9708686134FB2892CBB285042F1796326BAF36AB4F3AD3033B7B969F824EA885546398A9536EC42A5C692B736854A0F864
Malicious:	false

Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.656655848161272e+12,"network":1.65662345e+12,"ticks":125155003.0,"uncertainty":4118664.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639031191"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\eb1e3843-b299-4531-bbb2-c8c0f9ef648e.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	205821
Entropy (8bit):	6.042966268754943
Encrypted:	false
SSDEEP:	6144:ZSeqcBrQFL5X5phQl3Zkq+lnVA1yo+aqfIlUOoSiuRx:ZSPcBMFPQl3mz8yotoy
MD5:	43BDD78E5F3806D036DFF9B836FD8746
SHA1:	084AFF7870BB5C0755EEA4E6DD62C4174D4A6C0E
SHA-256:	4DAD508672903D2E100BC5562A8D0048544A02E7396DEC7D6E51EA44FAA37D99
SHA-512:	C75E35408A67F8C090EBF0482C1A175F5EEEAD35B32F8F4C89A644F054754195087FB2A098BDB4814919F7A7B4BBC1D2ECCFB86F737E024CF36A86515630E69
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.656655848161272e+12,"network":1.65662345e+12,"ticks":125155003.0,"uncertainty":4118664.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639031191"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\ec96d661-b31f-4e9a-b125-d48d98660367.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	214262
Entropy (8bit):	6.0708605267196765
Encrypted:	false
SSDEEP:	6144:NYSeqcBrQFL5X5phQl3Zkq+lnVA1yo+aqfIlUOoSiuRx:NYSPcBMFPQl3mz8yotoy
MD5:	0D47ACA787DAD249482096FC8F1F6681
SHA1:	FCBBB0B894B41102F4874ADDA42276715D2FC144
SHA-256:	BEB7E9E7483A5D08C3DFA79AA88596EC57A556DBFE986810C42E2AB26ACBCE20
SHA-512:	A30ACD1BE098D8AB01EA84461B8113ADB622459360EFEB68F2ED47168CC2E693C1BDE2063BAEF6E0580AC0C977C34E35CBFE28C2B9D3D30C931CA5EAD01F1D0B
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.656655848161272e+12,"network":1.65662345e+12,"ticks":125155003.0,"uncertainty":4118664.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Temp\201465c9-d45e-4764-9cc5-184c46c51ed9.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F332688
Malicious:	false

Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u.. ..k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..)....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2.. ;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.I....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z ....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5SI..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\6304_1644556325\LICENSE

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1558
Entropy (8bit):	5.11458514637545
Encrypted:	false
SSDEEP:	48:OBOCrYJ4rYJVwUCLHDy43HV713XEyMmZ3teTHn:LCrYJ4rYJVwUCHZ3Z13XtdUTH
MD5:	EE002CB9E51BB8DFA89640A406A1090A
SHA1:	49EE3AD535947D8821FFDEB67FFC9BC37D1EBBB2
SHA-256:	3DBD2C90050B652D63656481C3E5871C52261575292DB77D4EA63419F187A55B
SHA-512:	D1FDCC436B8CA8C68D4DC7077F84F803A535BF2CE31D9EB5D0C466B62D6567B2C59974995060403ED757E92245DB07E70C6BDDBF1C3519FED300CC5B9BF917C
Malicious:	false
Preview:	// Copyright 2015 The Chromium Authors. All rights reserved..//.// Redistribution and use in source and binary forms, with or without.// modification, are permitted provided that the following conditions are.// met:.//.// * Redistributions of source code must retain the above copyright.// notice, this list of conditions and the following disclaimer..// * Redistributions in binary form must reproduce the above.// copyright notice, this list of conditions and the following disclaimer.// in the documentation and/or other materials provided with the.// distribution..// * Neither the name of Google Inc. nor the names of its.// contributors may be used to endorse or promote products derived from.// this software without specific prior written permission..//.// THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS.// "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT.// LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR.// A PARTICULAR

C:\Users\user\AppData\Local\Temp\6304_1644556325_metadata\verified_contents.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1511
Entropy (8bit):	5.971158422968611
Encrypted:	false
SSDEEP:	24:pZRj/flTU3Yb7/ejoY87aoXcaVuceTyA5x0amDoXtW6+XctkJsn:p/hUIb7h7akkXROkt9+Xctkq
MD5:	67731A13FC7FF5B166626E577295C6CE
SHA1:	7C03CD4C3EA30961E598DD4B2C96DF4186A9E108
SHA-256:	563872418ECB5B9F0E2E0CDE98C54D34BE34EF1F28F9EE56A620213B6E0E0042
SHA-512:	34BB8CFECB2376C3105353389A36880D692FF482B4684D927DFB77E9A1C4613BBEC6C5E4C26C0070ACDBA16828A856676BE0FF9EADB4EBBC1A06316D581DBE4
Malicious:	false
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJMSUNFTlNFIiwicm9vdF9oYXNoIjoiUGIwc2tBVUxaUzFqWldTQnctV0hIRkltRlhVcExiZDlUcVkwR2ZHSHBWcyJ9LHsicGF0aCI6ImNybC1zZXQiLCJyb290X2hhc2giOiJEOU5kUEQ4Z21GeHhRQmhBS2d6aDFiWXFRbTBGTTFRcEIxWUhGY1lHLW5rln0seyJwYXRoIjoibWFuaWZlc3QuanNvbiIsInJvb3RfaGFzaCI6ImdQWkkwbzBlS0JFYnpXMXhBWjJWZWJ2RDY3TjJNSmVqVzU4N0hBS1cxa1UifV0sImZvcm1hdCI6InRyZWVoYXNoIiwiaGFzaF9ibG9ja19zaXplIjo0MDk2fV0sIml0ZW1faWQiOiJoZm5rcGltbGhoZ2llYWRkZ2ZlbWpob2ZtZmJsbW5pYiIsIml0ZW1fdmVyc2lvbiI6IjciLCJwcm90b2NvbF92ZXJzaW9uIjoxfQ","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"Phvwi6D2rDPbJaWY1kfCpYTbWr6caO1CHH9B2H0rYtPOvQH1l6HH_9QEFs4U_A63RQkD5FcI_JGpKn_lmpWQYkCkbWxW7E-0yfG608lr3P8e0l6EN8ajsd570h8ZE7v_gzCFMBf0Bc8lHC4eiLc7r37aCZTVoWkZENQAteUnTJujAl2WVzSudhyv5eC9ymP-S8kj2P8LUtp8VL0LkU86uNyX2Y3h2HtegIUecJMrAFpsGla1TSHvoPj-ltlAa9H4PCI

C:\Users\user\AppData\Local\Temp\6304_1644556325\crl-set

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	22448
Entropy (8bit):	7.833567444076544
Encrypted:	false
SSDEEP:	384:u26XPKXVeWcURWVPHM4m8eWxmtoBZKbh4n5bk8QzsvFUtr4G9htt/HDsJBr:uf+8ZV/5YW0tozGh4pk8SgUr4G/Ps
MD5:	0E4F8BCC871B84AF17EB57F8C58D9E5A
SHA1:	AC00C6903745FA75E75AE7ED0D3F3260E7B8BC44
SHA-256:	ACD5BEAF4322D512B4C4DE3628D09EAE463BBCEDEEE243E54B8E9CE04533ED63
SHA-512:	ED560A8D86B81B463386834871A1FD06A03742A00F042164D90BFF3BDA6CBEC0B22F5C9AE6F43CD48BBD1663DA818F999495E8CF7AE8AC85147AD55B077B145
Malicious:	false

Preview:	".{"Version":0,"ContentType":"CRLSet","Sequence":7430,"DeltaFrom":0,"NumParents":191,"BlockedSPKIs":["Jdoa1Yu/z7In2HI7GFfUwY57qnQXtPnv+TZrXoafizk=","Ii5LVLuYp+5dX+uWM/mR08MwDpUU2t57DU+CjHlPjoc=","yP3cdcsb27WMB7TqhHKH9iZIndZrwQomrdm1dbOgo40=","BN3pqpp59hSYaCMl+ghwJ2cH+5ypU4QSC0aJMmhJT8k=","tbqN1/iVZMKInT1kU8hJmMd4JJGbZOoINapimGWRvlA=","wO0gU0a7veButWD1zuAqNjTiR0p+ds+PvvVjuxF90OM=","eBpM8ukkUvPuAdDDgaQhTzkEFlw5CtvWH80RJE4Jstw=","/NdsyiNH5c1bOTR/Uc9DZUtpor/JBzZwpr5H2HAebg4=","lo26afv/Fb83YgiUMa3lp+rUt+rxvnACaBC8V9HGT24=","fNKVt1VEgIq9lAlGbwg3xarcAuM7YVDGZE3goJZZ8jw=","9Sk9R+041MMbLULe47WzrOl8omyirANl42Iu6AITH7s=","nFmjzK6kaZhCsGjPxSz5RdtRmGlXyDLNsYynOEn7ue4=","OUz/WJ5okxLPwHHuC8Gf5MYGIWzlQ0Kd5tti5C27O8E=","NuqWEoyJg5+2IfitDh7gucIgb2Kre02ixnZYk8m3ztI=","pqyh7JgJzFtIIf+dKcXr5lGWC5Gx8ZzIm1Xvh4GKlQk=","MO/kE4JHbDOA8C9+I+ZrovhnsFnuHqaHlrRBuFtdElY=","r1kVGOLmxg67/AkHr6pJvEBR1F5/IUq/7nUS7gD2Ye0=","6EnHF2yT32X2S2FpgjZuVmMReBK2+ivAyPqK6u5Bgcw=","0x7DkoW3pTGdAVfbQg7YfHQ+Mzu8d/h3H3BGT0NqYEk=","h7/Yr

C:\Users\user\AppData\Local\Temp\6304_1644556325\manifest.fingerprint

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.909396158440505
Encrypted:	false
SSDEEP:	3:SSXqnwAB6PBWIXcVdsSDX5E6YWXBn:SSm7MgIMVd3N7XBn
MD5:	494B29B8E6BF5044BFCFCD24308A68C2
SHA1:	3B425E87AA936C764297DA04B8142F2AA5CFF259
SHA-256:	29C07BF1803B5CDBF01719F942114BCE662D727AC5ABA5CFC1D5A06C19DF0E4F
SHA-512:	2F46C9CEA9DD0D4718255B4D49B231A50682B7712399FC8A2D97B3144E1DB3A5C27351A1FC8643CA7DE20728497D064F763B71CF366D1A9766A6B3B44F99485(
Malicious:	false
Preview:	1.7350ebb98957cc2f840118c6fd121714ce90898753767282fa7196f551b9a32d

C:\Users\user\AppData\Local\Temp\6304_1644556325\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	192
Entropy (8bit):	4.828405371904226
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFJX16lqhFgS1vLEeSWU4pv/8F/FxLj2RF2fcTZTotL:F6VlMd6lq0S1YWfB0NpK4aotL
MD5:	24E7BFFB39398D75E2F4BF869AAE955A
SHA1:	F04440018D7355E10EBB4BCB3A8BF5835E5CA6BF
SHA-256:	80F648D28D1E28111BCD6D71019D9579BBC3EBB3763097A35B9F3B1C0296D645
SHA-512:	0188E6075B60DB7BB8FC9511B86F598D988D513324DF317148618195165F399D1A2FE78DA83BB57CD06F87D3926CAE2B112F9FD6C06A9261241EC65523D17839
Malicious:	false
Preview:	{. "manifest_version": 2,. "name": "crl-set-16460828476158530195.data",. "version": "7430",. "imageName": "image.squash",. "squash": true,. "fsType": "squashfs",. "isRemovable": false.}

C:\Users\user\AppData\Local\Temp\6304_2066690316\Filtering Rules

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97968
Entropy (8bit):	5.489893397464442
Encrypted:	false
SSDEEP:	1536:ojHlFMJw9il9Yh9FHc6cPC3CpBHTrDo630a8Q78xRAQudDv4NZ/p2GuN+BO1:6FMJw9v9efHc6cPCURDR30EYnAQuJANw
MD5:	3846A25BC9191585763E06550798BAB1
SHA1:	F43D903B13AB969E2276E304795CE164F22F893C
SHA-256:	C7D5D133E8F995D3E4D5B68F28BE0D7B1F290DFBD1502E0EC260142325FA8F88
SHA-512:	6B1E1776DE4B4B7D7BD7E6252F555AD84CC689EFE1F3920B3ACFE23DE65212254FC219E0A530037A5EA819894BC2F5B85ECFC0ADDEE9AF3163393AA32F97BA44
Malicious:	false
Preview:	.....0.8.@.R.-728x90.....0.8.@.R.adtdp.com^.....0.8.@.R.yomeno.xyz^.:.....*...adcore.com.au..*...adcore.ch..0.8.@.R./adcore_.....0.8.@.R.uwoapte e.com^.8.....*...safeway.com0.8.@.R.fwcdn2.com/js/embed-feed.js.....0.8.@.R._468_60..3.....0.8.@.R#/wp-content/plugins/wp-super-popup/.9.....0.8.@.R)bancodevenezuela.com/imagenes/publicidad/.....0.8.@.R..adbutler-.....0.8.@.R.adrecover.com^.....0.8.@.R.hdbcode.com^.?.....*...google.com0.8.@.R!develo pers.google.com/google-ads/.-.....*...konograma.com..0.8.@.R./adserver.....*...vk.com0.8.@.R.vk.me/css/al/ads.css.,.....0.8.@.R.mysmth.net/nForum/*/ADAgent_.. .....0.8.@.R.indoleads.com^.%.....0.8.@.R.discordapp.com/banners/.E.....*...daum.net0.8.@.R)daumcdn.net/adfit/static/ad-native.min.js.(.....0.8.@.R.looker.com/a pi/internal/.#.....0.8.@.R.broadstreetads.com^.....0.8.@.R./banner.cgi?.....*...thefreedictionary.com*...downloads.codefi.re*...windows7themes.net

C:\Users\user\AppData\Local\Temp\6304_2066690316\LICENSE.txt

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	24623
Entropy (8bit):	4.588307081140814
Encrypted:	false
SSDEEP:	384:mva5sf5dXrCN7tnBxpxkepTqzazijFgZk231Py9zD6WApYbm0:mvagXreRnTqzazWgj0v6XqD
MD5:	D33AAA5246E1CE0A94FA15BA0C407AE2
SHA1:	11D197ACB61361657D638154A9416DC3249EC9FB
SHA-256:	1D4FF95CE9C6E21FE4A4FF3B41E7A0DF88638DD449D909A7B46974D3DFAB7311
SHA-512:	98B1B12FF0991FD7A5612141F83F69B86BC5A89DD62FC472EE5971817B7BBB612A034C746C2D81AE58FDF6873129256A89AA8BB7456022246DC4515BAAE2454E
Malicious:	false
Preview:	EasyList Repository Licences.... Unless otherwise noted, the contents of the EasyList repository.. (https://github.com/easylist) is dual licensed under the GNU General.. Public License version 3 of the License, or (at your option) any later.. version, and Creative Commons Attribution-ShareAlike 3.0 Unported, or.. (at your option) any later version. You may use and/or modify the files.. as permitted by either licence; if required, "The EasyList authors.. (https://easylist.to/)" should be attributed as the source of the.. material. All relevant licence files are included in the repository..... Please be aware that files hosted externally and referenced in the.. repository, including but not limited to subscriptions other than.. EasyList, EasyPrivacy, EasyList Germany and EasyList Italy, may be.. available under other conditions; permission must be granted by the.. respective copyright holders to authorise the use of their material.....Creative Commons Attribut

C:\Users\user\AppData\Local\Temp\6304_2066690316_metadata\verified_contents.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1529
Entropy (8bit):	5.993915630498445
Encrypted:	false
SSDEEP:	24:pZRj/flTHYfcl5kYbKqLjeT3azkaoX1pF/kSYYRVHbo0doXxOB6G6QL3foQ3QL5D:p/h4ElBbKdTakak1pFcSfRV7o0dkx8L4
MD5:	6B2EDD2D0C16E5D77BD2C3E4AE88C95F
SHA1:	BC82982FA8A04FA6FD9F17DA03D443A57E0F78D4
SHA-256:	CA0F5F75FC56FBEDA7522B2C83707A451D01760F417C497A37C70554E290B737
SHA-512:	533026A33030795ABF24B6E78D26763734D98CA74BFA4FAC2073EFAD0BB5CA1C38E7036BEAF17E6ABBFE56CF968E80EB3CA3CFD23AEEC10CE1280E8DB1C4078C
Malicious:	false
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJGaWx0ZXJpbmcgUnVsZXMiLCJyb290X2hhc2giOiJMTF90X0NkWWRYUnpMSHJBZ3hmUW5tcENTaXlkWEtzVVlJZnZjLTR0czRBIn0seyJwYXRoIjoiTElDRU5TRS50eHQiLCJyb290X2hhc2giOiIyaWswNmk0TFlCdVNHNWphRGFIS253NE9pdnVSRzZsQ0JKMVk0TGtzRFJJJln0seyJwYXRoIjoibWFuaWZlc3QuanNvbiIsInJvb3RfaGFzaCI6Imo4MmhRZGhaa0MwMjFWOEZ1MHUtMExvMnVJdXl5SzdFem5JcHE3WHd2YlkifV0sImZvcm1hdCI6InRyZWVoYXNoIiwiaGFzaF9ibG9ja19zaXplIjo0MDk2fV0sIml0ZW1faWQiOiJnY21qa21nZGxnbmtrY29jbW9laW1pbmFpam1tam5paSIsIml0ZW1fdmVyc2lvbiI6IjkuMzYuMCIsInByb3RvY29sX3ZlcnNpb24iOjF9","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"VM_rIA1uXuXjbhz_uZ8uQp9F3FfgEgGTjCXL08Q_jrGXXH-Yty1DqAw4yzWsadeOjVRozUf_7kBrYJ2U8Y8slircdLRbrqJejQeyyrJx4HFT8qgZEb60YHdsOd76C57YzF5dXErpjT7_FkWA41lTxLQvdWbACMO0DE7uOHO9mZx5pM98Ni9GsM_yxJbRSyDZWa8BdPHErfMuO6YE6D8tbnYTr2tXcMV9p2ZEAFMiso2B-6DSr

C:\Users\user\AppData\Local\Temp\6304_2066690316\manifest.fingerprint

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.9458563396006063
Encrypted:	false
SSDEEP:	3:SWllBTGVn1VJ8U1hRGGpWdTdSATn:SWNT+eKhRR4dTVT
MD5:	991F44CE02222E783A1FEFE4187727CE
SHA1:	9855D1CA0338ADCD5829C3260BF7FAAF88A23509
SHA-256:	58704ADE087671AA1226BC9CEC1719F5B80B90C571EF747812A64458BBEA0F50
SHA-512:	C2616426939B235620A22B24A9BEC6D4F7DBB695C812F1784A4C95B41E53A21F371A6C440177CFABDE47E203EB83269F9013FC75C6D758EA6FDFE7B52B4A554E
Malicious:	false
Preview:	1.34ff2e9d7a7ce81c5d760d4b0f4b59a0237dd5db0d1e84ccd5103a30687eac17

C:\Users\user\AppData\Local\Temp\6304_2066690316\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	115

Entropy (8bit):	4.563301657145084
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFHXG7LGMdv5HcDKhtUJKS1Avn:F6VlMZWuMt5SKPS1Avn
MD5:	47B89067C397B3EABBD04E6FC4008B71
SHA1:	7B4E623806D7EA8BFCD2FE6836A21E50C9F9340E
SHA-256:	8FCDA141D859902D36D55F05BB4BBED0BA36B88BABF4AEC4CE7229ABB5F0BDB6
SHA-512:	FDA1CE8EB24A05F65E8132248EEF96C422E5AA2D3254B590FBFD3FCB2016E3B7F6E4B53702D88E1695D4BEC0175F72EB4256CDAA2FF72DDF4390D480D04BA373
Malicious:	false
Preview:	{. "manifest_version": 2,. "name": "Subresource Filtering Rules",. "ruleset_format": 1,. "version": "9.36.0".}.

C:\Users\user\AppData\Local\Temp\6304_848482870\Recovery.crx3

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	145035
Entropy (8bit):	**7.995615725071868**
Encrypted:	**true**
SSDEEP:	3072:TdgEhmDf+E8VY0x81Rkc6L2oqzqkPEu30gZlc3G2ZknF:TyEhmDf+/+Fnkj6lEukgZyyF
MD5:	EA1C1FFD3EA54D1FB117BFDBB3569C60
SHA1:	10958B0F690AE8F5240E1528B1CCFFFF28A33272
SHA-256:	7C3A6A7D16AC44C3200F572A764BCE7D8FA84B9572DD028B15C59BDCCBC0A77D
SHA-512:	6C30728CAC9EAC53F0B27B7DBE2222DA83225C3B63617D6B271A6CFEDF18E8F0A8DFFA1053E1CBC4C5E16625F4BBC0D03AA306A946C9D72FAA4CEB779F8FFCAF
Malicious:	false
Preview:	Cr24.....0.."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....S'.....2.{.....'....+.'..".Y.x.ISa...)....H.&92..?!..~..F.5."...n,.B.-|\.)..(.....]G..j.-M)... .C.....o&L..0.K.....UtP.&.N...;..^w/a{}v...~KG;...?.1...k.c..D.U.....J.6.`.G.5.x.k..[...i.A.@I^..I.<A. J...j.'.G.`.$q.N..Tdq]2]p.OF..#.#.....'....8.3.....0.."0...*.H.....0.....O..(...':19..O/.>....=.....m.n\.z..q.....JW..F.....+H.Z+KGO.9....8.....U...&.y....,$...?.Eo.....\f/.Z..+M8...B.3'..Y.r...X.AS?.~..k..n..... Z...&.G....."n.....l.0v.x#<....Lx,-.w..-..d.....J.pT..(' e~*{%kQ.Q.....rI.....Z....v.N.....J.d_.....rX.....w@.b.[.c../V.'c...!.~.k..}z...U.S..nC.....@.....Y..#.D.z.....5&.1O...X=p..2.F..P.6yP..>{.....HBX.*.E5....y..

