ID: 655873
Sample Name: ClosingDoc.html
Cookbook:
defaultwindowshtmlcookbook.jbs
Time: 20:55:44
Date: 01/07/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report ClosingDoc.html 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Process Tree 5
Malware Configuration 5
Yara Signatures 5
HTML 5
Sigma Signatures 5
Snort Signatures 6
Joe Sandbox Signatures 6
Phishing 6
System Summary 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 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 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic 12
C:\Users\user\AppData\Local\Google\Chrome\User Data\05177d59-1ac6-4172-bf90-9d4d0db75458.tmp 13
C:\Users\user\AppData\Local\Google\Chrome\User Data\1fdbc81e-f4a3-46ca-976b-5297dc767efc.tmp 13
C:\Users\user\AppData\Local\Google\Chrome\User Data\3d732c96-1dcf-4e61-bc21-37146533d5ef.tmp 13
C:\Users\user\AppData\Local\Google\Chrome\User Data\45a7e7c8-6f04-47c9-8c63-6dcef45a9b89.tmp 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\53914a93-2093-4aa7-bad6-935287d288ca.tmp 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\5cdc808e-57e4-41f1-a10d-f9e756319a36.tmp 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\6f8db5c9-c440-491e-8eaa-2f7057031dca.tmp 15
C:\Users\user\AppData\Local\Google\Chrome\User Data\712d8625-191a-4a96-a318-238daa121581.tmp 15
C:\Users\user\AppData\Local\Google\Chrome\User Data\71a01078-cc72-4fff-b45e-ed1d8da38a74.tmp 15
C:\Users\user\AppData\Local\Google\Chrome\User Data\7d14a367-b8b6-461c-813a-e2d51bb03563.tmp 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\837a1e94-5d5e-4253-a0d2-1101a64e776f.tmp 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\91617a51-4ee5-494c-9fe1-a96fc9306244.tmp 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat 17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\00afc427-620e-441b-9d55-f2fccb3b72e8.tmp 17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1958cd92-269a-440d-94ce-21e9cf707246.tmp 17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\64fa19b3-e5c0-44bf-bb7e-f771696cfb5c.tmp 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8573d12c-b96a-4d16-917b-88ec3b064883.tmp 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\969bdb64-81a0-4122-9156-01dfb77266cc.tmp 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy) 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy) 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy) 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy) 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State

(copy) 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\d5b098ac-4631-4a9e-b4a4-5f95b793f089.tmp 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Network Persistent State (copy) 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\c3374c7e-019a-40ee-bf72-030709ff5750.tmp 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a1f83762-104f-4b3c-86cb-f81b59a166c7.tmp 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b7c55baf-1466-4b5b-8ec5-f79a396f70ce.tmp 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bb7097c4-4445-4094-8a93-0f275566722a.tmp 23
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) 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ef0232b0-f2c9-454e-8a64-e82d66657865.tmp 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f28ac788-1b15-49e6-b6a9-3ff69264f316.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) 25
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_dir5412_192052981\Ruleset Data 26
C:\Users\user\AppData\Local\Google\Chrome\User Data\aea53507-d1b9-4e25-8112-37a6b52191e5.tmp 26
C:\Users\user\AppData\Local\Google\Chrome\User Data\c4d69481-e7c9-454f-8517-0c34bc76516d.tmp 27
C:\Users\user\AppData\Local\Google\Chrome\User Data\e91058a8-5ed5-4bd0-af37-7524b343cb75.tmp 27
C:\Users\user\AppData\Local\Temp\2d2579c9-4c37-4da6-89e6-380180b88327.tmp 27
C:\Users\user\AppData\Local\Temp\5412_2066527378\Filtering Rules 28
C:\Users\user\AppData\Local\Temp\5412_2066527378\LICENSE.txt 28
C:\Users\user\AppData\Local\Temp\5412_2066527378_metadata\verified_contents.json 28
C:\Users\user\AppData\Local\Temp\5412_2066527378\manifest.fingerprint 29
C:\Users\user\AppData\Local\Temp\5412_2066527378\manifest.json 29
C:\Users\user\AppData\Local\Temp\5412_515056959_metadata\verified_contents.json 29
C:\Users\user\AppData\Local\Temp\5412_515056959_platform_specific\x86_64\pnacl_public_pnacl_json 30
C:\Users\user\AppData\Local\Temp\5412_515056959_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_for_eh_o 30
C:\Users\user\AppData\Local\Temp\5412_515056959_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_o 30
C:\Users\user\AppData\Local\Temp\5412_515056959_platform_specific\x86_64\pnacl_public_x86_64_crtend_o 31
C:\Users\user\AppData\Local\Temp\5412_515056959_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe 31
C:\Users\user\AppData\Local\Temp\5412_515056959_platform_specific\x86_64\pnacl_public_x86_64_libcrt_platform_a 31
C:\Users\user\AppData\Local\Temp\5412_515056959_platform_specific\x86_64\pnacl_public_x86_64_libgcc_a 32
C:\Users\user\AppData\Local\Temp\5412_515056959_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_a 32
C:\Users\user\AppData\Local\Temp\5412_515056959_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_dummy_a 32
C:\Users\user\AppData\Local\Temp\5412_515056959_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe 32
C:\Users\user\AppData\Local\Temp\5412_515056959_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe 33
C:\Users\user\AppData\Local\Temp\5412_515056959\manifest.fingerprint 33
C:\Users\user\AppData\Local\Temp\5412_515056959\manifest.json 33
C:\Users\user\AppData\Local\Temp\5412_75593435\Recovery.crx3 34
C:\Users\user\AppData\Local\Temp\5412_75593435_metadata\verified_contents.json 34
C:\Users\user\AppData\Local\Temp\5412_75593435\manifest.fingerprint 34
C:\Users\user\AppData\Local\Temp\5412_75593435\manifest.json 35
C:\Users\user\AppData\Local\Temp\6ad0a865-d5b4-4a63-8b44-f76c272eb0b4.tmp 35
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\2d2579c9-4c37-4da6-89e6-380180b88327.tmp 35
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\bg\messages.json 36
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\ca\messages.json 36
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\cs\messages.json 36
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\da\messages.json 36
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\de\messages.json 37
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\el\messages.json 37
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\en\messages.json 37
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\en_GB\messages.json 38
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\es\messages.json 38
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\es_419\messages.json 38
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\et\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\fi\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\fil\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\fr\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\hi\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\hr\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\hu\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\id\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\it\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\ja\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\ko\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\lt\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\lv\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\nb\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\nl\messages.json 43
C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\pl\messages.json 43
Static File Info 43
General 43
Network Behavior 44
Network Port Distribution 44
TCP Packets 44
UDP Packets 46

DNS Queries 47
DNS Answers 47
HTTP Request Dependency Graph 48
HTTPS Proxied Packets 48
Statistics 56
Behavior 56
System Behavior 56
Analysis Process: chrome.exePID: 5412, Parent PID: 820 56
General 56
File Activities 57
Registry Activities 57
Key Value Modified 57
Analysis Process: chrome.exePID: 5052, Parent PID: 5412 57
General 57
File Activities 57
Disassembly 58

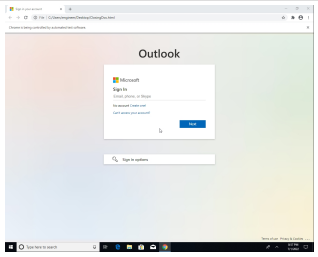
Windows Analysis Report

ClosingDoc.html

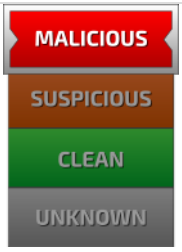
Overview

General Information

Sample Name:	ClosingDoc.html
Analysis ID:	655873
MD5:	3755ba4cfcde83…
SHA1:	058fa6f78bf7369..
SHA256:	1b174509a2b040.
Infos:	



Detection



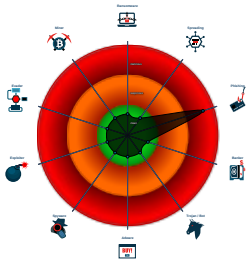
HTMLPhisher

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- HTML document with suspicious title
- Phishing site detected (based on log…
- Phishing site detected (based on im…
- Invalid 'forgot password' link found
- None HTTPS page querying sensitiv…
- No HTML title found
- JA3 SSL client fingerprint seen in co…
- HTML body contains low number of …
- IP address seen in connection with …

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5412 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "C:\Users\user\Desktop\ClosingDoc.html MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5052 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1580,15663332800411292547,115680743419720232 3,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1920 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
87841.0.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Phishing

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

Phishing site detected (based on logo template match)

Phishing site detected (based on image similarity)

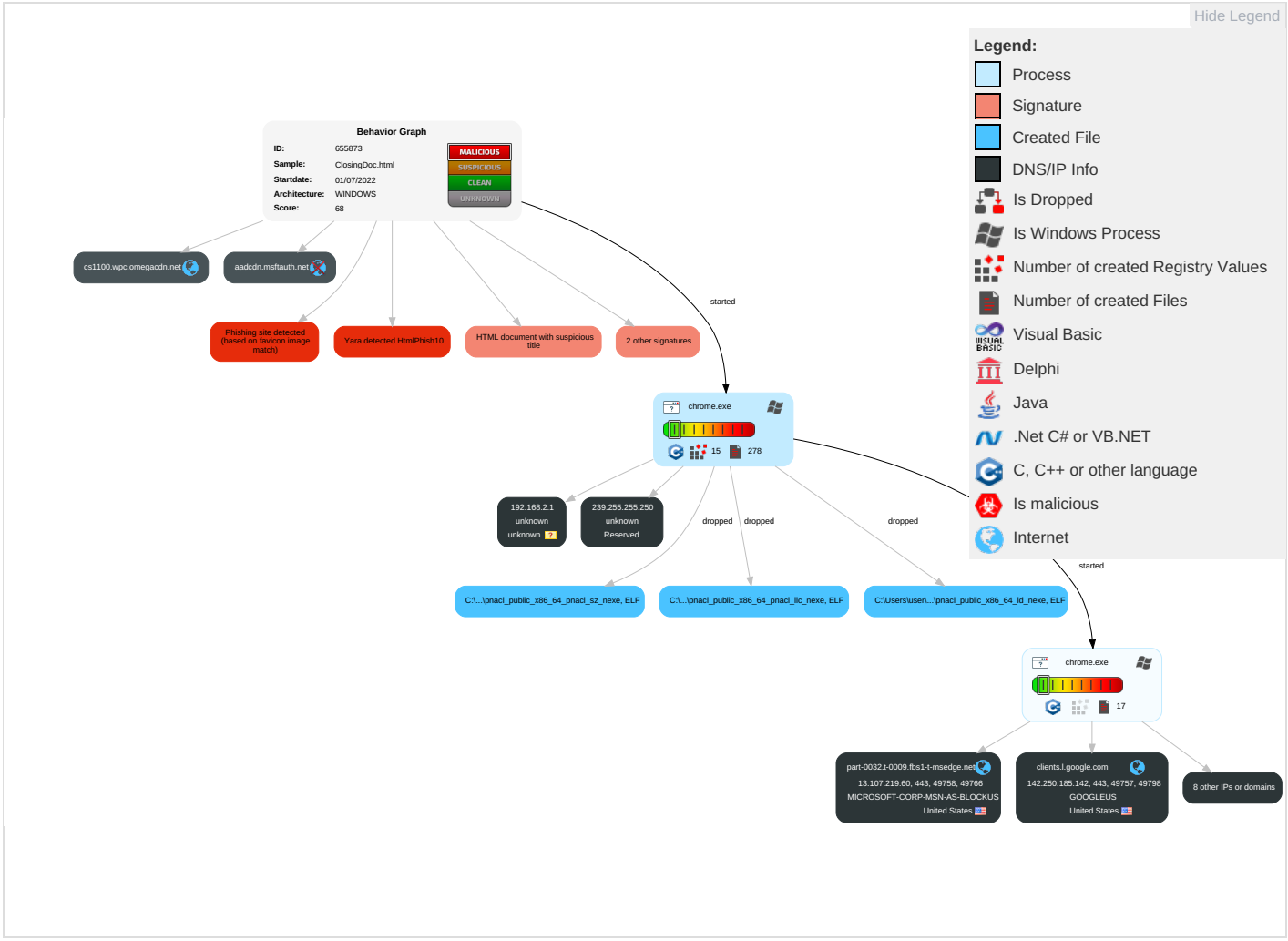
System Summary

HTML document with suspicious title

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	3 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	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

