

ID: 679623
Cookbook: browseurl.jbs
Time: 06:57:39
Date: 06/08/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report https://spatterjointposition.com 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Process Tree 5
Malware Configuration 5
Yara Signatures 5
Sigma Signatures 5
Snort Signatures 6
Joe Sandbox Signatures 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 9
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 10
World Map of Contacted IPs 10
Public IPs 11
Private 11
General Information 12
Warnings 12
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASNs 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic 13
C:\Users\user\AppData\Local\Google\Chrome\User Data\0a573f8e-bd08-4920-8498-e5c7053e5ca3.tmp 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\25f82938-ee41-4f40-9e6c-18c30ac62ada.tmp 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\5c0070c2-6756-422a-bed5-359dd6946545.tmp 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\5cc06899-b404-40bb-9912-447e6526c319.tmp 15
C:\Users\user\AppData\Local\Google\Chrome\User Data\6407301f-2944-473a-a98b-406abc9eb29b.tmp 15
C:\Users\user\AppData\Local\Google\Chrome\User Data\67766df0-1589-4501-a1e4-47170e46c919.tmp 15
C:\Users\user\AppData\Local\Google\Chrome\User Data\79c829ea-58df-49d0-b7b7-b3d8bbd3be57.tmp 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\906f612a-faf8-4e40-9854-60460b5be071.tmp 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0498d8d1-998e-4aee-b8a8-5b426a0a1c56.tmp 17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\06e9b1b8-b1d9-45a0-b2e8-f0e6c8f4f1d8.tmp 17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\078edded-353d-4e52-b959-05f9076e9ba2.tmp 17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0d6da62f-a154-49fe-8eaa-ed2edc2c87d5.tmp 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\153de007-3e71-43d7-a576-3a47475081a4.tmp 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\380ad8f8-bfd5-4529-a024-948ab59738b0.tmp 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3b95c536-2787-469a-92fe-4110bdc6db58.tmp 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3e35ca23-d733-4921-b152-31cbac549ba1.tmp 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\50dc6200-9d3b-44eb-a267-f16cc4296171.tmp 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\52c535f4-1515-4338-8400-b9e7ea56a616.tmp 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5960d875-92fc-4fe5-9a6f-d66e299973b2.tmp 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\80771ced-65a4-4539-8578-d57ff99918ee.tmp 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\91cc80f6-5ef4-4a97-a5cf-80fbfda4b929.tmp 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\94b40b6d-c495-4f3d-8e49-978879b4338a.tmp 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\94b44d5f-e7cd-4a45-96ed-526273df694a.tmp 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy) 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_www.youtube.com_0.indexeddb.leveldb\000001.dbtmp 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_www.youtube.com_0.indexeddb.leveldb\CURRENT (copy) 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_www.youtube.com_0.indexeddb.leveldb\MANIFEST-000001 24

Copyright Joe Security LLC 2022

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy) 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy) 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy) 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\379f1cbab5b08b6fc9e08681e42d8be311441c88\ae478fa7-70c5-4e36-b39b-4be498dc31c7\index 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\379f1cbab5b08b6fc9e08681e42d8be311441c88\ae478fa7-70c5-4e36-b39b-4be498dc31c7\index-dir\temp-index 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\379f1cbab5b08b6fc9e08681e42d8be311441c88\ae478fa7-70c5-4e36-b39b-4be498dc31c7\index-dir\the-real-index (copy) 26
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\379f1cbab5b08b6fc9e08681e42d8be311441c88\index.txt (copy) 26
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\379f1cbab5b08b6fc9e08681e42d8be311441c88\index.txt.tmp 26
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1 26
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy) 27
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\ea3d7a3a-1959-4235-bac5-e3894f7e2431.tmp 27
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\3059c87a-6592-453b-a83b-7efd9ea88152.tmp 27
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1 28
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Network Persistent State (copy) 28
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity (copy) 28
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\aa2a95b0-bf77-4388-8452-3b2282038708.tmp 29
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b7fbad58-f0aa-4441-9a85-fe27e9e0ed77.tmp 29
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b8689bd8-874f-4663-8900-5cd354e668ce.tmp 29
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d66d4c49-2e56-4c40-b3c7-b4283c8599d2.tmp 30
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp 30
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy) 30
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e45ba11d-f760-4aa2-902c-2c2f4639e799.tmp 31
C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser 31
C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version 31
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy) 31
C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy) 32
C:\Users\user\AppData\Local\Google\Chrome\User Data\a63e5fd8-a01d-4e45-9c44-7330264d4008.tmp 32
C:\Users\user\AppData\Local\Google\Chrome\User Data\d2919e16-2e5f-4d2d-b26b-f93daf9d6b3c.tmp 33
C:\Users\user\AppData\Local\Temp\02bf7525-dc4c-4c93-a8a6-85a18a8cc3ca.tmp 33
C:\Users\user\AppData\Local\Temp\6060_1494985660_metadata\verified_contents.json 33
C:\Users\user\AppData\Local\Temp\6060_1494985660_platform_specific\x86_64\pnacl_public_pnacl_json 34
C:\Users\user\AppData\Local\Temp\6060_1494985660_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_for_eh_o 34
C:\Users\user\AppData\Local\Temp\6060_1494985660_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_o 34
C:\Users\user\AppData\Local\Temp\6060_1494985660_platform_specific\x86_64\pnacl_public_x86_64_crtend_o 35
C:\Users\user\AppData\Local\Temp\6060_1494985660_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe 35
C:\Users\user\AppData\Local\Temp\6060_1494985660_platform_specific\x86_64\pnacl_public_x86_64_libcrt_platform_a 35
C:\Users\user\AppData\Local\Temp\6060_1494985660_platform_specific\x86_64\pnacl_public_x86_64_libgcc_a 36
C:\Users\user\AppData\Local\Temp\6060_1494985660_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_a 36
C:\Users\user\AppData\Local\Temp\6060_1494985660_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_dummy_a 36
C:\Users\user\AppData\Local\Temp\6060_1494985660_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe 37
C:\Users\user\AppData\Local\Temp\6060_1494985660_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe 37
C:\Users\user\AppData\Local\Temp\6060_1494985660\manifest.fingerprint 37
C:\Users\user\AppData\Local\Temp\6060_1494985660\manifest.json 38
C:\Users\user\AppData\Local\Temp\6060_1654857163\Recovery.crx3 38
C:\Users\user\AppData\Local\Temp\6060_1654857163_metadata\verified_contents.json 38
C:\Users\user\AppData\Local\Temp\6060_1654857163\manifest.fingerprint 39
C:\Users\user\AppData\Local\Temp\6060_1654857163\manifest.json 39
C:\Users\user\AppData\Local\Temp\d5fcf379-0e69-4ef2-b6f1-ad49e4693103.tmp 39
C:\Users\user\AppData\Local\Temp\scoped_dir6060_68835047\02bf7525-dc4c-4c93-a8a6-85a18a8cc3ca.tmp 40
C:\Users\user\AppData\Local\Temp\scoped_dir6060_68835047\CRX_INSTALL_locales\bg\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir6060_68835047\CRX_INSTALL_locales\ca\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir6060_68835047\CRX_INSTALL_locales\cs\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir6060_68835047\CRX_INSTALL_locales\da\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir6060_68835047\CRX_INSTALL_locales\de\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir6060_68835047\CRX_INSTALL_locales\el\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir6060_68835047\CRX_INSTALL_locales\en\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir6060_68835047\CRX_INSTALL_locales\en_GB\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir6060_68835047\CRX_INSTALL_locales\es\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir6060_68835047\CRX_INSTALL_locales\es_419\messages.json 43
C:\Users\user\AppData\Local\Temp\scoped_dir6060_68835047\CRX_INSTALL_locales\et\messages.json 43
C:\Users\user\AppData\Local\Temp\scoped_dir6060_68835047\CRX_INSTALL_locales\fi\messages.json 43
C:\Users\user\AppData\Local\Temp\scoped_dir6060_68835047\CRX_INSTALL_locales\fil\messages.json 44
C:\Users\user\AppData\Local\Temp\scoped_dir6060_68835047\CRX_INSTALL_locales\fr\messages.json 44
C:\Users\user\AppData\Local\Temp\scoped_dir6060_68835047\CRX_INSTALL_locales\hi\messages.json 44
C:\Users\user\AppData\Local\Temp\scoped_dir6060_68835047\CRX_INSTALL_locales\hr\messages.json 45
C:\Users\user\AppData\Local\Temp\scoped_dir6060_68835047\CRX_INSTALL_locales\hu\messages.json 45
C:\Users\user\AppData\Local\Temp\scoped_dir6060_68835047\CRX_INSTALL_locales\id\messages.json 45
C:\Users\user\AppData\Local\Temp\scoped_dir6060_68835047\CRX_INSTALL_locales\it\messages.json 46
Static File Info 46
Network Behavior 46
TCP Packets 46
DNS Queries 48

DNS Answers 49
Statistics 52
Behavior 52
System Behavior 52
Analysis Process: chrome.exePID: 6060, Parent PID: 1280 52
General 52
File Activities 53
Registry Activities 53
Analysis Process: chrome.exePID: 4116, Parent PID: 6060 53
General 53
File Activities 53
Analysis Process: chrome.exePID: 2368, Parent PID: 1280 53
General 53
File Activities 54
Registry Activities 54
Analysis Process: chrome.exePID: 1108, Parent PID: 6060 54
General 54
Analysis Process: chrome.exePID: 2068, Parent PID: 6060 54
General 54
File Activities 55
Registry Activities 55
Disassembly 55

Copyright Joe Security LLC 2022

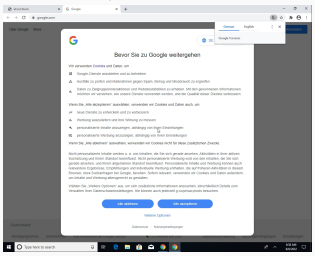
Windows Analysis Report

https://spatterjointposition.com

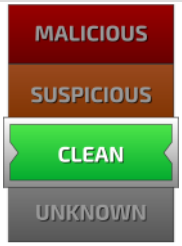
Overview

General Information

Sample URL:	http://https://spatterjointposition.com
Analysis ID:	679623
Infos:	



Detection

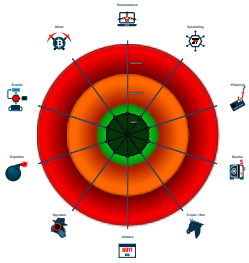


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 6060 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 4116 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1612,17434451715936591080,16828468669034620011,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1920 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 1108 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1612,17434451715936591080,16828468669034620011,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=6248 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 2068 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --field-trial-handle=1612,17434451715936591080,16828468669034620011,131072 --lang=en-US --service-sandbox-type=video_capture --enable-audio-service-sandbox --mojo-platform-channel-handle=6236 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 2368 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://spatterjointposition.com MD5: C139654B5C1438A95B321BB01AD63EF6)
- cleanup

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Copyright Joe Security LLC 2022

Snort Signatures

No Snort rule has matched

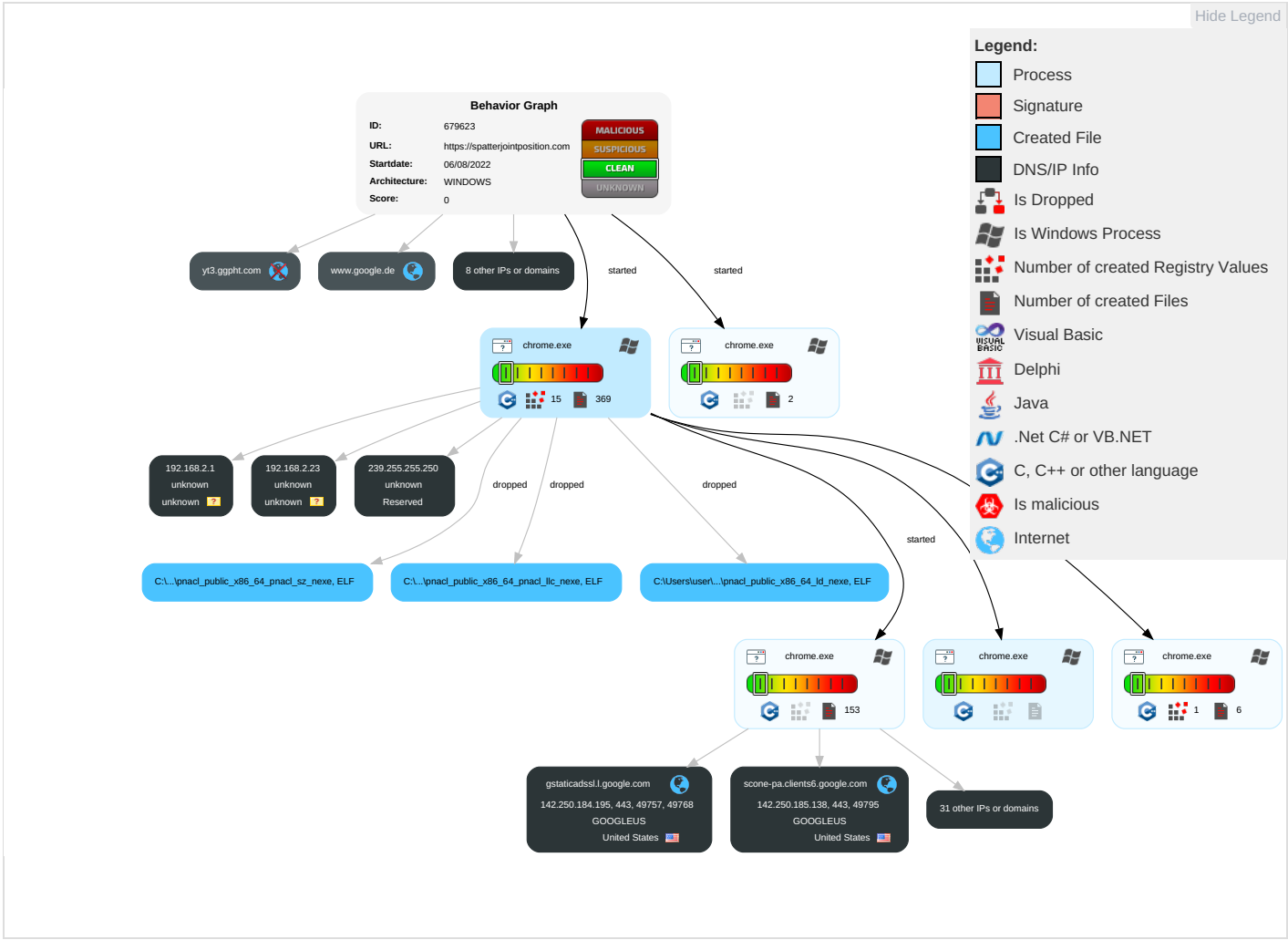
Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