C:\Users\user\AppData\Local\Temp\6304_848482870_metadata\verified_contents.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1765
Entropy (8bit):	6.027545161275716
Encrypted:	false
SSDEEP:	48:p/hii6zkvVl1Jip2qRNHvakuQkCNFxdsGwmBKkgum91:Rz0kv6cNvaYNFwSEhug
MD5:	45821E6EB1AEC30435949B553DB67807
SHA1:	B3CADEB17FE5B76B5DBB428B8D3A07B341F8B1BC
SHA-256:	E5FAE91295BECF7F66BFA4BE1061CA5537ED763EB5D01485F23ECFB583304FEE
SHA-512:	BCBE40CAFAA4B14566D91E361D8FB7F0288D5C459FA478AA4C575444DA4D406E1076FC0B3A31D4A9E5EE034F0FE15A0EFE8A8A52B838DE94B96D3E488D28FCFE
Malicious:	false
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJSZWNvdmVyeS5jcngzIiwicm9vdF9oYXNoIjoiaGdCR051SzhNR2NKaDlfNmZQaFdEWmpVYUFKeklzeDlJS21DUEZvb0dfUSJ9LHsicGF0aCI6Im1hbmlmZXN0Lmpzb24iLCJyb290X2hhc2giOiIwYXduVFBFQmdDRHkyV05hVVk3Um9mSWN3c3ZwNHFRNUxzZVMxVXRiVXY0In1dLCJmb3JtYXQiOiJ0cmVlaGFzaCIsImhhc2hfYmxvY2tfc2l6ZSI6NDA5Nn1dLCJpdGVtX2lkIjoiaWhubGNlbm9jZWhnZGFlZ2RtaGJpZGpobmhkY2hmbW0iLCJpdGVtX3ZlcnNpb24iOiIxLjMuMzYuMTQxIiwicHJvdG9jb2xfdmVyc2lvbiI6MX0","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"iFuMX_kOZ-zJ7KVu6Lxb3rHWZgQvkZhv25x_SGlBiDV_okALrGbj6rUOWyNNNsHXMnT118XZmA696XR8qkr4dwT5Gvez-9gi-WYBY7XBkgo7v6NspGgJF89BNCeI-P9k-zBHOGgrf-fCEiAcoM7xCx9_f8qlRy7nhQPyjOIHn5eEJEir0uSu6gdqR9afnVZ3UoR-VOLdOBt7fA4ee38MP2ut5qWU50F5dvIezfKkTVDMHwztvcLCy6R9SVkdSYv6jwWGccYRl-aclvkkHu6SnbZGI7fmDZdkcBAxBHYEZZMmvb76ro4SO15GDyEVAo_Qf4trdrY_GyN_Bm73imCTjgtoGc

C:\Users\user\AppData\Local\Temp\6304_848482870\manifest.fingerprint

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.7900469623255675
Encrypted:	false
SSDEEP:	3:SpOXzxlQ4BdPWfDL9c:SpOjDQFfVc
MD5:	2AE14F91312C4E8034366B09D49D5B18

SHA1:	AD4933A5D838D0FA0B960C327A5039A9E8249642
SHA-256:	4F122332EF0F2BB490EF59619D3602C1A7277C0A7A19C132202DB4803A09BFA2
SHA-512:	FB0CC467A4B8463F6A3BF42CDC11C23B34EB94A9397644B68714DCB819EE326BAE05022D59D23DC9907DF1E6928064D853FD0900BB6083417892D4D5A9BA771
Malicious:	false
Preview:	1.aeedb246d19256a956fedaa89fb62423ae5bd8855a2a1f3189161cf045645a19

C:\Users\user\AppData\Local\Temp\6304_848482870\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	195
Entropy (8bit):	4.682333395896383
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFJ9LAG9Xg0XTFHqS1wP/pEeSWU4pv/8F/FxLj2RF2fcTZTotL:F6VlM90ggITgS1wnuWfB0NpK4aotL
MD5:	7A8E3A0B6417948DF4D49F3915428D7A
SHA1:	4FC084AABDB13483567D5C417C7ED8FD16726A80
SHA-256:	D1AC274CF1018020F2D9635A518ED1A1F21CC2CBE9E2A4392EC792D54B5B52FE
SHA-512:	064D84A57B28C19AD10742859DA493D0826B47ADC632F6C623DFB4DE36D72A9D29BE98518061A9FFD42D99FCF01F27DE39CE74782B3A5ACBBE11DFDDEEAB59A1
Malicious:	false
Preview:	{. "manifest_version": 2,. "name": "ImprovedRecoveryComponentInner",. "version": "1.3.36.141",. "imageName": "image.squash",. "squash": true,. "fsType": "squashfs",. "isRemovable": false.}

C:\Users\user\AppData\Local\Temp\6304_91553969_metadata\verified_contents.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3034
Entropy (8bit):	5.876664552417901
Encrypted:	false
SSDEEP:	48:p/hEc9q0S+UTKYM43z8nqMsfWRUWEADM/W9n7lqFkakzcVTGkcYTPi6zM:RGcg5z/jjjHgUnV278+aWLy4
MD5:	8B6C3E16DFBF5FD1C9AC2267801DB38E
SHA1:	F5CADC5914DF858C96C189B092BC89C29407BBAA
SHA-256:	FD986A547D9585E98F451B87CA85DEB4B61EE540C6FAC678D7BEDABF04653095
SHA-512:	37048EF8FADF62A26CAEC6EE90AC192429AB1E99424E5C68FACA90C0DAD68642C761FDCAC03FC38FA930841F91FA145A6943EC7F168D4F2FA426F1F092C2F502
Malicious:	false
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY19wbmFjbF9qc29uIiwicm9vdF9oYXNoIjoiVkNUSHNJVHNUSXVncWNhV2ctWHVpTU1sdWloV1FSTE1sQnpTTGprdGhETSJ9LHsicGF0aCI6Il9wbGF0Zm9ybV9zcGVjaWZpYy94ODZfNjQvcG5hY2xfcHVibGljX3g4Nl82NF9jcnRiZWdpbl9mb3JfZWhfbyIsInJvb3RfaGFzaCI6ImxINWt2a1BvSVZZczZKVHhyOHc5Q2MxXzIoVEJCX3lVSlF6VDZseVVNd0kifSx7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY194ODZfNjRfY3J0YmVnaW5fbyIsInJvb3RfaGFzaCI6IkVuLVFQTW1HUm1xbG9Ud1gzOTAzckpsMkw0R25sQmdET1FhZlNKaHJ4Nk0ifSx7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY194ODZfNjRfY3J0ZW5kX28iLCJyb290X2hhc2giOiJkT2lJVzRmdEdGNW9FY0k1UXYyYjBmdXNrUlYyaUVtdmxhbmV6MlpFc3VvIn0seyJwYXRoIjoiX3BsYXRmb3JtX3NwZWNpZmljL3g4Nl82NC9wbmFjbF9wdWJsaWNfeDg2XzY0X2xkX25leGUiLCJyb290X2hhc2giOiIzNEU5QU9EMmpqLWNoMzZQZ0NVV0YtMUpYWVhVdlNGY1I4bks1aWppcWNjIn0seyJwYXRoIjoiX3B

C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_pnacl_json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	507
Entropy (8bit):	4.68252584617246
Encrypted:	false
SSDEEP:	12:TjLJ7qaVgPPd8bdzQBXefosmc5T9+n6e1Cetm1JXcAwA:TJ7jViPOd8wfHmZ6RP15
MD5:	35D5F285F255682477F4C50E93299146
SHA1:	FB58813C4D785412F05962CD379434669DE79C2B
SHA-256:	5424C7B084EC4C8BA0A9C69683E5EE88C325BA28564112CC941CD22E392D8433
SHA-512:	59DF2D5F2684FACC80C72F9C4B7E280F705776076C9D843534F772D5A3D578BEE04289AEE81320F23FB4D743F3969EDF5BA53FEBBAC8A4D27F3BC53BCF271CE
Malicious:	false
Preview:	{. "COMMENT": [. "This file serves as a template for the resource info description used by ", . "the NaCl Chrome plugin. It is kept in the NaCl repository to prevent ", . "hard-coding of NaCl-specific information inside the Chrome repository.".], . "abi-version": 1, . "pnacl-arch": "x86-64", . "pnacl-ld-name": "ld.nexe", . "pnacl-llc-name": "pnacl-llc.nexe", . "pnacl-sz-name": "pnacl-sz.nexe", . "pnacl-version": "5dfe030a71ca66e72c5719ef5034c2ed24706c43".}

C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_for_eh_o	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	2712
Entropy (8bit):	3.4025803725190906
Encrypted:	false
SSDEEP:	48:b/5D5V5PK82aTS6aTTw0Do1DttoyDNsEA:b/hbVic1ZtLDNsE
MD5:	604FF8F351A88E7A1DBD7C836378AE86
SHA1:	9D8D89AE9F13D6306E619A4EAAD51EDE91A5F9F3
SHA-256:	947E64BE43E821562CE894F1AFCC3D09CD7FF614C107FC94250CD3EA5C943302
SHA-512:	85B1EDA4C473E00034EE627B7ABB894A77E521BC6A91A91A4A3744CA7511CB0AF10B9723D9ECC2CE3378DD70B659DF842D8C11875958CB77070CF01EC0A158 40
Malicious:	false
Preview:	.ELF.....>.....@.....@.....PH.....,$J.l=....J.$<A[..@.A...M..A..ffffff.....PH.....,$J.l=....J.$<A[..D..A...M..A..ffffff..... ....PH..1..,$J.l=....J.$<A[.....A...M..A..ffffff.....PH..SP..h.....fff.....h.....fff.....J.$<[.,$J.l=....J.$<....f..... .....NaCl....x86-64.....zR..x.....@....C....C.....8.....@....C....C.....T.....@....C....C .....p.....`....C....C..B..... .....<.....@.....X.....t.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl- clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pna

C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_o	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	2776
Entropy (8bit):	3.5335802354066246
Encrypted:	false
SSDEEP:	48:b/5D5V5ej5ej5PjDdaTS6aTTw6DV1DtFouoyDOsTy:b/hbEEVJB1ZFhLDOsT
MD5:	88C08CD63DE9EA244F70BFC53BBCADF6
SHA1:	8F38A113A66B18BAA02E2C995099CF1145A29DAA
SHA-256:	127F903CC986466AA5A13C17DFDD37AC99762F81A794180339069F48986BC7A3
SHA-512:	78D2500493A65A23D101EC2420DC5F0CE8C75EFAC425C28547121643E4FB568E9D827EF2C0F7068159E043C86B986F29BF92C6BADC675F160B63C7B3512EB95
Malicious:	false
Preview:	.ELF.....>.....X.....@.....@.....PH.....,$J.l=....J.$<A[..@.A...M..A..ffffff.....PH.....,$J.l=....J.$<A[..D..A...M..A..ffffff..... ....PH..1..,$J.l=....J.$<A[.....A...M..A..ffffff.....PH..,$J.l=....J.$<A[f.....A...M..A..ffffff.....PH..,$J.l=....J.$<A[f.....A...M..A..ffffff.....PH..SP..h..... ..fff.....J.$<[.,$J.l=....J.$<.....f.K.....`.....P.....z.....NaCl....x86-64...clang version 3.7.0 (https://chromium.googlesource.com /a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c9 4a3a7da70f0081724448f).....zR..x.....@....C....C.....8.....@....C....C.....T.....@....C....C.....p.....@....C....C.....@....C....C.....@...

C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_crtend_o	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	1520
Entropy (8bit):	2.799960074375893
Encrypted:	false
SSDEEP:	12:Bvx/ekjlM/NQQmTfR9yp9396QQmTfR9C6wRqD8MTDDw7lEOkSbfuEAXwX6BX2U8b:bDjO/NbmT3296bmT3Twk8qDwh7b7CD8
MD5:	75E79F5DB777862140B04CC6861C84A7
SHA1:	4DB7BDC80206765461AC68CEC03CE28689BBEE0C
SHA-256:	74E8885B87ED185E6811C23942FD9BD1FBAC9115768849AF95A9DECF6644B2EA
SHA-512:	FE3F86E926759E71494F2060C4ED3C883EBCAF20CB129A5AD7F142766C33FAB10B5FABC3C7C938E0E895E27EA0AC03CBFE8D0EEABF5300A4AD07F67FD96CC 253
Malicious:	false
Preview:	.ELF.....>.....@.....@.....NaCl....x86-64.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f)...text..comment..bss..group..note.GNU-stack..eh_frame..shstrtab..strtab..symtab..data..note.NaCl.ABI.x86-64.....!..... ..../../../pnacl/support/crtend.c.__EH_FRAME_END__..... .....@.....H.....P.....H.....

C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=7511538a3a6a0b862c772eace49075ed1bbe2377, stripped
Category:	dropped
Size (bytes):	2163864
Entropy (8bit):	6.07050487397106
Encrypted:	false
SSDEEP:	24576:HPHonIwYZJ0ykwVO7Owf31yJKzCtxO8RSV4lY+PbeHVxCtjFV4lBNeSAmfGqa+A7:HvSMRwf3SKmlY+PyPvnM2Gq+
MD5:	0BB967D2E99BE65C05A646BC67734833
SHA1:	220A41A326F85081A74C4BB7C5F4E115D1B4B960
SHA-256:	C6C2D0C2FC3E38A9BFA19C78066439C2F745393F1FD1C49C3C6777F697222C76
SHA-512:	8EF8689E00E4B210A30444D18ED6247F364995ABEB2FD272064C3AF671EEDB4D9B8B67CA56F72FEBF8F56896D4EA7EC4B10CB445FFA1C710C1F312E9DA0E4896
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	.ELF.....>.... .....@.....!.....@.8...@.....{.....W.....@.....@.....P.td.....h.....h.....h.....4b.....4b.....Q.td.....NaCl....x86-64.....GNU.u.S.:j..,w...u...#w.....?.....Y@.....@.....1@.....B@.....P@.....@X@.....``@.....h@.....pp@.....H.@.....@.....@.....@.....@.....@....`..@.....@.....A.....A.....p.....@.....?.....A.....5.....?5.5...?.5.....?.....P9.....PC.....?.....0@.....aCoc...?..`.(..?.y.P.D.?<.s..O.u.....$@.....@.....@..... ... .@...`...`...`...`.....`...`...`...`...`...`...`.....`...

C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_libcrt_platform_a

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	40552
Entropy (8bit):	4.127255967843258
Encrypted:	false
SSDEEP:	768:xlP+1fzyUNVU5LmKxeOnjpD5eA/eUnUUxvT:xlP+1ryYMTekpD5eAWjuvT
MD5:	0CE951B216FCF76F754C9A845700F042
SHA1:	6F99A259C0C8DAD5AD29EE983D35B6A0835D8555
SHA-256:	7A1852EA4BB14A2A623521FA53F41F02F8BA3052046CF1AA0903CFAD0D1E1A7B
SHA-512:	7C2F9BF90EB1F43C17B4E14A077759FA9DC62A7239890975B2D6FD543B31289DC3B49AE456CA73B98DE9AC372034F340C708D23D9D3AAB05CCBDABDC56A634E
Malicious:	false
Preview:	!<arch>./ 0 0 0 0 624 `.....,...8...Z(..e...e...t...t...y`..y`..y`..y`..y`..y`..y`..y`..y`..y`..y`..y`.....fmod.fmodf.memcmp.memcpy.memmove.memset.__nacl_read_tp.__pnacl_init_irt.longjmp.setjmp.__Sz_fptosi_f32_i64.__Sz_fptosi_f64_i64.__Sz_fptoui_f32_i32.__Sz_fptoui_f32_i64._Sz_fptoui_f64_i32.__Sz_fptoui_f64_i64.__Sz_sitofp_i64_f32.__Sz_sitofp_i64_f64.__Sz_uitofp_i32_f32.__Sz_uitofp_i32_f64.__Sz_uitofp_i64_f32.__Sz_uitofp_i64_f64.nacl_tp_tdb_offset.nacl_tp_tls_offset.__Sz_bitcast_16xi1_i16.__Sz_bitcast_8xi1_i8.__Sz_bitcast_i16_16xi1.__Sz_bitcast_i8_8xi1.__Sz_fptoui_4xi32_f32.__Sz_uitofp_4xi32_4xf32..e_fmod.o/ 0 0 0 644 2792 `..ELF.....>.....(.....@.....@.....PH..AVAUATSfI.~.M..I.. E....@.A.....D..D1.....8fI.~.M....I.. E..A.....D..D..t.D....D..f....D..=....r...Y...^.[A\A]A^..@..,$J.I=....J.$<A[A...M..

C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_libgcc_a

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	132784
Entropy (8bit):	3.6998481247844937
Encrypted:	false
SSDEEP:	384:Hf0mOXYmeKzQUIdedRFvT5p1Ee2HyAlL3O4:Hf7OXdmWRJT5p1R2HyAhO4
MD5:	C37CA2EB468E6F05A4E37DF6E6020D0F
SHA1:	EA787E5EADFB488632EC60D8B80B555796FA9FE9
SHA-256:	C1483ED423FEE15D86E8B5D698B2CDAB89186CE7FF9C4E3D5F3F961FD80D7C6E
SHA-512:	01281DE92B281FB29E1ACA96AA64B740B65CC3A9097307827F0D8DB9E1C164C56AFCDFA0BF138EA670A596D55CE2C8D722760744E9FC9343BB6514417BF333EA
Malicious:	false
Preview:	!<arch>./ 0 0 0 0 942 `....;...|.....4...x..#...-...4l..E...M...U...]...n...u...~X...4.....L.....t...p.....`.....''...*...1...:....D...K...T...\...d...r|..|0.....x.....L.....\...8.....__clzti2.__compilerrt_fmax.__compilerrt_fmaxf.__compilerrt_logb.__compilerrt_logbf.__ctzti2.__divdc3.__divdi3.__divmoddi4.__divmodsi4.__divsc3.__divsi3.__divti3.__fixdfdi.__fixdfsi.__fixdfti.__fixsfdi.__fixsfsi.__fixsfti.__fixunsdfdi.__fixunsdfsi.__fixunsdfti.__fixunssfdi.__fixunssfsi.__fixunssfti.__floatdidf.__floatdisf.__floatsidf.__floatsisf.__floattidf.__floattisf.__floatundidf.__floatundisf.__floatunsidf.__floatunsisf.__floatuntidf.__floatuntisf.compilerrt_abort_impl.__moddi3.__modsi3.__modti3.__muldc3.__muloti4.__mulsc3.__multi3.__popcountdi2.__popcountsi2.__popcountti2.__powidf2.__powisf2.__udivdi3.__udivmoddi4.__udivmodsi4.__udivmodti4.__udivsi3.__udivti3.__umoddi3.__umodsi3.

C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_a

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

File Type:	current ar archive
Category:	dropped
Size (bytes):	13514
Entropy (8bit):	3.8217211433441904
Encrypted:	false
SSDEEP:	192:uU9v4pXizdrEuxwk3vp20tprpdSGFwDqO:P9v4palvvc0tpFdSGFwmO
MD5:	4E8BEDA73EB7BD99528BF62B7835A3FA
SHA1:	DC0F263A7B2A649D11FF7B56FE9CFAC44F946036
SHA-256:	6B835FD48DF505EB336FF6518CE7B93BB0ED854DADAA5C1EEED48D420291F62C
SHA-512:	46116B8BABC719676D68FD40D2AC82F38A3D13D8A482ADFC6FC32A99170AC3420E52CC33242CCD0FA723ABF4FA5EDBB9CE16A09C729BF04AE4AFBB2F67A1E 38B
Malicious:	false
Preview:	!<arch>./ 0 0 0 0 94 `................_pnacl_wrapper_start.__pnacl_real_irt_query_func.__pnacl_wrap_irt_query_func..shim_entry.o/ 0 0 0 644 7392 `..ELF.............>.................... ....@.....@.........................NaCl....x86-64.................................A.L....A.L...D...........D....A.....t+.. u..t"..A.D..... .....A... .....A.D...........f..D..<......................Q.......................V.......................clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f).../../ppapi/native_client/src/untrusted/pnacl_irt_shim/shim_entry.c./mnt/data/b/build/slave/sdk/build/src/out_pnacl/x64.NACL_STARTUP_FINI.NACL_STARTUP_ENVC. NACL_STARTUP_ARGC.NACL_STARTUP_ARGV.NaClStartupInfoIndex.unsigned int.size_t.char.TYPE_na

C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_dummy_a

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	2078
Entropy (8bit):	3.21751839673526
Encrypted:	false
SSDEEP:	24:MOcpdhWE5O/bZbmT3296bmT3TwQwDnvD/+R3:MHuECdaTS6aTTwXDvD/+l
MD5:	F950F89D06C45E63CE9862BE59E937C9
SHA1:	9CFAD34139CC428CE0C07A869C15B71A9632365D
SHA-256:	945B1C8A1666CBF05E8B8941B70D9D044BAAFB59B006F728F8995072DE7C4C40
SHA-512:	F9AFBB800A875EDCC63DEA4986179E73632B3182951A99C8B3D37DB454EFD7CC7192ECA5AC87514918A858BAD6DAEAB59548CA2E90EADA9900EF5B9F08E62 CFC
Malicious:	false
Preview:	!<arch>./ 0 0 0 0 30 `........_pnacl_wrapper_start..// 20 `.dummy_shim_entry.o/./0 0 0 0 644 1840 `..ELF.............>................................@.....@......................................PH..,$J.l=....J.$<.....f..D......................................NaCl....x86-64...clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f)............zR..x...................... ....C....C..... ....rela.text..comment..bss..group..note.GNU-stack..rela.eh_frame..shstrtab..strtab..symtab..data..note.NaCl.ABI.x86-64...

C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=309d6d3d463e6b1b0690f39eb226b1e4c469b2ce, stripped
Category:	dropped
Size (bytes):	14091416
Entropy (8bit):	5.928868737447095
Encrypted:	false
SSDEEP:	196608:tKVqXp3Qev4dg6ilfHM8KLM2J3jqjnkZ:uqufB
MD5:	9B159191C29E766EBBF799FA951C581B
SHA1:	D1D4BBC63AB5FC1E4A54EB7B82095A6F2CE535EE
SHA-256:	2F4A3A0730142C5EE4FA2C05D27A5DEFC18886A382D45F5DB254B61B28ED642B
SHA-512:	0B4FF60B5428F81B8B1BCF3328CF80CBD88D8CE5E8BDBC236B06D5A54E7CF26168A3ABB348D87423DA613AB3F0B4D9B37CB5180804839F1CA158EC2B315DD 00
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	.ELF.............>..... ....@..................@.8...@..............$..!.......!......'......G.................................. ....@.......@..............P.td...........................D.......D..............Q.td..NaCl....x86-64.............GNU.0.m=F>k....&...i...................... ..0C......0C..0C..0E..............0C......0E.-DT.!.?.-DT.!.........................?........-DT.!...-DT.!.?.......?......................?..............?."..."..."..."......@.......`...................... ...@...`................ ....@...`...................... ...@...`...................... ...@...`.......................................`... ...@...`...........`...`.......@...@....... ....1..`3.. 4..`-..`-...:...:...F..@H..`H...H...F...F...G...H.. H. ..F..@G...I.. I..@I..@G...G...I...I...J...G..`I..

C:\Users\user\AppData\Local\Temp\6304_91553969_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=4b15de4ab227d5e46213978b8518d53c53ce1db9, stripped

Category:	dropped
Size (bytes):	1901720
Entropy (8bit):	5.955741933854651
Encrypted:	false
SSDEEP:	12288:gXqUSpBjwQO2o8k+7zjidg4euCAauOILffvCpGy4Wh3BTFmHpq82K2/KsvPyla9d:gafZwcOdNe2auOepCBTFmJq3Kf8ksr
MD5:	9DC3172630E525854B232FF71499D77C
SHA1:	0082C58EDCE3769E90DB48E7C26090CE706AD434
SHA-256:	6AA1DA6C264E0AF4E32A004F4076C7557C6AC6D9C38B0C5DE97302D83FA248C3
SHA-512:	9E9584241A39EED1463D7D4C1B26AE570B839AA315778FF3400C61341EBA43B630307DE9F1532A265CA82EA69BDEA03EC9D963E59A18569C02DA8285449870F
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	.ELF.....>..... .....@.....@.8...@.....0.....0.....Y..... .....@.....@.....P.td....t^.....t^.....t^.....W.....W.....Q.td.....NaCl....x86-64.....GNU.K..J.'..b.....<S...`...`.. ...@... @.....@.....Y@.....p.....@.....?.....?.....A.....5.....?5.5...?.5.....?.....P9.....PC.....?.....0@.....aCoc...?..`.(..? .y.P.D.?<.s..O.u.....$@.....@.....@`..`.....@..... ...`.. ... .`..... .. ...@...`.....@... Z...[...[...e..... ...@... ...@.. .`.....0...0...2..`4.. 6...7...9...~...~...z...{...{..