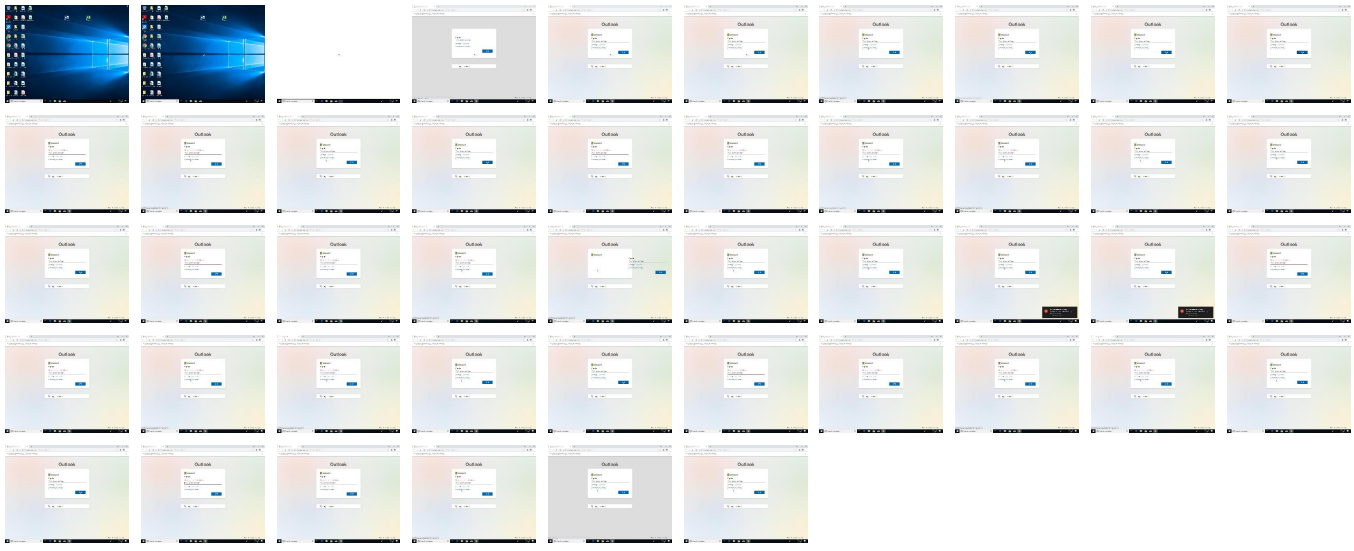
Behavior Graph

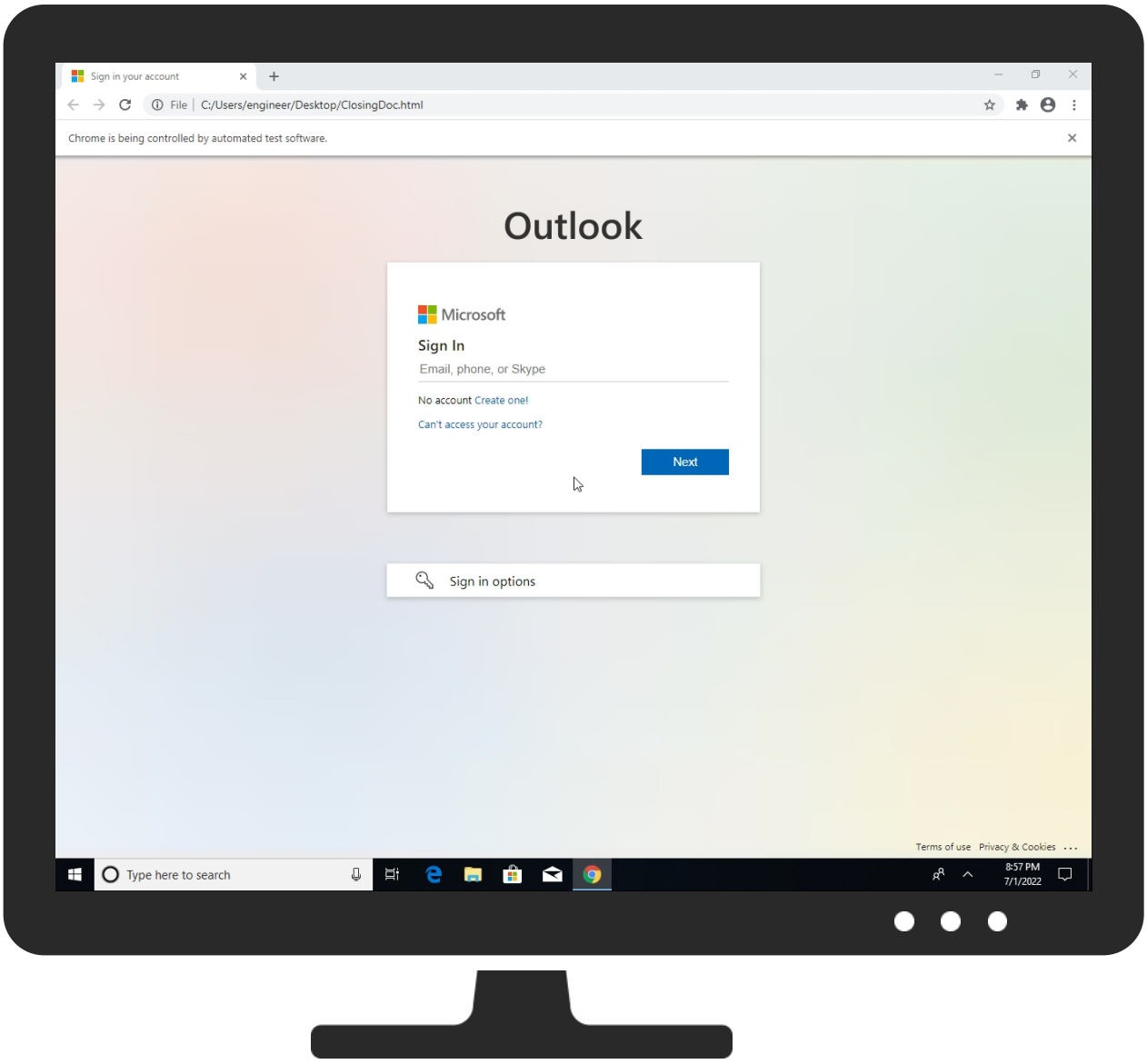


Screenshots

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\5412_515056959_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\5412_515056959_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\5412_515056959_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\5412_515056959_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\5412_515056959_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\5412_515056959_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/signin-options_4e48046ce74f4b89d45037c90576bfac.svg	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/applogos/53_8b36337037cff88c3df203bb73d58e41.png	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cs1100.wpc.omegacdn.net	152.199.23.37	true	false		unknown
accounts.google.com	172.217.16.205	true	false		high
clients.l.google.com	142.250.185.142	true	false		high
part-0032.t-0009.fbs1-t-msedge.net	13.107.219.60	true	false		unknown
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
aadcdn.msftauth.net	unknown	unknown	false		unknown

Contacted URLs

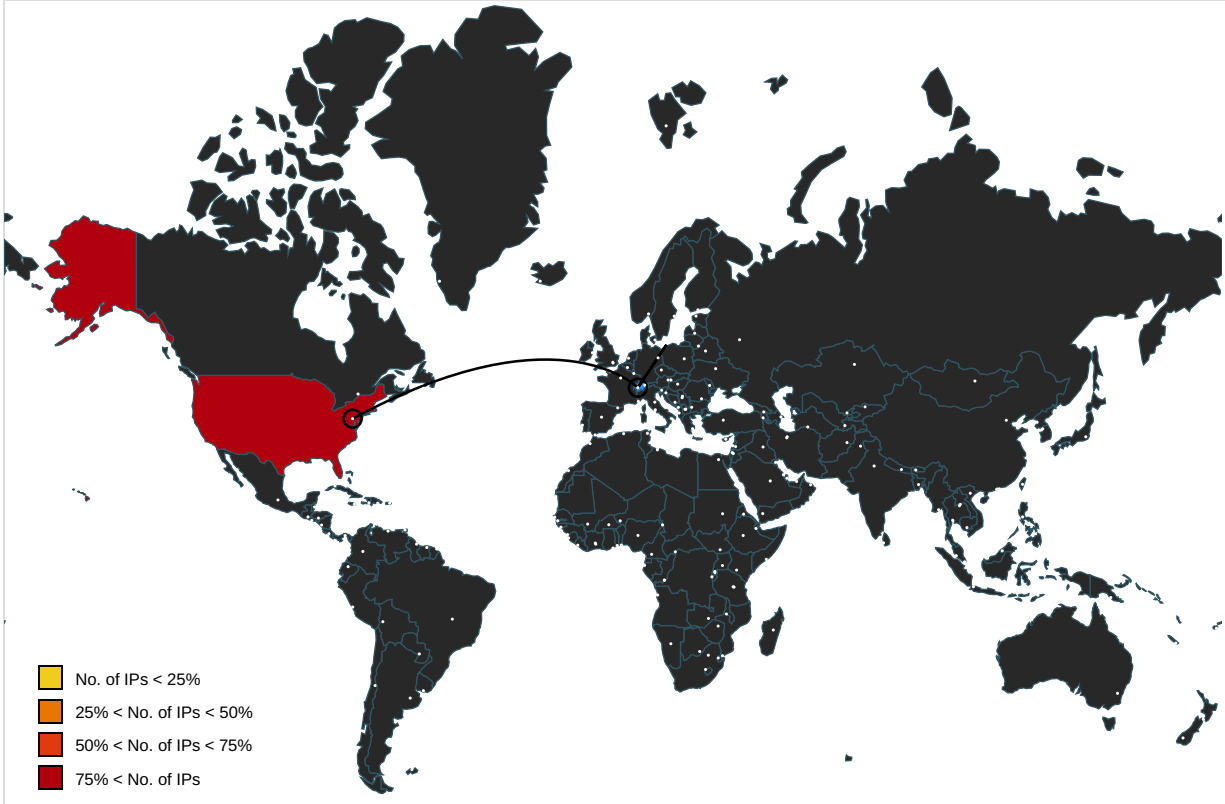
Name	Malicious	Antivirus Detection	Reputation
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
file:///C:/Users/user/Desktop/ClosingDoc.html	true		low
http://https://aadcdn.msftauth.net/shared/1.0/content/images/signin-options_4e48046ce74f4b89d45037c90576bfac.svg	false	• URL Reputation: safe	unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg	false	• URL Reputation: safe	unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/images/applogos/53_8b36337037cff88c3df203bb73d58e41.png	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	d5b098ac-4631-4a9e-b4a4-5f95b793f089.tmp.1.dr, ef0232b0-f2c9-454e-8a64-e82d66657865.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	ef0232b0-f2c9-454e-8a64-e82d66657865.tmp.1.dr	false		high
http://https://www.google.com/images/cleardot.gif	craw_window.js.0.dr	false		high
http://https://payments.google.com/payments/v4/js/integrator.js	craw_window.js.0.dr, manifest.json.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://chromium.googlesource.com/a/native_client/pnacl-llvm.git	pnacl_public_x86_64_crtend_o.0.dr, pnacl_public_x86_64_ld_nexe.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
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	ef0232b0-f2c9-454e-8a64-e82d66657865.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	ef0232b0-f2c9-454e-8a64-e82d66657865.tmp.1.dr	false		high
http://https://clients2.googleusercontent.com	ef0232b0-f2c9-454e-8a64-e82d66657865.tmp.1.dr	false		high
http://https://apis.google.com	ef0232b0-f2c9-454e-8a64-e82d66657865.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_crtend_o.0.dr, pnacl_public_x86_64_ld_nexe.0.dr	false		high
http://https://clients2.google.com	ef0232b0-f2c9-454e-8a64-e82d66657865.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
13.107.219.60	part-0032.t-0009.fbs1-t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
172.217.16.205	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.185.142	clients.l.google.com	United States		15169	GOOGLEUS	false
152.199.23.37	cs1100.wpc.omegacdn.net	United States		15133	EDGECASTUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	655873
Start date and time: 01/07/202220:55:44	2022-07-01 20:55:44 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ClosingDoc.html
Cookbook file name:	defaultwindowshtmlcookbook.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:	17
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:	mal68.phis.winHTML@29/128@5/7
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, backgroundTaskHost.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): 142.250.184.238, 69.16.175.42, 69.16.175.10, 172.217.23.99, 173.194.160.70, 74.125.108.198, 142.250.185.163, 142.250.185.131
- Excluded domains from analysis (whitelisted): cds.s5x3j6q5.hwcdn.net, clientservices.googleapis.com, arc.msn.com, r5---sn-1gi7znek.gvt1.com, r1---sn-1gi7znek.gvt1.com, r1---sn-1gi7znes.gvt1.com, redirector.gvt1.com, login.live.com, sls.update.microsoft.com, update.googleapis.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, www.gstatic.com, cdn.onenote.net, global-entry-afdthirdparty-fallback.trafficmanager.net, www.bing.com, r4---sn-1gi7znek.gvt1.com, client.wns.windows.com, fs.microsoft.com, aadcdnoriginwus2.azureedge.net, r1.sn-1gi7znek.gvt1.com, ctldl.windowsupdate.com, aadcdn.msauth.net, r1.sn-1gi7znes.gvt1.com, firstparty-azurefd-prod.trafficmanager.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, aadcdnoriginwus2.afd.azureedge.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