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	2 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	1 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	2 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

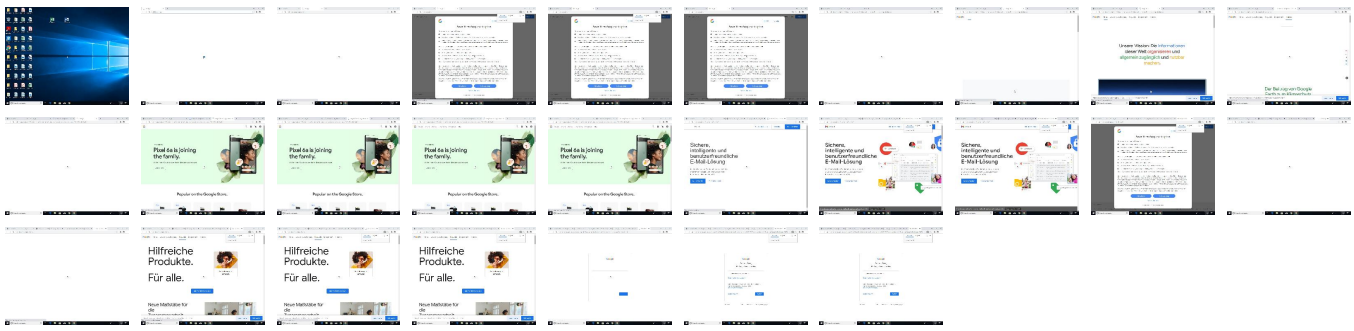
Behavior Graph

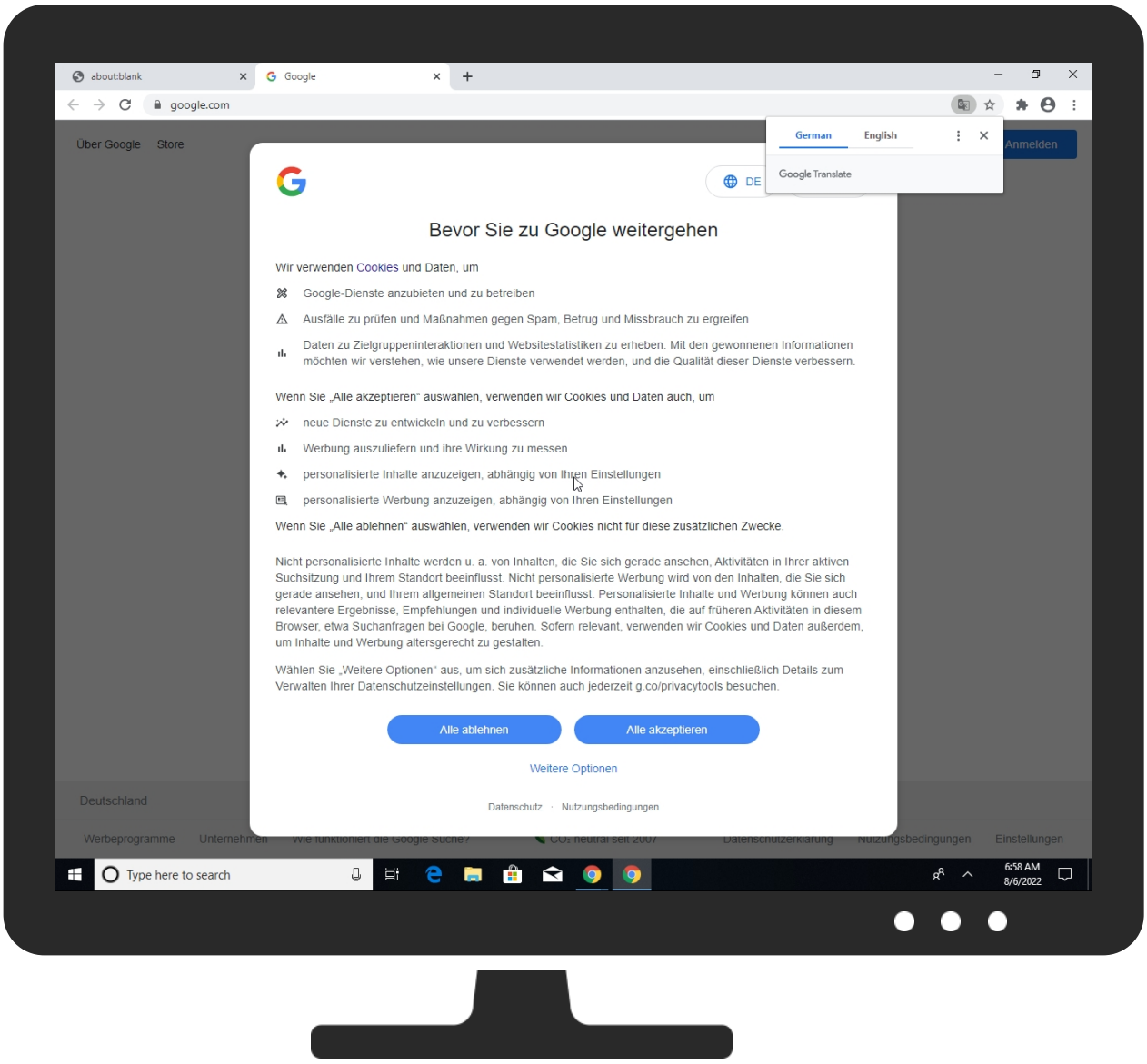


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://spatterjointposition.com	2%	Virustotal		Browse
http://https://spatterjointposition.com	0%	Avira URL Cloud	safe	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\6060_1494985660_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\6060_1494985660_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\6060_1494985660_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\6060_1494985660_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\6060_1494985660_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\6060_1494985660_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\6060_1494985660_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\6060_1494985660_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	ReversingLabs		

Copyright Joe Security LLC 2022

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://about.google/products/	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://about.google/stories/timelapse-planetary-changes/	0%	Virustotal		Browse
http://https://about.google/products/	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	142.250.184.195	true	false		high
scone-pa.clients6.google.com	142.250.185.138	true	false		high
www.google.de	172.217.18.3	true	false		high
google.com	172.217.16.206	true	false		high
csp.withgoogle.com	172.217.16.209	true	false		unknown
accounts.google.com	142.250.185.205	true	false		high
plus.l.google.com	216.58.212.142	true	false		high
stats.l.doubleclick.net	66.102.1.156	true	false		high
www-googletagmanager.l.google.com	142.250.186.168	true	false		high
i.ytimg.com	142.250.185.214	true	false		high
mail.google.com	142.250.186.165	true	false		high
store.google.com	172.217.16.142	true	false		high
spatterjointposition.com	192.243.59.12	true	false		unknown
static-doubleclick-net.l.google.com	142.250.186.134	true	false		high
about.google	216.239.32.29	true	false		unknown
youtube-ui.l.google.com	142.250.186.110	true	false		high
googleads.g.doubleclick.net	142.250.185.162	true	false		high
play.google.com	142.250.186.142	true	false		high
www3.l.google.com	172.217.23.110	true	false		high
photos-ugc.l.googleusercontent.com	142.250.186.33	true	false		high
www.google.com	142.250.185.196	true	false		high
clients.l.google.com	142.250.186.110	true	false		high
googlehosted.l.googleusercontent.com	172.217.23.97	true	false		high
kstatic.googleusercontent.com	35.241.11.240	true	false		high
yt3.ggpht.com	unknown	unknown	false		high
lh3.googleusercontent.com	unknown	unknown	false		high
static.doubleclick.net	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
accounts.youtube.com	unknown	unknown	false		high
www.youtube.com	unknown	unknown	false		high
apis.google.com	unknown	unknown	false		high

Contacted URLs

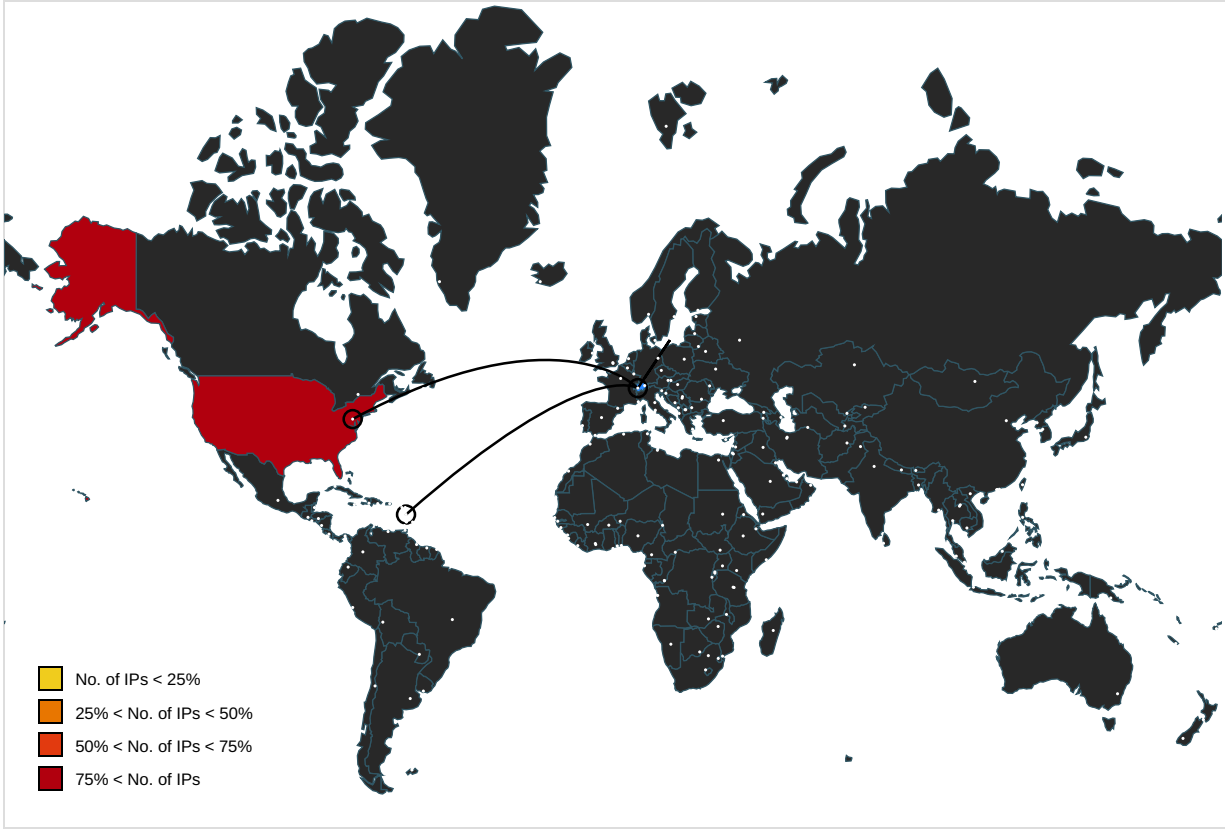
Name	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/	false		high
http://https://about.google/stories/timelapse-planetary-changes/	false	• 0%, Virustotal, Browse	unknown

Name	Malicious	Antivirus Detection	Reputation
http://https://www.youtube.com/embed/by-kTJ0DOLc?rel=0&vq=hd720&start=0&cc_load_policy=1&playsinline=1&origin=https%3A%2F%2Fabout.google&enablejsapi=1&widgetid=1	false		high
http://https://www.google.de/imghp?hl=de&ogbl	false		high
http://https://accounts.google.com/signin/v2/identifier?hl=de&passive=true&continue=https%3A%2F%2Fwww.google.com%2F&ec=GAZAmgQ&flowName=GlifWebSignIn&flowEntry=ServiceLogin	false		high
http://https://about.google/products/	false	• 0%, Virustotal, Browse • URL Reputation: safe	unknown
http://https://www.google.com/intl/de/gmail/about/#	false		high
http://https://store.google.com/DE?utm_source=hp_header&utm_medium=google_ooo&utm_campaign=GS100042&hl=de-DE	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	94b44d5f-e7cd-4a45-96ed-526273df694a.tmp.1.dr, 3059c87a-6592-453b-a83b-7efd9ea88152.tmp.1.dr, ea3d7a3a-1959-4235-bac5-e3894f7e2431.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	94b44d5f-e7cd-4a45-96ed-526273df694a.tmp.1.dr	false		high
http://https://www.google.com/images/cleardot.gif	craw_window.js.0.dr	false		high
http://https://play.google.com	94b44d5f-e7cd-4a45-96ed-526273df694a.tmp.1.dr	false		high
http://https://payments.google.com/payments/v4/js/integrator.js	craw_window.js.0.dr, manifest.json.0.dr	false		high
http://https://chromium.googlesource.com/a/native_client/pnacl-llvm.git	pnacl_public_x86_64_libpnacl_irt_shim_dummy_a.0.dr	false		high
http://https://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://www.youtube.com/	index.txt.tmp.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://www.google.com	94b44d5f-e7cd-4a45-96ed-526273df694a.tmp.1.dr	false		high
http://https://www.google.com/images/dot2.gif	craw_window.js.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	94b44d5f-e7cd-4a45-96ed-526273df694a.tmp.1.dr	false		high
http://https://clients2.googleusercontent.com	94b44d5f-e7cd-4a45-96ed-526273df694a.tmp.1.dr	false		high
http://https://apis.google.com	94b44d5f-e7cd-4a45-96ed-526273df694a.tmp.1.dr	false		high
http://https://www.google.com/accounts/OAuthLogin?issueuberauth=1	craw_window.js.0.dr	false		high
http://https://www.google.com/	manifest.json.0.dr	false		high
http://https://www-googleapis-staging.sandbox.google.com	craw_window.js.0.dr, craw_background.js.0.dr	false		high
http://https://chromium.googlesource.com/a/native_client/pnacl-clang.git	pnacl_public_x86_64_libpnacl_irt_shim_dummy_a.0.dr	false		high
http://https://clients2.google.com	94b44d5f-e7cd-4a45-96ed-526273df694a.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
216.58.212.142	plus.l.google.com	United States		15169	GOOGLEUS	false
142.250.185.205	accounts.google.com	United States		15169	GOOGLEUS	false
172.217.23.110	www3.l.google.com	United States		15169	GOOGLEUS	false
172.217.23.97	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
66.102.1.156	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
142.250.185.162	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
142.250.186.110	youtube-ui.l.google.com	United States		15169	GOOGLEUS	false
142.250.186.134	static-doubleclick-net.l.google.com	United States		15169	GOOGLEUS	false
35.241.11.240	kstatic.googleusercontent.com	United States		15169	GOOGLEUS	false
142.250.186.33	photos-ugc.l.googleusercontent.com	United States		15169	GOOGLEUS	false
172.217.16.142	store.google.com	United States		15169	GOOGLEUS	false
142.250.184.195	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
216.239.32.29	about.google	United States		15169	GOOGLEUS	false
172.217.16.206	google.com	United States		15169	GOOGLEUS	false
172.217.18.3	www.google.de	United States		15169	GOOGLEUS	false
172.217.16.209	csp.withgoogle.com	United States		15169	GOOGLEUS	false
142.250.185.138	scone-pa.clients6.google.com	United States		15169	GOOGLEUS	false
142.250.185.214	i.ytimg.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.185.196	www.google.com	United States		15169	GOOGLEUS	false
192.243.59.12	spatterjointposition.com	Dominica		39572	ADVANCEDHOSTERS-ASNL	false
142.250.186.165	mail.google.com	United States		15169	GOOGLEUS	false
142.250.186.168	www-googletagmanager.l.google.com	United States		15169	GOOGLEUS	false