C:\Users\user\AppData\Local\Temp\6304_91553969\manifest.fingerprint

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.928261499316817
Encrypted:	false
SSDEEP:	3:STDLGswXEVBcVdBiTDt3zLsW:SPLGLErcVdBiDtf3
MD5:	C00BCE97F21B1AD61EB9B8CD001795EE
SHA1:	8E0392FF3DB267D847711C3F4E0D7468060E1535
SHA-256:	59F06F04230E32E8BC839F45B984D31D611930427B631C963D09E7064A602363
SHA-512:	9930E44A6ECC62505DBADCEED5E05645909FF09816FB12AAC0414E6D2830AC09758366C3B7D4EDD7839C87EB16DFA4C66D8981AE6237D408B37135C3506F4C2
Malicious:	false
Preview:	1.6f6bc93dcd62dc251850d2ff458fda96083ceb7fbe8eeb11248b8485ef2aea23

C:\Users\user\AppData\Local\Temp\6304_91553969\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	573
Entropy (8bit):	4.859567579783832
Encrypted:	false
SSDEEP:	12:BLqG6yDJmL4mLDlG9hQ181G46XzrXc+EFfNqpaiOc+T5NqXIOclNqXL:BkylmL4mLDlJ18116XsRNqtZeNqXIZlE
MD5:	1863B86D0863199AFDA179482032945F
SHA1:	36F56692E12F2A1EFCA7736C236A8D776B627A86
SHA-256:	F14E451CE2314D29087B8AD0309A1C8B8E81D847175EF46271E0EB49B4F84DC5
SHA-512:	836556F3D978A89D3FC1F07FCED2732A17E314ED6A021737F087E32A69BFA46FD706EBBDFD3607FF42EDCB75DC463C29B9D9D2F122504F567BB95844F579831
Malicious:	false
Preview:	{."update_url": "https://clients2.google.com/service/update2/crx",.. "description": "Portable Native Client Translator Multi-CRX",. "name": "PNaCl Translator Multi-CRX",. "manifest_version": 2,. "minimum_chrome_version": "30.0.0.0",. "version": "0.57.44.2492",. "platforms": [. {. "nacl_arch": "x86-32",. "sub_package_path": "_platform_specific/x86_32/". },. {. "nacl_arch": "x86-64",. "sub_package_path": "_platform_specific/x86_64/". },. {. "nacl_arch": "arm",. "sub_package_path": "_platform_specific/arm/". }.].}.

C:\Users\user\AppData\Local\Temp\eced9d10-a2e5-4d97-8392-cfa9e1143505.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D

SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\201465c9-d45e-4764-9cc5-184c46c51ed9.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326088
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u.. ..k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..)......,b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2.. ;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.I....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\bg\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F7700C
Malicious:	false
Preview:	{.. "app_description": {.. "message": "..... . ... Chrome".. },.. "app_name": {.. "message": "..... . ... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "...., ...".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "...., ... Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\ca\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CB4
Malicious:	false

Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "C onnecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\cs\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D8488 CB
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\da\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5 E0A
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_u navailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be comp leted.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\de\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB80 552
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_una vailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "The trans action could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\el\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	787
Entropy (8bit):	4.973349962793468
Encrypted:	false
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWlOGAOf+XD:WguYpCZnpEZbGoD
MD5:	05C437A322C1148B5F78B2F341339147
SHA1:	AB53003A678E44A170E73711FBD9949833BBF3AA
SHA-256:	A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070
SHA-512:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B4 0
Malicious:	false
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavail able": {.. "message": ". ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": ".. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\en\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\en_GB\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\es\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	661
Entropy (8bit):	4.450938335136508

Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyZnLAOfTY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OGAOffD
MD5:	82719BD3999AD66193A9B0BB525F97CD
SHA1:	41194D511F1ACC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE01 28
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "Los pagos en la aplicaci.n no est.n disponibles en este momento.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\es_419\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	637
Entropy (8bit):	4.47253983486615
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34GLO03OyZnLAOfTYiJD:1HEvaC6WYpcDeEFxq8Zp4LlOGAOfvD
MD5:	6B2583D8D1C147E36A69A88009CBEBC7
SHA1:	4D4DEEB4BE6AA0181825F3371A761ABC5B4D5937
SHA-256:	6659BC3705311D7641A73995DCFEA80C7734F2F4EBBC3787B3892A240348324F
SHA-512:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA 53
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "En este momento, Pagos En-Apps no est. disponible.".. },.. "jwt_retrieve_failed": {.. "message": "The tr ansaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\et\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\fi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.595421267152647
Encrypted:	false
SSDEEP:	12:1HEJRuzGGRuz+WYpU34ujSBu+dgYO8ZpU34J+Bu03OyZnLAOfTY5HN:1HEFcWYpPNa8ZpD+FOGAOfEHN
MD5:	3A01FEE829445C482D1721FF63153D16
SHA1:	F3EAAADDC03F943FC88B30B67F534AA13E3336DD
SHA-256:	0BDE54B20845124113383B6EB81E43A0F05E4EB0C44BEE3C1DFAC4CC5FEC2836

SHA-512:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BE/D8
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Web Storen maksut".. },.. "app_name": {.. "message": "Chrome Web Storen maksut".. },.. "craw_app_unavailable": {.. "message": "Sovellus ei ole t.ll. hetkell. k.ytett.viss..".. },.. "craw_connect_to_network": {.. "message": "Muodosta verkkoyhteys.".. },.. "iap_unavailable": {.. "message": "Sovelluksen sis.iset maksut eiv.t ole t.ll. hetkell. k.ytett.viss..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Kirjaudu sis..n Chromeen.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\fil\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	658
Entropy (8bit):	4.5231229502550745
Encrypted:	false
SSDEEP:	12:1HEJADlbGGADlb+WYpU34hTUT+dgHfZAFFZO8ZpU34hTjzeT03OyZnLAOfTYHfvF:1HEYah6WYp7TUSoxOS8Zp7TOsOGAOfqV
MD5:	57AF5B654270A945BDA8053A83353A06
SHA1:	EEEF7A4F869F97CF471A05D345E74F982D15E167
SHA-256:	EC002ED92359F67818B49455DFC579E140368E6A004080AF022FD4F57F6B03F2
SHA-512:	5F0AE839FCF3F4EA48FF41A76655AE0F3821564AFD5D42FBB9FBB9A38E8D8F7BB5E9B6F71064588CD441261F644095A44A755C134CE546D506D9A21E488BAF52
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "app_name": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Kasalukuyang hindi available ang app.".. },.. "craw_connect_to_network": {.. "message": "Mangyaring kumonekta sa isang network.".. },.. "iap_unavailable": {.. "message": "Kasalukuyang hindi available ang Mga Pagbabayad na In-App.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Mangyaring mag-sign in sa Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\fr\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir6304_1607013840\CRX_INSTALL_locales\hi\messages.json

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

Static File Info

General

File type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	3.718089614560754
TrID:	
File name:	office365 Validation.html
File size:	364416
MD5:	d093787907af4624bbaa6e3a0f655091
SHA1:	8b55805d15db65ba3b927b332a8ea0e9a8e18017
SHA256:	bffffe8e717d7e88f3485efe04f7609e90995c021c10e6060e7ca001150d163b
SHA512:	8f46bdce4ecf6019a0f93776feafe466e1022bf0de1ad5947751ddc05c7bbff02e0d2d0cbc444f95286cda5bc11f1cffb57841e707769af7ca4b0f260b9af263
SSDEEP:	1536:+/ezTojkUrjGCyWmaL276z+1nDy3UINKQINKldA1nZkp2FWv/tNOTrEJwDF:+/Uofz+1rFO/tMEJwDF
TLSH:	5F74569D77211C9DFC21652BE2DA736AD2E01C83F15DD843A9982480AF80E7DE1F177A
File Content Preview:	<script language="javascript">document.write(unescape('%3Chtml%3E%0A%20%20%3Chead%3E%0A%20%20%20%20%3Cmeta%20http-equiv%3D%22Content-Type%22%20content%3D%22text%2Fhtml%3B%20charset%3Dutf-8%22%20%2F%3E%0A%20%20%20%20%3Cmeta%20http-equiv%3D%22X-UA-Compati

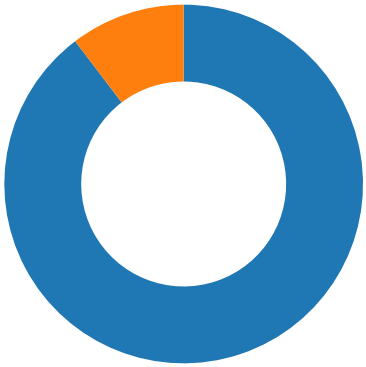
File Icon



Icon Hash:	e8d6a08c8882c461

Network Behavior

Network Port Distribution



Total Packets: 58

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 30, 2022 23:10:50.096465111 CEST	49737	443	192.168.2.3	142.251.36.238
Jun 30, 2022 23:10:50.096529007 CEST	443	49737	142.251.36.238	192.168.2.3
Jun 30, 2022 23:10:50.096597910 CEST	49737	443	192.168.2.3	142.251.36.238
Jun 30, 2022 23:10:50.096927881 CEST	49738	443	192.168.2.3	142.251.36.205
Jun 30, 2022 23:10:50.096961975 CEST	443	49738	142.251.36.205	192.168.2.3
Jun 30, 2022 23:10:50.097022057 CEST	49738	443	192.168.2.3	142.251.36.205
Jun 30, 2022 23:10:50.097395897 CEST	49737	443	192.168.2.3	142.251.36.238
Jun 30, 2022 23:10:50.097420931 CEST	443	49737	142.251.36.238	192.168.2.3
Jun 30, 2022 23:10:50.097640038 CEST	49738	443	192.168.2.3	142.251.36.205
Jun 30, 2022 23:10:50.097651005 CEST	443	49738	142.251.36.205	192.168.2.3
Jun 30, 2022 23:10:50.167325974 CEST	443	49737	142.251.36.238	192.168.2.3

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 30, 2022 23:10:50.168709993 CEST	49737	443	192.168.2.3	142.251.36.238
Jun 30, 2022 23:10:50.168745995 CEST	443	49737	142.251.36.238	192.168.2.3
Jun 30, 2022 23:10:50.169087887 CEST	443	49737	142.251.36.238	192.168.2.3
Jun 30, 2022 23:10:50.169161081 CEST	49737	443	192.168.2.3	142.251.36.238
Jun 30, 2022 23:10:50.169891119 CEST	443	49737	142.251.36.238	192.168.2.3
Jun 30, 2022 23:10:50.169950008 CEST	49737	443	192.168.2.3	142.251.36.238
Jun 30, 2022 23:10:50.174844980 CEST	443	49738	142.251.36.205	192.168.2.3
Jun 30, 2022 23:10:50.178966045 CEST	49738	443	192.168.2.3	142.251.36.205
Jun 30, 2022 23:10:50.179008961 CEST	443	49738	142.251.36.205	192.168.2.3
Jun 30, 2022 23:10:50.180200100 CEST	443	49738	142.251.36.205	192.168.2.3
Jun 30, 2022 23:10:50.180352926 CEST	49738	443	192.168.2.3	142.251.36.205
Jun 30, 2022 23:10:50.542772055 CEST	49737	443	192.168.2.3	142.251.36.238
Jun 30, 2022 23:10:50.543000937 CEST	443	49737	142.251.36.238	192.168.2.3
Jun 30, 2022 23:10:50.543018103 CEST	49738	443	192.168.2.3	142.251.36.205
Jun 30, 2022 23:10:50.543117046 CEST	443	49738	142.251.36.205	192.168.2.3
Jun 30, 2022 23:10:50.544358969 CEST	49737	443	192.168.2.3	142.251.36.238
Jun 30, 2022 23:10:50.544382095 CEST	443	49737	142.251.36.238	192.168.2.3
Jun 30, 2022 23:10:50.544555902 CEST	49738	443	192.168.2.3	142.251.36.205
Jun 30, 2022 23:10:50.544584036 CEST	443	49738	142.251.36.205	192.168.2.3
Jun 30, 2022 23:10:50.584183931 CEST	443	49737	142.251.36.238	192.168.2.3
Jun 30, 2022 23:10:50.584357977 CEST	443	49737	142.251.36.238	192.168.2.3
Jun 30, 2022 23:10:50.584379911 CEST	49737	443	192.168.2.3	142.251.36.238
Jun 30, 2022 23:10:50.584434986 CEST	49737	443	192.168.2.3	142.251.36.238
Jun 30, 2022 23:10:50.589726925 CEST	49737	443	192.168.2.3	142.251.36.238
Jun 30, 2022 23:10:50.589754105 CEST	443	49737	142.251.36.238	192.168.2.3
Jun 30, 2022 23:10:50.627181053 CEST	443	49738	142.251.36.205	192.168.2.3
Jun 30, 2022 23:10:50.627291918 CEST	49738	443	192.168.2.3	142.251.36.205
Jun 30, 2022 23:10:50.627300978 CEST	443	49738	142.251.36.205	192.168.2.3
Jun 30, 2022 23:10:50.627357006 CEST	49738	443	192.168.2.3	142.251.36.205
Jun 30, 2022 23:10:50.630651951 CEST	49738	443	192.168.2.3	142.251.36.205
Jun 30, 2022 23:10:50.630677938 CEST	443	49738	142.251.36.205	192.168.2.3
Jun 30, 2022 23:10:50.864840984 CEST	49740	443	192.168.2.3	151.101.112.193
Jun 30, 2022 23:10:50.864907980 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.865039110 CEST	49740	443	192.168.2.3	151.101.112.193
Jun 30, 2022 23:10:50.865266085 CEST	49740	443	192.168.2.3	151.101.112.193
Jun 30, 2022 23:10:50.865289927 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.929475069 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.955394983 CEST	49740	443	192.168.2.3	151.101.112.193
Jun 30, 2022 23:10:50.955450058 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.957446098 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.957561970 CEST	49740	443	192.168.2.3	151.101.112.193
Jun 30, 2022 23:10:50.959666967 CEST	49740	443	192.168.2.3	151.101.112.193
Jun 30, 2022 23:10:50.959810019 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.959820986 CEST	49740	443	192.168.2.3	151.101.112.193
Jun 30, 2022 23:10:50.985255003 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.985362053 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.985455990 CEST	49740	443	192.168.2.3	151.101.112.193
Jun 30, 2022 23:10:50.985496044 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.985569000 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.985569000 CEST	49740	443	192.168.2.3	151.101.112.193
Jun 30, 2022 23:10:50.985591888 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.985646963 CEST	49740	443	192.168.2.3	151.101.112.193
Jun 30, 2022 23:10:50.985661983 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.985804081 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.985882998 CEST	49740	443	192.168.2.3	151.101.112.193
Jun 30, 2022 23:10:50.985898018 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.987315893 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.987385035 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.987431049 CEST	49740	443	192.168.2.3	151.101.112.193

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 30, 2022 23:10:50.987443924 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.987509966 CEST	49740	443	192.168.2.3	151.101.112.193
Jun 30, 2022 23:10:50.988086939 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.988229990 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.988312006 CEST	49740	443	192.168.2.3	151.101.112.193
Jun 30, 2022 23:10:50.988325119 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.988898039 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.989003897 CEST	49740	443	192.168.2.3	151.101.112.193
Jun 30, 2022 23:10:50.989017010 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.989655018 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.989742041 CEST	49740	443	192.168.2.3	151.101.112.193
Jun 30, 2022 23:10:50.989757061 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.991075993 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.991144896 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.991158962 CEST	49740	443	192.168.2.3	151.101.112.193
Jun 30, 2022 23:10:50.991170883 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.991256952 CEST	49740	443	192.168.2.3	151.101.112.193
Jun 30, 2022 23:10:50.991816044 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.992690086 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.992770910 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.992772102 CEST	49740	443	192.168.2.3	151.101.112.193
Jun 30, 2022 23:10:50.992805004 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.992867947 CEST	49740	443	192.168.2.3	151.101.112.193
Jun 30, 2022 23:10:50.993387938 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.994187117 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.994282007 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.994286060 CEST	49740	443	192.168.2.3	151.101.112.193
Jun 30, 2022 23:10:50.994318962 CEST	443	49740	151.101.112.193	192.168.2.3
Jun 30, 2022 23:10:50.994374990 CEST	49740	443	192.168.2.3	151.101.112.193
Jun 30, 2022 23:10:51.003443003 CEST	443	49740	151.101.112.193	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 30, 2022 23:10:49.871686935 CEST	65358	53	192.168.2.3	8.8.8.8
Jun 30, 2022 23:10:49.899194956 CEST	53	65358	8.8.8.8	192.168.2.3
Jun 30, 2022 23:10:49.985115051 CEST	53802	53	192.168.2.3	8.8.8.8
Jun 30, 2022 23:10:49.987416983 CEST	65266	53	192.168.2.3	8.8.8.8
Jun 30, 2022 23:10:50.011090040 CEST	53	53802	8.8.8.8	192.168.2.3
Jun 30, 2022 23:10:50.759660959 CEST	63548	53	192.168.2.3	8.8.8.8
Jun 30, 2022 23:10:50.778783083 CEST	53	63548	8.8.8.8	192.168.2.3
Jun 30, 2022 23:10:56.744127035 CEST	63146	53	192.168.2.3	8.8.8.8
Jun 30, 2022 23:10:56.745260000 CEST	52985	53	192.168.2.3	8.8.8.8
Jun 30, 2022 23:10:56.762729883 CEST	53	63146	8.8.8.8	192.168.2.3
Jun 30, 2022 23:10:59.439673901 CEST	50780	443	192.168.2.3	142.251.36.238
Jun 30, 2022 23:10:59.480514050 CEST	443	50780	142.251.36.238	192.168.2.3
Jun 30, 2022 23:10:59.506714106 CEST	50780	443	192.168.2.3	142.251.36.238
Jun 30, 2022 23:10:59.547151089 CEST	443	50780	142.251.36.238	192.168.2.3
Jun 30, 2022 23:10:59.547192097 CEST	443	50780	142.251.36.238	192.168.2.3
Jun 30, 2022 23:10:59.547214985 CEST	443	50780	142.251.36.238	192.168.2.3
Jun 30, 2022 23:10:59.547234058 CEST	443	50780	142.251.36.238	192.168.2.3
Jun 30, 2022 23:10:59.547475100 CEST	50780	443	192.168.2.3	142.251.36.238
Jun 30, 2022 23:10:59.550307035 CEST	50780	443	192.168.2.3	142.251.36.238
Jun 30, 2022 23:10:59.641726971 CEST	50780	443	192.168.2.3	142.251.36.238
Jun 30, 2022 23:10:59.642077923 CEST	50780	443	192.168.2.3	142.251.36.238
Jun 30, 2022 23:10:59.687820911 CEST	443	50780	142.251.36.238	192.168.2.3
Jun 30, 2022 23:10:59.694807053 CEST	443	50780	142.251.36.238	192.168.2.3
Jun 30, 2022 23:10:59.695970058 CEST	443	50780	142.251.36.238	192.168.2.3
Jun 30, 2022 23:10:59.705185890 CEST	443	50780	142.251.36.238	192.168.2.3

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 30, 2022 23:10:59.705255985 CEST	443	50780	142.251.36.238	192.168.2.3
Jun 30, 2022 23:10:59.705296993 CEST	443	50780	142.251.36.238	192.168.2.3
Jun 30, 2022 23:10:59.708337069 CEST	50780	443	192.168.2.3	142.251.36.238
Jun 30, 2022 23:10:59.708595991 CEST	50780	443	192.168.2.3	142.251.36.238
Jun 30, 2022 23:10:59.817354918 CEST	443	50780	142.251.36.238	192.168.2.3
Jun 30, 2022 23:10:59.954797983 CEST	50780	443	192.168.2.3	142.251.36.238

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 30, 2022 23:10:49.871686935 CEST	192.168.2.3	8.8.8.8	0xd881	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jun 30, 2022 23:10:49.985115051 CEST	192.168.2.3	8.8.8.8	0xe241	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jun 30, 2022 23:10:49.987416983 CEST	192.168.2.3	8.8.8.8	0xbba	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Jun 30, 2022 23:10:50.759660959 CEST	192.168.2.3	8.8.8.8	0xa8d8	Standard query (0)	i.imgur.com	A (IP address)	IN (0x0001)
Jun 30, 2022 23:10:56.744127035 CEST	192.168.2.3	8.8.8.8	0x792d	Standard query (0)	i.imgur.com	A (IP address)	IN (0x0001)
Jun 30, 2022 23:10:56.745260000 CEST	192.168.2.3	8.8.8.8	0xb372	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 30, 2022 23:10:49.899194956 CEST	8.8.8.8	192.168.2.3	0xd881	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 23:10:49.899194956 CEST	8.8.8.8	192.168.2.3	0xd881	No error (0)	clients.l.google.com		142.251.36.238	A (IP address)	IN (0x0001)
Jun 30, 2022 23:10:50.008014917 CEST	8.8.8.8	192.168.2.3	0xbba	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 23:10:50.011090040 CEST	8.8.8.8	192.168.2.3	0xe241	No error (0)	accounts.google.com		142.251.36.205	A (IP address)	IN (0x0001)
Jun 30, 2022 23:10:50.778783083 CEST	8.8.8.8	192.168.2.3	0xa8d8	No error (0)	i.imgur.com	ipv4.imgur.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 23:10:50.778783083 CEST	8.8.8.8	192.168.2.3	0xa8d8	No error (0)	ipv4.imgur.map.fastly.net		151.101.112.193	A (IP address)	IN (0x0001)
Jun 30, 2022 23:10:56.762729883 CEST	8.8.8.8	192.168.2.3	0x792d	No error (0)	i.imgur.com	ipv4.imgur.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 23:10:56.762729883 CEST	8.8.8.8	192.168.2.3	0x792d	No error (0)	ipv4.imgur.map.fastly.net		151.101.12.193	A (IP address)	IN (0x0001)
Jun 30, 2022 23:10:56.775197029 CEST	8.8.8.8	192.168.2.3	0xb372	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- i.imgur.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49737	142.251.36.238	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Copyright Joe Security LLC 2022