- VT rate limit hit for: ClosingDoc.html

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\05177d59-1ac6-4172-bf90-9d4d0db75458.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):	409222
Entropy (8bit):	6.026498411403835
Encrypted:	false
SSDEEP:	12288:1NDdqe70oOl9gKVGGNPUZ+w7wJHyEtAWh:1Ge70o4VVxUMkEtAa
MD5:	A2B363FC1B7CA6840E6FA2D6F53643C2
SHA1:	5D719CAA7C7F201D27E7C5B5758F21123F35D363
SHA-256:	A5071F79CD129A7DD5B5A67E5CFC3A15DA0587E992C0D0B1FA7D3AFF16A75436
SHA-512:	8B73B81E81F711EA7E366EF966A1362CC480387B1218F068F36068021C6E10C334481492AA53F2C6A47055A5651FDC2AC3F6AC36ACA0D9C7922B84F6C550D8E8
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":1.656734219020455e+12,"network":1.65670182e+12,"ticks":174968958.0,"uncertainty":4046713.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230364624763"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\1fdbc81e-f4a3-46ca-976b-5297dc767efc.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7512633381310696
Encrypted:	false
SSDEEP:	384:Rv9yyMPtg3geVn52JNKr/v+G31+wdHY1GRYrzQ+0xdgkQnrv2mTwzgqKW5OAMqN5:xGeRZKYx5ge34qUoXf2+K4mKJl
MD5:	7906826BF78DC71231B5E736418A7452
SHA1:	73F93B9FA4B0AC61B892C41BE67E542717298376
SHA-256:	A080A6D6A5D67364D1B4A316B7826F7BECFFD79E08FF188C78555E0EB58554D6
SHA-512:	F8F18ADDBF32E459A69DE6C8F1DA9FAFC7FA987F154FE84A0D28131DFA6F23CA564D40E14E01B3826CE1B360DE005307D53367D81FCA37D7AF9ED726D9452F62
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....`8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\3d732c96-1dcf-4e61-bc21-37146533d5ef.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7512051919126046
Encrypted:	false
SSDEEP:	384:vv9yyMPtEg/2JNKr/v+G31+wdHY1GRYrzQ+0xdgkQnrv2mTwzgqKW5OAMqNz1KzZ:3eRZKYx5ge34qUoXf2+K4mKJG
MD5:	18B39C06B20A56C97C8EBEC30D6E0CA6
SHA1:	F2FE10E10A744136898F3AFFD40823D9F14C1890
SHA-256:	67BB1F4ECED802B4FDCC468FDF7D868F7320070FD988C34A4DFA03E6C538FB4C
SHA-512:	923F9C56A48D7785966FAEFD09D5B051E87FB4A93D2A1164817788D3EEB504DFBC2DA9DEE99B390B3FCA874B9D8E253C8E461AC94B31B35E93A27181F59FDB77
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 .0.0.....*...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\45a7e7c8-6f04-47c9-8c63-6dcef45a9b89.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):	417374
Entropy (8bit):	6.045905322966391
Encrypted:	false
SSDEEP:	12288:iNDdqe70oOl9gKVGGNPUZ+w7wJHyEtAWh:iGe70o4VVxUMkEtAa
MD5:	471C535806EAFB5D12BBFA293636C014
SHA1:	1001A378A07EF221BFA7C555E991F6C3E51DE208
SHA-256:	FAD9D9721AD502B707D47507E260B6F7A4AB0F40A262954401BFA79A2BE45C08
SHA-512:	1441258F9E474751964056F2C454DA09C5FDB8076C6846C75655F500D8F2B905665EB92F56F10C54FC113D6C81AC9E2C6B9A6B4D5517F2D4F4D4477D42078761
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":1.656734219020455e+12,"network":1.65670182e+12,"ticks":174968958.0,"uncertainty":4046713.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230364624763"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\53914a93-2093-4aa7-bad6-935287d288ca.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):	417374
Entropy (8bit):	6.045905636750197
Encrypted:	false
SSDEEP:	12288:jNDdqe70oOl9gKVGGNPUZ+w7wJHyEtAWh:jGe70o4VVxUMkEtAa
MD5:	912D859776B330666826026A555DBC82
SHA1:	31394AA7513EEBDAE48DF9C857AE75284DEBEC14
SHA-256:	A439E4962388F94DE4B753792C974C9F9BB42EC81A2F6513AB6211DFD204E5CA
SHA-512:	A9F587E4E5148094E47CBA5309B508657CB544B09B09CFA85F4A9D26C283284EF47C69A083A61E6515BEA05EE570A9E232DEE7F116CC0422267DFA1487B0175
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":1.656734219020455e+12,"network":1.65670182e+12,"ticks":174968958.0,"uncertainty":4046713.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"132459524880075 86"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\5cdc808e-57e4-41f1-a10d-f9e756319a36.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):	408933
Entropy (8bit):	6.02599406283335
Encrypted:	false
SSDEEP:	12288:1NDdqe70oOl9gKVGGNPUZ+w7wJHyEtAWh:1Ge70o4VVxUMkEtAa
MD5:	9DE6491EE7924025ADD2E98929303878
SHA1:	37871210B6C3346ADC91B7459906021208 31AB6B
SHA-256:	7ECA0635522B924317CB664D517B7F6AB4EB617156AF00A660766DDF66FB376E
SHA-512:	81BD729F882B43A32A6D3EEFB3C5F41C7AB07D40D43133603A9085233B62E866EDC3F9E5430E03B7A9D19A84F74FE4004A74D6054E06F4CC086F2E8058BF8AEF
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":1.656734219020455e+12,"network":1.65670182e+12,"ticks":174968958.0,"uncertainty":4046713.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230364624763"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\6f8db5c9-c440-491e-8eaa-2f7057031dca.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):	417374
Entropy (8bit):	6.045905490830705
Encrypted:	false
SSDEEP:	12288:LNDdqe70oOl9gKVGGNPUZ+w7wJHyEtAWh:LGe70o4VVxUMkEtAa
MD5:	1D68DB1BF51CC0FAA39FCE9A8A6515D2
SHA1:	766030B80E34AE809C118C11489067C739DD5A21
SHA-256:	37844807FD3C4D6A2C51C25635EDE55834EF99452A9CD5A9258A36B0BAE0D3AE
SHA-512:	C55764F582619779EDC2D3C4E5B47398103C8EA0B5B964FA08D840DB54E35640A547AD44DF83DD15D4D6DEE4233C17B48D8E745F1F32DA6A213BE0961363FF
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":1.656734219020455e+12,"network":1.65670182e+12,"ticks":174968958.0,"uncertainty":4046713.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"132459524880075 86"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\712d8625-191a-4a96-a318-238daa121581.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):	409119
Entropy (8bit):	6.026321889078436
Encrypted:	false
SSDEEP:	12288:jNDdqe70oOl9gKVGGNPUZ+w7wJHyEtAWh:jGe70o4VVxUMkEtAa
MD5:	F7E4D0A14F6BE3246E0E151B44CA3FFE
SHA1:	DB9D44924761B37A0F6E0791F82875B97B3C71E1
SHA-256:	726148EAFD76CADD9116290897C7A48B2F293B3D067B17BFAB4549E70D3AA983
SHA-512:	5B9935DFFE0DB548B0C56BE7D8082B97D7B000BD00876F65475FE696511CD8F7A7DFAC4E5E93552AF1D330930F2BEF9DB1C4CA462A26B093570060A6F4C4228A
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":1.656734219020455e+12,"network":1.65670182e+12,"ticks":174968958.0,"uncertainty":4046713.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230364624763"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\71a01078-cc72-4fff-b45e-ed1d8da38a74.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):	417374
Entropy (8bit):	6.0459058355050415
Encrypted:	false
SSDEEP:	12288:lNDdqe70oOl9gKVGGNPUZ+w7wJHyEtAWh:lGe70o4VVxUMkEtAa
MD5:	A431C714AC407B56AF5BD04A6E9B6805
SHA1:	8DEBDD192D96E86F7ACB1B99D127B7A48EC84A13
SHA-256:	B140DA7C604ED1AD0316A410F270A374C70B1AFF60E0F7A223FC831EA5E20964
SHA-512:	384C1DCC235ED4A1224F3275AF85336114CEE106661637A1B99DBA232143169BA37608ECB2ED4F4C9A7084857DB4D743B0FB382D9BCBBC25232B8BECEC45905
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":1.656734219020455e+12,"network":1.65670182e+12,"ticks":174968958.0,"uncertainty":4046713.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\7d14a367-b8b6-461c-813a-e2d51bb03563.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):	409025
Entropy (8bit):	6.026159332361069
Encrypted:	false
SSDEEP:	12288:/NDdqe70oOl9gKVGGNPUZ+w7wJHyEtAWh:/Ge70o4VVxUMkEtAa
MD5:	8B43F89E230695FB7B84EB15256A4E34
SHA1:	1072CA4AB6B96E9831BCF853B68750BE5466E225
SHA-256:	46B61113BF24EA7F4463195423315B58979E41CC4A0CCEB6109FF6D94E06C6BD
SHA-512:	D1A2D23925900C82C7F13ACA32A152B1DEEA1D2083F8FDD21DF59456AC34491F6D47ADB7F8D5D2EA4A95D9F44ACE153ECC2C850D3B42D5C13EDED120D7AAB34
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":1.656734219020455e+12,"network":1.65670182e+12,"ticks":174968958.0,"uncertainty":4046713.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230364624763"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\837a1e94-5d5e-4253-a0d2-1101a64e776f.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):	409025
Entropy (8bit):	6.026159456009931
Encrypted:	false
SSDEEP:	12288:LNDdqe70oOl9gKVGGNPUZ+w7wJHyEtAWh:LGe70o4VVxUMkEtAa
MD5:	261982083D10255E1C0F88DB761D2243
SHA1:	0F23E35001677F12CB6077E896E748F6C95EFA5C
SHA-256:	539ECB907B73E2ABD4FA1F26B48D46CA1E53948B5E108A2F81CBB236D3D19274
SHA-512:	F9BB878645385FC99ACE6DB49EAB86805F6B003A026599BA6AFAB15E358E3D1CB3419AD6C77058C7BE97215732A17735781BA157941273697E060F730E3EC812
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":1.656734219020455e+12,"network":1.65670182e+12,"ticks":174968958.0,"uncertainty":4046713.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230364624763"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\91617a51-4ee5-494c-9fe1-a96fc9306244.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):	409222
Entropy (8bit):	6.026498613773912
Encrypted:	false
SSDEEP:	12288:NNDdqe70oOl9gKVGGNPUZ+w7wJHyEtAWh:NGe70o4VVxUMkEtAa
MD5:	0403790043999A78FCD4974B007BB8CE
SHA1:	9589FE1F16968C17D7AB677FBFB26095D21765C4
SHA-256:	3BDCAF8D64D01CD3E9C4A3F1B748D43ABA3DF66AAD8FFE31F939EDED19F35320
SHA-512:	4D975D721FD4173B7EE7C8E9B3624C04D725F1EE1FD06153DD752C0499C10E1DE86C926922D7E562C3A50141650E06B0A3F97066008B2D7C15501718FBF6B31
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":1.656734219020455e+12,"network":1.65670182e+12,"ticks":174968958.0,"uncertainty":4046713.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230364624763"},"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):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXEwozZHn:+EwozZHn
MD5:	BEBB369FF4A565B19D5E0BC83CD176AE
SHA1:	A6F07666F8DDDF61E5AACE533129BFB541A8A769
SHA-256:	8018F98553432706436A31FFD1E743018C3B7F1AA8D34B2FA18F494A4CFCEB19
SHA-512:	5D2F9F6E9502517AFF4673C3157D57046D4E38D70B5E228F468FB820363E559087D1A2F2E4006B4589BF3F175A4507F1FA3D7BE5FC34F9FA39EB17757DAEC17F
Malicious:	false
Preview:	sdPC......................y3..M.Y.NbD.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\00afc427-620e-441b-9d55-f2fccb3b72e8.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):	4888
Entropy (8bit):	4.952072646187769
Encrypted:	false
SSDEEP:	96:nOsXb1IfeT1paAKIlxk0JCKL8robOTQVuwn:nPXb1B1p9R4Ksa
MD5:	C19B19D705AB05A24F987A58EC2EF715
SHA1:	EB6E24E11C33CBCCCFFE6A625F5B79E2E3AAB9BC
SHA-256:	F789194465701633125FFCAD33A39E471F6C4AB074E4F14E094277DAADC66EEC
SHA-512:	1A4446789E4C8581069B0EA94EF4E1C43EFF32B9DAD57AA7AF180B0742BB0EFAC9DE00C3E03F4328395D87DAD0709B053D554A5C0D66727184FB2F479E7BF90 0
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301207817520444","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1958cd92-269a-440d-94ce-21e9cf707246.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):	4915
Entropy (8bit):	4.959601505712836
Encrypted:	false
SSDEEP:	96:nOsXb1IgeT1paAKIlxk0JCKL8rGbOTQVuwn:nPXb1C1p9R4Ks0
MD5:	1B9A4ADF66374682BF57726AC4AED068
SHA1:	8FC196B4B4EC05A945DC25A888FE04CED567B2F1
SHA-256:	584BD08C68189A2F941E3C9A97F9E15C88BCFD71EA6D435D8F05E319CE1BD91D
SHA-512:	C8B510C3A981AB758630D06653AEE4661B86142DE72A0DE2D13A4C79D81830DBDDD7A83CCFC862365EC5EC61BA5C84B362EB7898AE02D2CF51FD4D4CABC1 899
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301207817520444","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\64fa19b3-e5c0-44bf-bb7e-f771696cfb5c.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):	5.574135090272468
Encrypted:	false
SSDEEP:	384:XhztTLl/oXr1kXqKf/pUZNCgVLH2HfD9rUqzs4b:jLl6r1kXqKf/pUZNCgVLH2HfJrUKsQ
MD5:	F046F7B322319172A01A5193DD671541
SHA1:	97CFEE7C49813F8BA87B2957B524C5B1FF395998
SHA-256:	63A0920E11178CA86C0BA1C6951689FCC39D310F4F762043F63B6DA1585ECBD2
SHA-512:	0F57E29151CCD280319346A791241F1BF023EA6E046ADD68E8975D973500AB8C582641EFD097CB70A0E8D77C6F87CDE5F73E640282AB6D34A9F60FCBDBF51A E
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":"13301207816625451","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\8573d12c-b96a-4d16-917b-88ec3b064883.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):	5.564116427386737
Encrypted:	false
SSDEEP:	384:XhztuLl/oXr1kXqKf/pUZNCgVLH2HfD9rUBHGVQs4X:eLl6r1kXqKf/pUZNCgVLH2HfJrU1Gys8
MD5:	06BCB6976A98B6BA1AC1309D4AE58496
SHA1:	8E8EB874809C0522806F9686B2754067ADEAF39F
SHA-256:	646230206EB0A17C391386076C13E66000A329B83FA408FDC7682B11F1947E1B
SHA-512:	254A38BC05283D1A585E94E0ED5D33BBC13701BE02637859E29D5061C495DE230A52BC042C6D3BA409655BBE7390F8BCDBD7B84FBE6302EC98B02373CE5443 D
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":"13301207816625451","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\969bdb64-81a0-4122-9156-01dfb77266cc.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):	4888
Entropy (8bit):	4.952603206845905
Encrypted:	false
SSDEEP:	96:nOsXb1IMqm1paAKIlxk0JCKL8robOTQVuwn:nPXb1Am1p9R4Ksa
MD5:	622A1E461CD2DE5121D28B26DAE9B7C6
SHA1:	B285238B39402464D10083D35D28EB7FF1A83EE3
SHA-256:	4E79BC393235438BC88B8164696B7279DD5F2894A75BBF0B4D73EB3083FEF0C3
SHA-512:	813FB49696C1A58491C1306425279E806C211C939249BE315174829823ACC58E165B8CB4C00A29FE9B5A2813DB5F40B400D19952C2171267245F2838710A9062
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301207817520444","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0","

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvuI11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkIjEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Ffxs

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:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985DI
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):	375
Entropy (8bit):	5.201892183750294
Encrypted:	false
SSDEEP:	6:63n4q2PN723iKKdK25+Xqx8chI+IFUtqV53PFMXZmwYV53PFMFkwON723iKKdK2L:A4vVa5KkTXfchI3FUtLX/dF5Oa5KkTXc
MD5:	488DBDCBB13AC27F9AFEB88ED3CC51CF
SHA1:	DD58D8F79C1D6CCE510A9571D86A20213B32A59F
SHA-256:	4BBC6945CC660F305967A7F7FCA21114F9CEF0C5EFCADCDC641A50EAE9C0964D
SHA-512:	62A7583FD800696395C7CF203A94EAAE6894E1BE160C05269DD8A10F092B5B39E23F2D3CE9292CB2DF2664F38C3F2D60370C61507D26B04DB0492A5BED3E4CD
Malicious:	false
Preview:	2022/07/01-20:57:14.581 830 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/07/01-20:57:14.582 830 Recovering log #3.2022/07/01-20:57:14.582 830 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):	375

Entropy (8bit):	5.201892183750294
Encrypted:	false
SSDEEP:	6:63n4q2PN723iKKdK25+Xqx8chI+IFUtqV53PFMXZmwYV53PFMFkwON723iKKdK2L:A4vVa5KkTXfchI3FUtLX/dF5Oa5KkTXc
MD5:	488DBDCBB13AC27F9AFEB88ED3CC51CF
SHA1:	DD58D8F79C1D6CCE510A9571D86A20213B32A59F
SHA-256:	4BBC6945CC660F305967A7F7FCA21114F9CEF0C5EFCADCDC641A50EAE9C0964D
SHA-512:	62A7583FD800696395C7CF203A94EAAE6894E1BE160C05269DD8A10F092B5B39E23F2D3CE9292CB2DF2664F38C3F2D60370C61507D26B04DB0492A5BED3E4CE D
Malicious:	false
Preview:	2022/07/01-20:57:14.581 830 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MAN IFEST-000001.2022/07/01-20:57:14.582 830 Recovering log #3.2022/07/01-20:57:14.582 830 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):	700
Entropy (8bit):	5.3247375857990615
Encrypted:	false
SSDEEP:	12:j7mg4NSw3JedeZfHqlnBJVt2kcHyFPZBl4JLoj9uFk1TBk778B/xgskZBa9sNiy5:j7oNSC44RKlnzVt2jHUZBlQkj9mIY786
MD5:	D1EB83077FCC0C309005DF199F33B7D1
SHA1:	38CDC0652BDF56A45E81824F8B4BF9641D7022AE
SHA-256:	578E88F510D5E72A0B0EAD71533850C7EAC5198C2C64E56AE26FE9B843D2AD5D
SHA-512:	2E4A2471E6B61915AB5F2404423D6130D1589CD7420EE36B364FABAE6788B1A8281D27D3D6A7E44D80F6F12C7D7BB51A64492EC5602385165B99259D1F8EB347
Malicious:	false
Preview:	....."P....account..c..closingdoc..desktop..user..file..html..in..sign..users..your*|.....account.....c.....closingdoc.....desktop.....user.....file.....html.....in.....sign.....users .....your..2.....a.....c.....d.....e.....f.....g.....h.....i.....k.....l.....m.....n.....o.....p.....r.....s.....t.....u.....y...:e..... .....B..... .....*1file:///C:/Users/user/Desktop/ClosingDoc.html2.Sign in your account:.....:.....:.....J....."- .....