Private

Copyright Joe Security LLC 2022

IP
192.168.2.1
192.168.2.23
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679623
Start date and time: 06/08/202206:57:39	2022-08-06 06:57:39 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://spatterjointposition.com
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:	20
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:	CLEAN
Classification:	clean0.win@42/135@30/26
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://about.google/?fg=1&utm_source=google-DE&utm_medium=referral&utm_campaign=hp-header • Browse: https://store.google.com/DE?utm_source=hp_header&utm_medium=google_ooo&utm_campaign=GS100042&hl=de-DE • Browse: https://mail.google.com/mail/&ogbl • Browse: https://www.google.de/imghp?hl=de&ogbl • Browse: https://www.google.de/intl/de/about/products • Browse: https://accounts.google.com/ServiceLogin?hl=de&passive=true&continue=https://www.google.com/&ec=GAZAmgQ

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 142.250.186.142, 142.250.186.131, 74.125.108.201, 74.125.108.198, 142.250.185.195, 142.250.184.234, 142.250.186.170, 172.217.16.138, 172.217.16.202, 142.250.185.170, 142.250.185.202, 142.250.185.234, 142.250.181.234, 216.58.212.170, 142.250.74.202, 142.250.186.42, 142.250.186.74, 142.250.186.106, 142.250.186.138, 142.250.184.202, 172.217.18.10, 142.250.185.142, 216.239.32.36, 216.239.34.36, 142.250.185.176, 142.250.185.208, 142.250.185.240, 142.250.186.48, 142.250.181.240, 142.250.186.112, 142.250.186.144, 142.250.184.208, 142.250.186.80, 172.217.18.16, 142.250.186.176, 172.217.16.208, 216.58.212.176, 172.217.18.112, 172.217.23.112, 142.250.185.80, 172.217.18.98, 142.250.185.227, 80.67.82.211, 80.67.82.235, 20.238.103.94, 20.54.89.106, 52.242.101.226, 40.125.122.176, 20.223.24.244, 52.152.110.14
- Excluded domains from analysis (whitelisted): r5---sn-4g5edn6y.gvt1.com, ssl.gstatic.com, www.googleadservices.com, storage.googleapis.com, asf-ris-prod-neu-azsc.northeurope.cloudapp.azure.com, store-images.s-microsoft.com-c.edgekey.net, clientservices.googleapis.com, a1449.dscg2.akamai.net, arc.msn.com, region1.google-analytics.com, r1---sn-1gi7znek.gvt1.com, e12564.dspb.akamaiedge.net, r3---sn-1gi7znes.gvt1.com, rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, redirector.gvt1.com, login.live.com, www.googletagmanager.com, update.googleapis.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, www.gstatic.com, img-prod-cms-rt-microsoft-com.akamaized.net, r4.sn-1gi7znek.gvt1.com, www.google-analytics.com, glb.sls.prod.dcat.dsp.trafficmanager.net, www.bing.com, r4---sn-1gi7znek.gvt1.com, fonts.googleapis.com, fs.microsoft.com, content-autofill.googleapis.com, fonts.gstatic.com, ajax.googleapis.com, ris-prod.trafficmanager.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing network 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 NtWriteFile calls found.

- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA8321101
Malicious:	false
Reputation:	low
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\0a573f8e-bd08-4920-8498-e5c7053e5ca3.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):	211724
Entropy (8bit):	6.0423171436608865
Encrypted:	false
SSDEEP:	6144:AKaXlScilZFWzn/tu6I7pTqzKaqfIlUOoSiuR/:AKIMZMjFu6OpM5o4
MD5:	6761AEB2FCE89AA5830927B2C4A928E0
SHA1:	813AB1AE23902FA68602E353DCE07788994BD85D
SHA-256:	E1A3FD329AEADAAAE2B0F945FAAF8CCF16095449795336383D796A8E1D62F41B
SHA-512:	0AB76B289D9961B817751BBC8C232EFE9188A361AAB59A0A128F329154C543ADA0A7D1F1880194386E8B6AB2037D5D5092932A9A0533258AD95D46C041EBAE0
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":1.659794320508321e+12,"network":1.659761922e+12,"ticks":113483142.0,"uncertainty":4255693.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639496290"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\25f82938-ee41-4f40-9e6c-18c30ac62ada.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):	220084
Entropy (8bit):	6.0698514256457665
Encrypted:	false
SSDEEP:	6144:MYKaXlScilZFWzn/tu6I7pTqzKaqfIlUOoSiuR/:MYKIMZMjFu6OpM5o4
MD5:	80523D9433330E5E6F7815C883B4E80C
SHA1:	BAA4EE83D37C29A12074E18EF0E298654CB0756D
SHA-256:	147E8652209FB20C56A1AB48AD8B1AAB88CC82AFBDA5D108B704AD230E392843
SHA-512:	A819ABD0AB453042A456EFD2865DC6D49CAF632850E672E3FB67183769C455F324E3D9AC25723ED935D4D32CFF4F2B15BE3751ED17206D1FBAD1523417B7634
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":1.659794320508321e+12,"network":1.659761922e+12,"ticks":113483142.0,"uncertainty":4255693.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\5c0070c2-6756-422a-bed5-359dd6946545.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):	220084
Entropy (8bit):	6.069852557781486
Encrypted:	false
SSDEEP:	6144:JmKaXlScilZFWzn/tu6I7pTqzKaqfIlUOoSiuR/:JmKIMZMjFu6OpM5o4
MD5:	A1D034CB5D2D76100006B75BE5E59ED4
SHA1:	D2B34EEA7BC7C0F259D3D8ADBFC75D1EB8D8D954
SHA-256:	46A146B95C1189DC5D86254309137DE9CE72F9C4E79D63C290328BD8F8D70082
SHA-512:	9C8F41FF20DBC2F288F3CCC81351BF3055BD662876A6CDE2153A669518CA5149706D528149AAB29F1483D65D8A3C0E58F4CB2C5F3F2AAB670BBB29ABA6D8D9DA
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":1.659794320508321e+12,"network":1.659761922e+12,"ticks":113483142.0,"uncertainty":4255693.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP","password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\5cc06899-b404-40bb-9912-447e6526c319.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):	220084
Entropy (8bit):	6.069851732533528
Encrypted:	false
SSDEEP:	6144:IDKaXlScilZFWzn/tu6I7pTqzKaqfIlUOoSiuR/:IDKIMZMjFu6OpM5o4
MD5:	55E9657A6D1D9A744A3A301D5E827B7C
SHA1:	F5C5B335C35C155274ED8BBD09763B2622374B35
SHA-256:	B2A46BE16279B648519D9F58398CEDEF11FA3EE18B22F8BFD012523734A920D4
SHA-512:	6D6C4A65D798C5B8795892A74E123E531B7205550F99231CCD343237F97FA62F5E6BA69E9528F560AAD281F2C41736465EBC91B760961F62B4B6AA6FDAF4714D
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":1.659794320508321e+12,"network":1.659761922e+12,"ticks":113483142.0,"uncertainty":4255693.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP","password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\6407301f-2944-473a-a98b-406abc9eb29b.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):	211818
Entropy (8bit):	6.042558684735572
Encrypted:	false
SSDEEP:	6144:wKaXlScilZFWzn/tu6I7pTqzKaqfIlUOoSiuR/:wKIMZMjFu6OpM5o4
MD5:	39C0191113314AB863C3BB4BD50A472C
SHA1:	5B80772CFD179779B2F06A5697155BFBAEFD257E
SHA-256:	F79EF3197050A88D5D3DCED08D74E7BE58C206F03F712D6F2A7DE63756A8CDFF
SHA-512:	2FF06147690F020729080F318DB6E78D64F831AB96984CD606E3716A7EF11F074BCA78FD61565BF04DD3B5BC109B99D3CBF56C11758A7C8F50D39EBB0B592D9
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":1.659794320508321e+12,"network":1.659761922e+12,"ticks":113483142.0,"uncertainty":4255693.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP","password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639496290"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\67766df0-1589-4501-a1e4-47170e46c919.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):	211632
Entropy (8bit):	6.042072160686405
Encrypted:	false
SSDEEP:	6144:uKaXlScilZFWzn/tu6I7pTqzKaqfIlUOoSiuR/:uKIMZMjFu6OpM5o4
MD5:	1249A1F265109912CD10424E03A4B436
SHA1:	E611E01AFF525E7103821F3B48B1CBAB18D76D45
SHA-256:	52E61088D2A71F278093FB23869DB02808ACAA9B4572328A2B7DC9FEC40C006B
SHA-512:	2F9D8DB85CFAA7998E8B00F4343F7E69F61CA2C19646F9D6641CC032D0AAC51CFB1452EC440E94F6A43C14AA1365206786D801C4031B4B838E99F64C530960

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":1.659794320508321e+12,"network":1.659761922e+12,"ticks":113483142.0,"uncertainty":4255693.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639496290"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\79c829ea-58df-49d0-b7b7-b3d8bbd3be57.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7439481769839977
Encrypted:	false
SSDEEP:	384:NPLM8uhvu1ykVZrofN0rFvQ83/MWXHirGr+rZ+wexvSGi5r1omBNfNOsEwvOOSMb:RqWpJmWAzseXiMOIHf6oKiUU9J
MD5:	2B979F3AFD5E4CAC0343D48943132198
SHA1:	603F879F1FDE0AAC2F009493D6AD08C1CF218099
SHA-256:	9A87C9CC75A0679943EAAAD04DD2DC30B93DED2582EB66BD7A2EAA6DF4CCA4AE
SHA-512:	4A174A7206B64368ACA43BEDF7ADE41B8C4D9C8336A6AB8040F02DC98368C30921AC969A5AAA9D4344180B51809158903D964942E92474965128572258A87E06
Malicious:	false
Reputation:	low
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....d8.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\906f612a-faf8-4e40-9854-60460b5be071.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):	211632
Entropy (8bit):	6.042072759361193
Encrypted:	false
SSDEEP:	6144:tKaXlScilZFWzn/tu6I7pTqzKaqfIlUOoSiuR/:tKIMZMjFu6OpM5o4
MD5:	BBC76F7AE6BC5F2F3299B25A7C7090B1
SHA1:	1791188DBCFAA8692F3928ED8CC88F3B41AD8987
SHA-256:	6FBD6B6601C52249B4BBA9D9B4F072B311F5B766E31B0236938974943BFD594A
SHA-512:	3916451023B1C2DEB083328BCB23FB949FF6FF73F49323182CD9048297944BFFF4A89EC73F2B510F835D4AD199AB2932411A991CBDCE1AB8D51852359B898906
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":1.659794320508321e+12,"network":1.659761922e+12,"ticks":113483142.0,"uncertainty":4255693.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639496290"},"plugins":{"metadata":{"adobe-flash-player":{"disp

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	40
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1n:+ftlE1n
MD5:	BD4642AD6C750A12D912B20BCB92E14D
SHA1:	C549F0F48FDD4FBC62E51AC26D7E185160CE2123
SHA-256:	4FD71FE78DFE203137C89C9FB0734358FF432F2BC83338112DC7B830F9B30F2C

SHA-512:	04410D12EF327614C3AF1251C9906BFEB2977211A7F53CBB08A8C01F9465A382CD001E51AB936A0D196D359F1DECDDAEAF5E7D1DBD49CE5F4FF91BF5C332B6CF
Malicious:	false
Reputation:	low
Preview:	sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0498d8d1-998e-4aee-b8a8-5b426a0a1c56.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):	17702
Entropy (8bit):	5.577436770371343
Encrypted:	false
SSDEEP:	384:cVbtbLlKUXc1kXqKf/pUZNCgVLH2HfDYrU2EW614x:ULl5c1kXqKf/pUZNCgVLH2HfErUi612
MD5:	7E5C249E55341B9A5492B4F71146CF78
SHA1:	6B790A22346BA55E566780B2CCBB1CE3F859E12F
SHA-256:	04DAEDDB1444E97FF3C39E48A2169C7C366C9D3535E5DAB0BBC83329D243D772
SHA-512:	37180C1914EB2882A8DC279FB9BA998AE07707B3AFE91630D55206D455C86011D61579D5FD420BA1E22049117082BE995D0FF4D163A47C07692B86204A9100F3
Malicious:	false
Reputation:	low
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":"13304267918062255","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\06e9b1b8-b1d9-45a0-b2e8-f0e6c8f4f1d8.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):	1543
Entropy (8bit):	5.606440331818074
Encrypted:	false
SSDEEP:	48:YJUmyeU9ieUiUtPNwUYTq+UAKUMXlhXUdXFwUq:4U1eU9ieUiUtGUV+UAKUM3XUdWUq
MD5:	334624DBCC643B86E2878EEF0016A95B
SHA1:	EDDB7171412350419FCD27B543807932AED79F24
SHA-256:	1F3A6D4223B4844501867D3BAE1B56E25BBAF907E85608E73F6A1D7FF57430E0
SHA-512:	AA99E3F66327A35FB9B54AE19B074EC947B0E9FDCA08CE73F1B23E4B3C7AC734F507750A7C11AADECEF0341BC84F2AF9A2D32FD06A6B70C58CC19D3BF5AC5A41
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1691330364.049029,"host":"KVivTTKTVC3D7/hfpnbDFfPAgoVJQnjFfXBq+8P8zk8=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1659794364.049034},{"expiry":1670680760.757667,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1659794360.757673},{"expiry":1691330369.132631,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1659794369.132636},{"expiry":1691330350.945528,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1659794350.945534},{"expiry":1691330361.490677,"host":"i4hyKgaUoHZAMQSjjQXQTS/yqHojznpDCDbFdOAcMec=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1659794361.490681},{"expiry":1691330372.681662,"host":"jY3WZ/euW1Cj9dqyBGft5sGafpAINoKynr7n/PnwKYA=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\078edded-353d-4e52-b959-05f9076e9ba2.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):	5198
Entropy (8bit):	4.986183573181176
Encrypted:	false
SSDEEP:	96:nVl0W1n1pcKIQHok0JCKL89kL1sbOTctVuwn:nVr1pcmC4KSkLCb
MD5:	6B2B01ACD41DD80FC50F17918A239B10
SHA1:	849B2FC7AEE46C0C159BB1F9D38627BD577A59AD
SHA-256:	A6BCAF3322A4FD2A671831B83E2BB23A183E18C9D4267EAB9D1BEF1F8C98C389