Timestamp	kBytes transferred	Direction	Data
2022-06-30 21:10:50 UTC	0	OUT	GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1 HTTP/1.1 Host: clients2.google.com Connection: keep-alive X-Goog-Update-Interactivity: fg X-Goog-Update-AppId: nmmhkkegccagdldgiimedpiccmgmieda,pkedcjkdefgpdelpbcmbmeomcjbeemfm X-Goog-Update-Updater: chromecrx-85.0.4183.121 Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-06-30 21:10:50 UTC	1	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-fQnjj0bZ84X0ycL4CPuDvQ' 'unsafe-inline' 'strict-dynamic' https: http:;object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/clientupdate-aus/1 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Thu, 30 Jun 2022 21:10:50 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5659 X-Daystart: 51050 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-06-30 21:10:50 UTC	2	IN	Data Raw: 33 31 61 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 67 75 70 64 61 74 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 75 70 64 61 74 65 32 2f 72 65 73 70 6f 6e 73 65 22 20 70 72 6f 74 6f 63 6f 6c 3d 22 32 2e 30 22 20 73 65 72 76 65 72 3d 22 70 72 6f 64 22 3e 3c 64 61 79 73 74 61 72 74 20 65 6c 61 70 73 65 64 5f 64 61 79 73 3d 22 35 36 35 39 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 35 31 30 35 30 22 2f 3e 3c 61 70 70 20 61 70 70 69 64 3d 22 6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 22 20 63 6f 68 6f 72 74 3d 22 31 3a 3a 22 20 63 6f 68 6f 72 74 6e 61 6d 65 3d 22 22 Data Ascii: 31a<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" protocol="2.0" server="prod"><daystart elapsed_days="5659" elapsed_seconds="51050"/><app appid="nmmhkkegccagdldgiimedpiccmgmieda" cohort="1::" cohortname=""
2022-06-30 21:10:50 UTC	2	IN	Data Raw: 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 7a 65 3d 22 32 34 38 35 33 31 22 20 73 74 61 74 75 73 3d 22 6f 6b 22 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 2e 30 2e 36 22 2f 3e 3c 2f 61 70 70 3e 3c 61 70 Data Ascii: mhkkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" size="248531" status="ok" version="1.0.0.6"/></app><ap
2022-06-30 21:10:50 UTC	2	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49738	142.251.36.205	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 21:10:50 UTC	0	OUT	POST /ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard HTTP/1.1 Host: accounts.google.com Connection: keep-alive Content-Length: 1 Origin: https://www.google.com Content-Type: application/x-www-form-urlencoded Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-06-30 21:10:50 UTC	1	OUT	Data Raw: 20 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2022-06-30 21:10:50 UTC	2	IN	HTTP/1.1 200 OK Content-Type: application/json; charset=utf-8 Access-Control-Allow-Origin: https://www.google.com Access-Control-Allow-Credentials: true X-Content-Type-Options: nosniff Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Thu, 30 Jun 2022 21:10:50 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Content-Security-Policy: script-src 'report-sample' 'nonce-wq0SxULH0xApr0Xjkjqrkg' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'nonce-wq0SxULH0xApr0Xjkjqrkg' 'self' https://apis.google.com https://ssl.gstatic.com https://www.google.com https://www.gstatic.com https://www.google-analytics.com;report-uri /_/IdentityListAccountsHttp/cspreport Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport Cross-Origin-Opener-Policy: same-origin Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Server: ESF X-XSS-Protection: 0 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-06-30 21:10:50 UTC	4	IN	Data Raw: 31 31 0d 0a 5b 22 67 61 69 61 2e 6c 2e 61 2e 72 22 2c 5b 5d 5d 0d 0a Data Ascii: 11["gaia.l.a.r",[]]
2022-06-30 21:10:50 UTC	4	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49740	151.101.112.193	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 21:10:50 UTC	4	OUT	GET /UeUQRKC.png HTTP/1.1 Host: i.imgur.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-06-30 21:10:50 UTC	4	IN	HTTP/1.1 200 OK Connection: close Content-Length: 306493 Last-Modified: Sat, 19 Sep 2020 00:06:54 GMT ETag: "7d07c247e8dfd5bfaf9a7169b5c402bd" x-amz-storage-class: STANDARD_IA Content-Type: image/png cache-control: public, max-age=31536000 Accept-Ranges: bytes Date: Thu, 30 Jun 2022 21:10:50 GMT Age: 2032381 X-Served-By: cache-iad-kjyo7100178-IAD, cache-hhn4031-HHN X-Cache: HIT, HIT X-Cache-Hits: 1, 1 X-Timer: S1656623451.965591,VS0,VE6 Strict-Transport-Security: max-age=300 Access-Control-Allow-Methods: GET, OPTIONS Access-Control-Allow-Origin: * Server: cat factory 1.0 X-Content-Type-Options: nosniff
2022-06-30 21:10:50 UTC	5	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 07 80 00 00 04 38 08 06 00 00 00 e8 d3 c1 43 00 00 00 06 62 4b 47 44 00 ff 00 ff 00 ff a0 bd a7 93 00 04 ac f2 49 44 41 54 78 da ec dd 5b 6f 5d d7 95 27 7a 7e 93 73 e9 ae 8e 6d 39 4f a7 5f ba d2 27 b0 61 95 23 59 96 55 6c 82 20 d4 b2 5a a2 6d 5d 62 49 8e 74 a8 43 1e 1a 24 40 c8 68 41 46 33 92 43 93 32 2f 12 49 18 81 11 18 86 11 04 49 50 81 0d 1b 4e bb 5c fd b1 ce de dc 7b ed 3d d7 5c f3 32 c6 9c 63 5e d7 78 f8 43 e4 5e 73 ae 4d a7 de ea 87 ff 18 33 3f fd 7f 6f ff 7b 68 7e f8 7f ff eb 3f a4 cf dc 3f fc 2f 29 ff f3 ff 99 fd 0f dd 2c 28 32 9b 34 df fd e6 ad 9f fd 58 49 be bf 7d fe 05 6c 7e 12 e2 73 37 46 7e 78 ff dc 8b 9c c8 b9 1b 37 df de 39 fb d2 b7 77 2e 74 f2 c3 dd d9 17 55 9f 73 e6 69 b3 14 3f 7f 05 Data Ascii: PNGIHDR8CbKGDIDATx[o]'z~sm9O_'a#YUl Zm]bltC$@hAF3C2/IIPN\{=\2c^xC^sM3?o{h~??/),(24XI}l~s 7F~x79w.tUsi?

Timestamp	kBytes transferred	Direction	Data
2022-06-30 21:10:50 UTC	6	IN	Data Raw: 00 cc 20 cc 10 cc 6d e0 18 08 fc 57 4a 04 d6 80 30 0a 81 55 28 ac 6d 15 df 78 49 85 b6 ba cf eb 19 05 7d 37 9b 14 d1 02 d6 62 b0 04 b9 4e 08 ac c2 e0 e9 e7 8c c0 7a c8 c5 e0 6f eb ee 9e 47 7b 58 01 b8 68 38 56 64 af 92 f0 18 e8 1e 8f 81 3e d2 24 10 02 6f 24 08 04 7f 45 04 6e 50 16 0b c2 a3 f3 b7 5f c0 00 30 0c 89 a7 59 1a 9c 1d 86 11 d8 75 ff 2f 11 02 3f 85 9f 7b c7 84 c0 0d 00 53 22 f0 f3 71 0c 00 ac 7a f6 b6 21 94 00 1c 04 81 f7 f1 08 bc b0 1f 6f 24 b4 0d 80 df 00 34 85 b5 68 cc 63 a0 39 0c c3 d5 80 30 23 2f 43 70 9f f7 03 d7 06 c1 33 e5 e2 ef ac 01 72 17 92 c0 ef 77 0c bf 3c e2 99 01 38 7c ee e4 16 46 df 9c 21 38 1c 02 5f 3a 49 14 04 4e 8a bc 05 37 81 09 10 d8 b4 53 b8 db 2c be a1 0d 23 30 8f 82 86 61 f0 b2 06 83 97 91 08 2c be a3 fb 39 03 b0 7f 5a 70 Data Ascii: mWJ0U(mxI}7bNzoG{Xh8Vd>oEnP_0Yu/?{S"qz!o$4hc90#/Cp3rw<8|F!8_:IN7S,#0a,9Zp
2022-06-30 21:10:50 UTC	8	IN	Data Raw: 5b ff 48 e8 38 28 9c 1f 02 63 60 38 0e 02 eb 70 57 04 60 f1 b9 0a 7a 6d cf bb e3 9e c7 19 ff dc 00 70 6e 08 fc 75 ce 08 fc c4 31 32 02 3f a1 0b 03 30 10 83 5d 5b c0 3b 34 c1 8c 8f 6e c3 ec 06 1a 7f 5d c7 47 c7 86 60 06 e0 fc c6 40 cb 78 db fc 2d 24 10 6c 02 e0 13 e4 35 e0 af 84 c0 0f 5d 30 37 06 02 63 01 f8 68 1c 92 1d c0 f9 20 b0 a9 29 8c 1d 29 9d 2b 02 ff 26 33 00 fe 75 26 00 fc 8e 07 00 ab 3f 2b 04 81 a3 03 b0 1a 81 bd 00 58 81 c0 7d 00 47 15 00 fb 84 11 97 41 b8 26 10 66 f4 65 08 e6 36 70 cf 00 58 c4 5f 37 cc 8d 83 bf 25 c2 6f 08 00 66 f4 2d 17 7f 4b 83 5f 72 20 f6 c4 5f 1d 08 ff 5d 01 ba 3e 61 fc 2d 13 82 ff 8a 80 e0 7e 35 81 e9 61 b8 0c 04 d6 a1 70 1c 04 96 01 f7 4b c5 59 1d f2 aa ee 5a 11 f8 e3 69 44 fc 2d 0d 81 f3 1e fd 2c e2 ac 8c c0 0c c0 c9 47 Data Ascii: [H8(c`8pW`zmpnu12?0][;4n]G`@x-$l5]07ch))+&3u&?+X}GA&fe6pX_7%of-K_r _]>a-~5apKYZiD-,G
2022-06-30 21:10:50 UTC	9	IN	Data Raw: 31 e6 19 80 c0 9f 73 94 f0 fb 79 aa 16 f0 93 18 63 a0 d7 10 2d 60 13 ea ae a1 21 98 02 7f 65 e0 b5 3d 87 ee 09 d6 c1 af 0b 04 53 82 31 39 02 9b de 75 44 84 c0 d2 bd a0 63 a0 c5 fb 47 7e 08 ac c3 d7 c9 f3 56 56 9d f6 f8 5a 11 d8 f6 99 0a 82 05 68 5e 85 b4 80 5d da c0 47 b7 85 7b b7 9d 13 14 80 5b f7 ae 9f a4 c1 56 fd 1d 3b e8 ba 04 0a c6 d0 a6 71 59 08 fc 36 0e 81 01 0d 5f d5 bb 62 20 f0 bc 23 02 bb c0 6f 07 81 05 08 76 de 03 bc 8f db 21 6c 42 da d9 18 08 fc 5b 8f 31 d0 0c c0 0c c3 0c c2 8c c1 0c c1 0c c1 8c c0 e9 00 b8 5c fc 9d 1f a7 9f f0 cb f8 9b 07 f0 32 f2 f6 05 84 e9 c6 44 57 03 c1 15 8d 7c fe 6b f5 7b 81 17 93 c7 da 04 ae 7c df af 0b 04 e7 0e c0 be 78 9c c7 28 68 cd ae df 8f ef 3a 61 ad 57 18 81 9d da bf 9f 57 d7 02 16 47 41 8f 90 16 d6 02 56 c1 ee Data Ascii: 1syc-`!e=S19uDcG~VVZh^]G{[V;qY6_b #ov!lB[1\2DW|k{|x(h:aWWGAV
2022-06-30 21:10:50 UTC	10	IN	Data Raw: aa 8c c1 29 31 f8 bb 5b e7 4f f9 ec 09 a6 c6 df 7f 39 f9 7b e6 5f 02 a7 b2 b6 af 2d 65 01 f0 a5 4a 47 41 f7 0d 81 a7 31 8e 8a ee 11 02 bb ef fe 2d 07 81 ff d0 57 00 de 49 d5 02 16 c7 2e c7 bc 67 6e 01 97 84 c0 b6 16 f0 f4 99 ee bb d7 1c 11 18 70 1e d8 02 86 ec 1c d6 a1 ac 0c c0 2d f8 3d 18 47 42 e0 e1 67 56 00 c6 22 f0 1e 11 04 fb 02 f0 9e 0b 00 b7 cf 91 20 6d 84 d1 cf 2d 04 de d3 20 f0 51 00 04 56 b5 80 8f d4 ad df 06 70 57 8f f4 10 1c 0f 80 d5 ad df 2e 00 a7 47 60 3b 00 87 45 60 15 e0 36 30 ec 0e c0 1a 04 7e 9e 1a 81 e7 8b 47 60 2d ee 3e b5 c4 02 c0 b3 a9 c6 40 63 00 78 db 33 0c c0 1c c6 e0 ea 31 98 21 98 21 98 11 98 10 80 4b c7 df be 00 f0 4f 91 92 1a 5b 53 46 86 de 2e fc 32 fe 32 08 fb 43 f0 10 70 c5 0c 01 d5 f4 dc 14 19 62 21 51 41 b0 ee 2c e6 bd 20 Data Ascii:)1[O9{_-eJGA1-WI.gnp-=GBgV" m- QVpW.G`;E`60~G`->@cx31!!KO[SF.22Cpb!QA,
2022-06-30 21:10:50 UTC	12	IN	Data Raw: 60 0b f6 fa 42 b0 01 65 9b 7b a8 16 b0 66 34 b4 33 00 9b f0 57 fe ae f1 cf 4a b0 75 18 ff fc 91 f0 ae c9 fb f6 68 30 79 14 13 02 f7 0c 80 8f f0 00 6c 42 60 2b da 42 9f 79 22 70 17 5d 65 00 8e d3 06 be 9e c9 48 68 6a 00 d6 21 f0 e8 d9 c5 69 3e 9d e6 9d e7 0a ac f5 45 60 f0 fb 2a 18 03 fd d4 31 68 04 7e 23 3a 02 9f 00 f0 6f 47 d1 8e 6d a6 02 60 86 64 86 61 c6 e0 de a0 30 43 30 23 70 1f 10 18 0c c0 61 e0 97 12 7f e7 15 e9 07 fe 72 fb 17 02 bc ed cf fe 6d f0 d9 30 ee e3 9d 4d 80 98 0a 85 5f cb 34 61 01 58 95 10 ef 84 60 70 7c 00 86 63 70 79 10 2c 25 11 02 d3 bd cb 0c c0 3e 08 ac 3c d7 67 fc 65 04 76 04 60 a9 09 6c 41 60 06 e0 25 40 60 e7 5d f0 97 5b c0 9e 8d 5f 03 00 7f 8e 6d f9 3e a1 de 01 0c 41 5d 7f 3c de c9 22 18 00 76 83 63 fa 16 b0 a5 01 8c 80 5d e8 59 Data Ascii: `Be{f43WJuh0ylB`+By"p]eHhj!i>E`*1h~#:oGm`da0C0#parm0M_4aX`p|cpy,%><gev`lA`%@`][_m>A]<"vc]Y
2022-06-30 21:10:50 UTC	13	IN	Data Raw: 6b af 9e 6a e7 57 9c 8a c7 43 93 c3 f1 3d 29 c5 b6 81 2f 06 cf 9f 2c b1 01 af 2f 00 8f de 21 c2 ab ea bd 79 e3 6f 5f 11 58 09 c0 0f 6f b4 77 fd 32 fe d2 01 f0 66 5a fc a5 1a 21 ad c3 df ac 47 42 77 30 78 4d 88 84 c0 3b 26 04 6e 90 d4 15 79 cb 00 e0 83 a2 1b c1 76 00 6e 43 30 c5 1e 60 15 02 af b9 21 f0 01 20 c2 b8 66 06 e0 f8 99 c2 ef f2 8b a3 d8 01 18 83 c3 58 50 c6 c0 ed f2 e0 5d c3 a4 02 60 af bd c0 14 63 a0 15 67 d4 3b 7f 75 08 7c 3d ca 18 68 15 02 5f 67 04 c6 a5 01 5d 0c 00 0b 9f c9 3b 81 df ce 12 81 03 ec 01 46 01 b0 65 14 f4 53 0c 02 b7 01 58 85 c0 e2 b9 d7 72 6b 02 e7 dc 4c e6 30 08 d7 00 c1 aa 86 6e 02 10 3e bb 37 00 d2 3d 86 60 6e 03 97 85 c0 1d 00 8e 8f bf 0b 8e f8 fb 96 12 7f b9 f5 db cf 11 cf ff c6 f0 9b 21 fe 32 e4 f6 0d 75 a3 20 f0 24 f5 8d Data Ascii: kjWC=)/,/!yo_Xow2fZ!GBw0xM;&nyvnC0`! fXP]`cg;u|=h_g];FeSXrkL0n>7=`n!2u $
2022-06-30 21:10:50 UTC	14	IN	Data Raw: bf ea ac 08 09 06 c1 57 48 a2 1b 1b 6d db 29 dc c2 5a 4b 6b 58 79 87 01 98 47 41 93 01 f0 52 d5 0d 60 5f 04 76 0d 05 1e 4f de b1 d5 4e 1b 74 a1 2d 60 19 82 a1 00 9c 7f fa 32 06 fa 49 e7 b3 29 ca ee a8 00 18 82 c1 50 00 0e 80 c0 1f 4b 00 7c 82 c0 ad 70 1b 38 cc e8 67 15 00 d7 83 c0 32 04 9b cf d2 00 b0 16 7e 35 08 ac 6c 05 63 51 58 b9 07 58 03 b6 e2 9e 60 2b 18 6b 00 d8 03 82 73 6a 01 5f 8f da 06 be ea 87 c0 32 e8 3a 9c 7d fb f9 00 7c 9f 0b d8 db 3a 33 a7 c4 df b9 3d 43 0b 78 af 8b c0 10 0c 1e 02 af 9c f3 27 ff ce b5 7e cf 01 81 cf e8 10 f8 93 74 08 1c 0d 80 7f 1b 78 dc 74 9f c2 18 cc 18 9c 63 3c 70 98 11 98 47 42 a7 42 e0 99 14 f8 0b 47 df f4 f8 5b fa ae df 9a e0 97 61 b6 f6 11 cf 3d 04 62 c6 60 82 36 f0 dc 09 00 33 02 03 10 d8 92 d4 08 8c c5 61 28 e6 1a Data Ascii: WHm)ZKkXyGAR`_vONt-`2I)PK|p8g2~5lcQXX`+ksj_2:}|:3=Cx'~txtc<pGBBG[a=b`63a(
2022-06-30 21:10:50 UTC	16	IN	Data Raw: 5c 35 00 6f ba b4 82 d5 a9 09 80 75 e0 fb fb 64 00 ac 80 e0 2d 53 64 c4 6d 03 b0 09 7b 77 81 08 0c 01 60 13 ea 52 b4 87 43 8d 81 3e a8 6d 0c 34 b4 e1 eb 3a 26 da 0b 82 f5 67 6d 7b 80 bb fb 7e 4d 08 bc c6 63 a0 49 11 f8 6e 00 04 5e ae 00 80 c3 21 70 70 00 de bb fd 82 12 78 3b 08 ac 7e e6 8a c0 32 fa 0e f3 9e 10 67 04 1e 7c 57 1b 76 0d 58 7c 54 02 02 5f 8d b8 03 18 8e c3 73 aa 96 30 74 0c 34 29 00 e7 8b c0 5e 00 cc 08 cc 38 cc 20 cc e9 31 04 33 02 f3 48 e8 48 00 3c 0b 6e 05 c3 01 38 2e fc 96 8a bf 79 00 30 c3 2f 03 30 3d 1a f7 0e 84 19 82 09 11 b8 c6 e4 8f c0 fa 94 8d c0 5f 49 99 3e 73 07 e0 f2 d0 f8 4e a7 ed 3b c5 60 7d 0b b8 aa 86 f0 26 7e 17 70 df 10 38 fd f8 e7 55 47 08 5e d5 40 b0 bd f1 bb ab 80 60 11 80 a1 f8 ab c3 5c ea f6 70 af 5a c0 3b 1e bb 80 31 Data Ascii: \5oud-Sdm{w`RC>m4:&gm{~McIn^!ppx;~2g|WvX|T_s0t4)^8 13HH<n8.y0/0=_I>sN;`}&~p8UG^@`\pZ;1
2022-06-30 21:10:50 UTC	17	IN	Data Raw: 15 fb 7a 31 e3 9e 65 f8 dd 5c f5 1e f7 9c 3b 02 fb 36 87 75 ef b0 01 f0 81 06 76 4d c0 6b 7b 8e 06 60 19 7c 4d 00 ac b8 af 02 60 14 04 fb e2 6f 40 3c 36 8f 81 36 41 f0 5a 16 7b 7e eb dd 03 bc 9c 04 82 97 0b 82 e0 12 00 f8 ae 23 02 47 03 e0 3d a1 e9 2b 83 6c 0b 81 2f 0b a0 3b 1d 2d dd 42 df ce d8 69 e1 ce 0e 2c 1d e8 3d 30 00 f0 11 7c 27 70 fb ee 42 27 79 ee 09 0e 08 c0 c8 1d c1 22 cc a6 1e 07 6d 42 e0 d7 3f 7d fd 05 63 36 a5 9f 07 61 04 66 14 ae 72 cf 6f c4 bf 9f 21 b8 1e 08 66 04 66 04 26 02 e0 f9 80 f8 0b c9 7c 16 f8 db a7 3d bf 72 be 65 e8 a5 c3 5e 29 3f 5a 40 f8 c7 ca 12 a2 9d ac 3e 4f 87 b7 51 30 f8 56 aa 30 02 33 02 33 02 9b 40 b8 24 00 b6 dd e5 5d c0 86 6c 8e 03 44 e0 df 43 c3 00 ac 68 fe 6a c6 35 bb 02 f0 56 dd 00 1c ba 3d 0c 05 e0 2d 05 18 cb d0 Data Ascii: z1e\;6uvMk{`|M`o@<66AZ{~#G=+l/;-Bi,=0|'pB'y"mB?}c6afro!ff&|=re^)?Z@>OQ0V033@$]lDChj5V=-
2022-06-30 21:10:50 UTC	18	IN	Data Raw: 0f f1 17 07 c0 12 04 6f 99 10 58 81 bb dc 0a 8e 06 c0 b6 e7 c1 20 78 b7 0d c1 ba 9d be 4a fc b5 c4 06 c0 32 fe 96 08 c1 b8 96 6f 3e 00 fc 71 55 00 8c 4d fd 00 5c 1a 02 e3 01 38 31 fa 82 10 f8 b2 1a 81 ad 91 f6 00 63 47 40 bb 22 30 19 16 9b 11 78 41 01 bd 3a 00 0e d1 04 96 11 77 76 67 f6 c5 26 41 10 78 cf d0 04 de 1b e5 fc 5e ba 71 d0 d4 00 6c 1b 11 cd 50 ca 20 cc 71 c7 e2 9a 77 05 17 89 c3 8f 1d 21 b8 60 14 e6 bd c0 1e 00 1c 06 7f e7 85 e4 df fc fd a9 68 fc e5 9d bf 54 4d df 22 80 97 f1 37 18 06 7f ff ee eb 2f 8b f1 81 60 28 24 ff 6d f0 3d 4d 30 58 fb b7 9b b8 f3 b8 f7 e6 00 bc 52 18 81 19 81 49 11 b8 01 db 1e b6 80 85 a6 ef 49 44 04 46 b4 80 4d cf be b2 00 af 78 2f 0d 02 6b 30 d8 15 80 7b 1c 3c 02 37 60 0b 00 60 19 76 33 da 0f 7c 58 29 02 ef 22 11 78 2b Data Ascii: oX xJ2o>qUM\81cG@"0xA:wvg&Ax^qlP qw!`hTM"7/`($m=M0XRIIDFMx/k0{<7``v3|X)"x+