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):	1961
Entropy (8bit):	4.895293456334768
Encrypted:	false
SSDEEP:	48:YALteBdpNntw3qyvTCXDHz5sTGsrRLs7arBsXMHPYhbG:2lNnOa+TCXDHzgpvkGghS
MD5:	1A749441CA9410522AA5C91A9C3A7383
SHA1:	E3FC5E978D94CD4DCAA3774571E7ADC59747BA75
SHA-256:	94444C1032EF7F4646267CCD1BE8388FB3AE87E09886C3A976C0680972800242
SHA-512:	A4082069102C31DC7E308E9B4B89B250CF9CFFDEE7585648F1E01D1B7AD5A7FE555DCC053A5656CD913E7C6FFCC8BF208A0C4A4A56995274D311B2ED28E924 8
Malicious:	false
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count ":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[ ],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.go ogleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com"," supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"is olation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"

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):	4915
Entropy (8bit):	4.959601505712836
Encrypted:	false
SSDEEP:	96:nOsXb1IgeT1paAKIlxk0JCKL8rGbOTQVuwn:nPXb1C1p9R4Ks0
MD5:	1B9A4ADF66374682BF57726AC4AED068
SHA1:	8FC196B4B4EC05A945DC25A888FE04CED567B2F1

SHA-256:	584BD08C68189A2F941E3C9A97F9E15C88BCFD71EA6D435D8F05E319CE1BD91D
SHA-512:	C8B510C3A981AB758630D06653AEE4661B86142DE72A0DE2D13A4C79D81830DBDDD7A83CCFC862365EC5EC61BA5C84B362EB7898AE02D2CF51FD4D4CABC1899
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301207817520444","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"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):	5.564318368294512
Encrypted:	false
SSDEEP:	384:XhztuLl/oXr1kXqKf/pUZNCgVLH2HfD9rUBHGYas4nY:eLl6r1kXqKf/pUZNCgVLH2HfJrU1GpsP
MD5:	FD0D4ABA57FE87B942DDAC1A065C0AA0
SHA1:	E8FD106AEFAC584063EE96E89493608F2BC70050
SHA-256:	0BF0882B3997CA8713CE5BD16A489ADCAB58E0E9BABAB4B826E2B9E9D72A1350
SHA-512:	78E9993AD34F84322EE27F739055A90AB01AB9A81B04CF068E2C5BD5F562587EEC6321FC8A84BDD8B608AC65F474FE31A650EAE809B23016C85A6AD3F2F924FB
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":"13301207816625451","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\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898D58
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.95629898779197
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5kjxZsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdSZsBdLJlyH7E4f3K33y
MD5:	D5BB2F0F1694209F0C6AE5BA44DAC338
SHA1:	41B2CDE10C8937FC9607E608AF65EDF709033350
SHA-256:	20FC2ED4DA8AC625B83B6B84C1B88B534BC35B18DC8BD7521C66FFDABAB53738

SHA-512:	A713918E0F88AE62AFAC2A6202107CF547B962900BCB779C7C5C2C8A228C140AAC5191A50BDAF5718EAAE91446DB21648CF2A7B967B9029AF16F13E923FD6E8 2
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544897343531","port":443,"protocol_str":"quic"}],"isol ation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\d5b098ac-4631-4a9e-b4a4-5f95b793f089.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.95629898779197
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5kjxZsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdSZsBdLJlyH7E4f3K33y
MD5:	D5BB2F0F1694209F0C6AE5BA44DAC338
SHA1:	41B2CDE10C8937FC9607E608AF65EDF709033350
SHA-256:	20FC2ED4DA8AC625B83B6B84C1B88B534BC35B18DC8BD7521C66FFDABAB53738
SHA-512:	A713918E0F88AE62AFAC2A6202107CF547B962900BCB779C7C5C2C8A228C140AAC5191A50BDAF5718EAAE91446DB21648CF2A7B967B9029AF16F13E923FD6E8 2
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544897343531","port":443,"protocol_str":"quic"}],"isol ation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\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):	325
Entropy (8bit):	4.958114650763609
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV59YIEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdXXEsBdLJlyH7E4f3K33y
MD5:	F08847672DDD58749FE32FEFD1DBBAE9
SHA1:	C4C1750B297311628D53B0D3DD473F3EDD6019E9
SHA-256:	4165A9C7A2CA81E34A969C02FC75FFA899F49A5B04899EBA10E341C44839CC90
SHA-512:	541C4ADF3A92398F61F1E90C9995FD9CCB668FF51F578968C6CCD73AB81AB24668D969A9F98A1B529F631022EF4A3D224D76B4EDCB656ADADB27A7E4065395A 0
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544901990438","port":443,"protocol_str":"quic"}],"isol ation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\c3374c7e-019a-40ee-bf72-030709ff5750.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.958114650763609
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV59YIEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdXXEsBdLJlyH7E4f3K33y
MD5:	F08847672DDD58749FE32FEFD1DBBAE9
SHA1:	C4C1750B297311628D53B0D3DD473F3EDD6019E9
SHA-256:	4165A9C7A2CA81E34A969C02FC75FFA899F49A5B04899EBA10E341C44839CC90
SHA-512:	541C4ADF3A92398F61F1E90C9995FD9CCB668FF51F578968C6CCD73AB81AB24668D969A9F98A1B529F631022EF4A3D224D76B4EDCB656ADADB27A7E4065395A0
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544901990438","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\a1f83762-104f-4b3c-86cb-f81b59a166c7.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\b7c55baf-1466-4b5b-8ec5-f79a396f70ce.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):	5.564318368294512
Encrypted:	false
SSDEEP:	384:XhztuLl/oXr1kXqKf/pUZNCgVLH2HfD9rUBHGYas4nY:eLl6r1kXqKf/pUZNCgVLH2HfJrU1GpsP
MD5:	FD0D4ABA57FE87B942DDAC1A065C0AA0
SHA1:	E8FD106AEFAC584063EE96E89493608F2BC70050
SHA-256:	0BF0882B3997CA8713CE5BD16A489ADCAB58E0E9BABAB4B826E2B9E9D72A1350
SHA-512:	78E9993AD34F84322EE27F739055A90AB01AB9A81B04CF068E2C5BD5F562587EEC6321FC8A84BDD8B608AC65F474FE31A650EAE809B23016C85A6AD3F2F924FB
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":"13301207816625451","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\bb7097c4-4445-4094-8a93-0f275566722a.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):	5.5770473861640895
Encrypted:	false
SSDEEP:	384:XhztuLl/oXr1kXqKf/pUZNCgVLH2HfD9rUNxos4FB:eLl6r1kXqKf/pUZNCgVLH2HfJrUPos0B
MD5:	882B3A8335B910B663D2D8EE5C2B7BF7
SHA1:	9708D720B795F5E9ECC5BF8F1EAB212AFC256ADD
SHA-256:	CBC41135640EB4EA7ADAE42D6FF3429DEEFCA6ECC4EA917E0177E774E6DE2F32
SHA-512:	5EC74E5D63FB4E030AFFFD9630655B809961084A66FA928BC2770ABFD157C83C8F7E782DE8724206B6447292F72AA86CAF3267DAC5BF00B969F79DD0C54E723
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":"13301207816625451","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\data_reduction_proxy_leveldb\000004.dbtmp

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

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ef0232b0-f2c9-454e-8a64-e82d66657865.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):	1961
Entropy (8bit):	4.895293456334768
Encrypted:	false
SSDEEP:	48:YALteBdpNntw3qyvTCXDHz5sTGsrRLs7arBsXMHPYhbG:2lNnOa+TCXDHzgpvkGghS
MD5:	1A749441CA9410522AA5C91A9C3A7383
SHA1:	E3FC5E978D94CD4DCAA3774571E7ADC59747BA75
SHA-256:	94444C1032EF7F4646267CCD1BE8388FB3AE87E09886C3A976C0680972800242
SHA-512:	A4082069102C31DC7E308E9B4B89B250CF9CFFDEE7585648F1E01D1B7AD5A7FE555DCC053A5656CD913E7C6FFCC8BF208A0C4A4A56995274D311B2ED28E924 8

Malicious:	false
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.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://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f28ac788-1b15-49e6-b6a9-3ff69264f316.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):	2825
Entropy (8bit):	4.86435102445835
Encrypted:	false
SSDEEP:	48:YALtdpBeMsNMHK5sJDysACs37sHWsd5/sSYMHCKs/MHCzsSOMHwsSJtFsX3RLs9D:HQxGKWDS1i/5vYGmGqOGKJ03QshS
MD5:	95488A82D5073BDAAFC1480073FF801F
SHA1:	E2E979B6D4A3EE16A815115C414D0A98E1DFA93F
SHA-256:	C091AE68AFCD5EC632B2C324B983D70F722463CB4D05A3CE8D52E07AA7E5A5D6
SHA-512:	D536466352320C5D394130A59B605617580050CDF325C4B3392D87D384C246E9D8C54FC16A247FF4B379F162536304E0D312D7781FFE245C643C5081B8BE08CD
Malicious:	false
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952675493","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":32613},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952813644","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952748754","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952634896","port":443,"protocol_str":"quic"}],"isolation":[],"server"

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

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

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

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

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

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

File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	409222
Entropy (8bit):	6.026498411403835
Encrypted:	false
SSDEEP:	12288:1NDdqe70oOl9gKVGGNPUZ+w7wJHyEtAWh:1Ge70o4VVxUMkEtAa
MD5:	A2B363FC1B7CA6840E6FA2D6F53643C2
SHA1:	5D719CAA7C7F201D27E7C5B5758F21123F35D363
SHA-256:	A5071F79CD129A7DD5B5A67E5CFC3A15DA0587E992C0D0B1FA7D3AFF16A75436
SHA-512:	8B73B81E81F711EA7E366EF966A1362CC480387B1218F068F36068021C6E10C334481492AA53F2C6A47055A5651FDC2AC3F6AC36ACA0D9C7922B84F6C550D8E8
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":1.656734219020455e+12,"network":1.65670182e+12,"ticks":174968958.0,"uncertainty":4046713.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACulP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230364624763"},"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):	3.751532666840267
Encrypted:	false
SSDEEP:	384:Bv9yyMPtg3geVn52JNKr/v+G31+wdHY1GRYrzQ+0xdgkQnrv2mTntzgqKW5OAMqn:BGeRZKY85ge34qUoXf2+K4mKJt
MD5:	637760753D5017B48184EA1253A1ABA7
SHA1:	1AD2963525CE79D5C475FB6F907E202EBA96E6FE
SHA-256:	8472D748F913952D7F4854E9D3AA66C8B62B4BE28550A605CC8FBB6A7427C033
SHA-512:	7912DB656AAAF78828A9E3AD36FB17C6E13701297C3801783DCBBEFD8CC6D0B6FBEF8FE5790301923A3399F6FFE56057FEE67ECF3AE6F4AD5612C29B1CB297 82
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_dir5412_192052981\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:	D993A324F5D9A1FC4FB3131252F48679750081D996295C994E2DCA4E84F2DECF7E90AF6766EFEDC2CEFC6B66194FFF38181C9E9CE45346BEEB8B3A09CE66BB 73
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...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...W...LT...W...W...W...W.. T...W..

C:\Users\user\AppData\Local\Google\Chrome\User Data\aea53507-d1b9-4e25-8112-37a6b52191e5.tmp

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

Size (bytes):	95428
Entropy (8bit):	3.751532666840267
Encrypted:	false
SSDEEP:	384:Bv9yyMPtg3geVn52JNKr/v+G31+wdHY1GRYrzQ+0xdgkQnrv2mTntzgqKW5OAMqn:BGeRZKY85ge34qUoXf2+K4mKJt
MD5:	637760753D5017B48184EA1253A1ABA7
SHA1:	1AD2963525CE79D5C475FB6F907E202EBA96E6FE
SHA-256:	8472D748F913952D7F4854E9D3AA66C8B62B4BE28550A605CC8FBB6A7427C033
SHA-512:	7912DB656AAAF78828A9E3AD36FB17C6E13701297C3801783DCBBEFD8CC6D0B6FBEF8FE5790301923A3399F6FFE56057FEE67ECF3AE6F4AD5612C29B1CB29782
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\c4d69481-e7c9-454f-8517-0c34bc76516d.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):	408933
Entropy (8bit):	6.025994056274808
Encrypted:	false
SSDEEP:	12288:JNDdqe70oOl9gKVGGNPUZ+w7wJHyEtAWh:JGe70o4VVxUMkEtAa
MD5:	83236CC8D10A4704E09720922844E3C8
SHA1:	27BC1A54E0952531BA364DDD1132B5A8A34353C9
SHA-256:	06915249ACCFC298D6FBB1B9161B66D3AAEFB7C447306DD14DE5EE86C756335C
SHA-512:	0A450DE927C7F7AFAEE121882ECF723FFA90B3BA2DF9EA7350B3B12EA73907A3C6FD0CA52A0A06EF9AEB69491BD2FA08935899242ADDB3F694331533D9C46D0E
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":1.656734219020455e+12,"network":1.65670182e+12,"ticks":174968958.0,"uncertainty":4046713.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230364624763"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\e91058a8-5ed5-4bd0-af37-7524b343cb75.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):	409119
Entropy (8bit):	6.026322103104616
Encrypted:	false
SSDEEP:	12288:zNDdqe70oOl9gKVGGNPUZ+w7wJHyEtAWh:zGe70o4VVxUMkEtAa
MD5:	C498BC24E31B8A266916DDD6EBBBAC06
SHA1:	60DC9429AE8C6A26EEDBE2192FC9DDBA331FF5E2
SHA-256:	2FDF1BC3FABB16CE3F3C54175E5842A7B2E5E7B1F9908686D36529D1A56C74A6
SHA-512:	1A1556F4CF82F4D8B760631C76E99F97FA5D0C1F5F43A3013397090DB1C08648BD1C61F131C7BDBB470DAC69E49FB45CB4604776B4E723D3CF3574CFCB2C0C2
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":1.656734219020455e+12,"network":1.65670182e+12,"ticks":174968958.0,"uncertainty":4046713.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230364624763"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Temp\2d2579c9-4c37-4da6-89e6-380180b88327.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..$.J....+M!.Hz.n`U.l)N.\|b.l....{.K@]6.LlP/....](.A.....l...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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\5412_2066527378\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:ojHlFMJw9iI9Yh9FHc6cPC3CpBHTrDo630a8Q78xRAQudDv4NZ/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\5412_2066527378\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\5412_2066527378_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":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJGaWx0ZXJpbmcgUnVsZXMiLCJyb290X2hhc2giOiJMTF90X0NkWWRYUnpMSHJBZ3hmUW5tcENTaXlkWEtzVVlJZnZjLTR0czRBIn0seyJwYXRoIjoiTElDRU5TRS50eHQiLCJyb290X2hhc2giOiIyaWswNmk0TFlCdVNHNWphRGFIS253NE9pdnVSRzZsQ0JKMVk0TGtzRFJJln0seyJwYXRoIjoibWFuaWZlc3QuanNvbiIsInJvb3RfaGFzaCI6Imo4MmhRZGhaa0MwMjFWOEZ1MHUtMExvMnVJdXI5SzdFem5JcHE3WHd2YlkifV0sImZvcm1hdCI6InRyZWVoYXNoIiwiaGFzaF9ibG9ja19zaXplIjo0MDk2fV0sIml0ZW1faWQiOiJnY21qa21nZGxnbmtrY29jbW9laW1pbmFpam1tam5paSIsIml0ZW1fdmVyc2IvbiI6IjkuMzYuMCIsInByb3RvY29sX3ZlcnNpb24iOjF9","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"VM_rIA1uXuXjbhz_uZ8uQp9F3FfgEgGTjCXL08Q_jrGXXH-Yty1DqAw4yzWsadeOjVRozUf_7kBrYJ2U8Y8slircdLRbrqJejQeyyrJx4HFT8qgZEb60YHdsOd76C57YzF5dXErpjT7_FkWA41lTxLQvdWbACMO0DE7uOHO9mZx5pM98Ni9GsM_yxJbRSyDZWa8BdPHErfMuO6YE6D8tbnYTr2tXcMV9p2ZEAFMiso2B-6DSr