SHA-512:	7A175F668A84E79D74397EC14C5D35B581F8DA29C993D389235B0CB84EBD1925A67ADBD4F9E04EE11A33A2FC4AD28AF6AE65017F052F6BBD590A87FED6CD61EB
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13304267918910757","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"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","

SHA-256:	1C7520B8BAB43DB1BE1D4BAECD0B32547F31C42DE3A931A6FC38A7FA7B3C7398
SHA-512:	F9FBB43B611FE6A602E0D0B76E65AFB83A7723044C3E37E9847C85F9C34B247A97545BAC82B99D4D6126E0EB18A127DD90A230DB1B41DE5B859AEAB5764479E3
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1691330377.459043,"host":"KVivTTKTVC3D7/hfpnbDFfPAgoVJQnjFfXBq+8P8zk8=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1659794377.459046},{"expiry":1670680760.757667,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1659794360.757673},{"expiry":1691330380.105219,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1659794380.105223},{"expiry":1691330350.945528,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1659794350.945534},{"expiry":1691330361.490677,"host":"i4hyKgaUoHZAMQSjjQXQTS/yqHojznpDCDbFdOAcMec=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1659794361.490681},{"expiry":1691330372.681662,"host":"jY3WZ/euW1Cj9dqyBGft5sGafpAINoKynr7n/PnwKYA=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3b95c536-2787-469a-92fe-4110bdc6db58.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):	5.564362623707267
Encrypted:	false
SSDEEP:	384:cVbtiLlKUXc1kXqKf/pUZNCgVLH2HfDYrUMHGm+WU140:XLl5c1kXqKf/pUZNCgVLH2HfErUAGcUF
MD5:	6AAC47FAEC681DFAAFE698A8D43676DF
SHA1:	CAB2A7D7F557D8759E15BD853EDDB35F4E416E1C
SHA-256:	A46D52CFD7ED5465395DE49CE30CC102F002959975BFBCFF7827B954FF5225CB
SHA-512:	EB457441A589D8BBDF1CF2694EEB5FE7EA2F73AA77996903243D180EDFE64B106BDFC276B0E1713C8AFA8D08839CA92D19F6DC334A69DB6878746CCCB4B5DB3F
Malicious:	false
Reputation:	low
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":"13304267918062255","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\3e35ca23-d733-4921-b152-31cbac549ba1.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):	1208
Entropy (8bit):	5.614013488746447
Encrypted:	false
SSDEEP:	24:Yf5+UnwyKeUCA9RAeUadKrfwUiIPNwUYTrG1KU9nmhQqU7hXsQ:YUUnyeUCQieUa3UtPNwUYTWKU9mhXUdV
MD5:	EBA699C38F78563D7D51D9A5472A0C88
SHA1:	7929B3F1D1A9E6DD03C7A735A329E412BCD639AE
SHA-256:	4F9E6544B82D9CB22040290F9E1CA140279C8CDFADFFA28A21B98A4B71FAC17E
SHA-512:	1E5A77148DCEB391C4823B3E4E298994ACF25267535723651B14BF8E4668D32D563FE428A1697AB3AD0D4F666B442233B98A994F77AC2DDB8081AED46AF43F8
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1691330346.771402,"host":"KVivTTKTVC3D7/hfpnbDFfPAgoVJQnjFfXBq+8P8zk8=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1659794346.771406},{"expiry":1670680760.757667,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1659794360.757673},{"expiry":1691330360.402184,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1659794360.40219},{"expiry":1691330350.945528,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1659794350.945534},{"expiry":1691330361.490677,"host":"i4hyKgaUoHZAMQSjjQXQTS/yqHojznpDCDbFdOAcMec=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1659794361.490681},{"expiry":1691330350.849871,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\50dc6200-9d3b-44eb-a267-f16cc4296171.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):	5.577168084606978
Encrypted:	false

SSDEEP:	384:cVbtiLlKUXc1kXqKf/pUZNCgVLH2HfDYrU2+W614w:XLl5c1kXqKf/pUZNCgVLH2HfErUM617
MD5:	E3AA6603164B458EDC04CA753D348B90
SHA1:	8388B11E94077AE507E492586F37F4AB2D44E905
SHA-256:	13F9DF33D35C0335E4F35375D4D1E9BDB38E28EA9069EDD82C35889F37230D4F
SHA-512:	27D86B646F3F513B7FA76A4B76CE233913F7E9ABC1D09CA04D41CD268E9FF8257520314A09614784AC6728D662D12A110FB1EF2ACFF48533C33C999767BE8F1
Malicious:	false
Reputation:	low
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":"13304267918062255","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\52c535f4-1515-4338-8400-b9e7ea56a616.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):	5368
Entropy (8bit):	4.9942728871522215
Encrypted:	false
SSDEEP:	96:nVl0W1n1pcKIQrok4Mun9JCKL89kL1sbOTcSVuwn:nVr1pcmeB94KSkLCk
MD5:	F3D15C7A37928A1CB985C12A59682075
SHA1:	5ADF6448DDC2AD13E99C6028E405C00CA2ED770E
SHA-256:	DD1F99E956309935C36DFE10F91D4FBCA6CFED3DA9A9799F7C80DA304A423980
SHA-512:	04A214778EE23C2E78949BC2E471BE24AECE12116DC01E8553FA328E0CB1E34DB0A2D7BBA6D38E6AB726AC9EEB18E3C97B1025729CA54733A4F66A55FAD621 9B
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13304267918910757","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"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","

Entropy (8bit):	5.612102326650459
Encrypted:	false
SSDEEP:	48:YB8UQyeUoieU/UtPNwUYTq+UttSU5KUphXUdXFwUq:PUzeUoieU/UtGUV+Ut0U5KUDXUdWUq
MD5:	DE70E94F5B163BA7DEF11625AD2715D8
SHA1:	9A2C6C026350E85794B9A2E179C106D617A70CBF
SHA-256:	B6B31897775C3A463DF68DEAA703461D583A16234EA6B7D3348E4540EA540735
SHA-512:	B6E5E87F8D83947454697A06BE8A6D33786D9CD3AFC88A9FABB03686734DB096233CE9E08E8E29DEB059BA00380F2E204C97FD4DA9EBAB437820BF7664781CE3
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1691330377.459043,"host":"KVivTTKTVC3D7/hfpnbDFfPAgoVJQnjFfXBq+8P8zk8=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1659794377.459046},{"expiry":1670680760.757667,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1659794360.757673},{"expiry":1691330380.105219,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1659794380.105223},{"expiry":1691330350.945528,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1659794350.945534},{"expiry":1691330361.490677,"host":"i4hyKgaUoHZAMQSjjQXQTS/yqHojznpDCDbFdOAcMec=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1659794361.490681},{"expiry":1691330372.681662,"host":"jY3WZ/euW1Cj9dqyBGft5sGafpAINoKynr7n/PnwKYA=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\91cc80f6-5ef4-4a97-a5cf-80fbfda4b929.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):	5.564224479290819
Encrypted:	false
SSDEEP:	384:cVbtiLlKUXc1kXqKf/pUZNCgVLH2HfDYrUMHG5+W814D:XLl5c1kXqKf/pUZNCgVLH2HfErUAGP8W
MD5:	8DEED20EF938FB4CF805EEE0DEA6B569
SHA1:	F99440B7A1268BE7CACECAF571C49A723EC0613C
SHA-256:	EE27DFE872FE6AE60C97B3FAA0A843075E2B4581F414A794912C33ED0BAC68DC
SHA-512:	112CD91AD48C8DA01528CBBEB4E7061C1A3981328852A21C79E162D5C2EE66BCDD4D3B69E60591D84DA534AB0326E56E26CE5A51DE1288EBD8EB48CE84D60858
Malicious:	false
Reputation:	low
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":"13304267918062255","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\94b40b6d-c495-4f3d-8e49-978879b4338a.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):	5613
Entropy (8bit):	5.0146670030698415
Encrypted:	false
SSDEEP:	96:nV0051n1pcKIQkok4Mun9JCKL8/kDjVkL1KRbOTccVuwn:nVZ1pcm/B94KUkDxkLwBq
MD5:	5E0A9DE76473FD20014A2DD290C08DAA
SHA1:	ECDED2C0329EAC5856D60D4317672BB7604C2FC8
SHA-256:	2B06E75A4773838666C810982C2D4EFF5074D390C4F1556AB2B21AC8B81D46F9
SHA-512:	035F119A197D21EF16462D4F2AA1467CB4C9766EF8A8A24E8184F24189865A0B20CC77398B58A387A50154CBE854C2D9C56548E80E9D65A907A97836129D7E78
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13304267918910757","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"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","

Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD160
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUscllJ5n0lTpw5JBHV1Kph3/KM=","i3l8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlXNQxlX:qTCT
MD5:	51A2CBB807F5085530DEC18E45CB8569
SHA1:	7AD88CD3DE5844C7FC269C4500228A630016AB5B
SHA-256:	1C43A1BDA1E458863C46DFAE7FB43BFB3E27802169F37320399B1DD799A819AC
SHA-512:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985DI
Malicious:	false
Reputation:	low
Preview:	.f.5.....f.5.....

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

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

Size (bytes):	372
Entropy (8bit):	5.2506205084606545
Encrypted:	false
SSDEEP:	6:ZoTKIZOq2PWXp+N23iKKdK25+Xqx8chI+IFUtqVOoTKIXaZmwYVOoTKIo+vzkwOx:yTvOva5KkTXfchI3FUtoTda/6TH75f5G
MD5:	0762EE5C4D142460D5464413BB721B31
SHA1:	DA24D3F73755F91F4DE88B428296A860CD08073A
SHA-256:	8070197FCAE0C0BCF0D7B7DD15373EE63CF9B419505D0B5A03534AEC40F097A1
SHA-512:	0666E5150717A048D20F637595530D7C7D61B92DCC0A20752C935F5521830612CE4243109CAF1B0D287819DAFE6ADA2490E78F4907D0A17B8A017FBA0BC2A85D
Malicious:	false
Reputation:	low
Preview:	2022/08/06-06:58:43.482 1a20 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/08/06-06:58:43.483 1a20 Recovering log #3.2022/08/06-06:58:43.484 1a20 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.2506205084606545
Encrypted:	false
SSDEEP:	6:ZoTKIZOq2PWXp+N23iKKdK25+Xqx8chI+IFUtqVOoTKIXaZmwYVOoTKIo+vzkwOx:yTvOva5KkTXfchI3FUtoTda/6TH75f5G
MD5:	0762EE5C4D142460D5464413BB721B31
SHA1:	DA24D3F73755F91F4DE88B428296A860CD08073A
SHA-256:	8070197FCAE0C0BCF0D7B7DD15373EE63CF9B419505D0B5A03534AEC40F097A1
SHA-512:	0666E5150717A048D20F637595530D7C7D61B92DCC0A20752C935F5521830612CE4243109CAF1B0D287819DAFE6ADA2490E78F4907D0A17B8A017FBA0BC2A85D
Malicious:	false
Reputation:	low
Preview:	2022/08/06-06:58:43.482 1a20 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/08/06-06:58:43.483 1a20 Recovering log #3.2022/08/06-06:58:43.484 1a20 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\IndexedDB\https_www.youtube.com_0.indexeddb.leveldb\000001.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//Uv:1qIFUv
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_www.youtube.com_0.indexeddb.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//Uv:1qIFUv
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23

Malicious:	false
Reputation:	low
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_www.youtube.com_0.indexeddb.leveldb\MANIFEST-000001

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	23
Entropy (8bit):	4.142914673354254
Encrypted:	false
SSDEEP:	3:Fdb+4Ll:Zl
MD5:	3FD11FF447C1EE23538DC4D9724427A3
SHA1:	1335E6F71CC4E3CF7025233523B4760F8893E9C9
SHA-256:	720A78803B84CBCC8EB204D5CF8EA6EE2F693BE0AB2124DDF2B81455DE02A3ED
SHA-512:	10A3BD3813014EB6F8C2993182E1FA382D745372F8921519E1D25F70D76F08640E84CB8D0B554CCD329A6B4E6DE6872328650FEFA91F98C3C0CFC204899EE824
Malicious:	false
Reputation:	low
Preview:	.....idb_cmp1.....