Timestamp	kBytes transferred	Direction	Data
2022-06-30 21:10:50 UTC	20	IN	Data Raw: 0f 81 67 c2 e2 2f 74 e7 2f ae 19 5c ca d8 e7 74 f8 1b a0 f5 bb 18 10 7f 17 cb 85 df 1f 6b 4d 02 c4 2d 1f 7f e1 ad 60 df 94 8c bf 32 04 93 bc 47 81 bc 7f fb c0 86 c3 78 04 fe ae 26 04 8e 0e c0 17 0b c5 df f0 08 fc 55 05 08 fc 45 80 51 d1 94 18 6c be 6b d8 f7 bb 69 0a 03 30 19 02 6f ad 16 d5 e6 65 00 b6 8c 81 36 e1 2b 76 4c 33 05 02 47 06 60 5f fc f5 89 09 75 9b 33 0f 15 e7 64 f8 c5 03 70 77 7c b4 1e 80 d7 aa c6 df 8f 82 ef ff a5 69 0c 2f 17 83 c0 7a 98 9d 22 f1 dd e0 00 ec 3e 12 1a 3b 0e 5a be fb 7e 61 7b 81 1d 10 78 a7 1d 19 6e df 3b 30 80 af 94 f7 30 68 0c 41 da 83 18 08 6c 3f 33 4b 1c d7 bd c0 b3 3b e7 5e 3c c9 93 d1 bf 73 03 c0 9d 0b de 00 ee e6 f5 93 44 00 60 15 02 33 00 73 7a 30 2a 3a 3a 16 ff d6 7f 4f b0 2f 10 a7 83 e0 b7 fe 7d 3b 85 c0 70 e1 28 ac Data Ascii: g/t/\tkM-`2Gx&UEQlki0oe6+vL3G`_u3dpw|i/z">;Z~a{xn;00hAl?3K;^<sD`3sz0*::O/};p(
2022-06-30 21:10:50 UTC	20	IN	Data Raw: b4 3f 58 05 b3 1b 9a cf 43 9f 83 66 88 bf 7a 00 be 0b 00 e0 65 06 60 0b 06 2f 7f ae 02 e0 92 10 f8 7d c7 c4 69 01 93 22 30 12 7b 7d 11 58 39 0e 5a 6a ff ea 10 b8 35 06 fa c0 30 1e 3a 2a 00 87 69 02 bb 45 68 01 3f b1 b4 80 03 02 b0 8c c0 e2 a8 e8 90 00 7c 92 4f 85 26 b0 90 33 83 dd c0 62 94 bb 83 79 7f 30 a7 67 48 ec ba a7 38 45 1b 37 15 0e c3 11 38 5f 18 d6 fe 4d 05 80 b0 09 62 a1 18 1c 02 84 95 6d e0 03 42 00 a6 c3 df f2 00 b8 ac a6 2f 0d fe 66 b1 93 37 43 f8 65 e4 65 00 2e 02 82 6f 4e d3 d7 e6 af 32 1f 98 a3 43 e0 21 fe 36 f9 ce 00 c0 55 20 70 70 00 be 72 92 29 d0 32 02 7f 55 c2 b8 e7 8a 5a c0 ea dc 1b 07 86 c0 cd 79 e5 ee df 41 be 78 74 eb 94 0e 81 75 f7 fa 8d c0 ab bd 47 e0 9a 00 78 0b 0b c0 36 08 c6 ec f4 dd f5 c8 96 df 3b 4a 00 60 1d f6 ba 00 70 83 Data Ascii: ?XCfze`/}i"0{}X9Zj50:*iEh?|O&3by0gH8E78_MbmB/f7Cee.oN2C!6U ppr)2UZyAxtuGx6;J`p
2022-06-30 21:10:50 UTC	22	IN	Data Raw: 25 2c 04 cb c0 eb db 1c 5e 1c fc 0d 62 b2 6e 00 6b 10 78 01 d0 02 be bc 33 dd 17 ac 4c 84 26 f0 6c 4a 04 16 12 14 80 c1 bb 82 d3 03 f0 eb 42 18 85 39 a5 62 f0 1b 8e c9 1e 82 03 ee f0 0d b7 6b 38 15 02 d3 b4 85 9d 11 b8 03 c1 5d 10 fe e7 c8 08 3c 17 0d 84 e9 31 78 c6 7d ef ef 3c 11 00 33 fe d2 e1 ef 39 7a f8 5d 8c dc 10 26 de f1 9b 2f fa fe 22 62 dc fe 46 06 e0 14 10 0c 07 e2 bf 8d 03 c5 e2 de 22 30 78 2f 70 5c 04 fe b3 e5 5d dd 94 b3 0f 38 9b 46 30 03 b0 1f 00 3f 08 97 ac 5b c0 8f 88 10 58 78 1f 04 81 8f 07 e7 9a 7c 59 1d 02 af c2 5b c0 2e a8 ca 2d e0 bc 10 98 02 72 13 43 70 ed 00 bc 19 0c 80 b1 6d 60 58 cb 38 2b dc 3d a4 83 5f 9f 40 00 d8 04 bf 4d 96 26 08 bc 0c 46 e0 06 73 3b a8 0b 38 8b 39 2f 02 af 08 be f2 f9 65 09 7e 31 ad 5e 13 f8 b6 e2 d0 02 96 df Data Ascii: %,^bnkx3L&lJB9bk8]<1x}<39z]&/"bF"0x/p\]8F0?[Xx|Y[.-rCpm`X8+=_@M&Fs;89/e~1^
2022-06-30 21:10:50 UTC	23	IN	Data Raw: 1d 02 5f 4e 81 c0 8a dd c1 7a c4 75 d8 1d 2c 02 70 0b 81 17 d4 08 7c 90 0a 83 cf e1 76 05 43 00 98 18 81 63 ed 09 e6 31 d0 0c c2 39 63 b0 2a 2e a3 98 61 10 9c 08 89 7f db cd 6b 52 fc 11 38 1d 0c d7 88 c0 f4 23 a1 e9 40 d8 b7 ad 1b 1b 84 1b 04 9e 61 fc 65 fc ad 0d 7f bf 23 6f fb fe 22 db 30 00 33 04 e7 09 c1 8c c0 a5 20 b0 0a 80 c3 22 b0 19 78 9d 11 b8 30 f8 cd b6 05 fc 20 7e b2 dd 05 1c 01 83 73 03 e0 d8 08 2c 8f 70 16 f1 f7 f7 15 01 6f 55 2d e0 5d fc 1e 60 b2 66 70 e6 00 5c 62 1b 58 85 af b4 38 4c 3d 3e ba 0c 00 4e 31 12 ba 0d bc 4b e0 c6 ef c9 67 87 4d d4 ef 83 8c 7f 8e 01 c0 aa 96 ef d2 30 87 37 b4 f7 3a ad e0 43 0f bc 3d 74 b8 2f dd b9 11 35 8b c1 42 39 16 da 27 26 04 7e 0f 38 2e 1a 35 36 ba b5 2f 78 0c bc 32 06 ef 20 c7 42 63 77 07 5b a1 d8 ad 09 bc Data Ascii: _Nzu,p|vCc19c*.akR8#@ae#o"03 "x0 ~s,poU-]`fp\bX8L=>N1KgM07:C=t/5B9'&~8.56/x2 Bcw[
2022-06-30 21:10:50 UTC	24	IN	Data Raw: 80 c2 ce 08 9c a4 21 3c fd 3d 34 08 93 01 b0 3b fe ce bd 90 23 00 97 35 f6 39 32 fe 2e 3a 9e 4b d4 fa fd 91 f1 b7 a7 40 cc 10 5c de 6e e0 7e 23 f0 df 52 22 f0 7d 3a 04 c6 c5 0d 80 49 11 38 73 fc e5 16 30 b7 80 8f 2b 49 d3 f4 95 77 fe 8e 9e af 68 03 c5 5f 31 0c c1 89 76 fd ea 80 b7 81 60 79 e7 6f 05 00 5c 5b 0b 58 46 de 38 63 a0 a9 20 78 a9 48 04 5e 3d 0c 0c c0 4a e8 b5 20 30 00 7e 5b 60 ac 89 75 17 2f a4 1d 0c bd e3 da 02 56 7c 97 15 81 5d f1 f7 d0 10 13 00 cb cf 0f cd fb 82 6f 88 e7 64 30 36 01 b2 11 81 d5 80 eb fb 3c ed d8 68 f5 48 68 3f f8 85 00 70 17 81 2f 6d 0d ce 6e cd 2b 1b c4 c3 cc 0f 11 18 db 10 1e 3c 9b df bd f0 d2 30 0d f2 4e 22 c2 ae 0c c0 3b 7a 04 ae 02 80 77 fc 00 38 26 02 bf 92 3a 0c c2 85 82 f0 99 2c 83 1f bb fc 46 15 41 41 70 f2 c6 b0 3d Data Ascii: !<=4;#592.:K@\n~#R"}:I8s0+Iwh_1v`yo\[XF8c xH^=J 0~[`u/V[]od06<hHh?p/mn+<0N";zw8&:,FAAp=
2022-06-30 21:10:50 UTC	26	IN	Data Raw: 08 ac 18 0d dd 3a d3 79 ae 03 60 1d 28 2f c2 5a c3 16 ec bd 41 8e c0 30 bc b5 9d 09 0b c0 dd b3 26 b8 25 45 e2 2d f3 ae e0 49 04 00 3e c1 db dd 71 b6 fc 02 df 03 6c 6e 0b 9f 8b 11 dd ae 5f 22 00 86 20 f0 2b 8e 61 b8 2d 04 83 9f 9e c9 76 4f 2f 43 30 43 30 b7 81 03 80 70 c6 08 3c 93 1e 7f e7 84 84 01 e0 5e 8d 7d be 51 ee be df 1f b9 f1 cb 61 0c 8e 33 06 3a f2 48 e8 ef 73 1a fb 9c 00 81 b3 1d 05 7d 3f 3f 00 fe 33 01 00 9f 7c 6e 01 5e 1d 02 b7 9f 5d 3b 95 22 4e 00 2c a7 12 00 fe 22 17 00 e6 06 b0 a5 01 8c c8 63 33 02 63 83 69 0e 8b cf 6d 7b 87 8b 05 e0 dd f4 00 5c 6b 0b b8 36 00 86 ee 08 de 0c 89 bf 87 54 7b 84 91 68 9b 60 0c b4 0c b5 aa 06 31 0a 81 49 47 46 2b 76 07 0b 00 2c 8e 77 c6 be cb 88 b2 21 9a bf 3e a3 a3 27 7b 81 6f b8 01 f0 21 a2 05 0c 6d 04 ef 1a Data Ascii: :y`(/ZA0&%E-I>qln_" +a-vO/C0C0p<^}Qa3:Hs}??3|n^];"N,"c3cim{\k6T{h`1IGF+v,w!>'{o!m
2022-06-30 21:10:50 UTC	27	IN	Data Raw: 82 10 78 37 22 fe 1a 00 b8 2f fb 7f 7b 0b c0 87 1e e8 ab fb 1d 3d fe 59 7c 07 62 0c b4 0b 02 43 50 17 70 47 db ea cd 16 7f 65 e0 35 7d 66 07 e0 d5 d8 00 6c 18 fb 0c df 07 8c 19 0f 0d 6c 02 5b 77 07 3b 02 b0 06 7d c5 e7 ad 77 e8 46 40 ab da c2 3a 08 36 00 f0 0d 1d e6 62 00 d8 34 12 da ba 37 58 0f bb 8b 49 10 d8 8c b6 41 41 d8 15 80 77 01 00 bc 1b 06 80 a3 34 82 45 f0 35 ec 09 3e 6d 43 60 02 00 36 21 70 29 61 04 f6 df 19 ac cc a6 1c 08 06 43 c2 30 5c 25 02 67 00 c3 bd 42 e0 c0 20 5c 11 00 e3 30 f8 27 43 4a 05 e0 20 f8 bb 48 33 06 ba 8f f8 5b 02 00 ff 6b c1 89 f5 bf 01 6c 0f f0 2b 15 27 e7 91 d0 e7 f2 4e c2 7d c0 41 a1 37 1b 04 ae 03 80 a1 48 ac 6b 0e 07 05 60 f0 be 5f d3 1e e0 be 8d 81 8e 07 c0 22 92 e6 09 c0 12 e8 3e 76 bc 67 1b fb 5c 38 00 87 18 47 0d c1 Data Ascii: x7"/{=Y|bCPpGe5}fll[w;}wF@:6b47XIAAw4E5>mC`6!p)aC0\%gB \0'CJ H3[kl+'N}A7Hk`_">vg\8G
2022-06-30 21:10:50 UTC	29	IN	Data Raw: 04 be 71 08 db e9 7b 87 72 0c 34 02 80 55 20 dc 1a 13 6d 02 e1 43 1f 00 86 20 f0 f4 cc 95 ed 8b a7 94 08 7c 38 4e 40 04 b6 c1 ec 25 e1 df b0 88 7c a1 08 04 be 90 02 80 35 08 7c 1a 9a 27 98 11 d2 8c c1 23 10 0e dd 90 ad 10 82 a1 bb 82 9f 06 0c 43 70 5e 28 ec da e2 25 7c 3f 23 70 3a 04 9e a1 dd fd 3b d7 4b fc 85 a0 6f 17 80 fb 8e bf fd de ef 1b 63 ef 6d 29 c8 8b 89 2f 08 7f 33 78 c7 30 22 fe b6 21 f8 1f 9d 1a be 32 00 8b e7 75 cf 6c 68 0c 3d 87 f9 5b 47 cf 4e ff 3c 34 02 9b 9b c0 e7 0a db ff 1b 1e 81 b3 c1 5f 6e 01 27 45 60 d3 73 19 80 45 04 56 3e 33 22 70 5e bb 7f bf b0 20 30 ac 05 ac 1b f1 ec d0 00 ee cd 18 68 da b1 cd 9d 33 04 00 7c cc 00 8c 42 e0 16 fa 6e 5b c6 40 6b f7 fa ae 0f ce ac 2b 00 58 1f f1 fe 09 f0 3e 9e 02 af fc fe c7 42 e8 00 78 83 01 38 57 Data Ascii: q{r4U mC |8N@%|5|'#Cp^(%|?#p:;Kocm)/3x0"!2ulh=[GN<4_n'E`sEV>3"p^ 0h3|Bn[@k+X>Bx8W
2022-06-30 21:10:50 UTC	30	IN	Data Raw: 37 67 00 66 fc cd 1f 7f 19 7c 19 7f 7d 31 b8 81 5f 39 b9 42 b0 5f dc 10 78 f2 f9 f5 76 7c 10 f8 2f d7 df f8 79 b6 3b 80 b9 05 dc 33 00 7e 37 bb e0 10 f8 a6 02 82 6f 65 09 c0 5f 39 01 b0 6e df 2f 12 83 65 74 ad 76 0c 74 80 3c 46 ec fc d5 41 30 03 70 bc 16 f0 f6 0a ba cd ab 6c 04 23 00 f8 b1 05 80 5d 60 76 04 be eb a7 a0 00 ac fb 0e 5b 74 ed e4 4d cb 77 b8 42 ec a3 08 78 2c 7f c7 43 0c 00 1f 12 ee ef b5 bd 07 fb 3d 87 b8 58 47 3c ef da 47 41 cb 68 0b 6f 02 af 1a df 63 42 60 08 00 af 03 ef 50 01 b1 0d 7d cd df 33 c5 5f d5 f9 1c e0 57 06 5f 78 0b 58 87 ba 18 00 c6 21 b0 ee ec 35 68 b6 11 67 b5 a1 41 60 d3 73 08 1a ab 03 03 60 11 81 87 f0 ab da 0f 7c 32 22 9a 18 81 2f 0a df 3b 8d 3b 00 bb 83 30 be e1 0b 46 e0 40 a3 a0 6d a8 7b 81 04 81 89 01 d8 69 07 30 03 30 Data Ascii: 7gf\}1_9B_xv|/y;3~7oe_9n/etvt<FA0pl#]`v[tMwBx,C=XG<GAhocB`P}3_W_xX!5hgA`s`|2"/;;0F@m{i00
2022-06-30 21:10:50 UTC	31	IN	Data Raw: 48 00 dc af f6 6f ad f8 fb 23 e3 6f 60 f4 fd 8f 41 e3 07 bd 0c c0 93 58 ce 95 d7 06 ce 1f 81 bf 11 a2 7a 6e 42 5c db 73 18 02 cf 26 49 df 77 01 8b 80 eb 8d c0 b5 8f 82 0e d0 02 d6 dd 83 e0 2f e4 9e 2d d3 7b 22 00 13 a6 97 00 bc a2 c0 60 62 00 c6 60 30 03 b0 06 80 d7 f1 10 dc e0 6b 07 82 d7 35 08 bc 1e 08 80 d5 0d 5f 35 00 af 3b 8f 7a ce 01 80 4d 6d e0 47 83 bf 67 14 35 ba 42 f1 d7 84 b6 90 73 ae ad e2 0e fe 36 31 21 b0 01 7c c5 77 98 f0 f7 24 86 33 66 f4 5d 9a bc 47 84 55 15 56 37 18 8b 47 5f 57 10 be 67 41 5f 7c 13 58 07 a7 eb 8e 2d e0 1c c0 77 fa ef 2d 09 80 f3 6a 04 63 50 f7 5e 70 2c a6 69 01 5f b3 9c c9 ad 05 ec 8e c6 17 9d 62 c2 5e ed 59 1b 00 ef db 50 78 8c c0 fb a3 7f e7 a4 cc 07 6d fe ba 21 b0 aa 09 7c c1 35 20 00 b6 37 82 e3 02 30 60 54 f4 60 5f Data Ascii: Ho#o`AXznB\s&Iw/-{"`b`0k5_5;zMmGg5Bs61!|w$3f]GUV7G_WgA_|X-w-jcP^p,i_b^YPxm!|5 70`T`_