C:\Users\user\AppData\Local\Temp\5412_2066527378\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\5412_2066527378\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\5412_515056959_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":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiO lt7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY19wbmFjbF9qc29uIiwicm9vdF9oYXNoIjoiVkNUSHNJVHNUSXVncWNhV2ctWHVpTU1 sdWloV1FSTE1sQnpTTGprdGhETSJ9LHsicGF0aCI6Il9wbGF0Zm9ybV9zcGVjaWZpYy94ODZfNjQvcG5hY2xfcHVibGljX3g4Nl82NF9jcnRiZWdpbl9mb3JfZWhfbyIsI nJvb3RfaGFzaCI6ImxlNWt2a1BvSVZZczZKVHhyOHc5Q2MxXzloVEJCX3lVSlF6VDZseVVNd0kifSx7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWN sX3B1YmxpY194ODZfNjRfY3J0YmVnaW5fbyIsInJvb3RfaGFzaCI6IkVuLVFQTW1HUm1xbG9Ud1gzOTAzckpsMkw0R25sQmdET1FhZlNKaHJ4Nk0ifSx7InBhdGgiOiJfc GxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY194ODZfNjRfY3J0ZW5kX28iLCJyb290X2hhc2giOiJkT2lJVzRmdEdGNW9FY0k1UXYyYjBmd XNrUlYyaUVtdmxhbmV6MlpFc3VvIn0seyJwYXRoIjoiX3BsYXRmb3JtX3NwZWNpZmljL3g4Nl82NC9wbmFjbF9wdWJsaWNfeDg2XzY0X2xkX25leGUiLCJyb290X2hhc2g iOiIzNEU5QU9EMmpqLWNoMzZQZ0NVV0YtMUpYWVhVdlNGY1I4bks1aWppcWNjIn0seyJwYXRoIjoiX3B

C:\Users\user\AppData\Local\Temp\5412_515056959_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:	59DF2D5F2684FACC80C72F9C4B7E280F705776076C9D843534F772D5A3D578BEE04289AEE81320F23FB4D743F3969EDF5BA53FEBBAC8A4D27F3BC53BCF271C E
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\5412_515056959_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\5412_515056959_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\5412_515056959_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:	FE3F86E926759E71494F2060C4ED3C883EBCAF20CB129A5AD7F142766C33FAB10B5FABC3C7C938E0E895E27EA0AC03CBFE8D0EEABF5300A4AD07F67FD96CC253
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\5412_515056959_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: 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\5412_515056959_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`..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\5412_515056959_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:	01281DE92B281FB29E1ACA96AA64B740B65CC3A9097307827F0D8DB9E1C164C56AFCDFA0BF138EA670A596D55CE2C8D722760744E9FC9343BB6514417BF333E A
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.__div moddi4.__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\5412_515056959_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 ce163f dd0f16b4481e5cf77a16d45e9b4dc8300e) (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\5412_515056959_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\5412_515056959_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:	0B4FF60B5428F81B8B1BCF3328CF80CBD88D8CE5E8BDBC236B06D5A54E7CF26168A3ABB348D87423DA613AB3F0B4D9B37CB5180804839F1CA158EC2B315DD00
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\5412_515056959_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\5412_515056959\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\5412_515056959\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\5412_75593435\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:	6C30728CAC9EAC53F0B27B7DBE2222DA83225C3B63617D6B271A6CFEDF18E8F0A8DFFA1053E1CBC4C5E16625F4BBC0D03AA306A946C9D72FAA4CEB779F8FF CAF
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\5412_75593435_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/hii6zkvVI1Jip2qRNHvakuQkCNFxdsGwmBKkgum91:Rz0kv6cNvaYNFwSEhug
MD5:	45821E6EB1AEC30435949B553DB67807
SHA1:	B3CADEB17FE5B76B5DBB428B8D3A07B341F8B1BC
SHA-256:	E5FAE91295BECF7F66BFA4BE1061CA5537ED763EB5D01485F23ECFB583304FEE
SHA-512:	BCBE40CAFAA4B14566D91E361D8FB7F0288D5C459FA478AA4C575444DA4D406E1076FC0B3A31D4A9E5EE034F0FE15A0EFE8A8A52B838DE94B96D3E488D28F FE
Malicious:	false
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiO lt7InBhdGgiOiJSZWNvdmVyeS5jcngzIiwicm9vdF9oYXNoIjoiaGdCR051SzhNR2NKaDlfNmZQaFdEWmpVYUFKeklzeDlJS21DUEZvb0dfUSJ9LHsicGF0aCI6Im1hbml mZXN0Lmpzb24iLCJyb290X2hhc2giOiIwYXduVFBFQmdDRHkyV05hVVk3Um9mSWN3c3ZwNHFRNUxzZVMxVXRiVXY0In1dLCJmb3JtYXQiOiJ0cmVlaGFzaCI sImhhc2hfYmxvY2tfc2l6ZSI6NDA5Nn1dLCJpdGVtX2lkIjoiaWhubGNlbm9jZWhnZGFlZ2RtaGJpZGpobmhkY2hmbW0iLCJpdGVtX3ZlcnNpb24iOiIxLjMuMzYuMTQxI iwicHJvdG9jb2xfdmVyc2lvbiI6MX0","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"iFuMX_kOZ-zJ7KVu6Lxb3rHWZg QvkZhv25x_SGlBiDV_okALrGbj6rUOWyNNNsHXMnT118XZmA696XR8qkr4dwT5Gvez-9gi-WYBY7XBkgo7v6NspGgJF89BNCeI-P9k-zBHOGgrf-fCEiAcoM7xCx9_f8ql Ry7nhQPyjOIHn5eEJEir0uSu6gdqR9afnVZ3UoR-VOLdOBt7fA4ee38MP2ut5qWU50F5dvIezfKkTVDMHwztvcLCy6R9SVkdSYv6jwWGccYRI-aclvkkHu6SnbZGI7fmDZ dkcBAxBHYEZZMmvb76ro4SO15GDyEVAo_Qf4trdrY_GyN_Bm73imCTjgtoGc

C:\Users\user\AppData\Local\Temp\5412_75593435\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\5412_75593435\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:	064D84A57B28C19AD10742859DA493D0826B47ADC632F6C623DFB4DE36D72A9D29BE98518061A9FFD42D99FCF01F27DE39CE74782B3A5ACBBE11DFDDEEAB5 9A1
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\6ad0a865-d5b4-4a63-8b44-f76c272eb0b4.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F2 5F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\2d2579c9-4c37-4da6-89e6-380180b88327.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:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326 88
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.| 1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u.. ..k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2.. ;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z ....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5SI..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\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:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F770C
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_dir5412_1297531633\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": "Connecteu-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_dir5412_1297531633\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:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D8488SCB
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_dir5412_1297531633\CRX_INSTALL_locales\da\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624

Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5E0A
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_unavailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\de\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\el\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\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:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "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_dir5412_1297531633\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:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "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_dir5412_1297531633\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:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE0128
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_dir5412_1297531633\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:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA53
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_dir5412_1297531633\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_dir5412_1297531633\CRX_INSTALL_locales\fi\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\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:	5F0AE839FCF3F4EA48FF41A76655AE0F3821564AFD5D42FBB9FBB9A38E8D8F7BB5E9B6F71064588CD441261F644095A44A755C134CE546D506D9A21E488BAF5 2
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_dir5412_1297531633\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_dir5412_1297531633\CRX_INSTALL_locales\hi\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\hr\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\hu\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	683
Entropy (8bit):	4.675370843321512
Encrypted:	false
SSDEEP:	12:1HEJVJiGGVJi+WYpU34Hpo9O+dgMmfgijO8ZpU34Huo9O03OyZnLAOfTYBIAYm:1HEVrk5WYpQzTUg/8ZpwoXOGAOfYIAd

MD5:	85609CF8623582A8376C206556ED2131
SHA1:	1E16EB70DB5E59BB684866FF3E3925C2DEF25A12
SHA-256:	32A249749F12ADB6A220BF9ADC272C7E5D9AD5497A38B0086D961E3ABA17FBC6
SHA-512:	27883430865D3CFA6EDFE8C6CE1442BD96150B5CE520CCF7D556A330CAA6392C712B47BD86F7350E174876BC681F6DEC94D1312402655B0AF90883A2899EC78
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. },.. "app_name": {.. "message": "Chrome Internetes .ruh.z Fizet.si r endszere".. },.. "craw_app_unavailable": {.. "message": "Az alkalmaz.s jelenleg nem .rhet. el.".. },.. "craw_connect_to_network": {.. "message": "K.rj.k, csatlako zzon egy h.l.zathoz.".. },.. "iap_unavailable": {.. "message": "Az alkalmaz.son bel.li fizet.s jelenleg nem .rhet. el.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Jelentkezzen be a Chrome-ba.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\id\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\it\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\ja\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	697
Entropy (8bit):	5.20469020877498
Encrypted:	false
SSDEEP:	12:1HEJ07uGG07u+WYpU34DB+dgnsVztO8ZpU34MwiB03OyZnLAOfTYmSH:1HEcnDNWYp1kxU8Zp2wiqOGAOfpSH
MD5:	9B3A5D473C3F2BBFAEECE94A07A940B8
SHA1:	61BACA342CF766BBA15C7B4D892A0E7DAC9405AA
SHA-256:	706312A4A2AEF3317223F141EB2B82685345B7EED444F16BB4DF3A272716DA1F
SHA-512:	94F6FEE9A11BD890AB8211C98D1CC142348961EBCF756F66477A3E3A76519804B70BE0AE4E551739F8AFE32D7ADE6EDE04EF6B9B9EED03E3A857E6058EEDD4 C6
Malicious:	false

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

C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\ko\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\lt\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	665
Entropy (8bit):	4.66839186029557
Encrypted:	false
SSDEEP:	12:1HEJpqHnkGGpqHnk+WYpU346M+dgV6O8ZpU34WzSWz03OyZnLAOfTYx:1HELqHtKqHPWYpM3A8ZpwGzOGAOfg
MD5:	4CA644F875606986A9898D04BDAE3EA5
SHA1:	722A10569E93975129D67FBDB75B537D9D622AD1
SHA-256:	7C311AB751D840D750C11553C083785813E079C1D464FE568A98C9E3EF3DB96C
SHA-512:	E575E3D0622F5BD4B6C0EE79128A1B1F1882195670139D1983F4377D847141B8FB8EBB8BCED82AF3A220ED07D3577AFBE085BADC0E9C7678292B80E3EC5D344
Malicious:	false
Preview:	{.. "app_description": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema".. },.. "app_name": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema".. },.. "craw_app_unavailable": {.. "message": "Programa .iuo metu negalima.".. },.. "craw_connect_to_network": {.. "message": "Prisijunkite prie tinklo.".. },.. "iap_unavailable": {.. "message": "Mok.jimai programoje .iuo metu negalimi.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prisijunkite prie .Chrome..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\lv\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	671
Entropy (8bit):	4.631774066483956
Encrypted:	false
SSDEEP:	12:1HEJFhVbGGFhVb+WYpU34wDoz+dgGedBO8ZpU34wF03OyZnLAOfTYGYID:1HENQKkWYp2Doy/em8Zp2WOGAOfRYID
MD5:	C5CE2C51391EAFD3DA9E4C71549A3C28
SHA1:	1F67FF6EF6E90C0CE3AAF56ED543A3EFD381574D
SHA-256:	1FA1DF2CA8516DEF490FB8484E9AA498ACFF80EEF5C9258FFE42D3678E6C7DED
SHA-512:	C85F6281E682F52BC2147DEA7E2F3BB4DC48D98BADA8687B05C6C7271C78EA7F5431CD51671A4184C9AE004FC53C016E3C594697F483195CCBA08A93821EEF0
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome interneta veikala maks.jumu sist.ma".. },.. "app_name": {.. "message": "Chrome interneta veikala maks.jumu s ist.ma".. },.. "craw_app_unavailable": {.. "message": "Lietotne pagaid.m nav pieejama.".. },.. "craw_connect_to_network": {.. "message": "L.dzu, izveidojiet savienojumu ar t.klu.".. },.. "iap_unavailable": {.. "message": "Maks.jumi lietotn.s pa.laik nav pieejami.".. },.. "jwt_retrieve_failed": {.. "message": "The transacti on could not be completed.".. },.. "please_sign_in": {.. "message": "L.dzu, pierakstieties p.rl.k. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\nb\messages.json

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

Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.555032032637389
Encrypted:	false
SSDEEP:	12:1HEJhiOGGhiO+WYpU34OHSN+dgFjdGFZO8ZpU34JgdN03OyZnLAOfTYiD:1HEDiHIitWYpCYJ8ZpD1OGAOfRD
MD5:	93C459A23BC6953FF744C35920CD2AF9
SHA1:	162F884972103A08ADB616A7EB3598431A2924C5
SHA-256:	2CD700AEB57D89C2E73333D0702556EE3FF3863516170F85669BC680FCBDC4E0
SHA-512:	F76E6E8D8499306883C3EC1E774F7E8BB6B601096DA5A14D17D3E7D5732829542041E42B7350466589291ADCC83FB065FD591B4E20CFCF8EDC586E128ECBFCB5
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Nettmarked-betalinger".. },.. "app_name": {.. "message": "Chrome Nettmarked-betalinger".. },.. "craw_app_unavailable": {.. "message": "Appen er utilgjengelig for .yeblikket.".. },.. "craw_connect_to_network": {.. "message": "Du m. koble til et nettverk.".. },.. "iap_unavailable": {.. "message": "Betaling i app er ikke tilgjengelig for .yeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Du m. logge p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\nl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	615
Entropy (8bit):	4.4715318546237315
Encrypted:	false
SSDEEP:	12:1HEJJQGkbGGJQGkb+WYpU34OQKJT+dgiXUmvFZO8ZpU34g7JT03OyZnLAOfTYMD:1HErxkaqxk6WYptndXl8ZpTOGAOfbD
MD5:	7A8F9D0249C680F64DEC7650A432BD57
SHA1:	53477198AEE389F6580921B4876719B400A23CA1
SHA-256:	92BE7C2DC9CFBE5A65E9CE6488D364C8D7EC19E7B67A31E4D43C1CB2B169671C
SHA-512:	969AB979546A741C0F3EDBEEB21BABA375FA8870D4FB9248CDD4C305736E332E10CAB7B64C5C078E60EC0CD73848101B390BE8F44B89C310058AF4C1CA3C8A7
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Betalingen via Chrome Web Store".. },.. "app_name": {.. "message": "Betalingen via Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "App momenteel niet beschikbaar.".. },.. "craw_connect_to_network": {.. "message": "Maak verbinding met een netwerk.".. },.. "iap_unavailable": {.. "message": "In-app-betalingen is momenteel niet beschikbaar.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log in bij Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5412_1297531633\CRX_INSTALL_locales\pl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	636
Entropy (8bit):	4.646901997539488
Encrypted:	false
SSDEEP:	12:1HEJbiVbGGbiVb+WYpU34OBHlBi9+dgQUg6O8ZpU34bdbfilu03OyZnLAOfTYR5k:1HE5iVauiV6WYpIAYr8ZpxFiaOGAOflC
MD5:	0E6194126AFCCD1E3098D276A7400175
SHA1:	E8127B905A640B1C46362FA6E1127BE172F4A40F
SHA-256:	E2699F98C511B18A2AFB82EAE9A4804B646C4FF1077D80E77C17A3943A6373C2
SHA-512:	A71F7C7BFBBF1E37E699601AF2E095C56CBA91F90CB7556477DF31D01B83ADFB1271E1775C9BA299FF6875BBFC2B6AB47488CC88E33DEF2F6F2E0E5AC687B777
Malicious:	false
Preview:	{.. "app_description": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "app_name": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Aplikacja jest obecnie niedost.pna.".. },.. "craw_connect_to_network": {.. "message": "Po..cz si. z sieci..".. },.. "iap_unavailable": {.. "message": "P.atno.ci w ramach aplikacji s. teraz niedost.pne.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Zaloguj si. w Chrome.".. }..}..