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):	6397
Entropy (8bit):	4.896422804686323
Encrypted:	false
SSDEEP:	192:fNDH+zZKwPG4Pmpu6V16/X7JftuTfUztCTF+2P/ipdnKn6rP:fN7+tKwPG4Pmpu6V16/X7JftuTfUzt8I
MD5:	2FF74E28F4D1A7AB323BFA45686477F6
SHA1:	396B880CCF27F58D3DD1ECA4B68C67A7BA72279E
SHA-256:	C6632541864598406AA8A68521D355927D097CC28D7D77D99A307F587CABC7D6
SHA-512:	8C1FCA2F1FCF7102CF9411BDAEF0E9DD6335469F33215C30636359B5BA202A1457CF8C6D013E3CB9CD8FD661411D55CD788A0BA80FD70425821B5B9C733C0EA
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":6,"broken_until":"1659794946","host":"kstatic.googleusercontent.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13306859922068814","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13306859922069771","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advertised_versions":[50],"expiration":"13306859922284588","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"expiration":"13306859922284591","port":443

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):	5613
Entropy (8bit):	5.014586183328064
Encrypted:	false
SSDEEP:	96:nV0051n1pcKIQeEok4Mun9JCKL8/kDjVkL1KRbOTcJVuwn:nVZ1pcmefB94KUkDxkLwBv
MD5:	EE648AFC781264B0841B616E8B001CEE
SHA1:	F54F9793D5D0724578CB15292E89CEE100FDBA29
SHA-256:	761705BF49E448622E4A4FB7D466AA6762E41BEF206C40F049D3E89DEDA35508
SHA-512:	8327059A209A3961635D9A914D231EA2D20E597A6C628810A2F7963CAEA0AADC67A7CC8A2A6505E0BAF0EF6BE268D3A97517B7712BC9DACA230C54F51BA4ACE6
Malicious:	false
Reputation:	low

Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13304267918910757","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"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","

Malicious:	false
Reputation:	low
Preview:	(....9.woy retne.....i.G)D/.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\379f1cbab5b08b6fc9e08681e42d8be311441c88\ae478fa7-70c5-4e36-b39b-4be498dc31c7\index-dir\the-real-index (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	48
Entropy (8bit):	2.9972243200613975
Encrypted:	false
SSDEEP:	3:6DctTEKuigKl:6D1/igKl
MD5:	2A8039AB5C0C71D95E59512DCDA0353A
SHA1:	A336064FDFE91F6AA2BAD9CDD30EE927617ADA48
SHA-256:	EA077AD45D91A0E0CAEA72F37A334303C2D86815972AB36B55250ADFBE922C02
SHA-512:	CCB4D1185312BEE0ED5131743EE7BE55822250FE8BF1E329107CFB8643E6A967F586C7A57E78D45ECED757B618EB4B7D845B60558D26124BD3353B1EB0CCD3DD
Malicious:	false
Reputation:	low
Preview:	(....9.woy retne.....i.G)D/.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\379f1cbab5b08b6fc9e08681e42d8be311441c88\index.txt (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.921029621737615
Encrypted:	false
SSDEEP:	3:PySLUxGTKn:ZLUxGG
MD5:	2892EEE3E20E19A9BA77BE6913508A54
SHA1:	7C4EF82FAA28393C739C517D706AC6919A8FFC49
SHA-256:	4F110831BB434C728A6895190323D159DF6D531BE8C4BB7109864EEB7C989FF2
SHA-512:	B13A336DB33299AB3405E13811E3ED9E5A18542E5D835F2B7130A6FF4C22F74272002FC43E7D9F94AC3AA6A4D53518F87F25D90C29E0D286B6470667EA9336AE
Malicious:	false
Reputation:	low
Preview:	..https://www.youtube.com/

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\379f1cbab5b08b6fc9e08681e42d8be311441c88\index.txt.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.921029621737615
Encrypted:	false
SSDEEP:	3:PySLUxGTKn:ZLUxGG
MD5:	2892EEE3E20E19A9BA77BE6913508A54
SHA1:	7C4EF82FAA28393C739C517D706AC6919A8FFC49
SHA-256:	4F110831BB434C728A6895190323D159DF6D531BE8C4BB7109864EEB7C989FF2
SHA-512:	B13A336DB33299AB3405E13811E3ED9E5A18542E5D835F2B7130A6FF4C22F74272002FC43E7D9F94AC3AA6A4D53518F87F25D90C29E0D286B6470667EA9336AE
Malicious:	false
Reputation:	low
Preview:	..https://www.youtube.com/

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
Reputation:	low
Preview:	....

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\ea3d7a3a-1959-4235-bac5-e3894f7e2431.tmp

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\3059c87a-6592-453b-a83b-7efd9ea88152.tmp

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

File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BI
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

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

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BI
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity (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):	1879
Entropy (8bit):	5.611897807173598

Encrypted:	false
SSDEEP:	48:YB8USAFeUCieU/UtPNwUYTq+UttSU5KUG4TsUNkhXUdXpwUz:PUFFeUCieU/UtGUV+Ut0U5KU7sUNcXUL
MD5:	751A402359F0F772CC4550BBDC277085
SHA1:	730BD54ACF02F93248C2D0B263CECFC09C296F53
SHA-256:	6EA29EEF18E80D119DC4020945E1528CE6AA550564DA09F23B1F2B41D05BF0C0
SHA-512:	C7D3F774435886A490CC03EEBE6ADDAF5F0DA366D174572C3AD1D292973213EE653B75FC10C92A644673503F7237F8D707381DA82E2E7D2790172A079DF3272I
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1691330377.459043,"host":"KVivTTKTVC3D7/hfpnbDFfPAgoVJQnjFfXBq+8P8zk8=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1659794377.459046},{"expiry":1670680810.218128,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1659794410.218132},{"expiry":1691330380.105219,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1659794380.105223},{"expiry":1691330350.945528,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1659794350.945534},{"expiry":1691330361.490677,"host":"i4hyKgaUoHZAMQSjjQXQTS/yqHojznpDCDbFdOAcMec=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1659794361.490681},{"expiry":1691330372.681662,"host":"jY3WZ/euW1Cj9dqyBGft5sGafpAINoKynr7n/PnwKYA=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\aa2a95b0-bf77-4388-8452-3b2282038708.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):	6397
Entropy (8bit):	4.896422804686323
Encrypted:	false
SSDEEP:	192:fNDH+zZKwPG4Pmpu6V16/X7JftuTfUztCTF+2P/ipdnKn6rP:fN7+tKwPG4Pmpu6V16/X7JftuTfUzt8I
MD5:	2FF74E28F4D1A7AB323BFA45686477F6
SHA1:	396B880CCF27F58D3DD1ECA4B68C67A7BA72279E
SHA-256:	C6632541864598406AA8A68521D355927D097CC28D7D77D99A307F587CABC7D6
SHA-512:	8C1FCA2F1FCF7102CF9411BDAEF0E9DD6335469F33215C30636359B5BA202A1457CF8C6D013E3CB9CD8FD661411D55CD788A0BA80FD70425821B5B9C733C0EA
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":6,"broken_until":"1659794946","host":"kstatic.googleusercontent.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13306859922068814","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13306859922069771","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advertised_versions":[50],"expiration":"13306859922284588","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"expiration":"13306859922284591","port":443

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b7fbad58-f0aa-4441-9a85-fe27e9e0ed77.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
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b8689bd8-874f-4663-8900-5cd354e668ce.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):	5613
Entropy (8bit):	5.014586183328064
Encrypted:	false
SSDEEP:	96:nV0051n1pcKIQeEok4Mun9JCKL8/kDjVkL1KRbOTcJVuwn:nVZ1pcmefB94KUkDxkLwBv

MD5:	EE648AFC781264B0841B616E8B001CEE
SHA1:	F54F9793D5D0724578CB15292E89CEE100FDBA29
SHA-256:	761705BF49E448622E4A4FB7D466AA6762E41BEF206C40F049D3E89DEDA35508
SHA-512:	8327059A209A3961635D9A914D231EA2D20E597A6C628810A2F7963CAEA0AADC67A7CC8A2A6505E0BAF0EF6BE268D3A97517B7712BC9DACA230C54F51BA4AC E6
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13304267918910757","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcom e_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":1 0,"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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e45ba11d-f760-4aa2-902c-2c2f4639e799.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):	874
Entropy (8bit):	5.582853129548652
Encrypted:	false
SSDEEP:	24:Yf5+Ue9RAeUuKrfwUiGG1KU9nmhQqU7hXsQ:YUUyieU6U0KU9mhXUdXF
MD5:	BFC87D9FEC586FADDAB98B131A6964A3
SHA1:	8A375E3367AE646AEDF95D534F818957D82341C2
SHA-256:	98DF27114439A8713F072A983FDA584926866854A050BE61C118B44DF9AD1DEA
SHA-512:	CF1316690DF645D84CAD3825687F3C5759ACF0BA940D3136EE51647C1E83E13569C53945F88F5C7F4ABDD1207891B9E417895CBDABB3291DBB14A3FAB63374E0
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1691330346.771402,"host":"KVivTTKTVC3D7/hfpnbDFfPAgoVJQnjFfXBq+8P8zk8=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1659794346.771406},{"expiry":1691330346.919907,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1659794346.919913},{"expiry":1691330350.945528,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1659794350.945534},{"expiry":1691330350.849871,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1659794350.849875},{"expiry":1691330324.185718,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1659794324.185723}],"version":2}

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
Reputation:	low
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
Reputation:	low
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):	211818
Entropy (8bit):	6.042558684735572
Encrypted:	false
SSDEEP:	6144:wKaXlScilZFWzn/tu6I7pTqzKaqfIlUOoSiuR/:wKIMZMjFu6OpM5o4
MD5:	39C0191113314AB863C3BB4BD50A472C
SHA1:	5B80772CFD179779B2F06A5697155BFBAEFD257E
SHA-256:	F79EF3197050A88D5D3DCED08D74E7BE58C206F03F712D6F2A7DE63756A8CDFF
SHA-512:	2FF06147690F020729080F318DB6E78D64F831AB96984CD606E3716A7EF11F074BCA78FD61565BF04DD3B5BC109B99D3CBF56C11758A7C8F50D39EBB0B592D9
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":1.659794320508321e+12,"network":1.659761922e+12,"ticks":113483142.0,"uncertainty":4255693.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639496290"},"plugins":{"metadata":{"adobe-flash-player":{"disp

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7439481769839977
Encrypted:	false
SSDEEP:	384:NPLM8uhvu1ykVZrofN0rFvQ83/MWXHirGr+rZ+wexvSGi5r1omBNfNOsEwvOOSMb:RqWpJmWAzseXiMOIHf6oKiUU9J
MD5:	2B979F3AFD5E4CAC0343D48943132198
SHA1:	603F879F1FDE0AAC2F009493D6AD08C1CF218099
SHA-256:	9A87C9CC75A0679943EAAAD04DD2DC30B93DED2582EB66BD7A2EAA6DF4CCA4AE
SHA-512:	4A174A7206B64368ACA43BEDF7ADE41B8C4D9C8336A6AB8040F02DC98368C30921AC969A5AAA9D4344180B51809158903D964942E92474965128572258A87E06
Malicious:	false
Reputation:	low
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....d8.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\a63e5fd8-a01d-4e45-9c44-7330264d4008.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.744418824729187
Encrypted:	false
SSDEEP:	384:dPLM8uhvu1ykVZrofN0rFvQ83/MWXHirGr+rZ+wexvSGi5r1omBWNOsEwvOOSMNJ:BqWpJmWnzseXiMOIHf6oKiUU95
MD5:	B1C8FF453EF1BA3B045D5B0A91B9E2D5
SHA1:	7C31B00CDC4BA9AF572B83049B6B04A947B42900
SHA-256:	04672F6C32F77C471425891BB04737E514938211FE9E02361FAAF8BA63BFC9AF
SHA-512:	DCDF9DD8DB247AF9DC32F3CB90A6AF6492F381CF49D54F1F505371A47610411F1B7AD71080EFEFCC3638BAF2DE3928F0CE88AA38BABCA6D0FF2AF0EA6F64D 066
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....d8.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\d2919e16-2e5f-4d2d-b26b-f93daf9d6b3c.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):	220084
Entropy (8bit):	6.069851290618565
Encrypted:	false
SSDEEP:	6144:1IKaXlScilZFWzn/tu6I7pTqzKaqfIlUOoSiuR/:1IKIMZMjFu6OpM5o4
MD5:	8DFD69A32BDA5EB7ABE9FD554BF65408
SHA1:	9C15E09E4740A99F7D3F2F73781B4B024291DDE9
SHA-256:	99ED3BC4C594C4292C7B96D92F855B44FE9402326A457383F327FC4695E2D818
SHA-512:	E1E8AD3CCFA9F18F5C2477C857A6D22F7AF03EADEE009A8618636C4CC29900159FB199B554A308D065B45C1D33E6037F20AD8BF1289F6FF42F60CF302F36990
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":1.659794320508321e+12,"network":1.659761922e+12,"ticks":113483142.0,"uncertainty":4255693.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639496290"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\02bf7525-dc4c-4c93-a8a6-85a18a8cc3ca.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
Reputation:	low
Preview:	Cr24.....0.."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u.. ..k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2.. ;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.I....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5SI..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\6060_1494985660_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
Reputation:	low

Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiO lt7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY19wbWFpbl9xc29uIiwicm9vdF9oYXNoIjoiVkNUSHNJVHNUSXVncWNhV2ctWHVpTU1 sdWloV1FSTE1sQnpTTGprdGhETSJ9LHsicGF0aCI6Il9wbGF0Zm9ybV9zcGVjaWZpYy94ODZfNjQvcG5hY2xfcHVibGljX3g4Nl82NF9jcnRiZWdpbl9mb3JfZWhfbyIsI nJvb3RfaGFzaCI6ImxlNWt2a1BvSVZZczZKVHhyOHc5Q2MxXzloVEJCX3lVSlF6VDZseVVNd0kifSx7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWN sX3B1YmxpY194ODZfNjRfY3J0YmVnaW5fbyIsInJvb3RfaGFzaCI6IkVuLVFQTW1HUm1xbG9Ud1gzOTAzckpsMkw0R25sQmdET1FhZlNKaHJ4Nk0ifSx7InBhdGgiOiJfc GxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY194ODZfNjRfY3J0ZW5kX28iLCJyb290X2hhc2giOiJkT2lJVzRmdEdGNW9FY0k1UXYyYjBmd XNrUlYyaUVtdmxhbmV6MlpFc3VvIn0seyJwYXRoIjoiX3BsYXRmb3JtX3NwZWNpZmljL3g4Nl82NC9wbmFjbF9wdWJsaWNfeDg2XzY0X2xkX25leGUiLCJyb290X2hhc2g iOiIzNEU5QU9EMmpqLWNoMzZQZ0NVV0YtMUpYWVhVdlNGY1I4bks1aWppcWNjIn0seyJwYXRoIjoiX3B
C:\Users\user\AppData\Local\Temp\6060_1494985660_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
Reputation:	low
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\6060_1494985660_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
Reputation:	low
Preview:	.ELF.....>.....@.....@.....PH.....,$J.I=....J.$<A[..@.A...M..A..ffffff.....PH.....,$J.I=....J.$<A[..D..A...M..A..ffffff..... ....PH..1..,$J.I=....J.$<A[.....A...M..A..ffffff.....PH..SP..h.....fff.....h.....fff.....J.$<[.,$J.I=....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\6060_1494985660_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
Reputation:	low