Timestamp	kBytes transferred	Direction	Data
2022-06-30 21:10:50 UTC	33	IN	Data Raw: 07 02 8b c0 1b 6c 0c 74 01 11 c7 40 7f c1 63 a0 e3 ed fa 35 ed f4 65 00 8e 0e c0 2a 08 de c6 22 f0 76 5c 00 36 21 70 5e 00 bc 12 08 80 b1 08 ec da 1c f6 03 e0 66 2f b0 78 06 04 c0 8a 3d c0 98 3b a6 77 41 5a c1 98 51 cf e1 46 44 43 76 fa fa 02 b2 1d 96 57 1c 20 b8 ae 06 f0 3d 00 00 eb ce d0 ef 02 86 00 f1 3d 25 e8 c6 87 df 70 7b 80 e9 db be 2a c4 0d 8b c4 88 96 ef 3e 12 76 3d 5b c0 56 00 de a7 45 60 fb 0e e1 f3 a7 74 39 6f 79 86 01 e0 36 02 9f 45 e5 ac 26 b1 01 18 8d be a8 7d c0 1c c6 e0 ca f6 03 fb 02 31 43 70 5a 04 a6 18 1d cd 08 6c df f3 9b 1b 00 cb f0 5b 4b fb 17 36 fa 99 66 27 70 0b 7e b3 c2 5f 7f 1c 66 f8 ad 01 7f 7b d6 26 2e 16 81 4f f7 1a 81 5d 01 f8 2f d7 2f fc 5c 07 b4 7f b9 ad 7f c6 bb 80 13 03 f0 7d 8a a6 ef e5 6c 76 fd b6 9e 6f d8 12 6e 0c 74 Data Ascii: lt@c5e*"\6!p^f/x=;wAZQFDCvW ==%p{*>v=[VE`t9oy6E&}1CpZl[K6f'p~_f{&.O]//\}lvont
2022-06-30 21:10:50 UTC	34	IN	Data Raw: cb f8 5b 39 06 f7 1d 81 c9 f3 46 92 51 d0 3a 00 3e c9 6d 7d 42 8e 86 66 04 f6 40 e1 8c 9b be c9 c7 40 9b 40 b8 d0 31 d0 1d 00 96 30 58 87 ac f2 59 06 60 de 01 8c 03 60 0c 04 eb ce 1b 00 f8 b1 69 74 f3 3a 31 02 d3 8e 78 36 35 84 e3 00 b0 0d 77 71 68 fc c8 b2 6f 18 0e b8 11 00 78 bf 9b 07 16 04 d6 8d 7f 56 de af b0 19 bc 9e 65 e0 f8 2b 43 b0 15 88 8f 0b dd 13 3c c1 5f 53 c3 f7 1e fd 3e e0 63 45 1c 5a c0 e1 00 f8 56 46 00 7c cd 00 be d7 d0 00 7c 05 08 c4 f4 2d 60 d5 19 f5 3d 19 7c b5 0d e1 6d 1f 00 b6 8c 83 06 8c 8c 9e 8b b4 07 d8 86 c0 34 00 6c 46 60 15 e8 5e d0 e1 ae 0b 00 ef 9e 8d 37 ea 99 51 98 21 98 03 42 e1 b7 a4 e4 00 c3 43 04 9e 1d 20 aa 9c d4 a8 3b 5b 21 04 eb 40 38 04 02 8b c9 11 82 67 fa de fe f5 c7 5f 48 f3 d7 ad 0d dc 6a fd 5e 4b 35 f6 f9 17 24 Data Ascii: [9FQ:>m}Bf@@@10XY``it:1x65wqhoxVe+C<_S>cEZVF||-`=|m4lF`^7Q!BC ;[!@8g_Hj^K5$
2022-06-30 21:10:50 UTC	35	IN	Data Raw: fb 36 00 5e af a6 01 9c e7 18 68 15 e6 ae 68 10 d8 de 0c 76 de f7 7b ec 00 c0 c7 9a 50 01 f0 b1 9c 36 02 4f 5b bb 10 04 36 b5 7c a5 ef 91 11 d8 30 3a da a5 e9 2b fe 77 80 11 d8 13 80 6f 39 00 f0 2d 6f e8 c5 c2 af fd 7c 03 b3 71 81 f8 22 1a 80 e9 41 78 4e bf 13 58 d7 04 de d7 e0 6f 84 7d c0 18 0c 3e ef 15 00 fe 3e 9e 46 06 5e d3 b3 56 b6 15 28 9c 5d 03 f8 ff f6 48 a6 20 1c 2a 0c c1 0c c1 50 04 26 82 61 cc f7 86 c2 59 4a 04 36 7d 6f 08 04 3e c9 ef 46 a1 46 e0 9c 40 b8 20 00 66 fc cd 77 f4 b3 1f fe a6 1c f7 8c c7 5f 6e ff 32 04 a7 c0 5f 37 04 fe a1 f7 fb 80 d5 40 5c c3 28 68 57 38 66 00 86 03 b0 08 c1 a3 31 d0 75 00 f0 08 81 1b 00 96 f3 6e a5 00 fc 01 78 0c f4 e7 b6 04 04 60 e8 e8 68 dd b9 06 7f 9f 69 ee 1d c7 82 e0 47 e9 c6 40 ab 20 b8 ac b6 2f 1d 02 f7 09 Data Ascii: 6^hhv{P6O[6|0:+wo9-o|q"AxNXo}>>F^V(]H *P&aYJ6}o>FF@ fw_n2_7@\(hW8f1unx`hiG@ /
2022-06-30 21:10:50 UTC	36	IN	Data Raw: de 77 43 60 08 00 fb ed 09 36 01 30 70 4f b0 02 80 cf cb 00 0c 42 e0 d7 7a 88 c0 61 76 09 9f 64 13 1f 86 e0 bc 20 f8 fc 38 25 8d 85 26 c3 e1 4f 68 53 23 02 43 50 78 0e 1b 44 3b 38 54 93 97 ea 9d 0d 02 9b 30 78 86 16 7f 67 8d f8 db 06 60 6e ff 96 be f7 b7 ef f8 cb a8 ca 10 4c 03 c0 15 ed 03 ee 3b 02 17 0a c0 72 7a 81 c0 85 8d 7e b6 ed 02 fe 7a e3 dd 4a 01 b8 41 5e f8 1e e0 50 3b 7f 63 03 b0 0e 81 c5 67 41 00 58 6e f0 f6 0e 80 a1 10 ac 3b 0f 6d f4 e2 11 98 01 38 74 32 03 60 2b 04 cb fb 7d 4d b8 6b c0 63 00 1a cb d8 da 6e 08 b7 11 18 d2 20 a6 03 e0 f5 24 10 8c 01 e0 07 59 e3 b0 04 c2 c7 c3 8c 90 57 3c 37 85 5f 31 c0 11 d0 10 ec a5 00 60 c5 bb 1a e0 55 36 80 8f 55 f8 db a4 0d c0 6d 04 be 25 9d 6d df 43 23 b0 a2 2d dc 7c a7 ea ef b8 29 7d 7e 53 91 2e 00 df d2 Data Ascii: wC`60pOBzavd 8%&OhS#CPxD;8T0xg`nL;rz~zJA^P;cgAXn;m8t2`+}Mkcn $YW<7_1`U6Um%mC#-|)}~S.
2022-06-30 21:10:50 UTC	38	IN	Data Raw: 04 56 01 b0 3d 58 fc ed 17 00 47 08 05 04 6f 4b 08 bc 5d 1e 00 6f 33 00 bb 01 f0 3e 16 7e 57 3c e0 17 3b 5e 5a 8d c0 ba d6 f0 03 c3 df e6 0e b8 3a 00 5e 8f 0e c0 32 f6 46 1f 01 8d 41 60 1d fe 76 46 42 4b 7b 80 85 71 d0 f2 28 e9 06 71 27 20 3b 46 55 30 00 4b 08 dc 01 de 67 76 04 b6 bd bf d5 e8 1d 07 0d c0 27 90 6b 41 60 d5 18 67 a1 d9 eb 8a bf 0d f2 9a 1a c3 22 00 df 54 81 b1 8c c0 13 dc 15 5a c4 27 b0 0c 40 60 0d 0a bf 2b 23 b0 fc d9 b3 76 ae 01 da c2 4a 54 9e bc 83 08 80 9f 99 00 38 dc 3e e0 50 00 3c 8d e9 19 1c 80 d1 23 9e 03 81 6f 18 04 76 07 60 23 02 3f d6 07 33 ee 99 11 b8 67 18 9c 01 1a fb 42 70 88 11 cd e7 13 25 35 02 83 db c2 d9 20 f0 6c bf 10 58 01 c2 18 b0 9d 27 08 14 81 67 42 c1 6f 0a fc e5 f6 2f 35 fe b6 9f f5 09 7f b3 05 60 47 78 fd 29 60 ca Data Ascii: V=XGoK]o3>~W<;^Z:^2FA`vFBK{q(q' ;FU0Kgv'kA`g"TZ'@`+#vJT8>P<#ov`#?3gBp%5 lX'gBo/5`Gx)`
2022-06-30 21:10:50 UTC	39	IN	Data Raw: b6 ee ad 92 7b 76 7f 7b f1 7e 3f a1 33 05 63 71 0a 9a 06 c0 9f 02 ef 43 00 ec 88 c0 8a 09 e9 4f 19 10 98 d4 02 06 81 98 21 94 99 68 9b 40 00 7c 86 20 f0 71 19 08 ec 06 c0 e6 50 bc 28 fd d9 09 81 5f 48 13 d1 06 08 7c 47 83 c0 21 01 d8 08 81 a1 34 f8 3b fb 59 17 80 7d a7 82 70 c5 60 1b 28 ae 10 9c 09 04 27 73 17 d8 14 83 d5 28 ec 1f 81 f9 40 d8 1c 81 97 bd 41 70 84 06 b0 1f 00 ce a1 fd db 69 fe 26 0e c0 b1 e0 37 04 fe e6 04 bf b6 c8 fb 37 cb fc 97 36 61 da c1 3f 2c bd 7e bd b8 06 70 45 e0 24 5a c0 76 2d e1 05 29 a9 b4 80 19 10 78 33 04 02 cf 21 57 f5 cc 1b 00 ef a8 52 01 38 a5 5b bf b6 00 fc 87 ec 6e 00 6f 29 ee fd 46 00 60 07 f8 a5 02 30 e7 f7 b9 01 30 04 c1 bb 71 67 a1 89 ef bd 28 24 07 05 36 80 f7 4d 00 f8 4b e0 36 70 4f 00 58 c6 da 7d af 00 cc 88 be bf Data Ascii: {v{~?3cqCO!h@| qP(_H|G!4;Y}p`('s(@Api&776a?,~pE$Zv-)x3!WR8[no)F`00qg($6MK6pOX}
2022-06-30 21:10:50 UTC	40	IN	Data Raw: 0c e1 ef 24 20 20 ff 4e 83 cc 53 fc 1d 00 90 3a 90 d2 3c c7 26 a0 29 ed 61 2f 31 fc 3d 39 20 af 29 00 9b 01 f1 a7 3c 37 81 1d 10 f8 53 cd ad e0 4f bd cd 44 3f f4 37 11 7d 4c 99 8d 96 01 17 79 e6 02 c0 36 39 d3 21 70 fe 00 2c 22 b0 19 14 bf af 81 e1 45 3a 00 13 6e 06 5f 4d 47 07 44 60 37 00 8e 8f c0 97 79 4b 48 c5 e0 82 21 38 32 14 57 08 4e 60 0e 5a 78 be f8 e5 18 5a 9b 64 02 c2 ee 2d dd a5 00 09 81 c0 38 08 bf c2 89 bf df 7b 9e 7e ce 17 80 6f 27 07 c0 29 b5 7f 7d e3 af b7 b9 67 1d fe 2e 9b e3 ef df 14 73 ca 9c e8 fb d3 d2 ab d7 b9 42 99 72 36 ce aa 3a 61 20 b8 8b b6 3f ac be 71 5d 8c 0a 78 75 cf ed 10 f8 66 be 08 5c 5b c0 15 80 23 00 b0 f8 ac b6 80 53 84 5f 73 0c 56 01 f0 1f b2 c2 5f 3e 0c 4e 19 80 fd a5 c1 5b 18 80 75 b8 eb 13 80 af be ef 05 82 c0 2f 1c Data Ascii: $ NS:<&)a/1=9)<7SOD?7}Ly69!p,"E:n_MGD`7yKH!82WN`ZxZd-8{~o')}g.sBr6:a ?q]xuf\[#S_sV_>N[u/
2022-06-30 21:10:50 UTC	42	IN	Data Raw: 50 d6 5b 03 f8 39 00 c1 cf d3 4e 29 00 7c 85 bf d3 a0 f8 8b 00 f0 e1 f8 33 b9 03 6f 96 13 d0 10 f2 5a ce 42 db 00 b0 08 a4 25 a4 41 de 67 48 6c 00 b8 41 60 33 fc 95 1a c0 20 04 6f e1 21 34 7d b1 f7 44 98 ed 3c e3 84 df 08 2d 61 15 00 43 13 d2 79 23 f0 a7 49 cc 41 f3 03 b0 f8 0e ef cd 5f 13 20 d6 02 b0 12 76 2d 9a c2 32 02 b3 02 f0 87 5d d0 9d 25 95 69 68 19 81 f5 f0 cb 8b c0 0e 00 8c b4 86 ef a0 08 ec 1f 80 6f ab de e9 00 b0 04 c3 07 b7 8b 00 e0 da 0e ce 18 82 7f 13 2f 7d 83 e0 f0 18 2c 23 b0 1c 0b 04 96 43 82 e0 45 83 70 22 70 5c 10 06 01 18 05 e1 bb 7c 00 6c 03 bf 76 f8 0b 3d eb fe cc 27 fe 06 07 e0 7f b9 5d f1 b7 d7 f8 1b 1e 7e 8b 6a ff 26 03 c1 e1 11 78 fe 3c 16 02 e7 d1 02 fe 8b 06 81 dd d1 57 4c ba cd df 3e b7 80 31 00 16 d1 f7 eb ed f1 cf b6 c5 9f Data Ascii: P[9N)|3oZB%AgHlA`3 o!4}D<-aCy#IA_ v-2]%iho/},#CEp"p|lv=']~j&x<WL>1
2022-06-30 21:10:50 UTC	43	IN	Data Raw: 11 9a c7 87 cf 71 74 a5 e2 af 0d dc ba 7c 1f f5 77 26 07 c0 54 a8 f5 00 bf 2a 00 16 21 b8 f9 b3 2d e0 aa c0 95 32 0d ad fa ac cb ac 33 86 bf 1d 04 3e 36 69 e9 ee 74 e7 97 cf 76 d4 0d 60 e8 f7 9c a9 e2 d0 04 56 7c 97 0c c0 83 de c2 6f be 08 ec fa 3c 1f 00 7e 18 2d e6 ed df 87 71 01 f8 98 0b 80 29 d3 d1 b6 6d 60 4e e4 5d 29 17 80 45 04 b6 00 e0 3b 21 01 d8 65 0a 3a a3 54 e8 ad 40 5c 11 58 97 80 08 8c a0 b0 cd ed de 30 08 dc fe 77 a4 86 c0 4b 87 93 70 61 70 02 00 bc 98 0d fe 1a a3 af 7c fb 37 39 00 7e 33 38 00 ff 67 c5 df 0a bf a1 20 b8 e7 08 dc c4 04 80 2f 9f e7 81 c0 11 00 58 bc 05 fc 38 3d 00 96 71 b7 02 30 0f 00 db 46 87 c6 d6 19 54 00 4e 13 81 b7 82 44 d5 02 2e f5 f6 ef b1 22 c9 03 f0 73 3b 00 be cc a1 10 17 00 36 41 60 d7 ef a2 be 97 2d 00 7f 69 77 df Data Ascii: qt|w&T*!-23>6itv`V|o<~-q)m`N])E;!e:T@\X0wKpap|79~38g /X8=q0FTND."s;6A`-iw
2022-06-30 21:10:50 UTC	45	IN	Data Raw: 5f 1d 02 7f 28 fc b7 fd 99 7b c3 e5 6b 57 39 6a 07 6a fb 6a 1b c0 67 e9 21 f0 62 88 16 b0 8c c0 d8 6d e0 43 c5 cd 60 55 23 f8 98 af 05 4c 43 e0 da 04 ae 18 9c 01 04 5b de ed 2d 17 81 6d 60 b8 22 70 45 60 0d 02 23 18 1c 1d 80 43 b7 7f 7f 40 d0 57 d7 0e f6 06 c0 44 1c e6 03 60 0c 6a fd e0 b0 7b fb f7 7f 86 99 7e f6 32 fb fc 3f 2b fc 86 86 e0 55 bb 24 d3 fa d5 22 b0 1f 00 d6 21 30 fc 2c fd 19 68 2f 00 bc be 90 6c e2 03 f0 bd 0a c0 3e 01 b8 01 5d 0d 00 8b e9 db 0d e0 06 7f 2b 00 57 00 8e da f4 b5 c5 5f e9 3b 52 07 60 5b 34 a6 00 b0 0a 7f 29 00 0c be 27 42 2e f6 7d 5f ea db c2 31 83 c1 29 17 10 b3 e3 ef 19 e3 3d 60 ac 0d cc de e8 e5 02 60 f3 cf 50 00 38 c7 bb c0 e6 0d e2 cf 8a 83 60 77 00 fe 4c 09 bf 18 02 ab 9e eb e0 d7 04 80 db 9f a1 03 b0 0e 86 55 00 fc d8 Data Ascii: _({kW9jjjg!bmC`U#LC[-m`"pE`#C@WD`j{~2?+U$"!0,h/l>]+W_;R`[4)'B.}_1)=``P8`wLU

Timestamp	kBytes transferred	Direction	Data
2022-06-30 21:10:50 UTC	46	IN	Data Raw: 0f c3 6a 74 4d 0f 85 6b 0b 98 0f 83 af 10 b8 49 05 e0 2e fa 7a c3 df 8f c3 e0 2f 7d e2 d9 6f f3 d7 b4 fd 0b a3 6f 59 f8 5b 51 b6 54 04 7e 23 4c 12 6d 01 87 45 60 de 99 e7 bc ef 00 2f 4b 21 00 f0 e6 24 1d b0 ad 00 5c 01 b8 34 00 6e 6e 00 57 00 8e 8c c0 22 d6 da 7c 4e 0f c0 c9 41 f0 61 d8 94 08 c0 cf 89 38 8c 4e 36 53 e1 37 61 08 d6 cd 3c 3f cf 69 02 1a 6b 01 9f 59 02 b0 06 85 21 40 6d 01 71 56 f0 4b b9 13 5c de 4d 60 15 02 ef 28 d1 d7 1d 80 31 d0 85 10 58 f5 ae 0c c0 32 d4 aa ee 04 e3 40 eb 1f 80 d7 89 00 dc 7d fe c0 b2 0d 6c 33 17 4d 4f ac 39 68 37 00 be e7 15 80 af 5a c2 ba 19 68 6d 13 18 c7 dd 49 96 af a9 9e 67 d3 04 6e 00 f8 30 3d 00 be 05 20 af ee 79 d6 20 5c 21 b8 22 70 02 30 4c 47 da b4 50 d8 0c 61 e3 a3 70 45 60 3e 0c 6e 21 f0 6f 93 02 e0 70 10 fc Data Ascii: jtMkI.z/}ooY[QT~#LmE`/K!$\4nnW"|NAa8N6S7a<?ikY!@mqVK\M`(1X2@}l3MO9h7ZhmIgn0= y \!"p0LGPa pE`>n!op
2022-06-30 21:10:50 UTC	47	IN	Data Raw: 22 30 73 43 38 24 00 5b b7 83 2b fe f6 0e 82 b3 6b fd fe 06 ce 15 b4 da 20 30 14 2f 28 6c 07 ce 3e e7 9d 97 b9 11 f8 45 1a 18 9c 3a 02 5b 03 30 75 12 5a 0d bf 3d 04 60 e8 99 01 00 f3 e3 ef 9b d2 5d e0 14 d6 bf bf 48 1a 7f ff d6 0b f0 cd 0c 84 19 01 f8 a7 14 e0 37 f9 19 68 3f 00 3c cf bb 57 91 51 b7 f9 b9 2e 56 77 80 d7 53 42 60 3e 00 fe 4b 71 4d df 39 00 cb 49 1f 80 1b dc 35 98 82 96 50 d7 04 80 bf 0e 0a c0 93 7c b5 bb 3e fd 4c 38 00 fe 7d 05 e0 04 db bf 6e 13 cf 7d 06 e0 c3 82 01 98 04 c4 c7 36 00 3c c0 1b c1 99 dd f3 b5 41 63 08 7d 9f db 36 81 43 01 b0 e9 0d 60 0b fc 8d 07 c2 5b 81 00 78 c7 19 7f 07 89 82 af 2a 9b 46 20 1c 2e f2 6c 73 eb f9 48 3d 13 bd 49 85 5f 2a e8 46 01 e0 c7 86 d8 eb af 4d ec d6 ee 7d 90 30 fc 0a 39 32 68 01 5b a4 d5 06 56 01 f0 90 Data Ascii: "0sC8$[+k 0/(l>E:[0uZ=`]H7h?<WQ.VwSB`>KqM9l5P|>L8}n}6<Ac}6C`[x*F .lsH=I_*FM}092h[V
2022-06-30 21:10:50 UTC	49	IN	Data Raw: 81 27 69 b7 78 6f b1 df e6 ed 3b 02 93 40 d8 72 c6 59 89 c1 0c 6d e0 5f 4a c9 06 80 ff e6 15 80 79 26 a3 7f 0a 0a c0 b7 dd 00 18 6b ff 7e 9c 3e 00 63 cf 4a c5 df 34 00 38 35 f4 4d 01 81 79 f0 f7 87 14 11 78 8d 1f 81 fb 02 c0 df 4a f0 2b 03 f0 e5 9f 2b 00 97 75 03 b8 05 c0 db 29 00 30 4f 42 b4 7c 63 01 b0 cd 67 7e cf 8e c0 5b 59 01 f0 99 0d 00 8b e0 ea 05 80 6d 53 01 b8 ec 3b bf 03 21 ed 39 67 1c 80 07 e6 08 7c 68 8b b0 ae 58 3c 30 84 5b 13 f4 a5 7f df b3 14 e7 9f 13 80 5f 08 80 4b 84 e1 1d a4 19 ac 02 e0 1d 04 80 27 e0 ba 3d 8d 1d 00 2b 1b bd 23 0b 04 1e 75 c1 b7 0b c4 a6 33 ce 9b 48 3c 01 30 86 cb 23 c5 0d e0 11 d6 fa 8d 07 c0 eb 12 00 43 33 d3 66 00 fc 18 99 86 4e 01 7e fd 23 30 0c bc 26 00 cc 0c c4 47 48 c4 b9 e7 16 ec 62 73 d0 3c 00 bc 1c 01 80 f5 79 Data Ascii: 'ixo;@rYm_Jy&k~>cJ485MyxJ++u)0OB|cg~[YmS;!9g|hX<0[_K'=+#u3H<0#C3fN~#0&GHbs<y
2022-06-30 21:10:50 UTC	50	IN	Data Raw: ad 03 4f e1 06 e0 01 1e a4 e5 3b 03 60 ea 9c 73 26 e8 fb ac 80 d9 67 2a 00 63 4d 5e 3d 00 6b 9a bb dc 4d 60 47 04 c6 f0 17 07 e0 cd f9 2c b4 38 ff 6c 32 f3 3c d2 dc f6 05 fe be ae 69 00 6f 5a 01 f0 7a bb dd 7b f5 1e 61 d2 79 64 91 a1 29 fa 22 2d df 4b b8 1d 3d 76 6f 04 13 00 d8 1c 88 ef 05 9f 81 a6 b6 80 d5 53 d0 cb de d2 60 ec bd 69 2a 00 e3 08 ec 0c c0 14 04 0e 72 13 f8 4d 65 54 28 fb 7e c5 e0 a8 68 5c 2a 04 2f 7c f1 4f ad d8 21 ac 1f 04 e6 80 61 23 04 1e da cf 38 73 21 b0 2b d4 2e 5b c4 07 02 a3 20 ec 19 83 6d 11 d8 14 83 7b 03 c0 61 e1 d7 f6 36 30 0e c0 ff d9 3b 00 4e 0f 7f 7f a8 f8 9b 11 02 57 00 ae 00 4c 47 60 25 10 3f b9 7b 95 0a c0 f7 92 8e 72 02 5a 4c c1 00 fc 55 10 00 e6 6d 05 53 d1 98 0a c0 33 08 36 00 e0 39 04 6f 55 00 56 4e 3d a7 37 f1 cc 3a Data Ascii: O;`s&g*cM^=kM`G,8l2<ioZz{ayd)"-K=voS`i*rMeT(~h\*/|O!a#8s!+.[ m{a60;NWLG`%?{rZLUmS369oUVN=7:
2022-06-30 21:10:51 UTC	51	IN	Data Raw: e0 d0 99 81 2d 13 02 cf 30 f8 85 5b 7c 22 f0 2b 9c f8 5b 01 d8 1e 80 af a0 17 9b 7f 7e 08 a0 2f 1b fe be 59 2e fe f6 05 80 23 e0 af 7b 23 38 d4 ff dd dc 67 a0 93 02 e0 35 55 6e c4 6f 01 3f 0a 11 3f 00 fc 0d 13 00 ab de d7 a1 71 9a 00 7c 2f 8b f4 02 80 05 08 8e 0b c0 eb 59 03 f0 68 6f f3 da 24 66 00 dc 7c 2e 2b 00 26 b7 7e 2b 00 a7 0a c1 e1 a0 97 03 7e e5 cf 4b 3f 53 01 30 e5 99 08 bc ce 00 ec 3a bb bc 13 09 7d e9 98 ab 7d 6f 9a 6e bb 77 00 83 2d 04 b7 5a 04 96 be eb 8c da 18 4e 13 80 9f 79 04 60 d5 a4 33 17 fe ee 8a 60 db e0 ef 15 00 6f 23 00 ac 6a 0e cb 08 4c c0 5d 1d e0 8e 88 08 6c 71 03 18 6c 00 b7 d0 75 53 02 e0 4d fd 9c f3 c8 a2 01 ac 00 e0 75 0d 00 a3 77 84 b9 e0 97 02 c0 c4 ef c6 71 97 08 c0 23 04 80 55 08 3c b2 6b 00 9b fe dc 1a 81 35 00 ac 42 5e Data Ascii: -0[|"+[~/Y.#{#8g5Uno??q|/Yho$f|.+&~+~K?S0:}}onw-ZNy`3`o#jL]lqluSMuwq#U<k5B^
2022-06-30 21:10:51 UTC	52	IN	Data Raw: 06 f0 21 e3 9d df 5e 03 b0 0c c1 1a c4 d5 e0 ae f6 39 01 80 0f 8f b9 6e 04 67 08 bf 1d 04 de 99 64 0a bf 4d d3 17 43 63 63 00 b6 40 df 2e ca ca bf 6f 60 79 07 b8 f9 fe dd 6b 93 d8 03 f0 9e 06 75 e7 20 3a 47 e0 67 86 37 81 bd a3 2e 75 12 7a d4 8e 88 b4 4a 00 56 61 ae 6d 18 11 78 93 0c c0 9b 9a 06 30 33 02 7b 05 e0 75 22 f6 da c2 b1 59 03 78 dd 1a 80 25 0c 1e 22 37 81 a9 00 3c 52 e7 01 10 1c 80 db e8 fa 78 fa df b5 97 ab d7 c5 84 00 60 e8 56 70 17 85 7d 83 ef c2 55 96 5e de bd de 24 1a fe aa 66 a2 5b cf 91 39 e8 a1 9f 09 e8 ee cc f3 7b 42 de b1 4f 90 29 68 5e c0 cd 11 80 43 41 f0 1d 4d 72 68 03 73 cf 34 87 4a 45 e0 8a c0 ce 77 7f 1d 01 18 c3 e0 64 00 38 2c fc 96 02 c0 93 38 03 f0 87 be e2 86 be 49 01 b0 e5 fc f3 4f 2d fc 7d 3d af e9 e7 25 fd dd 5f 1b f4 e5 Data Ascii: !^9ngdMCcc@.o`yku :Gg7.uzJVamx03{u"Yx%"7<Rx`Vp}U^$f[9{BO)h^CAMrhs4JEwd8,8IO-}=%_
2022-06-30 21:10:51 UTC	54	IN	Data Raw: 17 07 e0 e5 6b f1 a7 a2 63 02 f0 7b 71 01 18 bb 13 dc a0 b0 c7 5b c0 94 29 68 dd 4c 34 e5 dd 10 51 fd 6f 2c 0f 82 6f c3 39 10 c3 0d c1 6f 57 04 ae 08 5c 9b c0 15 80 2b 00 6b d1 37 21 00 fe 5b 06 00 dc 9e 79 86 f0 37 26 00 ff f7 2c 00 18 cc 14 80 7f 14 10 f8 c7 e9 df e7 f9 19 9a 60 2d e0 55 73 04 ae 00 9c df cd df 12 01 b8 01 de cb 60 f8 8b 02 f0 66 05 e0 0a c0 65 01 30 9c cd 64 a3 84 df 06 71 01 00 16 bf c3 18 80 9b 69 e7 67 3b 15 80 a9 00 fc 1c 69 05 27 05 c0 03 a6 a9 e7 81 5b 12 87 df 43 64 ea b9 28 00 3e e3 81 5f 0a 0a 63 50 7b 09 a8 ba e7 34 00 de 01 3e bb 7d 0d 06 5e 5d 28 13 d0 e2 ef d0 87 02 c0 7b 29 22 b0 ea fb b1 06 2f 0a bd f8 cf 95 73 ce a3 74 62 db 10 4e 1d 81 5d 00 58 85 b2 dc f0 2b 23 30 76 ff f7 f2 f9 a3 59 24 f4 7d 09 00 b0 3c 11 fd 72 fe Data Ascii: kc{q[)hL4Qo,o9oW\+k7![y7&,`-Us`fe0dqig;i'[Cd(>_cP{4>}^](){}"/stbN]X+#0vY$}<r
2022-06-30 21:10:51 UTC	55	IN	Data Raw: a7 0b bf 7b 20 fe 02 00 ac 82 55 8e 39 68 97 ef 27 c2 2f d8 f0 45 00 b8 c1 5c e8 86 b0 1a 80 11 04 1e e6 31 19 8d 23 f0 a6 04 bf 9b c9 34 80 9f 74 e0 17 6a 00 3f f6 02 bf 14 ec 45 3f f7 32 31 00 96 10 98 74 0f 98 8a ba 4c 00 3c b9 fb 6b 08 c0 a7 d3 24 80 c0 7e 01 f8 2e 0c c0 2f a5 7c 0e fc 5d 00 e0 e5 23 9f 33 d1 ef 64 85 c0 dd 19 e9 9b 56 e1 c0 df f7 19 92 1b 04 df ce a6 1d fc d6 cf c2 4c 39 fb 01 e1 dc 10 38 77 14 2e 1a 83 23 20 f0 2b 50 d3 37 47 00 9e e0 af 0c c0 77 c6 00 7b 27 21 f4 cd 01 80 e1 98 02 f0 f7 89 02 30 0d 7d 53 00 60 0c 81 d5 38 fc f7 98 2d 60 01 7f 2f ff ce 0d c0 4e ed df 0a c0 15 80 2b 00 3b 01 70 0a 08 5c 01 38 04 00 af 57 00 4e 24 1d 00 de 33 00 e0 19 04 ef 14 15 2f e8 4b 9d 80 7e 1e f7 06 b0 d8 06 ee 36 83 03 b4 7f 4d db c0 c7 69 27 Data Ascii: { U9h'/E\1#4tj?E?21tL<k$~./|]#3dVL98w.# +P7Gw{'!0}S`8-`/N+;p\8WN$3/K~6Mi'
2022-06-30 21:10:51 UTC	56	IN	Data Raw: ae 13 d0 c1 00 78 8e be 72 f4 00 bc 5d 44 03 78 82 b1 9b c1 e0 57 04 e0 0d f0 c6 af 39 00 4f 12 16 80 4d 5a c1 4f 3a ad df 47 09 80 af 9c 55 ff 79 a9 9b 94 a6 00 f0 aa 39 f0 9e f2 4d 42 af 72 df ff 4d 0e 80 df 63 05 60 57 24 e6 87 e4 9b 3c 91 01 f8 78 8c a2 c7 7e ee ef a6 0c c1 bd 41 60 20 57 f3 cb 1c 08 1c 18 83 2b 02 87 05 e1 de 20 30 33 06 2b 01 f8 af 9f cc e1 b7 03 c0 4f 91 54 00 ae 00 ec 0d 80 ed 11 d8 16 7f b3 9c 81 96 10 18 9d 68 b6 81 e0 45 7d d2 c1 5f 61 02 1a 4a 05 60 3e 00 4e ec ce 6f 05 60 bf 00 2c b6 82 fd e2 b0 01 00 cb 20 1b 14 80 1f 17 00 c0 89 df 00 ee 0b 00 ef 4f c3 06 c0 db ed 3f 67 08 c0 c7 31 01 f8 d0 06 80 07 86 a0 cb 03 bf 4e 30 7c 5c 6e f3 b7 c1 5f 19 81 5d 6e fc 1e ba e2 b0 0a 80 35 b7 77 41 f8 95 ef fb 7a 06 60 9b 86 70 32 00 6c Data Ascii: xr]DxW9OMZO:GUy9MBrMc`W$<x~A` W+ 03+OThE}_aJ`>No`, O?g1N0|\n_]n5wAz`p2l
2022-06-30 21:10:51 UTC	58	IN	Data Raw: 04 8e d4 f0 a5 e0 af 0b 00 cb df 2d 02 b0 69 8c 1a bb 47 ee a0 9b 4a 74 d8 9a 2c 10 8f a4 c8 cf 28 0d 60 e0 06 f0 1c 73 77 81 94 0d c0 10 08 a7 72 fb 57 46 5d 1d 02 cb ef 74 27 a0 bb d3 d0 18 02 87 84 df 9c 10 58 06 de 14 01 78 cd 18 80 d7 24 b0 5d 63 01 e0 55 32 00 af c2 00 ac 9b 80 e6 00 e0 d9 ef b8 eb 14 3f 33 d0 ed e7 10 f8 aa 50 18 8a 16 80 8f d4 00 cc d1 f2 a5 20 70 88 c6 f1 55 a6 b7 7d 75 b7 7f c1 88 9f 6f 6e 04 07 ba d9 fb 7e a6 29 0a 81 49 d3 ce 79 20 70 4e 10 9c 3a 02 d7 29 68 3a 06 87 01 60 06 1c ce 09 80 ed f0 f7 16 02 bf b7 ec 01 f8 61 5c 00 fe 3e 05 00 be c7 83 bf e9 03 f0 ab 28 fc b6 c2 04 c0 3f 26 80 bf 6a 18 76 6f ff f6 09 80 bf d5 26 af fb bf c6 00 1c 1c 7f cb 04 60 15 f0 9a 03 f0 83 0e 00 7f 5d 01 d8 03 00 27 9e 3d 1d 00 6f 22 10 dc 03 Data Ascii: -iGJt,(`swrWF]t'Xx$]cU2?3P pU}uon~)Iy pN:)h:`a\>(?&jvo&`]'=o"