Static File Info

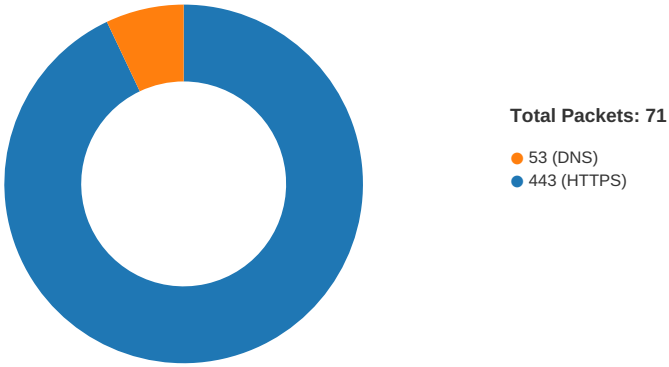
General

File type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Entropy (8bit):	5.494595862449742
TrID:	• HyperText Markup Language (31031/1) 100.00%

File name:	ClosingDoc.html
File size:	13026
MD5:	3755ba4cfcde83ecc11643096b157366
SHA1:	058fa6f78bf7369e33c0881cb8bf6d07a6bbb9ba
SHA256:	1b174509a2b0400085d634439672ed977c4cd733537ad47e6c0061d4d60c767a
SHA512:	2b3ba3734e05d7ce5917809fefb4f74e6f7cb423c07d7e20684c87dfc05c4dcc8f0294af9eea66df63a563a8128e93aa94d68430384ee2210856706c50285ece
SSDEEP:	384:qzhN62qXvhMhKehjpEEJPe680mmRM970OEZfl4mEZN38R0:q1KvhMhKehjGEJPe680mmRM99Mfl4lN1
TLSH:	4C42EA80FE96802E4C450E991F7DEC29E5DF9C751DE89322EB4688DDB5CC860C5B8CB9
File Content Preview:	<script type="text/javascript">..// <![CDATA[..function rot13(i){return i.replace(/[a-zA-Z]/g,function(c){return String.fromCharCode((c<="Z"?90:122)>=(c=c.charCodeAt(0)+13)?c:c-26)})}..function WriteHTMLtoJS(){..document.write(rot13("<?cuc\nvs (vffrg($_TR

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 1, 2022 20:56:59.650552988 CEST	49752	443	192.168.2.6	152.199.23.37
Jul 1, 2022 20:56:59.650594950 CEST	443	49752	152.199.23.37	192.168.2.6
Jul 1, 2022 20:56:59.650655031 CEST	49753	443	192.168.2.6	152.199.23.37
Jul 1, 2022 20:56:59.650686026 CEST	443	49753	152.199.23.37	192.168.2.6
Jul 1, 2022 20:56:59.650769949 CEST	49753	443	192.168.2.6	152.199.23.37
Jul 1, 2022 20:56:59.651458025 CEST	49754	443	192.168.2.6	152.199.23.37
Jul 1, 2022 20:56:59.651495934 CEST	49752	443	192.168.2.6	152.199.23.37
Jul 1, 2022 20:56:59.651506901 CEST	443	49754	152.199.23.37	192.168.2.6
Jul 1, 2022 20:56:59.651593924 CEST	49754	443	192.168.2.6	152.199.23.37
Jul 1, 2022 20:56:59.652249098 CEST	49756	443	192.168.2.6	172.217.16.205
Jul 1, 2022 20:56:59.652280092 CEST	443	49756	172.217.16.205	192.168.2.6
Jul 1, 2022 20:56:59.652355909 CEST	49756	443	192.168.2.6	172.217.16.205
Jul 1, 2022 20:56:59.652688026 CEST	49757	443	192.168.2.6	142.250.185.142
Jul 1, 2022 20:56:59.652719975 CEST	443	49757	142.250.185.142	192.168.2.6
Jul 1, 2022 20:56:59.652889013 CEST	49757	443	192.168.2.6	142.250.185.142
Jul 1, 2022 20:56:59.654237032 CEST	49752	443	192.168.2.6	152.199.23.37
Jul 1, 2022 20:56:59.654262066 CEST	443	49752	152.199.23.37	192.168.2.6
Jul 1, 2022 20:56:59.661186934 CEST	49753	443	192.168.2.6	152.199.23.37
Jul 1, 2022 20:56:59.661225080 CEST	443	49753	152.199.23.37	192.168.2.6
Jul 1, 2022 20:56:59.661474943 CEST	49754	443	192.168.2.6	152.199.23.37
Jul 1, 2022 20:56:59.661504030 CEST	443	49754	152.199.23.37	192.168.2.6
Jul 1, 2022 20:56:59.661856890 CEST	49756	443	192.168.2.6	172.217.16.205
Jul 1, 2022 20:56:59.661886930 CEST	443	49756	172.217.16.205	192.168.2.6
Jul 1, 2022 20:56:59.662316084 CEST	49757	443	192.168.2.6	142.250.185.142
Jul 1, 2022 20:56:59.662343979 CEST	443	49757	142.250.185.142	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 1, 2022 20:56:59.662708044 CEST	49758	443	192.168.2.6	13.107.219.60
Jul 1, 2022 20:56:59.662736893 CEST	443	49758	13.107.219.60	192.168.2.6
Jul 1, 2022 20:56:59.662838936 CEST	49758	443	192.168.2.6	13.107.219.60
Jul 1, 2022 20:56:59.663167953 CEST	49758	443	192.168.2.6	13.107.219.60
Jul 1, 2022 20:56:59.663186073 CEST	443	49758	13.107.219.60	192.168.2.6
Jul 1, 2022 20:56:59.717387915 CEST	443	49757	142.250.185.142	192.168.2.6
Jul 1, 2022 20:56:59.720567942 CEST	49757	443	192.168.2.6	142.250.185.142
Jul 1, 2022 20:56:59.720588923 CEST	443	49757	142.250.185.142	192.168.2.6
Jul 1, 2022 20:56:59.721013069 CEST	443	49757	142.250.185.142	192.168.2.6
Jul 1, 2022 20:56:59.721571922 CEST	443	49756	172.217.16.205	192.168.2.6
Jul 1, 2022 20:56:59.721854925 CEST	443	49757	142.250.185.142	192.168.2.6
Jul 1, 2022 20:56:59.721889019 CEST	49757	443	192.168.2.6	142.250.185.142
Jul 1, 2022 20:56:59.721905947 CEST	443	49757	142.250.185.142	192.168.2.6
Jul 1, 2022 20:56:59.721941948 CEST	49757	443	192.168.2.6	142.250.185.142
Jul 1, 2022 20:56:59.722049952 CEST	443	49752	152.199.23.37	192.168.2.6
Jul 1, 2022 20:56:59.727895975 CEST	49756	443	192.168.2.6	172.217.16.205
Jul 1, 2022 20:56:59.727930069 CEST	443	49756	172.217.16.205	192.168.2.6
Jul 1, 2022 20:56:59.729331017 CEST	49752	443	192.168.2.6	152.199.23.37
Jul 1, 2022 20:56:59.729340076 CEST	443	49754	152.199.23.37	192.168.2.6
Jul 1, 2022 20:56:59.729379892 CEST	443	49752	152.199.23.37	192.168.2.6
Jul 1, 2022 20:56:59.729875088 CEST	49754	443	192.168.2.6	152.199.23.37
Jul 1, 2022 20:56:59.729907990 CEST	443	49754	152.199.23.37	192.168.2.6
Jul 1, 2022 20:56:59.730326891 CEST	443	49753	152.199.23.37	192.168.2.6
Jul 1, 2022 20:56:59.730493069 CEST	443	49752	152.199.23.37	192.168.2.6
Jul 1, 2022 20:56:59.730664015 CEST	49752	443	192.168.2.6	152.199.23.37
Jul 1, 2022 20:56:59.730860949 CEST	49753	443	192.168.2.6	152.199.23.37
Jul 1, 2022 20:56:59.730889082 CEST	443	49753	152.199.23.37	192.168.2.6
Jul 1, 2022 20:56:59.731182098 CEST	443	49756	172.217.16.205	192.168.2.6
Jul 1, 2022 20:56:59.731281042 CEST	49756	443	192.168.2.6	172.217.16.205
Jul 1, 2022 20:56:59.731817961 CEST	443	49754	152.199.23.37	192.168.2.6
Jul 1, 2022 20:56:59.731924057 CEST	49754	443	192.168.2.6	152.199.23.37
Jul 1, 2022 20:56:59.733412981 CEST	443	49753	152.199.23.37	192.168.2.6
Jul 1, 2022 20:56:59.733431101 CEST	443	49758	13.107.219.60	192.168.2.6
Jul 1, 2022 20:56:59.733537912 CEST	49753	443	192.168.2.6	152.199.23.37
Jul 1, 2022 20:56:59.733889103 CEST	49758	443	192.168.2.6	13.107.219.60
Jul 1, 2022 20:56:59.733952045 CEST	443	49758	13.107.219.60	192.168.2.6
Jul 1, 2022 20:56:59.735017061 CEST	443	49758	13.107.219.60	192.168.2.6
Jul 1, 2022 20:56:59.735166073 CEST	49758	443	192.168.2.6	13.107.219.60
Jul 1, 2022 20:56:59.816518068 CEST	49757	443	192.168.2.6	142.250.185.142
Jul 1, 2022 20:57:00.409077883 CEST	49752	443	192.168.2.6	152.199.23.37
Jul 1, 2022 20:57:00.409285069 CEST	443	49752	152.199.23.37	192.168.2.6
Jul 1, 2022 20:57:00.409497023 CEST	49756	443	192.168.2.6	172.217.16.205
Jul 1, 2022 20:57:00.409638882 CEST	49757	443	192.168.2.6	142.250.185.142
Jul 1, 2022 20:57:00.409704924 CEST	443	49756	172.217.16.205	192.168.2.6
Jul 1, 2022 20:57:00.409853935 CEST	443	49757	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:00.411454916 CEST	49758	443	192.168.2.6	13.107.219.60
Jul 1, 2022 20:57:00.411623955 CEST	443	49758	13.107.219.60	192.168.2.6
Jul 1, 2022 20:57:00.411633968 CEST	49754	443	192.168.2.6	152.199.23.37
Jul 1, 2022 20:57:00.411792040 CEST	443	49754	152.199.23.37	192.168.2.6
Jul 1, 2022 20:57:00.412892103 CEST	49753	443	192.168.2.6	152.199.23.37
Jul 1, 2022 20:57:00.413127899 CEST	443	49753	152.199.23.37	192.168.2.6
Jul 1, 2022 20:57:00.413362980 CEST	49752	443	192.168.2.6	152.199.23.37
Jul 1, 2022 20:57:00.413393974 CEST	443	49752	152.199.23.37	192.168.2.6
Jul 1, 2022 20:57:00.413621902 CEST	49756	443	192.168.2.6	172.217.16.205
Jul 1, 2022 20:57:00.413647890 CEST	443	49756	172.217.16.205	192.168.2.6
Jul 1, 2022 20:57:00.413743973 CEST	49757	443	192.168.2.6	142.250.185.142
Jul 1, 2022 20:57:00.413760900 CEST	443	49757	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:00.414211988 CEST	49758	443	192.168.2.6	13.107.219.60
Jul 1, 2022 20:57:00.414237976 CEST	443	49758	13.107.219.60	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 1, 2022 20:57:00.414279938 CEST	49754	443	192.168.2.6	152.199.23.37
Jul 1, 2022 20:57:00.414316893 CEST	443	49754	152.199.23.37	192.168.2.6
Jul 1, 2022 20:57:00.414381981 CEST	49753	443	192.168.2.6	152.199.23.37
Jul 1, 2022 20:57:00.414407969 CEST	443	49753	152.199.23.37	192.168.2.6
Jul 1, 2022 20:57:00.434899092 CEST	443	49758	13.107.219.60	192.168.2.6
Jul 1, 2022 20:57:00.434911013 CEST	443	49752	152.199.23.37	192.168.2.6
Jul 1, 2022 20:57:00.434981108 CEST	49758	443	192.168.2.6	13.107.219.60
Jul 1, 2022 20:57:00.435003996 CEST	443	49758	13.107.219.60	192.168.2.6
Jul 1, 2022 20:57:00.435022116 CEST	443	49758	13.107.219.60	192.168.2.6
Jul 1, 2022 20:57:00.435043097 CEST	49752	443	192.168.2.6	152.199.23.37
Jul 1, 2022 20:57:00.435059071 CEST	443	49752	152.199.23.37	192.168.2.6
Jul 1, 2022 20:57:00.435082912 CEST	443	49752	152.199.23.37	192.168.2.6
Jul 1, 2022 20:57:00.435092926 CEST	49758	443	192.168.2.6	13.107.219.60
Jul 1, 2022 20:57:00.435162067 CEST	49752	443	192.168.2.6	152.199.23.37
Jul 1, 2022 20:57:00.436729908 CEST	443	49754	152.199.23.37	192.168.2.6
Jul 1, 2022 20:57:00.436803102 CEST	443	49754	152.199.23.37	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 1, 2022 20:56:59.607244968 CEST	51748	53	192.168.2.6	8.8.8.8
Jul 1, 2022 20:56:59.607728004 CEST	61116	53	192.168.2.6	8.8.8.8
Jul 1, 2022 20:56:59.609332085 CEST	50958	53	192.168.2.6	8.8.8.8
Jul 1, 2022 20:56:59.610646963 CEST	49695	53	192.168.2.6	8.8.8.8
Jul 1, 2022 20:56:59.632010937 CEST	53	61116	8.8.8.8	192.168.2.6
Jul 1, 2022 20:56:59.637995958 CEST	53	51748	8.8.8.8	192.168.2.6
Jul 1, 2022 20:56:59.638426065 CEST	53	49695	8.8.8.8	192.168.2.6
Jul 1, 2022 20:57:01.659256935 CEST	51666	53	192.168.2.6	8.8.8.8
Jul 1, 2022 20:57:01.679250002 CEST	53	51666	8.8.8.8	192.168.2.6
Jul 1, 2022 20:57:10.410531998 CEST	52091	443	192.168.2.6	142.250.185.142
Jul 1, 2022 20:57:10.437146902 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:10.466590881 CEST	52091	443	192.168.2.6	142.250.185.142
Jul 1, 2022 20:57:10.492902994 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:10.492961884 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:10.493002892 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:10.493043900 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:10.616821051 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:10.616863966 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:10.616890907 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:10.616914988 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:10.763015985 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:10.763045073 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:10.763062954 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:10.763079882 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:11.056320906 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:11.056355000 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:11.056380987 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:11.056389093 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:11.640305042 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:11.640341997 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:11.640360117 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:11.640373945 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:12.681159973 CEST	52091	443	192.168.2.6	142.250.185.142
Jul 1, 2022 20:57:12.700391054 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:12.700427055 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:12.741673946 CEST	52091	443	192.168.2.6	142.250.185.142
Jul 1, 2022 20:57:12.751703024 CEST	52091	443	192.168.2.6	142.250.185.142
Jul 1, 2022 20:57:12.751874924 CEST	52091	443	192.168.2.6	142.250.185.142
Jul 1, 2022 20:57:12.752037048 CEST	52091	443	192.168.2.6	142.250.185.142