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\6060_1494985660_platform_specific\x86_64\pnacl_public_x86_64_crtend_o

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	1520
Entropy (8bit):	2.799960074375893
Encrypted:	false
SSDEEP:	12:Bvx/ekjlM/NQQmTfR9yp9396QQmTfR9C6wRqD8MTDDw7lEOkSbfuEAXwX6BX2U8b:bDjO/NbmT3296bmT3Twk8qDwh7b7CD8
MD5:	75E79F5DB777862140B04CC6861C84A7
SHA1:	4DB7BDC80206765461AC68CEC03CE28689BBEE0C
SHA-256:	74E8885B87ED185E6811C23942FD9BD1FBAC9115768849AF95A9DECF6644B2EA
SHA-512:	FE3F86E926759E71494F2060C4ED3C883EBCAF20CB129A5AD7F142766C33FAB10B5FABC3C7C938E0E895E27EA0AC03CBFE8D0EEABF5300A4AD07F67FD96CC 253
Malicious:	false
Reputation:	low
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\6060_1494985660_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:	8EF8689E00E4B210A30444D18ED6247F364995ABEB2FD272064C3AF671EEDB4D9B8B67CA56F72FEBF8F56896D4EA7EC4B10CB445FFA1C710C1F312E9DA0E48 96
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
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\6060_1494985660_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:	7C2F9BF90EB1F43C17B4E14A077759FA9DC62A7239890975B2D6FD543B31289DC3B49AE456CA73B98DE9AC372034F340C708D23D9D3AAB05CCBDABDC56A63 4E

Malicious:	false
Reputation:	low
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.n acl_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_4 xi32_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\6060_1494985660_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:Hf0mOXYmeKzQUIdedRFvT5p1Ee2HyAIL3O4:Hf7OXdmWRJT5p1R2HyAhO4
MD5:	C37CA2EB468E6F05A4E37DF6E6020D0F
SHA1:	EA787E5EADFB488632EC60D8B80B555796FA9FE9
SHA-256:	C1483ED423FEE15D86E8B5D698B2CDAB89186CE7FF9C4E3D5F3F961FD80D7C6E
SHA-512:	01281DE92B281FB29E1ACA96AA64B740B65CC3A9097307827F0D8DB9E1C164C56AFCDFA0BF138EA670A596D55CE2C8D722760744E9FC9343BB6514417BF333E A
Malicious:	false
Reputation:	low
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\6060_1494985660_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
Reputation:	low
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\6060_1494985660_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/+I
MD5:	F950F89D06C45E63CE9862BE59E937C9
SHA1:	9CFAD34139CC428CE0C07A869C15B71A9632365D
SHA-256:	945B1C8A1666CBF05E8B8941B70D9D044BAAFB59B006F728F8995072DE7C4C40

SHA-512:	F9AFBB800A875EDCC63DEA4986179E73632B3182951A99C8B3D37DB454EFD7CC7192ECA5AC87514918A858BAD6DAEAB59548CA2E90EADA9900EF5B9F08E62CFC
Malicious:	false
Reputation:	low
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\6060_1494985660_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: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
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\6060_1494985660_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%
Reputation:	low
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\6060_1494985660\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
Reputation:	low
Preview:	1.6f6bc93dcd62dc251850d2ff458fda96083ceb7fbe8eeb11248b8485ef2aea23

C:\Users\user\AppData\Local\Temp\6060_1494985660\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
Reputation:	low
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\6060_1654857163\Recovery.crx3

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	145035
Entropy (8bit):	**7.995615725071868**
Encrypted:	**true**
SSDEEP:	3072:TdgEhmDf+E8VY0x81Rkc6L2oqzqkPEu30gZlc3G2ZknF:TyEhmDf+/+Fnkj6lEukgZyyF
MD5:	EA1C1FFD3EA54D1FB117BFDBB3569C60
SHA1:	10958B0F690AE8F5240E1528B1CCFFFF28A33272
SHA-256:	7C3A6A7D16AC44C3200F572A764BCE7D8FA84B9572DD028B15C59BDCCBC0A77D
SHA-512:	6C30728CAC9EAC53F0B27B7DBE2222DA83225C3B63617D6B271A6CFEDF18E8F0A8DFFA1053E1CBC4C5E16625F4BBC0D03AA306A946C9D72FAA4CEB779F8FFCAF
Malicious:	false
Reputation:	low
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\6060_1654857163_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:	BCBE40CAFAA4B14566D91E361D8FB7F0288D5C459FA478AA4C575444DA4D406E1076FC0B3A31D4A9E5EE034F0FE15A0EFE8A8A52B838DE94B96D3E488D28FCFE

Malicious:	false
Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJSZWNvdmVyeS5jcngzIiwicm9vdF9oYXNoIjoiaGdCR051SzhNR2NKaDlfNmZQaFdEWmpVYUFKeklzeDlJS21DUEZvb0dfUSJ9LHsicGF0aCI6Im1hbmlmZXN0Lmpzb24iLCJyb290X2hhc2giOiIwYXduVFBFQmdDRHkyV05hVVk3Um9mSWN3c3ZwNHFRNUxzZVMxVXRiVXY0In1dLCJmb3JtYXQiOiJ0cmVlaGFzaCIsImhhc2hfYmxvY2tfc2l6ZSI6NDA5Nn1dLCJpdGVtX2lkIjoiaWhubGNlbm9jZWhnZGFlZ2RtaGJpZGpobmhkY2hmbW0iLCJpdGVtX3ZlcnNpb24iOiIxLjMuMzYuMTQxIiwicHJvdG9jb2xfdmVyc2lvbiI6MX0","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"iFuMX_kOZ-zJ7KVu6Lxb3rHWZgQvkZhv25x_SGlBiDV_okALrGbj6rUOWyNNNsHXMnT118XZmA696XR8qkr4dwT5Gvez-9gi-WYBY7XBkgo7v6NspGgJF89BNCeI-P9k-zBHOGgrf-fCEiAcoM7xCx9_f8qlRy7nhQPyjOIHn5eEJEir0uSu6gdqR9afnVZ3UoR-VOLdOBt7fA4ee38MP2ut5qWU50F5dvIezfKkTVDMHwztvcLCy6R9SVkdSYv6jwWGccYRl-aclvkkHu6SnbZGI7fmDZdkcBAxBHYEZZMmvb76ro4SO15GDyEVAo_Qf4trdrY_GyN_Bm73imCTjgtoGc

C:\Users\user\AppData\Local\Temp\6060_1654857163\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
Reputation:	low
Preview:	1.aeedb246d19256a956fedaa89fb62423ae5bd8855a2a1f3189161cf045645a19

C:\Users\user\AppData\Local\Temp\6060_1654857163\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	195
Entropy (8bit):	4.682333395896383
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFJ9LAG9Xg0XTFHqS1wP/pEeSWU4pv/8F/FxLj2RF2fcTZTotL:F6VlM90ggITgS1wnuWfB0NpK4aotL
MD5:	7A8E3A0B6417948DF4D49F3915428D7A
SHA1:	4FC084AABDB13483567D5C417C7ED8FD16726A80
SHA-256:	D1AC274CF1018020F2D9635A518ED1A1F21CC2CBE9E2A4392EC792D54B5B52FE
SHA-512:	064D84A57B28C19AD10742859DA493D0826B47ADC632F6C623DFB4DE36D72A9D29BE98518061A9FFD42D99FCF01F27DE39CE74782B3A5ACBBE11DFDDEEAB59A1
Malicious:	false
Reputation:	low
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\d5fcf379-0e69-4ef2-b6f1-ad49e4693103.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
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\scoped_dir6060_68835047\02bf7525-dc4c-4c93-a8a6-85a18a8cc3ca.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
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.| 1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u.. ..k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..)....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2.. ;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z ....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir6060_68835047\CRX_INSTALL_locales\bg\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F7700C
Malicious:	false
Reputation:	low
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_dir6060_68835047\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
Reputation:	low
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_dir6060_68835047\CRX_INSTALL_locales\cs\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D8488 CB
Malicious:	false
Reputation:	low
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_dir6060_68835047\CRX_INSTALL_locales\da\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5 E0A
Malicious:	false
Reputation:	low
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_dir6060_68835047\CRX_INSTALL_locales\de\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB80 552
Malicious:	false
Reputation:	low
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_dir6060_68835047\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
Reputation:	low
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_dir6060_68835047\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
Reputation:	low
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_dir6060_68835047\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
Reputation:	low
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_dir6060_68835047\CRX_INSTALL_locales\es\messages.json

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

Entropy (8bit):	4.450938335136508
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyZnLAOfTY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OGAOffD
MD5:	82719BD3999AD66193A9B0BB525F97CD
SHA1:	41194D511F1ACC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE01 28
Malicious:	false
Reputation:	low
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_dir6060_68835047\CRX_INSTALL_locales\es_419\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	637
Entropy (8bit):	4.47253983486615
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34GLO03OyZnLAOfTYiJD:1HEvaC6WYpcDeEFxq8Zp4LlOGAOfvD
MD5:	6B2583D8D1C147E36A69A88009CBEBC7
SHA1:	4D4DEEB4BE6AA0181825F3371A761ABC5B4D5937
SHA-256:	6659BC3705311D7641A73995DCFEA80C7734F2F4EBBC3787B3892A240348324F
SHA-512:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA 53
Malicious:	false
Reputation:	low
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_dir6060_68835047\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
Reputation:	low
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_dir6060_68835047\CRX_INSTALL_locales\fi\messages.json

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

MD5:	3A01FEE829445C482D1721FF63153D16
SHA1:	F3EAAADDC03F943FC88B30B67F534AA13E3336DD
SHA-256:	0BDE54B20845124113383B6EB81E43A0F05E4EB0C44BEE3C1DFAC4CC5FEC2836
SHA-512:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BE/D8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Storen maksut".. },.. "app_name": {.. "message": "Chrome Web Storen maksut".. },.. "craw_app_unavailable": {.. "message": "Sovellus ei ole t.ll. hetkell. k.ytett.viss..".. },.. "craw_connect_to_network": {.. "message": "Muodosta verkkoyhteys.".. },.. "iap_unavailable": {.. "message": "Sovelluksen sis.iset maksut eiv.t ole t.ll. hetkell. k.ytett.viss..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Kirjaudu sis..n Chromeen.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6060_68835047\CRX_INSTALL_locales\fil\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	658
Entropy (8bit):	4.5231229502550745
Encrypted:	false
SSDEEP:	12:1HEJADlbGGADlb+WYpU34hTUT+dgHfZAFFZO8ZpU34hTjzeT03OyZnLAOfTYHfvF:1HEYah6WYp7TUSoxOS8Zp7TOsOGAOfqV
MD5:	57AF5B654270A945BDA8053A83353A06
SHA1:	EEEF7A4F869F97CF471A05D345E74F982D15E167
SHA-256:	EC002ED92359F67818B49455DFC579E140368E6A004080AF022FD4F57F6B03F2
SHA-512:	5F0AE839FCF3F4EA48FF41A76655AE0F3821564AFD5D42FBB9FBB9A38E8D8F7BB5E9B6F71064588CD441261F644095A44A755C134CE546D506D9A21E488BAF52
Malicious:	false
Reputation:	low
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_dir6060_68835047\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
Reputation:	low
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_dir6060_68835047\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
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome ... .".. },.. "app_name": {.. "message": "Chrome ... .".. },.. "craw_app_unavailable": {.. "messa ge": "......... .. ..".. },.. "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_dir6060_68835047\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:	D7629978FC031EA5F716F9C1065FB2FEAB48C15F10CD68830DC966FA1002C03DDC7ACDE314C7D075F9F3A0A68552A6ACBCCDEE24CF20B6C3DD1BCE6562D0 96E
Malicious:	false
Reputation:	low
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 comple ted.".. },.. "please_sign_in": {.. "message": "Prijavite se na Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6060_68835047\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
Reputation:	low
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_dir6060_68835047\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
Reputation:	low

Preview:	{.. "app_description": {.. "message": "Pembayaran Chrome Webstore".. },.. "app_name": {.. "message": "Pembayaran Chrome Webstore".. },.. "craw_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 completed.".. },.. "please_sign_in": {.. "message": "Harap masuk ke Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6060_68835047\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
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamenti Chrome Web Store".. },.. "app_name": {.. "message": "Pagamenti Chrome Web Store".. },.. "craw_app_unavailable": {.. "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.".. }..}..