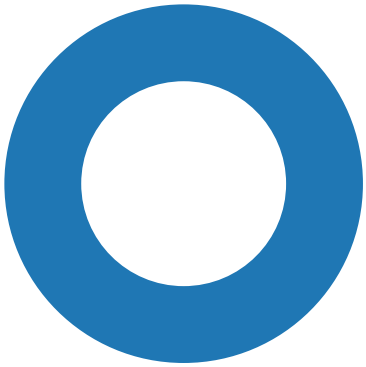
Timestamp	kBytes transferred	Direction	Data
2022-06-30 21:10:51 UTC	59	IN	Data Raw: 77 6c 01 78 f2 39 1d fe 0a d1 7d a7 aa 3d 1c b1 09 2c 03 70 83 c0 18 00 1f 46 02 60 1b 88 f5 85 bf e2 f7 63 cf 1a e4 a5 00 b0 d3 8c 73 4f da bf 51 00 78 44 01 5c 05 00 8f 4c 00 18 fb 9c 00 c3 43 29 d2 3b 32 96 96 08 c3 38 fe 72 dc 04 8e 8f bf 5b c6 ad df 14 00 f8 d1 2c 54 00 6e bf ab 42 db d0 58 9c 22 00 cb 2d e0 55 fb bc b4 fd ac 0e 81 71 00 5e e3 6c 01 77 72 57 d9 f4 bd ca 69 9a 00 bc 04 61 2e 05 77 5f 52 ef 07 bf 6d 9c 77 a7 79 2f 28 e4 a6 8f c0 15 82 5d 20 f8 76 3f da c0 15 81 d3 04 60 43 10 ae 08 ec 0c c0 ed 9f cf 00 f8 a9 7f 00 e6 c1 df 12 00 f8 96 1b 00 3f 8c 03 c0 fe 10 18 8e 6f 00 ce ad 05 1c 06 82 7f 96 4c ae 00 d8 11 7f a3 b6 7f d7 a0 84 c6 df 1b 01 9a bf 15 80 e3 02 70 7c 08 76 01 e0 7f db 58 bb ae 45 de 5c 00 d8 02 83 fb 00 c0 22 04 97 dc f4 Data Ascii: wlx9}=,pF`csOQxD\LC);28r[,TnBX"-Uq^lwrWia.w_Rmwy/(] v?`C?oLp|vXE\"
2022-06-30 21:10:51 UTC	61	IN	Data Raw: 25 04 de af 00 ac 06 60 09 82 65 18 6d 01 b0 88 bb 3a 00 56 63 2b f7 fd 5e ca 73 d5 bf 47 07 c0 9d 9f 21 b7 7f 4d 00 38 25 c0 65 8d 04 c0 fb 9a 89 68 10 73 7b d4 00 f6 09 c0 fb a1 26 a0 c9 f0 2b dc 1a 1e 6e 1b 35 81 75 00 bc db 23 00 de 9a e2 6f 93 36 0c 6f 5c df 41 90 b5 0d bb 5b d7 c3 e1 ae cf 1b c1 1b 99 e0 6f 3a 00 0c 07 07 e0 27 49 00 f0 5a 05 e0 97 86 00 fc 32 ce 04 b4 2b 02 9b 01 b0 1c 22 00 3b 20 f0 bb e3 f0 dc f2 8d 09 c1 ef 54 08 ae 08 5c 11 b8 ef 2d 60 24 1d 04 4e 04 83 a3 4c 40 27 01 c0 4f fd e2 af 1a 80 dd db c1 d9 00 f0 c3 3e 01 30 71 06 da 71 26 3a e5 26 70 af 10 78 c5 07 00 bf 51 01 b8 18 00 be 8b a7 02 70 62 59 bb ce 0d c0 32 fe 96 05 c0 65 60 30 09 80 8b bf ff db 00 2f 0c c0 7d 0f 7c df 77 92 e1 3e 36 f3 ac 00 d2 7d 08 6d 77 82 01 b0 0e Data Ascii: %`em:Vc+^sG!M8%ehs{&+n5u#o6o\A[o:'IZ2+"; T\-`$NL@'O>0qq&:&pxQpbY2e`0/}|w>6}mw
2022-06-30 21:10:51 UTC	62	IN	Data Raw: bf 10 72 02 64 fa 0c 85 df cb ef b9 7a e7 03 30 8b ce b9 2d 65 f2 f3 10 00 bc a4 9d 82 7e db 0d 81 0d f3 2e 03 06 fb bf f7 4b 79 7e d3 7b f2 c6 dc 5b 40 ca bf 0b 9c 0a 06 2f 43 09 80 c0 9c 28 ac fa 5e 63 b0 35 44 60 5f 20 bc 3a ce fd 31 b8 de 2f 18 81 7b 03 c0 df 15 05 c0 e6 08 fc fd 83 31 cc 36 b9 17 22 05 b4 80 33 45 e0 a2 e1 d7 23 fe 8a ed 5f 08 80 a9 cf 8c b3 76 c3 4b d2 9d 7f 0e 71 ff 37 55 00 36 43 5e 1b 00 fe a6 2f 00 0c 35 83 0d db bf fa 76 b0 87 96 6f af 01 78 73 9a 0a c0 60 74 f8 bb 37 4d 4f 00 f8 88 8c bf ee 00 cc 9d d8 f0 8b e6 48 01 bb 40 4b 38 ef c6 ef 9e 14 43 f0 25 be 67 77 d3 17 98 7a 16 a0 b9 e4 d9 68 ca fd df e0 00 9c 01 04 53 f1 75 8f b9 99 eb a3 dd 6b 9f 0d 00 80 b7 10 04 4e 1b 7c e1 1b c1 63 5c bd d8 48 16 80 45 c4 ed 36 81 55 c8 fb Data Ascii: rdz0-e~.Ky~{[@/C(^c5D`_ :1/{16"3E#_vKq7U6C^/5voxs`t7MOH@K8C%gwzhSukN|c\HE6U
2022-06-30 21:10:51 UTC	63	IN	Data Raw: 9c a6 ef 1c 7f b7 c0 3f ab 00 58 95 8d 2c a6 a1 b7 48 00 bc c1 0b be 50 08 00 4c bb 07 2c b6 88 1f 4d 72 e1 1f 7b f5 b1 03 60 3b d8 cd 11 80 17 ad c3 03 c0 1f b0 00 30 fa 9e 6a 0a 1a 68 01 47 03 60 ac f9 9b 50 0b 98 07 81 6f cc 12 03 6c eb 2c 74 fe 10 bc 64 18 af 08 6c 8a c2 5f d8 7f 8f 0a 81 73 09 47 bb b7 83 c0 8e 18 7c 05 c0 e7 e6 00 ec 82 c1 f7 5f 2e 93 be 2f 5b 00 6e e1 6f 40 00 b6 9b 88 be 9d 24 02 ff 27 18 45 f3 57 95 cc 01 d8 bc 85 f9 7a 45 60 2f d8 fb 73 9e ac c4 c7 5f 13 18 36 02 e0 5c f1 b7 02 70 74 00 fe 63 05 e0 e0 ed df 0a c0 91 00 78 b7 02 b0 16 82 2b 00 57 00 36 6c ff 82 18 7c 80 c4 3b fc 42 90 cb d1 fa e5 46 e0 3d 70 02 7a 02 bf 62 4c 01 18 46 5e 15 00 c3 73 d0 b1 51 78 cf 1f 02 13 f0 b7 79 9f 04 bd 9c 00 1c f0 1e b0 39 fe b6 d1 77 70 ba Data Ascii: ?X,HPL,Mr{`;0jhG`Pol,tdl_sG|_./[no@$'EWzE`/s_6\ptcx+W6l|;BF=pzbLF^sQxy9wp
2022-06-30 21:10:51 UTC	65	IN	Data Raw: ce 41 f7 0a 80 61 f8 9d e3 6f 1b 81 07 42 c4 9f a9 11 56 0f c9 71 6f 00 c3 cf a2 02 f0 05 10 2b 04 c6 e0 57 9a 8d be 90 f0 d7 47 c3 77 0a bf 4d 94 f3 d2 b3 26 f0 93 f6 4d e0 0b 31 86 73 ce 26 a8 ab 7b f7 9c 11 80 cf eb 14 74 9c 9b c0 50 80 f7 0c 00 58 df 06 86 01 78 82 c0 fe 1a c0 f3 67 e9 ce 3a fb 08 ed 56 f0 8d 59 38 c0 35 39 00 96 6f 08 1f 8f 11 16 0b 0a b5 fc 10 bc 38 fe 5e 28 1c 08 ec 1b 87 39 7f b7 2d da 7a 41 e1 2f d4 c9 11 85 a3 20 30 01 84 61 00 f6 89 c1 26 08 dc 44 8f c1 91 00 78 f9 7f cc d1 77 a9 0d c0 bf 52 e0 6f 04 00 fe 8f 87 ef bf da 4e 05 e0 94 10 38 6a 0b 18 43 60 c2 3b 2d fc b5 46 e0 d7 ad b1 37 2a fa 3a c0 6f ca f8 3b 6b f8 aa f0 b7 78 00 8e 85 bf 31 db bf 15 80 f3 03 60 39 1e 01 58 4c 0f ef ff 8e 14 f8 fb 55 51 f3 cf 0e 00 dc 73 fc f5 Data Ascii: AaoBVqo+WGwM&M1s&{tPXxg:VY859o8^(9-zA/ 0a&DxwRoN8jC`;-F7*:o;kx1`9XLUQs
2022-06-30 21:10:51 UTC	66	IN	Data Raw: fa 00 c0 f3 dc 00 a2 7b 3e cf c2 d5 8d df 02 11 78 1c 6d 33 17 80 60 55 dc 10 d8 1e 88 53 b8 eb eb 92 8a c0 29 4d 41 2f 05 c0 60 01 81 83 60 f0 32 2b 02 a7 09 c0 01 a0 97 82 bf b9 01 f0 7f 18 01 f0 3b d7 ac 6f 04 f7 a2 05 fc 06 00 c0 d8 cf 2c db c3 54 08 f6 38 11 9d 12 f6 f2 c2 6f 1a f8 7b 09 b4 61 f1 b7 1f 00 fc 6d 5f 01 98 04 c2 15 80 63 01 70 eb 19 02 c0 5f 69 a0 17 47 e2 82 01 18 82 e0 c2 01 18 83 e0 fe 01 f0 ae c5 9d 5f e1 e7 15 7e f5 6d e0 80 0d e0 a3 31 92 1e 79 03 e0 5d fe fb c1 4a f8 dd 55 df 00 a6 b4 86 95 13 d1 bb 9a 86 70 17 82 f5 f3 d2 36 78 4b 85 5f 8e 46 31 e1 9d 11 82 c0 10 0e 2b 00 58 7b 0b 38 22 fa 42 00 ec 0f 7e e5 99 68 bc e9 5b 62 03 58 06 60 35 02 37 f3 d1 5b f4 06 2f 15 80 c5 bf 93 1b c2 12 00 5f 88 00 bc 71 5d 37 c7 dc c1 5f 6a 03 Data Ascii: {>xm3`US)MA/``2+;o,T8o{am_cp_iG_~m1y]JUp6xK_F1+X{8"B~h[bX`57[/_q]7_j
2022-06-30 21:10:51 UTC	67	IN	Data Raw: ee d7 86 70 ab 15 dc 02 df 3d 21 5d e0 25 37 84 49 77 7a 33 01 60 a7 39 67 9e 98 ce 3c 1f 58 37 81 29 90 6b da 28 26 86 0a c0 23 42 08 70 4c 46 dc 61 ae e8 eb 1e 15 dc 0e 8c 01 78 87 a7 fd 7b 81 63 ae 0d 18 6f 5d c8 69 00 78 03 fc 3d ad 86 30 34 0f 8d dd ef 55 a1 ef 05 b1 35 8c 35 83 35 bf 63 03 08 09 61 bd b4 7a 01 5c d6 de 05 fe a8 75 23 98 34 e5 7c 6e 01 c0 ba cf 1b 00 b0 b7 79 e8 73 45 0c 01 f8 a3 4c 00 18 82 60 f8 e7 31 01 f8 03 00 7e c3 40 30 8e bf 3a 04 ee 26 49 0c 36 c5 e2 97 e6 08 2c 43 b0 0a 80 73 44 60 52 13 f8 f8 f2 be 6f 37 be 91 d8 05 81 55 38 5c 11 38 0c 08 f7 1b 81 cd 31 b8 83 c0 89 63 70 3e 00 fc 2b 20 1f 2b de 09 36 01 6d da 12 2e b4 05 cc dc 10 d6 01 70 5a 08 1c bf 35 fc 93 65 42 01 f0 77 45 c0 6f aa f8 db 9f f6 ef b7 26 e0 eb f5 f6 ef Data Ascii: p=!]%7Iwz3`9g<X7)k(&#BpLFax{co]ix=04U555caz\u#4|nysEL`1~@0:&I6,CsD`Ro7U8\81cp>+ +6m.pZ5e BwEo&
2022-06-30 21:10:51 UTC	68	IN	Data Raw: 26 38 8b 4d 45 6f d1 e6 99 4f d5 68 6b 8b be 1d fc 3d 99 06 f8 de c9 ec f3 3c c9 20 30 05 80 cf 89 f8 eb 33 57 b0 7c df 3c 10 fc 22 00 3c 6b 08 73 40 b1 a6 05 ac 03 de 8f 12 01 e0 15 2b 00 fe 80 00 c0 fc 59 24 01 30 80 c0 01 41 98 13 81 93 01 e1 a8 08 7c 33 0a 02 fb 06 e3 20 08 8c e6 96 1a 82 2d 71 b8 22 30 33 00 cb b7 80 45 00 86 52 11 b8 05 c1 6a c4 75 c0 e0 94 01 f8 af 6c f0 6b 01 c0 b6 cf 80 e4 04 c0 18 fc 96 d4 02 86 11 f8 06 90 da 08 2e 03 7b 53 40 df f8 f8 fb e7 ce 73 1c 6e 4b 6f ff c6 03 60 bf ed df 0a c0 5c 00 1c bf f9 ab 02 e0 36 f2 d2 f1 d7 16 80 4d 90 97 76 53 78 d3 78 e6 59 09 c0 0d a6 26 0b c0 db bc 00 bc 5f 22 00 ef 1a 00 70 13 35 00 0f 0f 90 76 70 e9 b7 7e 1b 98 d5 ce 3d ef 21 08 bc d7 69 f9 ea 6f fc ee 96 81 bf 10 ce fa 9a 7c 3e 8a 77 1b Data Ascii: &8MEoOhk=< 03W|<"<ks@+Y$0A|3 -q"03ERjulk.{S@snKo`\6MvSxxY&_"p5vp~=!io|>w
2022-06-30 21:10:51 UTC	84	IN	Data Raw: 3a 0d c0 ae 0d 60 cf ad 5f 17 fc 1d 85 c6 5f ca ad de 0c 62 44 da 01 43 e8 4d e2 81 c5 04 34 07 02 a3 00 d8 77 0b 58 d7 f4 65 47 e0 fa b3 0a 7f 45 00 86 be a7 7a 9e 0f fc da 02 f0 26 3a 54 dc 65 c5 df a9 10 0c 00 4f 37 cd f8 3b cf 63 09 74 1b ed df 63 35 02 e3 01 98 80 ba 96 f0 0b 02 f0 71 60 00 3e 8c 08 c0 c7 1a f8 7d 59 c5 04 c0 97 ac 00 18 d3 1a b6 07 60 dc bb 22 dc 62 01 18 77 1f 38 34 00 ff 86 05 80 d3 c3 60 1e e0 a5 e4 a2 d4 fc 45 df f8 d5 20 f0 c5 56 21 30 06 71 19 80 b8 4c 41 a7 0d c0 ac 28 5c 5a c0 a1 30 b8 00 70 52 08 1c af 1d 4c 81 5f 7f 08 4c 84 e2 cc 11 58 0f c1 bf 2d 08 dc 16 ec 65 40 5f 5e f8 cd 00 80 23 c1 6f 3b f1 77 05 85 bf 10 00 ff 2c 00 f0 94 08 c0 e6 77 34 00 9c 34 fe 96 f9 e7 49 88 74 a9 fd db 65 fc 1d 28 26 9f 07 98 c9 e7 1e 39 23 Data Ascii: :`__bDCM4wXeGEz&:TeO7;ctc5q`>}Y`"bw84`E V!0qLA(\Z0pRL_LX-e@_^#o;w,w44Ite(&9#
2022-06-30 21:10:51 UTC	100	IN	Data Raw: ed d4 06 6f 5d db bf 3a 00 de 61 05 60 13 fe 62 de 69 27 00 c3 53 d0 db de 01 58 85 b2 7c b7 80 37 08 00 5c bf 07 9c 12 00 af a2 f0 d7 df fc 33 fe dd 9b 09 02 f0 0d 45 e4 06 b0 29 d1 00 58 40 e0 95 88 b7 80 4d 08 5c 5a c0 05 81 6b 00 3c 31 03 f0 2a e1 be 6f 01 e0 82 c0 d9 00 30 23 06 c7 00 60 15 04 67 03 c0 3e 10 38 24 04 b7 19 80 dd 21 f8 ea 79 7e 0e 92 4b 25 c9 83 71 41 5c b7 99 e7 1b 2d 86 df 8c f0 77 a3 0d ad df 9c f1 77 33 3f fc dd 69 ce 44 57 00 5c 6f ff 36 a3 82 de ec 01 b8 a7 c3 df 96 40 b0 d8 f6 05 9e 8d 50 f7 7b a1 0c 14 ef 43 ed de 1e 09 6f 59 6e 03 63 e6 9f b3 cb d0 6e ee 59 35 ed 6c 9c 7d 6e 13 02 1b ee 0e 63 10 58 80 d4 25 ac 9a ee fc 52 01 18 ff 19 a8 21 2c cf 3b 8b bf 03 06 e0 a1 05 00 0f df dc 55 ce 48 33 01 30 34 f3 dc 41 fc d5 cf 47 6b Data Ascii: o]:a`bi'SX|7\3E)X@M\Zk<1*o0#`g>8$!y~K%qA\-ww3?iDW\o6@P{CoYncnY5l}ncX%R!,;UH304AGk