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 1, 2022 20:57:12.752121925 CEST	52091	443	192.168.2.6	142.250.185.142
Jul 1, 2022 20:57:12.752190113 CEST	52091	443	192.168.2.6	142.250.185.142
Jul 1, 2022 20:57:12.752394915 CEST	52091	443	192.168.2.6	142.250.185.142
Jul 1, 2022 20:57:12.752456903 CEST	52091	443	192.168.2.6	142.250.185.142
Jul 1, 2022 20:57:12.752531052 CEST	52091	443	192.168.2.6	142.250.185.142
Jul 1, 2022 20:57:12.752603054 CEST	52091	443	192.168.2.6	142.250.185.142
Jul 1, 2022 20:57:12.768074036 CEST	52091	443	192.168.2.6	142.250.185.142
Jul 1, 2022 20:57:12.770061970 CEST	52091	443	192.168.2.6	142.250.185.142
Jul 1, 2022 20:57:12.801403046 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:12.803262949 CEST	52091	443	192.168.2.6	142.250.185.142
Jul 1, 2022 20:57:12.813108921 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:12.813138008 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:12.813152075 CEST	443	52091	142.250.185.142	192.168.2.6
Jul 1, 2022 20:57:12.814902067 CEST	52091	443	192.168.2.6	142.250.185.142
Jul 1, 2022 20:57:12.840781927 CEST	52091	443	192.168.2.6	142.250.185.142

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 1, 2022 20:56:59.607244968 CEST	192.168.2.6	8.8.8.8	0x8e69	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jul 1, 2022 20:56:59.607728004 CEST	192.168.2.6	8.8.8.8	0x79bd	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
Jul 1, 2022 20:56:59.609332085 CEST	192.168.2.6	8.8.8.8	0xf6ca	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jul 1, 2022 20:56:59.610646963 CEST	192.168.2.6	8.8.8.8	0x59d0	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jul 1, 2022 20:57:01.659256935 CEST	192.168.2.6	8.8.8.8	0xa0a4	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 1, 2022 20:56:59.630891085 CEST	8.8.8.8	192.168.2.6	0xf6ca	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 1, 2022 20:56:59.632010937 CEST	8.8.8.8	192.168.2.6	0x79bd	No error (0)	aadcdn.msftauth.net	cs1100.wpc.omegacdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 1, 2022 20:56:59.632010937 CEST	8.8.8.8	192.168.2.6	0x79bd	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Jul 1, 2022 20:56:59.637995958 CEST	8.8.8.8	192.168.2.6	0x8e69	No error (0)	accounts.google.com		172.217.16.205	A (IP address)	IN (0x0001)
Jul 1, 2022 20:56:59.638426065 CEST	8.8.8.8	192.168.2.6	0x59d0	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 1, 2022 20:56:59.638426065 CEST	8.8.8.8	192.168.2.6	0x59d0	No error (0)	clients.l.google.com		142.250.185.142	A (IP address)	IN (0x0001)
Jul 1, 2022 20:56:59.652978897 CEST	8.8.8.8	192.168.2.6	0x2fc9	No error (0)	dual.part-0032.t-0009.t-msedge.net	global-entry-afdthirdparty-fallback.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jul 1, 2022 20:56:59.652978897 CEST	8.8.8.8	192.168.2.6	0x2fc9	No error (0)	dual.part-0032.t-0009.fbs1-t-msedge.net	part-0032.t-0009.fbs1-t-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jul 1, 2022 20:56:59.652978897 CEST	8.8.8.8	192.168.2.6	0x2fc9	No error (0)	part-0032.t-0009.fbs1-t-msedge.net		13.107.219.60	A (IP address)	IN (0x0001)
Jul 1, 2022 20:56:59.652978897 CEST	8.8.8.8	192.168.2.6	0x2fc9	No error (0)	part-0032.t-0009.fbs1-t-msedge.net		13.107.227.60	A (IP address)	IN (0x0001)
Jul 1, 2022 20:57:01.542516947 CEST	8.8.8.8	192.168.2.6	0xe482	No error (0)	dual.part-0032.t-0009.t-msedge.net	global-entry-afdthirdparty-fallback.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jul 1, 2022 20:57:01.542516947 CEST	8.8.8.8	192.168.2.6	0xe482	No error (0)	dual.part-0032.t-0009.fbs1-t-msedge.net	part-0032.t-0009.fbs1-t-msedge.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 1, 2022 20:57:01.542516947 CEST	8.8.8.8	192.168.2.6	0xe482	No error (0)	part-0032.t-0009.fbs1-t-msedge.net		13.107.219.60	A (IP address)	IN (0x0001)
Jul 1, 2022 20:57:01.542516947 CEST	8.8.8.8	192.168.2.6	0xe482	No error (0)	part-0032.t-0009.fbs1-t-msedge.net		13.107.227.60	A (IP address)	IN (0x0001)
Jul 1, 2022 20:57:01.679250002 CEST	8.8.8.8	192.168.2.6	0xa0a4	No error (0)	aadcdn.msftauth.net	cs1100.wpc.omegacdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 1, 2022 20:57:01.679250002 CEST	8.8.8.8	192.168.2.6	0xa0a4	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- aadcdn.msftauth.net
- accounts.google.com
- clients2.google.com
- aadcdn.msauth.net

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49752	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 18:57:00 UTC	0	OUT	GET /shared/1.0/content/images/applogos/53_8b36337037cff88c3df203bb73d58e41.png HTTP/1.1 Host: aadcdn.msftauth.net 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
2022-07-01 18:57:00 UTC	3	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Length,Date,Transfer-Encoding Age: 833388 Cache-Control: public, max-age=31536000 Content-MD5: izYzcDfP+Iw98gO7c9WOQQ== Content-Type: image/png Date: Fri, 01 Jul 2022 18:57:00 GMT Etag: 0x8D7AF695D6C58F2 Last-Modified: Wed, 12 Feb 2020 03:12:17 GMT Server: ECAcc (frc/8FBC) X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 1182cd20-c01e-004f-3ae7-851dc4000000 x-ms-version: 2009-09-19 Content-Length: 5139 Connection: close
2022-07-01 18:57:00 UTC	5	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 56 00 00 00 48 08 06 00 00 00 ad 04 dd dc 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 03 25 69 54 58 74 58 4d 4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 00 00 00 00 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 36 2d 63 31 34 38 20 37 39 2e 31 36 34 30 33 36 2c 20 32 30 31 39 2f 30 38 2f 31 33 2d 30 31 3a 30 36 3a 35 37 20 20 Data Ascii: PNGIHDRVHtEXtSoftwareAdobe ImageReadyqe<%iTXtXML:com.adobe.xmp<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49756	172.217.16.205	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 18:57:00 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
2022-07-01 18:57:00 UTC	0	OUT	Data Raw: 20 Data Ascii:
2022-07-01 18:57:00 UTC	18	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: Fri, 01 Jul 2022 18:57:00 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains 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=* Content-Security-Policy: script-src 'report-sample' 'nonce-tqYaZrQ1VOt65Xt1We3JxQ' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'nonce-tqYaZrQ1VOt65Xt1We3JxQ' '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 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 Report-To: {"group":"IdentityListAccountsHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external"}]} Cross-Origin-Opener-Policy: same-origin; report-to="IdentityListAccountsHttp" 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
2022-07-01 18:57:00 UTC	20	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",[]]
2022-07-01 18:57:00 UTC	20	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.6	49780	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 18:57:01 UTC	57	OUT	GET /shared/1.0/content/images/applogos/53_8b36337037cff88c3df203bb73d58e41.png HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: aadcdn.msftauth.net

Timestamp	kBytes transferred	Direction	Data
2022-07-01 18:57:01 UTC	63	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Length,Date,Transfer-Encoding Age: 833389 Cache-Control: public, max-age=31536000 Content-MD5: izYzcDfP+Iw98gO7c9WOQQ== Content-Type: image/png Date: Fri, 01 Jul 2022 18:57:01 GMT Etag: 0x8D7AF695D6C58F2 Last-Modified: Wed, 12 Feb 2020 03:12:17 GMT Server: ECAcc (frc/8FBC) X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 1182cd20-c01e-004f-3ae7-851dc4000000 x-ms-version: 2009-09-19 Content-Length: 5139 Connection: close
2022-07-01 18:57:01 UTC	63	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 56 00 00 00 48 08 06 00 00 00 ad 04 dd dc 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 03 25 69 54 58 74 58 4d 4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 00 00 00 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 36 2d 63 31 34 38 20 37 39 2e 31 36 34 30 33 36 2c 20 32 30 31 39 2f 30 38 2f 31 33 2d 30 31 3a 30 36 3a 35 37 20 20 Data Ascii: PNGIHDRVHtEXtSoftwareAdobe ImageReadyqe<%iTXtXML:com.adobe.xmp<?xpacket begin="" id="W5M 0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.6	49782	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 18:57:01 UTC	68	OUT	GET /shared/1.0/content/images/signin-options_4e48046ce74f4b89d45037c90576bfac.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: aadcdn.msftauth.net
2022-07-01 18:57:01 UTC	69	IN	HTTP/1.1 200 OK Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Age: 29356739 Cache-Control: public, max-age=31536000 Content-MD5: R2FAVxfpONfnQAuxVxXbHg== Content-Type: image/svg+xml Date: Fri, 01 Jul 2022 18:57:01 GMT Etag: 0x8D8852A740F01B9 Last-Modified: Tue, 10 Nov 2020 03:41:05 GMT Server: ECAcc (frc/8FFC) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: a3f9aa36-901e-008e-257c-82e72e000000 x-ms-version: 2009-09-19 Content-Length: 1592 Connection: close
2022-07-01 18:57:01 UTC	69	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 34 38 22 20 68 65 69 67 68 74 3d 22 34 38 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 34 38 20 34 38 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 61 7b 66 69 6c 6c 3a 6e 6f 6e 65 3b 7d 2e 62 7b 66 69 6c 6c 3a 23 34 30 34 30 34 30 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 72 65 63 74 20 63 6c 61 73 73 3d 22 61 22 20 77 69 64 74 68 3d 22 34 38 22 20 68 65 69 67 68 74 3d 22 34 38 22 2f 3e 3c 70 61 74 68 20 63 6c 61 73 73 3d 22 62 22 20 64 3d 22 4d 34 30 2c 33 32 2e 35 37 38 56 34 30 48 33 32 56 33 36 48 32 38 56 33 32 48 32 34 56 32 38 2e 37 36 36 41 31 30 2e 36 38 39 2c 31 30 2e 36 38 39 2c 30 2c 30 2c Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="48" height="48" viewBox="0 0 48 48"><defs><style>.a {fill:none;}.b{fill:#404040;}</style></defs><rect class="a" width="48" height="48"/><path class="b" d="M40,32.578V40H32V36H28V32H24V28.766A10.689,10.689,0,0,

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49757	142.250.185.142	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 18:57:00 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
2022-07-01 18:57:00 UTC	17	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-5WbciJbOhTqrTfkTtvz0kQ' '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: Fri, 01 Jul 2022 18:57:00 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5660 X-Daystart: 43020 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
2022-07-01 18:57:00 UTC	17	IN	Data Raw: 33 31 62 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 36 30 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 34 33 30 32 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: 31b<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" protocol="2.0" server="prod"><daystart elapsed_days="5660" elapsed_seconds="43020"/><app appid="nmmhkkegccagdldgiimedpiccmgmieda" cohort="1::" cohortname=""
2022-07-01 18:57:00 UTC	18	IN	Data Raw: 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 7a 65 3d 22 32 34 38 35 33 31 22 20 73 74 61 74 75 73 3d 22 6f 6b 22 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 2e 30 2e 36 22 2f 3e 3c 2f 61 70 70 3e 3c 61 Data Ascii: mmhkkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" size="248531" status="ok" version="1.0.0.6"/></app><a
2022-07-01 18:57:00 UTC	18	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49758	13.107.219.60	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 18:57:00 UTC	1	OUT	GET /shared/1.0/content/images/appbackgrounds/49-small_e58aafc980614a9cd7796bea7b5ea8f0.jpg HTTP/1.1 Host: aadcdn.msauth.net 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

Timestamp	kBytes transferred	Direction	Data
2022-07-01 18:57:00 UTC	3	IN	HTTP/1.1 200 OK Cache-Control: public, max-age=31536000 Content-Length: 987 Content-Type: image/jpeg Content-MD5: 5YqvyYBhSpzXeWvqe16o8A== Last-Modified: Fri, 27 Mar 2020 19:41:47 GMT ETag: 0x8D7D286E322A911 X-Cache: TCP_HIT Server: Windows-Azure-Blob/1.0 Microsoft-HTTPAPI/2.0 x-ms-request-id: 72e47f8d-001e-002f-6c58-8a2f5f000000 x-ms-version: 2009-09-19 x-ms-lease-status: unlocked x-ms-blob-type: BlockBlob Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Access-Control-Allow-Origin: * X-Azure-Ref: 0fEO/YgAAAAAmIhdG0C7zQa4kezh5MM7FRlJBMjMxMDUwNDE3MDI3ADM5YTEyZjdlLTg5OWYtNDZjZi1hNmQwLTI0YmJiYTI3ZDk1Ng== Date: Fri, 01 Jul 2022 18:57:00 GMT Connection: close
2022-07-01 18:57:00 UTC	4	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 48 00 48 00 00 ff e1 00 66 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 04 01 1a 00 05 00 00 00 01 00 00 00 3e 01 1b 00 05 00 00 00 01 00 00 00 46 01 28 00 03 00 00 00 01 00 02 00 00 01 31 00 02 00 00 00 10 00 00 00 4e 00 00 00 00 00 00 00 48 00 00 00 01 00 00 00 48 00 00 00 01 70 61 69 6e 74 2e 6e 65 74 20 34 2e 32 2e 39 00 ff db 00 43 00 02 01 01 01 01 01 02 01 01 01 02 02 02 02 02 04 03 02 02 02 02 05 04 04 03 04 06 05 06 06 06 05 06 06 06 07 09 08 06 07 09 07 06 06 08 0b 08 09 0a 0a 0a 0a 0a 06 08 0b 0c 0b 0a 0c 09 0a 0a 0a ff db 00 43 01 02 02 02 02 02 02 05 03 03 05 0a 07 06 07 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a Data Ascii: JFIFHHfExifMM*>F(1NHHpaint.net 4.2.9CC