Static File Info

No static file info

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 6, 2022 06:58:41.534568071 CEST	49741	443	192.168.2.3	142.250.186.110
Aug 6, 2022 06:58:41.534605026 CEST	443	49741	142.250.186.110	192.168.2.3
Aug 6, 2022 06:58:41.534693956 CEST	49741	443	192.168.2.3	142.250.186.110
Aug 6, 2022 06:58:41.534923077 CEST	49742	443	192.168.2.3	192.243.59.12
Aug 6, 2022 06:58:41.535006046 CEST	443	49742	192.243.59.12	192.168.2.3
Aug 6, 2022 06:58:41.535101891 CEST	49742	443	192.168.2.3	192.243.59.12
Aug 6, 2022 06:58:41.535533905 CEST	49743	443	192.168.2.3	142.250.185.205
Aug 6, 2022 06:58:41.535566092 CEST	443	49743	142.250.185.205	192.168.2.3
Aug 6, 2022 06:58:41.535660028 CEST	49743	443	192.168.2.3	142.250.185.205
Aug 6, 2022 06:58:41.536438942 CEST	49745	443	192.168.2.3	192.243.59.12
Aug 6, 2022 06:58:41.536492109 CEST	443	49745	192.243.59.12	192.168.2.3
Aug 6, 2022 06:58:41.536577940 CEST	49745	443	192.168.2.3	192.243.59.12
Aug 6, 2022 06:58:41.536827087 CEST	49741	443	192.168.2.3	142.250.186.110
Aug 6, 2022 06:58:41.536856890 CEST	443	49741	142.250.186.110	192.168.2.3
Aug 6, 2022 06:58:41.537133932 CEST	49742	443	192.168.2.3	192.243.59.12
Aug 6, 2022 06:58:41.537193060 CEST	443	49742	192.243.59.12	192.168.2.3
Aug 6, 2022 06:58:41.537497044 CEST	49743	443	192.168.2.3	142.250.185.205
Aug 6, 2022 06:58:41.537514925 CEST	443	49743	142.250.185.205	192.168.2.3
Aug 6, 2022 06:58:41.537852049 CEST	49745	443	192.168.2.3	192.243.59.12
Aug 6, 2022 06:58:41.537905931 CEST	443	49745	192.243.59.12	192.168.2.3
Aug 6, 2022 06:58:41.596227884 CEST	443	49743	142.250.185.205	192.168.2.3
Aug 6, 2022 06:58:41.597384930 CEST	443	49741	142.250.186.110	192.168.2.3
Aug 6, 2022 06:58:41.600312948 CEST	49741	443	192.168.2.3	142.250.186.110
Aug 6, 2022 06:58:41.600327015 CEST	443	49741	142.250.186.110	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 6, 2022 06:58:41.600641012 CEST	443	49741	142.250.186.110	192.168.2.3
Aug 6, 2022 06:58:41.600716114 CEST	49741	443	192.168.2.3	142.250.186.110
Aug 6, 2022 06:58:41.600860119 CEST	49743	443	192.168.2.3	142.250.185.205
Aug 6, 2022 06:58:41.600895882 CEST	443	49743	142.250.185.205	192.168.2.3
Aug 6, 2022 06:58:41.601423979 CEST	443	49741	142.250.186.110	192.168.2.3
Aug 6, 2022 06:58:41.601499081 CEST	49741	443	192.168.2.3	142.250.186.110
Aug 6, 2022 06:58:41.602092981 CEST	443	49743	142.250.185.205	192.168.2.3
Aug 6, 2022 06:58:41.602164030 CEST	49743	443	192.168.2.3	142.250.185.205
Aug 6, 2022 06:58:41.878138065 CEST	443	49745	192.243.59.12	192.168.2.3
Aug 6, 2022 06:58:41.887106895 CEST	443	49742	192.243.59.12	192.168.2.3
Aug 6, 2022 06:58:41.979054928 CEST	49745	443	192.168.2.3	192.243.59.12
Aug 6, 2022 06:58:41.980992079 CEST	49742	443	192.168.2.3	192.243.59.12
Aug 6, 2022 06:58:42.142581940 CEST	49742	443	192.168.2.3	192.243.59.12
Aug 6, 2022 06:58:42.142637014 CEST	443	49742	192.243.59.12	192.168.2.3
Aug 6, 2022 06:58:42.142760992 CEST	49745	443	192.168.2.3	192.243.59.12
Aug 6, 2022 06:58:42.142812014 CEST	443	49745	192.243.59.12	192.168.2.3
Aug 6, 2022 06:58:42.143049955 CEST	49743	443	192.168.2.3	142.250.185.205
Aug 6, 2022 06:58:42.143290997 CEST	443	49743	142.250.185.205	192.168.2.3
Aug 6, 2022 06:58:42.143877983 CEST	49741	443	192.168.2.3	142.250.186.110
Aug 6, 2022 06:58:42.144144058 CEST	443	49741	142.250.186.110	192.168.2.3
Aug 6, 2022 06:58:42.145649910 CEST	443	49742	192.243.59.12	192.168.2.3
Aug 6, 2022 06:58:42.145678997 CEST	443	49742	192.243.59.12	192.168.2.3
Aug 6, 2022 06:58:42.145819902 CEST	443	49745	192.243.59.12	192.168.2.3
Aug 6, 2022 06:58:42.145848989 CEST	443	49745	192.243.59.12	192.168.2.3
Aug 6, 2022 06:58:42.145880938 CEST	49742	443	192.168.2.3	192.243.59.12
Aug 6, 2022 06:58:42.145904064 CEST	49745	443	192.168.2.3	192.243.59.12
Aug 6, 2022 06:58:42.167382002 CEST	49743	443	192.168.2.3	142.250.185.205
Aug 6, 2022 06:58:42.167423964 CEST	443	49743	142.250.185.205	192.168.2.3
Aug 6, 2022 06:58:42.167493105 CEST	49741	443	192.168.2.3	142.250.186.110
Aug 6, 2022 06:58:42.167543888 CEST	443	49741	142.250.186.110	192.168.2.3
Aug 6, 2022 06:58:42.168541908 CEST	49742	443	192.168.2.3	192.243.59.12
Aug 6, 2022 06:58:42.168828964 CEST	443	49742	192.243.59.12	192.168.2.3
Aug 6, 2022 06:58:42.168889046 CEST	49745	443	192.168.2.3	192.243.59.12
Aug 6, 2022 06:58:42.169121027 CEST	443	49745	192.243.59.12	192.168.2.3
Aug 6, 2022 06:58:42.169720888 CEST	49742	443	192.168.2.3	192.243.59.12
Aug 6, 2022 06:58:42.169747114 CEST	443	49742	192.243.59.12	192.168.2.3
Aug 6, 2022 06:58:42.195791960 CEST	443	49741	142.250.186.110	192.168.2.3
Aug 6, 2022 06:58:42.195921898 CEST	49741	443	192.168.2.3	142.250.186.110
Aug 6, 2022 06:58:42.195943117 CEST	443	49741	142.250.186.110	192.168.2.3
Aug 6, 2022 06:58:42.196019888 CEST	49741	443	192.168.2.3	142.250.186.110
Aug 6, 2022 06:58:42.220875025 CEST	443	49743	142.250.185.205	192.168.2.3
Aug 6, 2022 06:58:42.220972061 CEST	49743	443	192.168.2.3	142.250.185.205
Aug 6, 2022 06:58:42.220997095 CEST	443	49743	142.250.185.205	192.168.2.3
Aug 6, 2022 06:58:42.221149921 CEST	443	49743	142.250.185.205	192.168.2.3
Aug 6, 2022 06:58:42.221426010 CEST	49743	443	192.168.2.3	142.250.185.205
Aug 6, 2022 06:58:42.243319988 CEST	49743	443	192.168.2.3	142.250.185.205
Aug 6, 2022 06:58:42.243397951 CEST	443	49743	142.250.185.205	192.168.2.3
Aug 6, 2022 06:58:42.244895935 CEST	49741	443	192.168.2.3	142.250.186.110
Aug 6, 2022 06:58:42.244926929 CEST	443	49741	142.250.186.110	192.168.2.3
Aug 6, 2022 06:58:42.279084921 CEST	49745	443	192.168.2.3	192.243.59.12
Aug 6, 2022 06:58:42.279114008 CEST	443	49745	192.243.59.12	192.168.2.3
Aug 6, 2022 06:58:42.279145002 CEST	49742	443	192.168.2.3	192.243.59.12
Aug 6, 2022 06:58:42.281856060 CEST	443	49742	192.243.59.12	192.168.2.3
Aug 6, 2022 06:58:42.282006025 CEST	443	49742	192.243.59.12	192.168.2.3
Aug 6, 2022 06:58:42.282155037 CEST	49742	443	192.168.2.3	192.243.59.12
Aug 6, 2022 06:58:42.326669931 CEST	49742	443	192.168.2.3	192.243.59.12
Aug 6, 2022 06:58:42.326725006 CEST	443	49742	192.243.59.12	192.168.2.3
Aug 6, 2022 06:58:42.377476931 CEST	49750	443	192.168.2.3	172.217.16.206
Aug 6, 2022 06:58:42.377502918 CEST	443	49750	172.217.16.206	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 6, 2022 06:58:42.377613068 CEST	49750	443	192.168.2.3	172.217.16.206
Aug 6, 2022 06:58:42.377789974 CEST	49750	443	192.168.2.3	172.217.16.206
Aug 6, 2022 06:58:42.377803087 CEST	443	49750	172.217.16.206	192.168.2.3
Aug 6, 2022 06:58:42.379074097 CEST	49745	443	192.168.2.3	192.243.59.12
Aug 6, 2022 06:58:42.430558920 CEST	443	49750	172.217.16.206	192.168.2.3
Aug 6, 2022 06:58:42.432329893 CEST	49750	443	192.168.2.3	172.217.16.206
Aug 6, 2022 06:58:42.432360888 CEST	443	49750	172.217.16.206	192.168.2.3
Aug 6, 2022 06:58:42.433281898 CEST	443	49750	172.217.16.206	192.168.2.3
Aug 6, 2022 06:58:42.433401108 CEST	49750	443	192.168.2.3	172.217.16.206
Aug 6, 2022 06:58:42.435565948 CEST	443	49750	172.217.16.206	192.168.2.3
Aug 6, 2022 06:58:42.435698986 CEST	49750	443	192.168.2.3	172.217.16.206
Aug 6, 2022 06:58:42.437128067 CEST	49750	443	192.168.2.3	172.217.16.206
Aug 6, 2022 06:58:42.437292099 CEST	49750	443	192.168.2.3	172.217.16.206
Aug 6, 2022 06:58:42.437306881 CEST	443	49750	172.217.16.206	192.168.2.3
Aug 6, 2022 06:58:42.437335968 CEST	443	49750	172.217.16.206	192.168.2.3
Aug 6, 2022 06:58:42.485987902 CEST	443	49750	172.217.16.206	192.168.2.3
Aug 6, 2022 06:58:42.486116886 CEST	49750	443	192.168.2.3	172.217.16.206

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 6, 2022 06:58:41.501072884 CEST	192.168.2.3	8.8.8.8	0xd83c	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:41.504105091 CEST	192.168.2.3	8.8.8.8	0xab47	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:41.508738995 CEST	192.168.2.3	8.8.8.8	0x343f	Standard query (0)	spatterjointposition.com	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:42.335333109 CEST	192.168.2.3	8.8.8.8	0x4ed5	Standard query (0)	google.com	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:42.513662100 CEST	192.168.2.3	8.8.8.8	0x410f	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:43.448754072 CEST	192.168.2.3	8.8.8.8	0xf2ff	Standard query (0)	apis.google.com	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:46.155169964 CEST	192.168.2.3	8.8.8.8	0x85ad	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:02.631071091 CEST	192.168.2.3	8.8.8.8	0xe00	Standard query (0)	about.google	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:03.080589056 CEST	192.168.2.3	8.8.8.8	0x217f	Standard query (0)	csp.withgoogle.com	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:04.423790932 CEST	192.168.2.3	8.8.8.8	0x2ece	Standard query (0)	lh3.googleusercontent.com	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:05.010010958 CEST	192.168.2.3	8.8.8.8	0x2d07	Standard query (0)	scone-pa.clients6.google.com	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:05.218149900 CEST	192.168.2.3	8.8.8.8	0x740	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:06.356579065 CEST	192.168.2.3	8.8.8.8	0x91b7	Standard query (0)	kstatic.googleusercontent.com	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:10.204241991 CEST	192.168.2.3	8.8.8.8	0x6ee3	Standard query (0)	store.google.com	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:20.080449104 CEST	192.168.2.3	8.8.8.8	0x6efe	Standard query (0)	www.youtube.com	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:21.207308054 CEST	192.168.2.3	8.8.8.8	0xe550	Standard query (0)	www.google.de	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:21.209151030 CEST	192.168.2.3	8.8.8.8	0xab97	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:22.041565895 CEST	192.168.2.3	8.8.8.8	0xf03f	Standard query (0)	play.google.com	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:26.042717934 CEST	192.168.2.3	8.8.8.8	0xbccf	Standard query (0)	lh3.googleusercontent.com	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:26.335093975 CEST	192.168.2.3	8.8.8.8	0x7928	Standard query (0)	mail.google.com	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:33.837563038 CEST	192.168.2.3	8.8.8.8	0xcf8f	Standard query (0)	about.google	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:39.890069962 CEST	192.168.2.3	8.8.8.8	0x9f93	Standard query (0)	www.google.de	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 6, 2022 06:59:41.603730917 CEST	192.168.2.3	8.8.8.8	0xadbd	Standard query (0)	static.doubleclick.net	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:42.432980061 CEST	192.168.2.3	8.8.8.8	0xa042	Standard query (0)	yt3.ggpht.com	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:42.439502954 CEST	192.168.2.3	8.8.8.8	0x9703	Standard query (0)	i.ytimg.com	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:46.941505909 CEST	192.168.2.3	8.8.8.8	0x3ac6	Standard query (0)	yt3.ggpht.com	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:46.948540926 CEST	192.168.2.3	8.8.8.8	0x539d	Standard query (0)	i.ytimg.com	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:47.860265970 CEST	192.168.2.3	8.8.8.8	0x1ea5	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:49.696127892 CEST	192.168.2.3	8.8.8.8	0x10b0	Standard query (0)	accounts.youtube.com	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:10.279745102 CEST	192.168.2.3	8.8.8.8	0x214c	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 6, 2022 06:58:41.527452946 CEST	8.8.8.8	192.168.2.3	0x343f	No error (0)	spatterjointposition.com		192.243.59.12	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:41.527452946 CEST	8.8.8.8	192.168.2.3	0x343f	No error (0)	spatterjointposition.com		192.243.59.20	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:41.527452946 CEST	8.8.8.8	192.168.2.3	0x343f	No error (0)	spatterjointposition.com		192.243.61.225	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:41.527452946 CEST	8.8.8.8	192.168.2.3	0x343f	No error (0)	spatterjointposition.com		192.243.59.13	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:41.527452946 CEST	8.8.8.8	192.168.2.3	0x343f	No error (0)	spatterjointposition.com		192.243.61.227	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:41.528584957 CEST	8.8.8.8	192.168.2.3	0xd83c	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 6, 2022 06:58:41.528584957 CEST	8.8.8.8	192.168.2.3	0xd83c	No error (0)	clients.l.google.com		142.250.186.110	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:41.531418085 CEST	8.8.8.8	192.168.2.3	0xab47	No error (0)	accounts.google.com		142.250.185.205	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:42.376682997 CEST	8.8.8.8	192.168.2.3	0x4ed5	No error (0)	google.com		172.217.16.206	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:42.532346964 CEST	8.8.8.8	192.168.2.3	0x410f	No error (0)	www.google.com		142.250.185.196	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:42.861210108 CEST	8.8.8.8	192.168.2.3	0x73e9	No error (0)	gstaticadssl.l.google.com		142.250.184.195	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:43.474267006 CEST	8.8.8.8	192.168.2.3	0xf2ff	No error (0)	apis.google.com	plus.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 6, 2022 06:58:43.474267006 CEST	8.8.8.8	192.168.2.3	0xf2ff	No error (0)	plus.l.google.com		216.58.212.142	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:46.182383060 CEST	8.8.8.8	192.168.2.3	0x85ad	No error (0)	www.google.com		142.250.185.196	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:46.183928013 CEST	8.8.8.8	192.168.2.3	0x3357	No error (0)	gstaticadssl.l.google.com		142.250.184.195	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:02.650856018 CEST	8.8.8.8	192.168.2.3	0xe00	No error (0)	about.google		216.239.32.29	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:03.108639002 CEST	8.8.8.8	192.168.2.3	0x217f	No error (0)	csp.withgoogle.com		172.217.16.209	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:03.444885015 CEST	8.8.8.8	192.168.2.3	0x28e	No error (0)	www-googletagmanager.l.google.com		142.250.186.168	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:04.449615002 CEST	8.8.8.8	192.168.2.3	0x2ece	No error (0)	lh3.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 6, 2022 06:59:04.449615002 CEST	8.8.8.8	192.168.2.3	0x2ece	No error (0)	googlehosted.l.googleusercontent.com		172.217.23.97	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:05.037427902 CEST	8.8.8.8	192.168.2.3	0x2d07	No error (0)	scone-pa.clients6.google.com		142.250.185.138	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:05.246292114 CEST	8.8.8.8	192.168.2.3	0x740	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)