Timestamp	kBytes transferred	Direction	Data
2022-06-30 21:10:51 UTC	116	IN	Data Raw: bb e3 00 60 43 1e 6b b1 7e 7e f5 4e 1c 00 1b 76 fa 32 c2 ef e3 01 fa 9a 01 f8 b1 05 72 a1 08 fc 18 89 c0 58 2c 4e b6 fb 97 13 80 4f 6a 00 60 38 e4 b2 02 f0 11 12 7d d7 79 00 b8 47 e0 5c 18 0c 85 e8 3b 00 d6 f2 eb 63 7f 62 80 f0 d4 da c1 68 00 96 fd bf f5 00 f0 94 21 d8 04 c0 3e 08 3e f3 64 7b f7 d7 9b 08 fe 0a fc 4a 04 79 f9 c0 56 1d d5 4c cd f4 da be 2f 70 a9 7c 7f 6f 8f bd 6a ba c9 e2 ef 22 79 20 70 db 32 02 30 f8 79 c1 df 0a 01 78 95 be 09 3c 87 06 b1 8a bf c9 00 b8 b5 00 30 e4 39 fd 79 46 fc 85 02 30 09 79 13 8f 5b ae a9 fd bb 9e 5e fb 17 3a 1e ba 0d 01 60 07 ba da da bb 2a fe b6 80 dd c0 6d 08 de 46 6f fe 4e 17 80 0f 90 00 6c 85 db 4b f7 fe 5f 74 b3 d8 b5 1f f8 d2 d1 00 be bb 67 d9 ff 1b 69 fc b3 7d 0c f4 06 79 4f 6c ed df 21 02 63 00 98 65 0c 74 32 Data Ascii: `Ck~~Nv2rX,NOj`8}yG\;cbh!>>d{JyVL/p\oj"y p20yx<09yF0y[^:`*mFoNlK_tgi}yOl!cet2
2022-06-30 21:10:51 UTC	132	IN	Data Raw: d4 15 00 16 f0 15 f8 9d 01 fc 1e 68 b1 41 f0 10 6e 6d f7 b7 77 5d cf 1c bc 37 af b6 af 03 78 ef f6 f6 42 f1 57 87 60 08 be e6 c7 5f 15 81 ad e7 ca 68 e7 c6 31 fa 99 82 ac 4d 44 90 9d 0e fe 06 ee dc 05 3d 4b f9 6e 24 fe da 10 d8 f7 bd 82 b9 3c f8 7b 34 c5 5d bf d4 f6 2f 20 17 48 00 ae 72 ec 33 47 fb 57 7d 47 53 31 fc aa a3 9f 37 d0 3b 6a e2 2e fd 00 7c 46 d8 f9 1b b4 37 58 c3 d5 b3 4d 32 e0 af e9 7b a0 ed df 43 2d b1 c1 77 fb 3d c3 f1 cf ea 48 e8 10 00 ce dd 04 5e 00 90 17 07 c8 25 34 7c eb 00 e0 c5 a4 f1 f7 67 23 f4 65 07 60 0d 4f 5f 21 92 7f 0f 30 ef 9e e0 aa e1 97 71 17 f0 ae 05 7f 6b 81 60 3b fe 52 01 f8 83 82 01 38 0e 08 53 01 d8 85 c1 90 96 ef be 16 01 e0 88 fb 7f 6d 60 4b 82 e0 07 a0 44 01 e0 12 f0 37 64 64 f4 94 e1 57 30 78 6e 28 bc 37 8f cc 04 80 Data Ascii: hAnmw]7xBW`_h1MD=Kn$<{4]/ Hr3GW}GS17;j.|F7XM2{C-w=H^%4|g#e`O_!0qk`;R8Sm`KD7ddW0xn(7
2022-06-30 21:10:51 UTC	148	IN	Data Raw: a5 e3 6f ed 80 bf 15 01 7f 13 46 e0 82 bf 3c 00 b6 8e 7d de 8f 96 b6 80 2c b7 01 ec b2 f7 97 82 ba 94 91 cf f3 56 cb 77 8e e0 af 7d 44 74 32 cd df 1d 05 7f a7 a7 b3 50 38 7b 81 77 84 9d c1 41 5a c0 a9 01 f0 d9 00 f1 f7 4c be b1 db d8 10 f8 a5 f9 dd 6d df 00 fc 12 07 dc ed 09 80 1f 42 04 e0 05 67 f7 2f 11 7d a1 18 c7 3b df 7d 66 7d 87 03 c0 19 8c 7f a6 ed fc f5 03 60 d7 c4 06 e0 82 ba 9e 08 dc 13 00 73 e0 97 03 c4 53 0d 8a 73 83 e0 cb 1f ef 00 56 0d 88 c0 2a d6 c6 06 61 2e f6 c2 ef a5 39 02 3a 2c 00 e7 84 c1 de f8 db 33 06 f7 0f c1 f4 77 58 00 ac 02 eb db 7d f2 c6 5f 5b b8 98 eb 83 c0 f0 3d 63 03 e0 02 b6 29 c0 ef e5 38 e0 77 f0 7b 76 0b 28 4b c3 af cc 3d 0b 06 fa 62 e3 97 29 f0 4b 78 2f 02 fc 86 0c 65 b4 74 a8 91 d0 13 25 56 24 ee 6d 0c 34 07 81 a9 2d 61 Data Ascii: oF<},Vw}Dt2P8{wAZLmBg/};}f}`sSsV*a.9:,3wX}_[=c)8w{v(K=b)Kx/et%V$m4-a
2022-06-30 21:10:51 UTC	164	IN	Data Raw: f7 1b 10 7f 6b 21 fc ad 58 a3 9f 55 f0 9d 26 06 c0 6e 10 1c 1c 7f 3b cd 61 02 fc 52 11 d7 b6 f7 d7 f8 9e e3 d8 67 12 ec 52 13 08 7f 59 a8 cc 40 5b 2a 0c 6f 99 f7 a9 08 6c 1a e9 dc 58 60 97 ba 2b 98 ba 07 78 6b c0 60 6a eb 17 6d ff 3e 2f e8 3b 1a 00 b6 e3 f0 23 8c fe 4a cb 00 00 78 93 2f 00 3f e6 c9 3e 3a 0c 0f 60 44 f4 8f e3 06 60 5f 04 d6 31 f8 eb bf 11 b2 2b a3 9f 45 21 98 3a 16 fa 87 90 b1 23 30 0b 80 8f 10 7c e9 89 b7 81 f0 37 1e 00 17 fc 2d f8 5b f0 d7 3f c3 87 df fe da bd ef c3 a4 e0 67 09 b6 17 58 30 63 45 e0 b3 2b 2d 97 79 b7 79 a3 e0 af 06 c0 93 85 7c db 37 16 fe 86 dc 05 0c 45 7f 8e e2 af 08 00 af 1d 47 3a 4b e1 ef 5a 1c 81 e7 42 f8 6b 6a 01 cf 5c da bf eb 18 00 3c 30 fc dd c8 e2 ef 9c 8d bf 03 03 e0 e3 de df b9 cc d8 67 6e d3 97 82 c7 0e 00 1c Data Ascii: k!XU&n;aRgRY@[*olX`+xk`jm>/;#Jx/?>:`D`_1+E!:#0|7-[?gX0cE+-yy|7EG:KZBkj\<0gn
2022-06-30 21:10:51 UTC	180	IN	Data Raw: bb 07 60 08 02 8f df fb e3 4d 4a 01 60 0a 04 3e 42 e3 ef 38 5a 00 7e 38 06 e1 01 0c 03 00 f8 6b 5b 26 01 c1 4d f2 70 69 ea 86 01 f0 38 15 7f 2b fe e6 c0 5e 28 e0 e6 84 e5 20 08 5e 94 05 c0 c5 b4 83 1f b9 23 c3 ef 17 0e 00 de a3 ae 01 80 bd 66 a3 27 03 c0 88 cf 9c aa 00 fc 23 1c 80 0d ef 4d 19 80 f7 f8 bb ca d9 fe a5 c0 df 96 fc de 6f f0 4d 60 0c fe ae 78 e1 2f 1e 80 9b 01 fc 42 00 78 19 63 02 9a 6c 42 5a 87 bf 2b 03 fe e2 11 b8 78 fc 15 c4 00 8c c2 62 1d fe 9e 58 f1 77 05 c4 df 55 c5 5f 05 7b 21 3f 23 c0 df ce 13 7f 85 07 fe 0a 0c fe da 00 f8 c8 0d c0 10 24 06 37 88 ef 02 60 99 f0 ae 2f 18 7f 3f b7 3e b3 c1 af 0e 7f 75 00 dc 6a f1 f7 4e 10 fe b6 1e 13 cf ae e9 67 4c 1a c8 7b 40 ac 6d 30 00 dc 51 85 18 7b d5 9f 85 b4 7c 31 00 dc 05 24 64 46 9a 02 a0 bb 0a Data Ascii: `MJ`>B8Z~8k[&Mpi8+^(^#f'#MoM`x/BxclBZ+xbXwU_{!?#$7`/?>ujNgL{@m0Q{\|1$dF
2022-06-30 21:10:51 UTC	196	IN	Data Raw: 9a f7 7f 43 1c 14 c8 32 04 60 3b 0a f3 05 e0 10 ec 2d 15 7f cb 40 60 e1 f9 1c 0a c0 3f 45 07 60 ea 46 2f fa fd 00 00 ce 05 bf be f8 3b 00 60 0a e8 05 00 b0 dc f8 fd f2 34 05 00 af 3d e7 9f dd ef eb 9b bf cc 01 78 75 00 e0 52 e7 9f b1 f8 7b 9c 0a 7f 19 01 f0 82 25 00 03 f0 b7 dd fd d9 04 c0 ad 04 bf 7b 30 8e 80 bf 4d 0e fc 5d 39 67 9f af f1 f7 8c 0d fe 22 10 98 a2 f9 6b 78 b7 07 60 15 7b 8d f8 2b 2a fe c2 00 78 c1 00 80 35 cf 08 f1 b7 91 f1 b7 73 e3 6f 83 99 7d ee 10 cd df ae 14 fc bd cb 1e 7f ed b9 42 58 51 a7 9f 63 64 3a 8d df 0a c0 15 80 7d 01 18 d3 de ad 00 1c 6d 02 7a 0d 08 e0 bd f5 ba ac 66 70 0f c0 24 10 2c ca 80 60 71 85 be a2 00 f8 8d 31 09 5d 0a fc 26 45 60 c1 11 80 a3 23 6f 05 e0 50 d8 9d 13 00 bb b0 56 0b bd 25 03 70 86 f8 03 b0 48 0e c0 1f 93 Data Ascii: C2`;-@`?E`F/;`4=xuR{%{0M]9g"kx`{+*x5so}BXQcd:}mzfp$,`q1]&E`#oPV%pH
2022-06-30 21:10:51 UTC	212	IN	Data Raw: 00 a7 80 bf 61 e7 a0 27 de 01 f8 d7 f3 c6 ef 11 fe 82 00 ac 83 5f 13 00 af c3 00 4c 9d 86 c6 df 07 ce 7c fe 59 07 be 54 20 56 be ff b9 12 7f 17 9f 6d f6 e3 06 f0 2d 02 04 b7 00 d8 a2 f5 bb f8 be aa fd 2b 42 ef 48 07 c0 a3 0c 01 58 84 dd 2d 36 fc 5d e3 6e ff 82 f8 bb 41 c7 df b1 e5 fd 5f 14 fe ae 15 fc 4d 04 7f 21 00 1e 69 a6 9f 9d f0 17 33 fb cc 0d c0 18 fc 3d 0c 05 7f 2b 2d fe 5e 0a 88 bf 1f b2 e2 6f 85 c4 5f b1 d5 6b 0a 0d 7f cf 5a 4f 3f bb 03 b0 7b f3 57 06 60 1c 04 f3 61 ed 7e 7d e2 78 0e 00 5c e0 b7 00 f0 e0 e6 9f 13 6b fa ea de e1 02 e1 98 b7 80 49 f3 d0 32 d8 ee 18 20 98 11 7e b3 81 e0 47 42 5a 08 6c 6e 03 2b 41 36 91 bb c0 5c 08 6c 07 bf 8e 08 9c 28 fc 72 4f 41 7f 6b d9 f8 05 10 78 bd b4 80 53 07 60 3d 0c 4b d8 0b 45 07 c0 16 b3 cd 69 00 b0 db 2d Data Ascii: a'_L|YT Vm-+BHX-6]nA_M!i3=+-^o_kZO?{W`a~}x\kI2 ~GBZln+A6\l(rOAkxS`=KEi-
2022-06-30 21:10:51 UTC	228	IN	Data Raw: 95 00 38 16 02 9b f0 37 97 16 70 aa f0 4b 05 e0 dd dd ff f5 1d 1c 00 23 30 98 e7 ce 6f b8 16 30 7c cf d7 a6 05 7c d0 49 0e 00 6c df 02 46 20 70 96 2d e0 7d 00 80 dd 93 37 00 c3 08 5c 20 38 2c 08 f7 0e 86 3f 32 00 70 04 f4 55 01 b0 ea bb 32 f4 ca 71 87 5f d3 34 34 fc fe 99 d8 b9 9b 22 fe d2 a0 78 89 bf 22 00 9b 1a be 07 af 79 6f ff ce 21 15 fd 1d 08 77 37 89 00 4c c4 df 06 80 e1 69 e8 b4 01 58 85 bf 97 11 f0 8b 02 60 44 e4 f9 e7 6b 23 33 00 e7 00 bf 22 f6 fa 99 84 f6 04 c0 10 fc 62 a0 77 04 cc 42 83 77 7e 0d f8 cb 00 c0 d0 bd e0 d4 e1 77 8a bc 15 7c 1b 98 05 7f 3d cf 3f 6f c9 51 c1 6f b4 f6 2f bd f9 bb 45 04 e0 dc f0 77 64 8d bf d7 f2 c3 df 79 5a ed 5f 10 7d 3f e4 c7 5f f0 06 f0 0c 80 8d f8 5b 51 f1 f7 3c 3f fe 56 16 f8 3b 07 e0 fd 6a 06 b7 79 e2 ef c9 5e Data Ascii: 87pK#0o0||IlF p-}7\ 8,?2pU2q_44"x"yo!w7LiX`Dk#3"bwBw~w|=?oQo/EwdyZ_}?_[Q<?V;jy^
2022-06-30 21:10:51 UTC	244	IN	Data Raw: 5e 38 04 8e 02 c0 02 d8 9a 01 98 da fc ed 7f 0b d8 37 fc c6 68 01 3b dd 01 7e dc 73 00 fe 0d b2 ad eb 03 80 1b 04 96 43 46 60 b9 e1 4b 44 60 f5 0d df 74 10 d8 84 c3 b1 00 d8 1a 81 4d 98 eb 80 c5 7d 40 e0 34 20 f8 79 12 19 1e ec f6 20 02 ca fe 48 13 7f 0d e0 17 0c 81 7e 8b 7a 1b 98 fb 06 f0 8b 76 c3 57 f5 ef 12 e0 57 79 ff 57 c8 bb 1f 87 6f fe 86 05 60 08 79 55 20 6c 6e 06 37 ad 5e 08 88 bd c0 ef 96 dd fc 33 ea be ef 86 0b 00 ab f0 57 05 c0 75 6f 00 78 8a bf 8b f9 e7 9a ef be 2f 15 80 4d bf a1 c1 df 6b 12 fe 5e 9b e7 e6 c3 9d 25 c4 7e 66 06 60 4c cb 57 97 5b c0 e7 58 00 86 db c4 0f 83 47 dd fe 85 f0 f7 a1 b7 b9 67 fa ef 1e c2 ef c3 59 ee b5 6e 06 c7 00 60 3a fe de 4b 15 7f 77 90 00 bc 43 c0 60 19 7f 5d 00 78 87 0f 80 8d f8 3b f1 35 0d 9d eb fc b3 1e 87 ff Data Ascii: ^87h;~sCF`KD`tM}@4 y H~zvWWyWo`yU In7^3Wuox/Mk^%~f`LW[XGgYn`:KwC`]x;5
2022-06-30 21:10:51 UTC	251	IN	Data Raw: 38 ce 29 e8 df 4e 00 b7 48 0c 00 9c 5b c0 b8 19 68 a7 00 ac 9b 81 f6 06 bf 6e 66 a0 13 01 60 11 02 8b 13 1a 80 9b 85 c0 96 28 bc b3 48 c2 08 9c 21 d8 24 0f 2b c9 0d 5d 1a b0 8d e9 7f 7f 21 f2 22 f0 d7 05 00 63 a0 b7 8c be 9f 2e 72 9f 34 5e e1 97 12 80 3f 44 7e c7 10 98 cd 6f fd da 34 84 e1 2d e0 20 f8 ab 9b 80 36 05 60 c9 44 74 fd 00 18 86 bf 55 04 3e 04 03 f0 15 01 fe 5e 75 8d bf cb f7 bb 2b f8 b5 04 e0 e2 fb 31 dd 00 be 19 11 fe 6e 48 f1 b7 fc 8c c5 df 0d 09 e8 6e d8 02 30 ba 25 5c 05 e0 e2 06 f0 76 3b cd f6 ef b6 51 eb d7 7f fb 57 05 c3 7b 12 a4 dd 73 8e bf 1b 42 f4 15 e2 6f 57 0c bf fb d2 86 af 0a 80 89 9a bf 08 fc 15 01 70 3b cf 3f 67 00 8e 10 80 7d cf 3f cb 5a c1 58 fc 7d 3c fa 61 06 e0 e4 da bf 09 03 b0 4b fc 1d 7b c2 5f e9 77 0d 1a be 50 00 9e 3c Data Ascii: 8)NH[hnf`(H!$+]!"c.r4^?D~o4- 6`DtU>^u+1nHn0%\v;QW{sBoWp;?g}?ZX}<aK{_wP<

Timestamp	kBytes transferred	Direction	Data
2022-06-30 21:10:51 UTC	267	IN	Data Raw: 00 ec f3 fe ef 73 f5 89 0a 80 67 7f 76 0b c0 df d4 0c 80 ff 58 c1 df 38 01 b8 82 bf 19 80 57 e9 87 05 e0 2f 02 a1 af 10 80 7b 19 80 83 00 30 1c 85 eb 80 c0 81 e6 a0 55 08 8c 48 ec 10 ec 1f 83 1b 7a 43 98 00 92 63 98 71 36 bd 07 9c 11 d8 d5 cd 60 cf 37 80 41 31 9f 6e b6 07 e0 63 c2 19 67 0a 00 2e 37 80 cf ea d0 37 14 00 27 d8 f8 a5 c5 df 11 f9 c4 b3 aa 01 8c c1 5f 14 00 93 81 af a8 e9 2b 86 df 94 1b c0 f3 cf 86 1c fe 86 01 e0 1b 8a 06 70 15 7b f9 cf 44 53 d0 fe 01 b8 fa b9 08 5d 63 c3 df 16 d7 02 16 00 b0 eb 3b c0 3d 71 e3 57 0a c0 02 f8 2d 02 9e 70 ee 00 a3 6b fc 02 01 98 7f 27 16 f8 e5 01 b8 25 00 60 ff f8 cb 03 f0 0d 65 3a c6 b9 e6 15 80 7b 5e 82 9f 7f c6 00 70 2f 03 30 18 80 d9 50 00 f0 c9 f0 cd b5 e6 00 f0 0f f5 00 0c 79 a7 46 00 fc 04 04 c0 df cb 00 Data Ascii: sgvX8W/{0UHzCcq6`7A1ncg.77'_+p{DS]c;=qW-pk'%`e:{^p/0PyF
2022-06-30 21:10:51 UTC	283	IN	Data Raw: f0 a1 b7 16 b1 72 77 af 00 bc fa 77 ee 36 a1 77 49 c8 ca a1 03 02 23 f6 0e a3 f7 02 e7 0b c0 d6 40 6c 02 60 1d fa ae 84 03 e0 b7 06 b0 f9 56 03 7e 55 7f 6f 23 fc f6 c3 02 b0 dc 18 76 01 e0 ad 44 00 bc 2e 25 49 33 78 0b 00 60 35 da 7e 20 c4 1a 7d 77 b0 f7 d7 95 00 7c 85 02 c0 3b 44 04 f6 81 c8 06 00 5e c2 b6 81 0b fe 7a 06 e0 4b d1 82 85 df 20 00 ac 0b 12 80 77 fa bc 00 b8 4f 06 e0 76 8f 81 c6 02 30 84 c0 14 00 a6 b5 83 53 b5 80 4f 44 01 e0 32 06 3a 21 00 df 9a 24 30 00 6b 11 b8 c7 af 05 4c 6b 07 3f 5d 10 d8 13 02 ff d9 12 5b 7d 42 70 dc 44 46 df 9e 1e 7e e3 e2 2f 04 c0 22 dc fa c1 5f 2b 00 ee a7 05 e0 d0 e8 5b da bf 86 f6 6f b7 8c 7f 6e c3 fe 5f bf 0d e0 75 7d e8 10 5c 85 e3 28 e8 7b d6 d1 02 70 8b 20 38 15 18 bb 43 b0 65 0a 02 17 10 e6 8c c0 5e fe 8d 26 Data Ascii: rww6wI#@l`V~Uo#vD.%l3x`5~ }w|;D^zK wOv0SOD2:!$0kLk?][}BpDF~/"_+[on_u}\({p 8Ce^&
2022-06-30 21:10:51 UTC	299	IN	Data Raw: 57 00 56 8c 79 d6 36 7a 01 e0 d5 02 30 80 be b5 bf 53 c6 3c 6f 6f 78 c3 5f 6a 33 58 8f bd 36 00 bc 31 42 5b 68 5c b4 8c bf 7a 04 86 10 36 3d 0a 63 9a bf 32 00 53 ef a3 01 b8 2b 00 70 87 37 fe 96 31 d0 8e 63 a0 7b 96 00 bc 67 d3 14 d6 e0 6f 6f 1c ff 00 4c 47 60 cc 7d 5c 0b 98 e7 5e 60 15 fe 1e 32 6c 01 df 0d 85 c0 58 00 46 de fb ae df 9e 51 d0 ba 33 19 7a 45 00 ce 01 81 7f 50 e0 af 1a 84 9f cd 24 3f cf 1a 84 fd fe de 39 dd e7 8b dc ed 0b e3 ef 51 64 28 bb 82 dd f0 f7 71 c1 df a8 cd 5f ff f8 5b da bf 39 e2 2f b7 f1 cf 77 a8 00 8c 87 e1 88 08 8c 46 e1 b6 40 70 3d 6f 0c 30 f8 b5 eb 03 64 55 25 00 06 bb 62 31 47 08 76 46 e0 a5 fc c7 44 17 00 8e 37 82 ba 20 70 be 10 ac 43 d8 53 9f 0c ee c8 a1 8e 99 9e 77 00 de 18 07 0d b8 ba bb 18 48 8e 30 66 3a ee ae 5f bf 00 Data Ascii: WVy6z0S<oox_j3X61B[h\z6=c2S+p71c{gooLG`}\^`2lXFQ3zEP$?9Qd(q_[9/wF@p=o0dU%b1GvFD7 pCSwH0f :_

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **6304**, Parent PID: **1468**

General

Target ID:	0
Start time:	23:10:42
Start date:	30/06/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "C:\Users\user\Desktop\office365 Validation.html
Imagebase:	0x7ff7f6290000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6

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

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}	dr	unicode	0	1	success or wait	1	7FF7F62CFC4B	RegSetValueExW

Analysis Process: chrome.exe PID: **6572**, Parent PID: **6304**

General

Target ID:	1
Start time:	23:10:44
Start date:	30/06/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1560,15957 04125475944836,7329412530459423612,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1956 /prefetch:8
Imagebase:	0x7ff7f6290000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Disassembly

No disassembly

Copyright Joe Security LLC 2022