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49754	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 18:57:00 UTC	2	OUT	GET /shared/1.0/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg HTTP/1.1 Host: aadcdn.msftauth.net 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
2022-07-01 18:57:00 UTC	10	IN	HTTP/1.1 200 OK Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Length,Date,Transfer-Encoding Age: 5319271 Cache-Control: public, max-age=31536000 Content-MD5: nzaLxFgP7ZB3dfMcaybWzw== Content-Type: image/svg+xml Date: Fri, 01 Jul 2022 18:57:00 GMT Etag: 0x8D79A1B9F5E121A Last-Modified: Thu, 16 Jan 2020 00:32:52 GMT Server: ECAcc (frc/8E9E) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 3d61ac0e-001e-004e-351b-5de3c9000000 x-ms-version: 2009-09-19 Content-Length: 3651 Connection: close
2022-07-01 18:57:00 UTC	11	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 30 38 22 20 68 65 69 67 68 74 3d 22 32 34 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 31 30 38 20 32 34 22 3e 3c 74 69 74 6c 65 3e 61 73 73 65 74 73 3c 2f 74 69 74 6c 65 3e 3c 70 61 74 68 20 64 3d 22 4d 34 34 2e 38 33 36 2c 34 2e 36 56 31 38 2e 34 68 2d 32 2e 34 56 37 2e 35 38 33 48 34 32 2e 34 4c 33 38 2e 31 31 39 2c 31 38 2e 34 48 33 36 2e 35 33 31 4c 33 32 2e 31 34 32 2c 37 2e 35 38 33 68 2d 2e 30 32 39 56 31 38 2e 34 48 32 39 2e 39 56 34 2e 36 68 33 2e 34 33 36 4c 33 37 2e 33 2c 31 34 2e 38 33 68 2e 30 35 38 4c 34 31 2e 35 34 35 2c 34 2e 36 5a 6d 32 2c 31 2e 30 34 39 61 31 2e 32 36 38 2c 31 2e 32 36 38 2c 30 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38.119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49753	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 18:57:00 UTC	2	OUT	GET /shared/1.0/content/images/signin-options_4e48046ce74f4b89d45037c90576bfac.svg HTTP/1.1 Host: aadcdn.msftauth.net 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
2022-07-01 18:57:00 UTC	14	IN	HTTP/1.1 200 OK Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Age: 29356738 Cache-Control: public, max-age=31536000 Content-MD5: R2FAVxfpONfnQAuxVxXbHg== Content-Type: image/svg+xml Date: Fri, 01 Jul 2022 18:57:00 GMT Etag: 0x8D8852A740F01B9 Last-Modified: Tue, 10 Nov 2020 03:41:05 GMT Server: ECAcc (frc/8FFC) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: a3f9aa36-901e-008e-257c-82e72e000000 x-ms-version: 2009-09-19 Content-Length: 1592 Connection: close
2022-07-01 18:57:00 UTC	15	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 34 38 22 20 68 65 69 67 68 74 3d 22 34 38 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 34 38 20 34 38 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 61 7b 66 69 6c 6c 3a 6e 6f 6e 65 3b 7d 2e 62 7b 66 69 6c 6c 3a 23 34 30 34 30 34 30 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 72 65 63 74 20 63 6c 61 73 73 3d 22 61 22 20 77 69 64 74 68 3d 22 34 38 22 20 68 65 69 67 68 74 3d 22 34 38 22 2f 3e 3c 70 61 74 68 20 63 6c 61 73 73 3d 22 62 22 20 64 3d 22 4d 34 30 2c 33 32 2e 35 37 38 56 34 30 48 33 32 56 33 36 48 32 38 56 33 32 48 32 34 56 32 38 2e 37 36 36 41 31 30 2e 36 38 39 2c 31 30 2e 36 38 39 2c 30 2c 30 2c Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="48" height="48" viewBox="0 0 48 48"><defs><style>.a{fill:none;}.b{fill:#404040;}</style></defs><rect class="a" width="48" height="48"/><path class="b" d="M40,32.578V40H32V36H28V32H24V28.766A10.689,10.689,0,0,

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49766	13.107.219.60	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 18:57:00 UTC	20	OUT	GET /shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico HTTP/1.1 Host: aadcdn.msauth.net 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

Timestamp	kBytes transferred	Direction	Data
2022-07-01 18:57:00 UTC	20	IN	HTTP/1.1 200 OK Cache-Control: public, max-age=31536000 Content-Length: 17174 Content-Type: image/x-icon Content-MD5: EuPayFgGHQiAI7K9SOL6lg== Last-Modified: Sun, 18 Oct 2020 03:02:03 GMT ETag: 0x8D8731230C851A6 X-Cache: TCP_HIT Server: Windows-Azure-Blob/1.0 Microsoft-HTTPAPI/2.0 x-ms-request-id: d8d8fc17-d01e-003a-73e2-8a1877000000 x-ms-version: 2009-09-19 x-ms-lease-status: unlocked x-ms-blob-type: BlockBlob Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Access-Control-Allow-Origin: * X-Azure-Ref: 0fEO/YgAAAABiUHXElv3jS4TAZNSCF9eiRlJBMjMxMDUwNDE3MDA5ADM5YTEyZjdlLTg5OWYtNDZjZi1hNmQwLTI0YmJiYTI3ZDk1Ng== Date: Fri, 01 Jul 2022 18:57:00 GMT Connection: close
2022-07-01 18:57:00 UTC	21	IN	Data Raw: 00 00 01 00 06 00 80 80 10 00 00 00 00 00 68 28 00 00 66 00 00 00 48 48 10 00 00 00 00 00 e8 0d 00 00 ce 28 00 00 30 30 10 00 00 00 00 00 68 06 00 00 b6 36 00 00 20 20 10 00 00 00 00 00 e8 02 00 00 1e 3d 00 00 18 18 10 00 00 00 00 00 e8 01 00 00 06 40 00 00 10 10 10 00 00 00 00 00 28 01 00 00 ee 41 00 00 28 00 00 00 80 00 00 00 00 01 00 00 01 00 04 00 00 00 00 00 00 28 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 ef a4 00 00 00 b9 ff 00 00 ba 7f 00 22 50 f2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 20 00 00 03 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 Data Ascii: h(fHH(00h6 =@(A(("P"""""""""""""""""""""""""""""""""" 333333333333333
2022-07-01 18:57:00 UTC	36	IN	Data Raw: 00 00 00 01 80 00 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 28 00 00 00 20 00 00 00 40 00 00 00 01 00 04 00 00 00 00 00 80 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 ef a4 00 00 00 b9 ff 00 00 bc 7b 00 1f 4c f9 00 22 50 f2 00 f7 a6 00 00 00 ba 7f 00 f3 a6 00 00 1e 4e f6 00 23 4e f4 00 f3 a4 00 00 00 bc 7d 00 00 ba 7d 00 00 00 00 00 22 22 22 22 22 22 c0 03 33 33 33 33 33 33 33 22 22 22 22 22 22 c0 03 33 33 33 33 33 33 33 22 22 22 22 22 22 c0 03 33 33 33 33 33 33 33 22 22 22 22 22 22 Data Ascii: (@{L"PN#N}}""""""""""""3333333""""""""""""3333333""""""""""""3333333""""""""""""

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.6	49775	13.107.219.60	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 18:57:01 UTC	38	OUT	GET /shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: aadcdn.msauth.net
2022-07-01 18:57:01 UTC	38	IN	HTTP/1.1 200 OK Cache-Control: public, max-age=31536000 Content-Length: 17174 Content-Type: image/x-icon Content-MD5: EuPayFgGHQiAI7K9SOL6lg== Last-Modified: Sun, 18 Oct 2020 03:02:03 GMT ETag: 0x8D8731230C851A6 Server: Windows-Azure-Blob/1.0 Microsoft-HTTPAPI/2.0 X-Cache: TCP_HIT x-ms-request-id: 9858059c-501e-005a-37ae-885a55000000 x-ms-version: 2009-09-19 x-ms-lease-status: unlocked x-ms-blob-type: BlockBlob Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Access-Control-Allow-Origin: * X-Azure-Ref-OriginShield: 01sy5YgAAAAArhJbPvZ65T5s7ELABj3i+RlJBMjMxMDUwNDE4MDA5ADM5YTEyZjdlLTg5OWYtNDZjZi1hNmQwLTI0YmJiYTI3ZDk1Ng== X-Azure-Ref: 0fUO/YgAAAAC06/+slP/CQ7WUdyWWMnvURlJBMjMxMDUwNDIwMDM3ADM5YTEyZjdlLTg5OWYtNDZjZi1hNmQwLTI0YmJiYTI3ZDk1Ng== Date: Fri, 01 Jul 2022 18:57:01 GMT Connection: close
2022-07-01 18:57:01 UTC	39	IN	Data Raw: 00 00 01 00 06 00 80 80 10 00 00 00 00 00 68 28 00 00 66 00 00 00 48 48 10 00 00 00 00 00 e8 0d 00 00 ce 28 00 00 30 30 10 00 00 00 00 00 68 06 00 00 b6 36 00 00 20 20 10 00 00 00 00 00 e8 02 00 00 1e 3d 00 00 18 18 10 00 00 00 00 00 e8 01 00 00 06 40 00 00 10 10 10 00 00 00 00 00 28 01 00 00 ee 41 00 00 28 00 00 00 80 00 00 00 00 01 00 00 01 00 04 00 00 00 00 00 00 28 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 ef a4 00 00 00 b9 ff 00 00 ba 7f 00 22 50 f2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 20 00 00 03 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 Data Ascii: h(fHH(00h6 =@(A(("P"""""""""""""""""""""""""""""""""" 333333333333333

Timestamp	kBytes transferred	Direction	Data
2022-07-01 18:57:01 UTC	54	IN	Data Raw: 01 80 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 ff ff ff ff ff ff 00 00 ff ff ff ff ff 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 00 01 80 00 00 00 00 28 00 00 00 20 00 00 00 40 00 00 00 01 00 04 00 00 00 00 00 80 02 00 00 00 Data Ascii: (@

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.6	49778	13.107.219.60	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 18:57:01 UTC	56	OUT	GET /shared/1.0/content/images/appbackgrounds/49-small_e58aafc980614a9cd7796bea7b5ea8f0.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: aadcdn.msauth.net
2022-07-01 18:57:01 UTC	57	IN	HTTP/1.1 200 OK Cache-Control: public, max-age=31536000 Content-Length: 987 Content-Type: image/jpeg Content-MD5: 5YqvyYBhSpzXeWvqe16o8A== Last-Modified: Fri, 27 Mar 2020 19:41:47 GMT ETag: 0x8D7D286E322A911 X-Cache: TCP_HIT Server: Windows-Azure-Blob/1.0 Microsoft-HTTPAPI/2.0 x-ms-request-id: 72e47f8d-001e-002f-6c58-8a2f5f000000 x-ms-version: 2009-09-19 x-ms-lease-status: unlocked x-ms-blob-type: BlockBlob Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Access-Control-Allow-Origin: * X-Azure-Ref: 0fUO/YgAAAAAdD33WUsp8RqO5sksop8ZfRlJBMjMxMDUwNDE4MDA5ADM5YTEyZjdlLTg5OWYtNDZjZi1hNmQwLTI0YmJiYTI3ZDk1Ng== Date: Fri, 01 Jul 2022 18:57:01 GMT Connection: close
2022-07-01 18:57:01 UTC	58	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 48 00 48 00 00 ff e1 00 66 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 04 01 1a 00 05 00 00 00 01 00 00 00 3e 01 1b 00 05 00 00 00 01 00 00 00 46 01 28 00 03 00 00 00 01 00 02 00 00 01 31 00 02 00 00 00 10 00 00 00 4e 00 00 00 00 00 00 00 48 00 00 00 01 00 00 00 48 00 00 00 01 70 61 69 6e 74 2e 6e 65 74 20 34 2e 32 2e 39 00 ff db 00 43 00 02 01 01 01 01 01 02 01 01 01 02 02 02 02 02 04 03 02 02 02 02 05 04 04 03 04 06 05 06 06 06 05 06 06 06 07 09 08 06 07 09 07 06 06 08 0b 08 09 0a 0a 0a 0a 0a 06 08 0b 0c 0b 0a 0c 09 0a 0a 0a ff db 00 43 01 02 02 02 02 02 02 05 03 03 05 0a 07 06 07 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a Data Ascii: JFIFHHfExifMM*>F(1NHHpaint.net 4.2.9CC

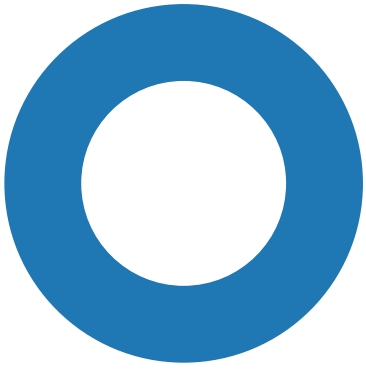
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.6	49779	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

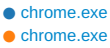
Timestamp	kBytes transferred	Direction	Data
2022-07-01 18:57:01 UTC	56	OUT	GET /shared/1.0/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: aadcdn.msftauth.net

Timestamp	kBytes transferred	Direction	Data
2022-07-01 18:57:01 UTC	59	IN	HTTP/1.1 200 OK Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Length,Date,Transfer-Encoding Age: 5319272 Cache-Control: public, max-age=31536000 Content-MD5: nzaLxFgP7ZB3dfMcaybWzw== Content-Type: image/svg+xml Date: Fri, 01 Jul 2022 18:57:01 GMT Etag: 0x8D79A1B9F5E121A Last-Modified: Thu, 16 Jan 2020 00:32:52 GMT Server: ECAcc (frc/8E9E) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 3d61ac0e-001e-004e-351b-5de3c9000000 x-ms-version: 2009-09-19 Content-Length: 3651 Connection: close
2022-07-01 18:57:01 UTC	59	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 30 38 22 20 68 65 69 67 68 74 3d 22 32 34 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 31 30 38 20 32 34 22 3e 3c 74 69 74 6c 65 3e 61 73 73 65 74 73 3c 2f 74 69 74 6c 65 3e 3c 70 61 74 68 20 64 3d 22 4d 34 34 2e 38 33 36 2c 34 2e 36 56 31 38 2e 34 68 2d 32 2e 34 56 37 2e 35 38 33 48 34 32 2e 34 4c 33 38 2e 31 31 39 2c 31 38 2e 34 48 33 36 2e 35 33 31 4c 33 32 2e 31 34 32 2c 37 2e 35 38 33 68 2d 2e 30 32 39 56 31 38 2e 34 48 32 39 2e 39 56 34 2e 36 68 33 2e 34 33 36 4c 33 37 2e 33 2c 31 34 2e 38 33 68 2e 30 35 38 4c 34 31 2e 35 34 35 2c 34 2e 36 5a 6d 32 2c 31 2e 30 34 39 61 31 2e 32 36 38 2c 31 2e 32 36 38 2c 30 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38.119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: **5412**, Parent PID: **820**

General

Target ID:	0
Start time:	20:56:53
Start date:	01/07/2022
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\ClosingDoc.html

Imagebase:	0x7ff6220c0000
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	7FF6220FFC4B	RegSetValueExW

Analysis Process: chrome.exe PID: **5052**, Parent PID: **5412**

General

Target ID:	1
Start time:	20:56:56
Start date:	01/07/2022
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=1580,15663332800411292547,1156807434197202323,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1920 /prefetch:8
Imagebase:	0x7ff6220c0000
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