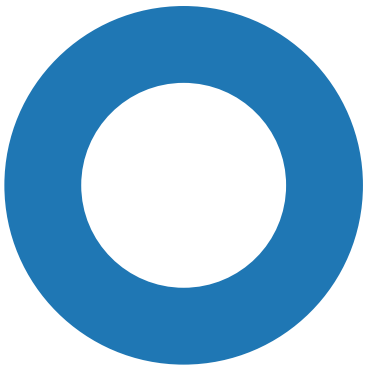
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 6, 2022 06:59:05.246292114 CEST	8.8.8.8	192.168.2.3	0x740	No error (0)	stats.l.doubleclick.net		66.102.1.156	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:05.246292114 CEST	8.8.8.8	192.168.2.3	0x740	No error (0)	stats.l.doubleclick.net		66.102.1.154	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:05.246292114 CEST	8.8.8.8	192.168.2.3	0x740	No error (0)	stats.l.doubleclick.net		66.102.1.155	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:05.246292114 CEST	8.8.8.8	192.168.2.3	0x740	No error (0)	stats.l.doubleclick.net		66.102.1.157	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:06.385415077 CEST	8.8.8.8	192.168.2.3	0x91b7	No error (0)	kstatic.googleusercontent.com		35.241.11.240	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:10.232460976 CEST	8.8.8.8	192.168.2.3	0x6ee3	No error (0)	store.google.com		172.217.16.142	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:20.106054068 CEST	8.8.8.8	192.168.2.3	0x6efe	No error (0)	www.youtube.com	youtube-ui.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 6, 2022 06:59:20.106054068 CEST	8.8.8.8	192.168.2.3	0x6efe	No error (0)	youtube-ui.l.google.com		142.250.186.110	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:20.106054068 CEST	8.8.8.8	192.168.2.3	0x6efe	No error (0)	youtube-ui.l.google.com		142.250.186.142	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:20.106054068 CEST	8.8.8.8	192.168.2.3	0x6efe	No error (0)	youtube-ui.l.google.com		172.217.16.142	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:20.106054068 CEST	8.8.8.8	192.168.2.3	0x6efe	No error (0)	youtube-ui.l.google.com		142.250.184.206	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:20.106054068 CEST	8.8.8.8	192.168.2.3	0x6efe	No error (0)	youtube-ui.l.google.com		142.250.186.78	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:20.106054068 CEST	8.8.8.8	192.168.2.3	0x6efe	No error (0)	youtube-ui.l.google.com		172.217.18.14	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:20.106054068 CEST	8.8.8.8	192.168.2.3	0x6efe	No error (0)	youtube-ui.l.google.com		142.250.186.174	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:20.106054068 CEST	8.8.8.8	192.168.2.3	0x6efe	No error (0)	youtube-ui.l.google.com		172.217.16.206	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:20.106054068 CEST	8.8.8.8	192.168.2.3	0x6efe	No error (0)	youtube-ui.l.google.com		216.58.212.174	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:20.106054068 CEST	8.8.8.8	192.168.2.3	0x6efe	No error (0)	youtube-ui.l.google.com		172.217.18.110	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:20.106054068 CEST	8.8.8.8	192.168.2.3	0x6efe	No error (0)	youtube-ui.l.google.com		142.250.74.206	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:20.106054068 CEST	8.8.8.8	192.168.2.3	0x6efe	No error (0)	youtube-ui.l.google.com		172.217.23.110	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:20.106054068 CEST	8.8.8.8	192.168.2.3	0x6efe	No error (0)	youtube-ui.l.google.com		216.58.212.142	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:20.106054068 CEST	8.8.8.8	192.168.2.3	0x6efe	No error (0)	youtube-ui.l.google.com		142.250.185.78	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:20.106054068 CEST	8.8.8.8	192.168.2.3	0x6efe	No error (0)	youtube-ui.l.google.com		142.250.185.110	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:20.106054068 CEST	8.8.8.8	192.168.2.3	0x6efe	No error (0)	youtube-ui.l.google.com		142.250.185.142	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:21.234868050 CEST	8.8.8.8	192.168.2.3	0xab97	No error (0)	googleads.g.doubleclick.net		142.250.185.162	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:21.234919071 CEST	8.8.8.8	192.168.2.3	0xe550	No error (0)	www.google.de		172.217.18.3	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:22.058999062 CEST	8.8.8.8	192.168.2.3	0xf03f	No error (0)	play.google.com		142.250.186.142	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:26.068675995 CEST	8.8.8.8	192.168.2.3	0xbccf	No error (0)	lh3.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 6, 2022 06:59:26.068675995 CEST	8.8.8.8	192.168.2.3	0xbccf	No error (0)	googlehosted.l.googleusercontent.com		172.217.23.97	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:26.360553980 CEST	8.8.8.8	192.168.2.3	0x7928	No error (0)	mail.google.com		142.250.186.165	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:33.856801987 CEST	8.8.8.8	192.168.2.3	0xcf8f	No error (0)	about.google		216.239.32.29	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:39.916663885 CEST	8.8.8.8	192.168.2.3	0x9f93	No error (0)	www.google.de		172.217.18.3	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:41.630605936 CEST	8.8.8.8	192.168.2.3	0xadbd	No error (0)	static.doubleclick.net	static-doubleclick-net.l.google.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 6, 2022 06:59:41.630605936 CEST	8.8.8.8	192.168.2.3	0xadbd	No error (0)	static-doubleclick-net.l.google.com		142.250.186.134	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:42.459023952 CEST	8.8.8.8	192.168.2.3	0xa042	No error (0)	yt3.ggpht.com	photos-ugc.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 6, 2022 06:59:42.459023952 CEST	8.8.8.8	192.168.2.3	0xa042	No error (0)	photos-ugc.l.googleusercontent.com		142.250.186.33	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:42.467551947 CEST	8.8.8.8	192.168.2.3	0x9703	No error (0)	i.ytimg.com		142.250.185.214	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:42.467551947 CEST	8.8.8.8	192.168.2.3	0x9703	No error (0)	i.ytimg.com		142.250.185.246	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:42.467551947 CEST	8.8.8.8	192.168.2.3	0x9703	No error (0)	i.ytimg.com		142.250.186.54	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:42.467551947 CEST	8.8.8.8	192.168.2.3	0x9703	No error (0)	i.ytimg.com		142.250.181.246	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:42.467551947 CEST	8.8.8.8	192.168.2.3	0x9703	No error (0)	i.ytimg.com		142.250.186.118	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:42.467551947 CEST	8.8.8.8	192.168.2.3	0x9703	No error (0)	i.ytimg.com		142.250.186.150	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:42.467551947 CEST	8.8.8.8	192.168.2.3	0x9703	No error (0)	i.ytimg.com		172.217.16.150	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:42.467551947 CEST	8.8.8.8	192.168.2.3	0x9703	No error (0)	i.ytimg.com		142.250.184.214	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:42.467551947 CEST	8.8.8.8	192.168.2.3	0x9703	No error (0)	i.ytimg.com		142.250.186.86	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:42.467551947 CEST	8.8.8.8	192.168.2.3	0x9703	No error (0)	i.ytimg.com		172.217.18.22	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:42.467551947 CEST	8.8.8.8	192.168.2.3	0x9703	No error (0)	i.ytimg.com		142.250.186.182	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:42.467551947 CEST	8.8.8.8	192.168.2.3	0x9703	No error (0)	i.ytimg.com		172.217.16.214	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:42.467551947 CEST	8.8.8.8	192.168.2.3	0x9703	No error (0)	i.ytimg.com		216.58.212.182	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:42.467551947 CEST	8.8.8.8	192.168.2.3	0x9703	No error (0)	i.ytimg.com		172.217.18.118	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:42.467551947 CEST	8.8.8.8	192.168.2.3	0x9703	No error (0)	i.ytimg.com		142.250.74.214	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:42.467551947 CEST	8.8.8.8	192.168.2.3	0x9703	No error (0)	i.ytimg.com		172.217.23.118	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:46.969397068 CEST	8.8.8.8	192.168.2.3	0x3ac6	No error (0)	yt3.ggpht.com	photos-ugc.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 6, 2022 06:59:46.969397068 CEST	8.8.8.8	192.168.2.3	0x3ac6	No error (0)	photos-ugc.l.googleusercontent.com		142.250.186.33	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:46.974189997 CEST	8.8.8.8	192.168.2.3	0x539d	No error (0)	i.ytimg.com		142.250.185.214	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:46.974189997 CEST	8.8.8.8	192.168.2.3	0x539d	No error (0)	i.ytimg.com		142.250.185.246	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:46.974189997 CEST	8.8.8.8	192.168.2.3	0x539d	No error (0)	i.ytimg.com		142.250.186.54	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:46.974189997 CEST	8.8.8.8	192.168.2.3	0x539d	No error (0)	i.ytimg.com		142.250.181.246	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:46.974189997 CEST	8.8.8.8	192.168.2.3	0x539d	No error (0)	i.ytimg.com		142.250.186.118	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:46.974189997 CEST	8.8.8.8	192.168.2.3	0x539d	No error (0)	i.ytimg.com		142.250.186.150	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:46.974189997 CEST	8.8.8.8	192.168.2.3	0x539d	No error (0)	i.ytimg.com		172.217.16.150	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:46.974189997 CEST	8.8.8.8	192.168.2.3	0x539d	No error (0)	i.ytimg.com		142.250.184.214	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:46.974189997 CEST	8.8.8.8	192.168.2.3	0x539d	No error (0)	i.ytimg.com		142.250.186.86	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:46.974189997 CEST	8.8.8.8	192.168.2.3	0x539d	No error (0)	i.ytimg.com		172.217.18.22	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:46.974189997 CEST	8.8.8.8	192.168.2.3	0x539d	No error (0)	i.ytimg.com		142.250.186.182	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:46.974189997 CEST	8.8.8.8	192.168.2.3	0x539d	No error (0)	i.ytimg.com		172.217.16.214	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 6, 2022 06:59:46.974189997 CEST	8.8.8.8	192.168.2.3	0x539d	No error (0)	i.ytimg.com		216.58.212.182	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:46.974189997 CEST	8.8.8.8	192.168.2.3	0x539d	No error (0)	i.ytimg.com		172.217.18.118	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:46.974189997 CEST	8.8.8.8	192.168.2.3	0x539d	No error (0)	i.ytimg.com		142.250.74.214	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:46.974189997 CEST	8.8.8.8	192.168.2.3	0x539d	No error (0)	i.ytimg.com		172.217.23.118	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:47.885421991 CEST	8.8.8.8	192.168.2.3	0x1ea5	No error (0)	accounts.google.com		142.250.185.205	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:49.715706110 CEST	8.8.8.8	192.168.2.3	0x10b0	No error (0)	accounts.youtube.com	www3.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 6, 2022 06:59:49.715706110 CEST	8.8.8.8	192.168.2.3	0x10b0	No error (0)	www3.l.google.com		172.217.23.110	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:10.305860043 CEST	8.8.8.8	192.168.2.3	0x214c	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Aug 6, 2022 07:00:10.305860043 CEST	8.8.8.8	192.168.2.3	0x214c	No error (0)	stats.l.doubleclick.net		66.102.1.156	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:10.305860043 CEST	8.8.8.8	192.168.2.3	0x214c	No error (0)	stats.l.doubleclick.net		66.102.1.155	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:10.305860043 CEST	8.8.8.8	192.168.2.3	0x214c	No error (0)	stats.l.doubleclick.net		66.102.1.154	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:10.305860043 CEST	8.8.8.8	192.168.2.3	0x214c	No error (0)	stats.l.doubleclick.net		66.102.1.157	A (IP address)	IN (0x0001)

Statistics

Behavior



chrome.exe
chrome.exe
chrome.exe
chrome.exe
chrome.exe

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: **6060**, Parent PID: **1280**

General

Target ID:	0
Start time:	06:58:36
Start date:	06/08/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	0x7ff7f6290000

Copyright Joe Security LLC 2022

File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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

Analysis Process: chrome.exe PID: **4116**, Parent PID: **6060**

General

Target ID:	1
Start time:	06:58:37
Start date:	06/08/2022
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=1612,17434451715936591080,16828468669034620011,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1920 /prefetch:8
Imagebase:	0x7ff7f6290000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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

Analysis Process: chrome.exe PID: **2368**, Parent PID: **1280**

General

Target ID:	2
Start time:	06:58:38
Start date:	06/08/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "https://spatterjointposition.com

Imagebase:	0x7ff7f6290000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

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

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

Analysis Process: chrome.exe PID: **1108**, Parent PID: **6060**

General

Target ID:	15
Start time:	06:59:43
Start date:	06/08/2022
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=audio.mojom.AudioService --field-trial-handle=1612,17434451715936591080,16828468669034620011,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=6248 /prefetch:8
Imagebase:	0x7ff7f6290000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: chrome.exe PID: **2068**, Parent PID: **6060**

General

Target ID:	16
Start time:	06:59:43
Start date:	06/08/2022
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=video_capture.mojom.VideoCaptureService --field-trial-handle=1612,17434451715936591080,16828468669034620011,131072 --lang=en-US --service-sandbox-type=video_capture --enable-audio-service-sandbox --mojo-platform-channel-handle=6236 /prefetch:8
Imagebase:	0x7ff7f6290000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly