ID: 668454
Sample Name: Hacxx MSDT 0-Day CVE-2022-30190 Exploit Generator.htm
Cookbook: defaultwindowshtmlcookbook.jbs
Time: 18:34:39
Date: 18/07/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report Hacxx MSDT 0-Day CVE-2022-30190 Exploit Generator.htm 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Process Tree 5
Malware Configuration 5
Yara Signatures 5
Initial Sample 5
HTML 5
Sigma Signatures 6
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Exploits 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 10
Public IPs 10
Private 10
General Information 10
Warnings 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASNs 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
C:\Users\user\AppData\Local\Google\Chrome\User Data\0d81cff3-497a-494d-a884-f64b2c59e3fd.tmp 12
C:\Users\user\AppData\Local\Google\Chrome\User Data\176502c7-4049-4132-927a-01997ef82a1a.tmp 12
C:\Users\user\AppData\Local\Google\Chrome\User Data\1801910f-cf6c-43b1-8045-4da5fc35d814.tmp 13
C:\Users\user\AppData\Local\Google\Chrome\User Data\3961b5fe-59f9-4443-98f7-faa899da2e12.tmp 13
C:\Users\user\AppData\Local\Google\Chrome\User Data\5a54882d-1928-41d1-97be-638fd89dfd86.tmp 13
C:\Users\user\AppData\Local\Google\Chrome\User Data\6b6e8037-92ce-4ca4-9844-540dc84d62c9.tmp 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\6ecda07e-541d-463c-8b9d-cc01c842a9e2.tmp 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\74b97186-944d-4d7d-bd79-5009d246120d.tmp 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\89363a91-dde3-4075-8cf7-91d666ea2293.tmp 15
C:\Users\user\AppData\Local\Google\Chrome\User Data\8ce8a778-73c1-4ee1-921d-501740badb08.tmp 15
C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat 15
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\114a658d-ecd8-43cb-9be7-13eba55e017a.tmp 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\46eeff2e-c4a7-4562-b899-53b19a8d0d59.tmp 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\56fe0613-2fa7-48d7-8456-da39dd4152e3.tmp 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7d5a61e7-35f3-4e76-8642-dae2ae803399.tmp 17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7e67fe26-1e55-4a3a-b912-26f7e5155c82.tmp 17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9ae7a855-5166-4070-9a01-71c526eb8520.tmp 17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy) 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy) 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy) 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy) 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\727a27ef-2203-4b69-a8bf-89c988389b14.tmp 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1 20

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy) 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\5fa60e0e-e2b5-4357-988a-4477fd114917.tmp 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Network Persistent State (copy) 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a0c37120-c382-49e4-8883-5472249fbc6b.tmp 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ca173ec6-7f47-4d84-bf32-be41c1efea0a.tmp 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy) 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e8e1b108-9b2b-438d-a725-5f2576c66354.tmp 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f8a16519-1264-457e-bd0e-0d7479d9eb2b.tmp 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy) 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy) 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir3628_360129491\Ruleset Data 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\b2c0e852-f021-448f-9c08-e38b954f106c.tmp 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\bca37c47-d014-4f7a-b1d6-5f2c7b48d818.tmp 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\c5c88fb3-f819-4ba0-bf6a-a459b9a5cc93.tmp 26
C:\Users\user\AppData\Local\Google\Chrome\User Data\cecc145c-6e1c-4fe2-8378-812c8c4b9c09.tmp 26
C:\Users\user\AppData\Local\Google\Chrome\User Data\d5b172b1-5595-4dae-853a-723d6f31977d.tmp 26
C:\Users\user\AppData\Local\Temp\3628_1040151320\LICENSE 27
C:\Users\user\AppData\Local\Temp\3628_1040151320_metadata\verified_contents.json 27
C:\Users\user\AppData\Local\Temp\3628_1040151320\crl-set 27
C:\Users\user\AppData\Local\Temp\3628_1040151320\manifest.fingerprint 28
C:\Users\user\AppData\Local\Temp\3628_1040151320\manifest.json 28
C:\Users\user\AppData\Local\Temp\3628_1290221689\Recovery.crx3 28
C:\Users\user\AppData\Local\Temp\3628_1290221689_metadata\verified_contents.json 29
C:\Users\user\AppData\Local\Temp\3628_1290221689\manifest.fingerprint 29
C:\Users\user\AppData\Local\Temp\3628_1290221689\manifest.json 29
C:\Users\user\AppData\Local\Temp\3628_1783822598_metadata\verified_contents.json 30
C:\Users\user\AppData\Local\Temp\3628_1783822598\manifest.fingerprint 30
C:\Users\user\AppData\Local\Temp\3628_1783822598\manifest.json 30
C:\Users\user\AppData\Local\Temp\3628_1783822598\ssl_error_assistant.pb 30
C:\Users\user\AppData\Local\Temp\3628_2036087933_metadata\verified_contents.json 31
C:\Users\user\AppData\Local\Temp\3628_2036087933_platform_specific\x86_64\pnacl_public_pnacl_json 31
C:\Users\user\AppData\Local\Temp\3628_2036087933_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_for_eh_o 31
C:\Users\user\AppData\Local\Temp\3628_2036087933_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_o 32
C:\Users\user\AppData\Local\Temp\3628_2036087933_platform_specific\x86_64\pnacl_public_x86_64_crtend_o 32
C:\Users\user\AppData\Local\Temp\3628_2036087933_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe 32
C:\Users\user\AppData\Local\Temp\3628_2036087933_platform_specific\x86_64\pnacl_public_x86_64_libcrt_platform_a 33
C:\Users\user\AppData\Local\Temp\3628_2036087933_platform_specific\x86_64\pnacl_public_x86_64_libgcc_a 33
C:\Users\user\AppData\Local\Temp\3628_2036087933_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_a 33
C:\Users\user\AppData\Local\Temp\3628_2036087933_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_dummy_a 34
C:\Users\user\AppData\Local\Temp\3628_2036087933_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe 34
C:\Users\user\AppData\Local\Temp\3628_2036087933_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe 34
C:\Users\user\AppData\Local\Temp\3628_2036087933\manifest.fingerprint 35
C:\Users\user\AppData\Local\Temp\3628_2036087933\manifest.json 35
C:\Users\user\AppData\Local\Temp\3628_2095119410_metadata\verified_contents.json 35
C:\Users\user\AppData\Local\Temp\3628_2095119410\manifest.fingerprint 36
C:\Users\user\AppData\Local\Temp\3628_2095119410\manifest.json 36
C:\Users\user\AppData\Local\Temp\3628_562390067\Filtering Rules 36
C:\Users\user\AppData\Local\Temp\3628_562390067\LICENSE.txt 36
C:\Users\user\AppData\Local\Temp\3628_562390067_metadata\verified_contents.json 37
C:\Users\user\AppData\Local\Temp\3628_562390067\manifest.fingerprint 37
C:\Users\user\AppData\Local\Temp\3628_562390067\manifest.json 37
C:\Users\user\AppData\Local\Temp\73a88e6c-8bc8-4e75-af96-e80b0ef97d01.tmp 38
C:\Users\user\AppData\Local\Temp\83e2d3a3-c39c-4d02-ac9e-2cb5ac7dc711.tmp 38
C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\83e2d3a3-c39c-4d02-ac9e-2cb5ac7dc711.tmp 38
C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\bg\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\ca\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\cs\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\da\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\de\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\el\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\en\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\en_GB\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\es\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\es_419\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\et\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\fi\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\fil\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\fr\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\hi\messages.json 43
Static File Info 43
General 43
Network Behavior 43
Network Port Distribution 43
TCP Packets 44

UDP Packets 45
DNS Queries 45
DNS Answers 45
HTTP Request Dependency Graph 45
HTTPS Proxied Packets 45
Statistics 47
Behavior 47
System Behavior 48
Analysis Process: chrome.exePID: 3628, Parent PID: 1636 48
General 48
File Activities 48
Registry Activities 48
Key Value Modified 48
Analysis Process: chrome.exePID: 3372, Parent PID: 3628 48
General 48
File Activities 49
Disassembly 49

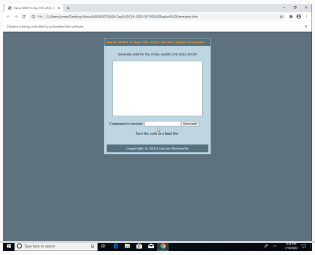
Windows Analysis Report

Hacxx MSDT 0-Day CVE-2022-30190 Exploit Generator.htm

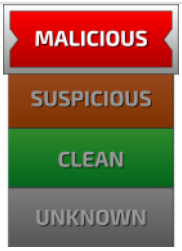
Overview

General Information

Sample Name:	Hacxx MSDT 0-Day CVE-2022-30190 Exploit Generator.htm
Analysis ID:	668454
MD5:	944593b21badb2.
SHA1:	737ec2a8778af5..
SHA256:	b2743f7047a711..
Tags:	CVE-2022-30190 ExploitGenerator html
Infos:	



Detection



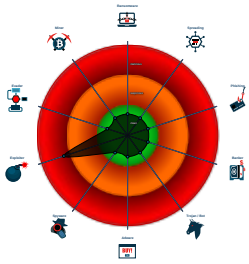
Follina CVE-2022-30190

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Microsoft Office Expl…
- Yara signature match
- IP address seen in connection with …

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 3628 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "C:\Users\user\Desktop\Hacxx MSDT 0-Day CVE-2022-30190 Exploit Generator.htm MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 3372 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1592,17218383300859783571,9943285069256131307,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1928 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Hacxx MSDT 0-Day CVE-2022-30190 Exploit Generator.htm	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x24bb:$a: PCWDiagnostic • 0x24af:$sa3: ms-msdt • 0x2533:$sb3: IT_BrowseForFile=
Hacxx MSDT 0-Day CVE-2022-30190 Exploit Generator.htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	

HTML

Source	Rule	Description	Author	Strings
83002.0.pages.csv	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x25d6:$a: PCWDiagnostic • 0x25ca:$sa3: ms-msdt • 0x264e:$sb3: IT_BrowseForFile=

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

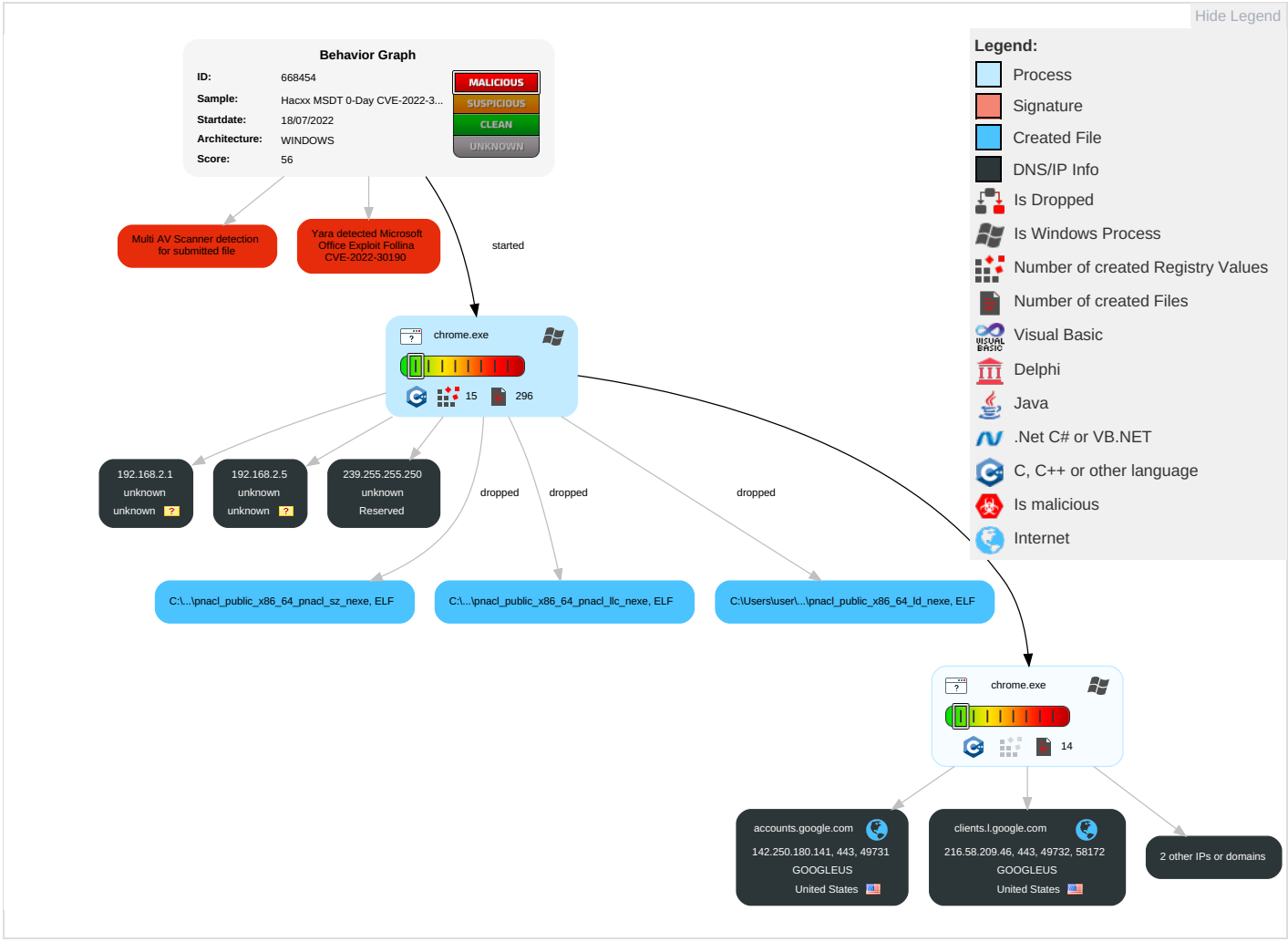
Exploits

Yara detected Microsoft Office Exploit Follina CVE-2022-30190

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

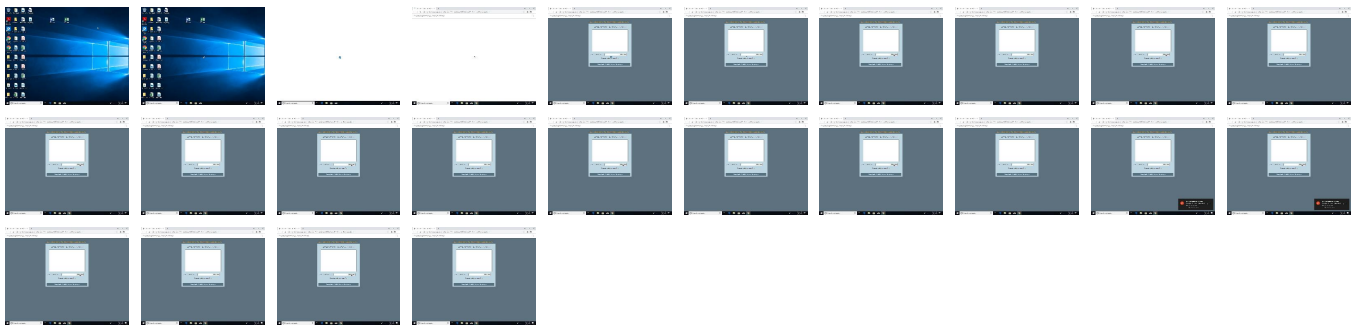
Behavior Graph

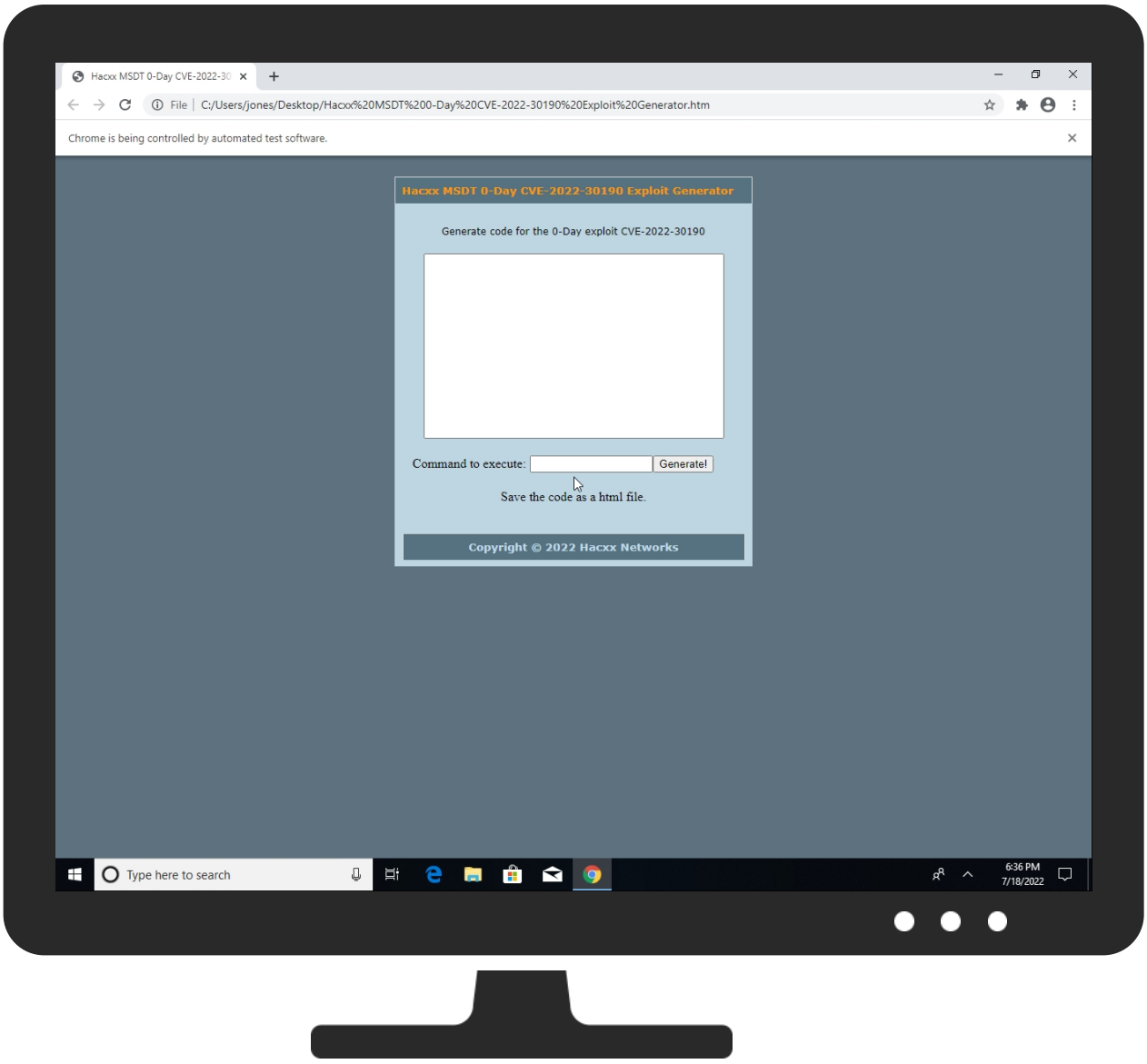


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Hacxx MSDT 0-Day CVE-2022-30190 Exploit Generator.htm	32%	Virustotal		Browse
Hacxx MSDT 0-Day CVE-2022-30190 Exploit Generator.htm	23%	Metadefender		Browse
Hacxx MSDT 0-Day CVE-2022-30190 Exploit Generator.htm	15%	ReversingLabs	Script-JS.Exploit.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\3628_2036087933_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\3628_2036087933_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.180.141	true	false		high
clients.l.google.com	216.58.209.46	true	false		high
clients2.google.com	unknown	unknown	false		high

Contacted URLs

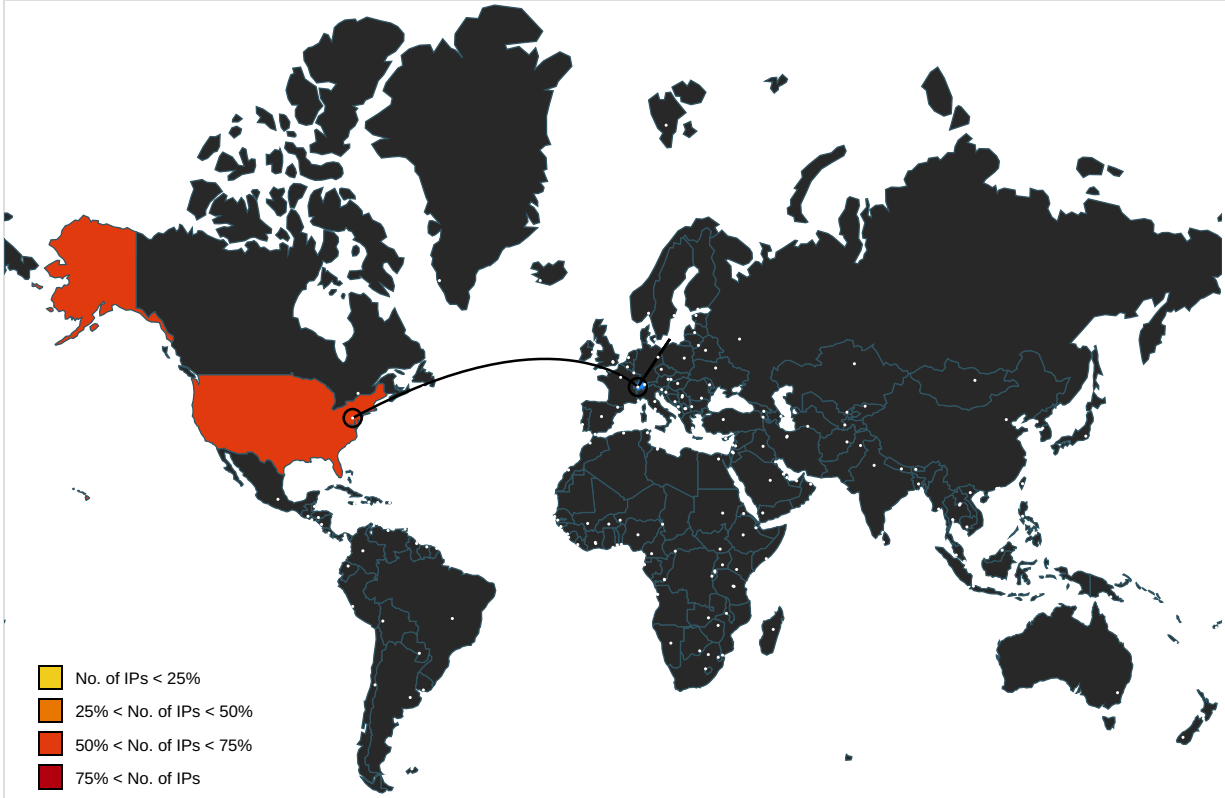
Name	Malicious	Antivirus Detection	Reputation
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-GB&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiime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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	7d5a61e7-35f3-4e76-8642-dae2ae803399.tmp.1.dr, 5fa60e0e-e2b5-4357-988a-4477fd114917.tmp.1.dr, 727a27ef-2203-4b69-a8bf-89c988389b14.tmp.1.dr, f8a16519-1264-457e-bd0e-0d7479d9eb2b.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	7d5a61e7-35f3-4e76-8642-dae2ae803399.tmp.1.dr, f8a16519-1264-457e-bd0e-0d7479d9eb2b.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	7d5a61e7-35f3-4e76-8642-dae2ae803399.tmp.1.dr, f8a16519-1264-457e-bd0e-0d7479d9eb2b.tmp.1.dr	false		high
http://https://payments.google.com/payments/v4/js/integrator.js	craw_window.js.0.dr, manifest.json.0.dr	false		high
http://https://chromium.googlesource.com/a/native_client/pnacl-llvm.git	pnacl_public_x86_64_libpnacl_irt_shim_dummy_a.0.dr	false		high
http://https://easylist.to/)	LICENSE.txt.0.dr	false		high
http://https://sandbox.google.com/payments/v4/js/integrator.js	craw_window.js.0.dr, manifest.json.0.dr	false		high
http://https://www.google.com/images/x2.gif	craw_window.js.0.dr	false		high
http://https://accounts.google.com/MergeSession	craw_window.js.0.dr	false		high
http://llvm.org/):	pnacl_public_x86_64_pnacl_sz_nexe.0.dr, pnacl_public_x86_64_pnacl_llc_nexe.0.dr	false		high
http://https://creativecommons.org/compatiblelicenses	LICENSE.txt.0.dr	false		high
http://https://www.google.com	7d5a61e7-35f3-4e76-8642-dae2ae803399.tmp.1.dr, f8a16519-1264-457e-bd0e-0d7479d9eb2b.tmp.1.dr	false		high
http://https://www.google.com/images/dot2.gif	craw_window.js.0.dr	false		high
http://https://github.com/easylist)	LICENSE.txt.0.dr	false		high
http://https://creativecommons.org/.	LICENSE.txt.0.dr	false		high
http://https://code.google.com/p/nativeclient/issues/entry%s:	pnacl_public_x86_64_ld_nexe.0.dr	false		high
http://https://code.google.com/p/nativeclient/issues/entry	pnacl_public_x86_64_ld_nexe.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://accounts.google.com	7d5a61e7-35f3-4e76-8642-dae2ae803399.tmp.1.dr, f8a16519-1264-457e-bd0e-0d7479d9eb2b.tmp.1.dr	false		high
http://https://clients2.googleusercontent.com	7d5a61e7-35f3-4e76-8642-dae2ae803399.tmp.1.dr, f8a16519-1264-457e-bd0e-0d7479d9eb2b.tmp.1.dr	false		high
http://https://apis.google.com	7d5a61e7-35f3-4e76-8642-dae2ae803399.tmp.1.dr, f8a16519-1264-457e-bd0e-0d7479d9eb2b.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	7d5a61e7-35f3-4e76-8642-dae2ae803399.tmp.1.dr, f8a16519-1264-457e-bd0e-0d7479d9eb2b.tmp.1.dr	false		high
http://https://clients2.google.com/service/update2/crx	manifest.json1.0.dr, manifest.json4.0.dr, manifest.json.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.180.141	accounts.google.com	United States		15169	GOOGLEUS	false
216.58.209.46	clients.l.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1
192.168.2.5

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	668454
Start date and time: 18/07/202218:34:39	2022-07-18 18:34:39 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Hacxx MSDT 0-Day CVE-2022-30190 Exploit Generator.htm
Cookbook file name:	defaultwindowshtmlcookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.expl.winHTM@31/139@2/6
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .htm • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.251.209.3, 142.250.184.78, 74.125.163.198, 142.250.184.35, 216.58.209.35
- Excluded domains from analysis (whitelisted): www.bing.com, r1---sn-5hne6nsz.gvt1.com, r5---sn-5hne6nsy.gvt1.com, fs.microsoft.com, r3---sn-5hne6nsy.gvt1.com, clientservices.googleapis.com, time.windows.com, r3---sn-5hne6n6l.gvt1.com, arc.msn.com, r1---sn-5hne6nzs.gvt1.com, ris.api.iris.microsoft.com, r1.sn-4g5lznle.gvt1.com, r1---sn-4g5lznle.gvt1.com, redirector.gvt1.com, store-images.s-microsoft.com, login.live.com, r3---sn-5hne6n6e.gvt1.com, sls.update.microsoft.com, update.googleapis.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, www.gstatic.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Google\Chrome\User Data\0d81cff3-497a-494d-a884-f64b2c59e3fd.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7475817837250522
Encrypted:	false
SSDEEP:	384:5Rpfux9jU2fsDrVQ29YNlr2vpz3SlDCHTeG2ZrUnxdxq3vHurshm8fkjtJ9WODDT:RqKl963i+kefF7T8/bO7KZXdBP
MD5:	01C7364D19FF3D8B5489F189BBA009E4
SHA1:	34BDFF0512ABDC8EAE614A38BD71800FEA23DB3E
SHA-256:	A874231A21FC7A96EF5AB1A33AB0D03EE40BADED7C06450E47A752FB57F3F7A2
SHA-512:	98D7CCA250FD63BEC330DED58A2F25A38C0E86F98A1B93DA787C2B2724745ECEF5D46989819AC1383ECD4F393D897145B65F3A576D2993EB80060950625FF7B C
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...Hb8.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\176502c7-4049-4132-927a-01997ef82a1a.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):	207310
Entropy (8bit):	6.044443507710714
Encrypted:	false
SSDEEP:	6144:AZpMpw3nP3OEwkqhGtA/UNm9FaqfIlUOoSiuRa:7w3/ejGtArmox
MD5:	B68E34465FCF49D4BBB1CE90DA10A9FD
SHA1:	8A62B68530CDF4D33A51835DAEA4319954ED0A4A
SHA-256:	B21AEB9B510C027A2EC864A043ABBC3CD50F787CB14D8D4398AC537D2640116C
SHA-512:	5AF46EC3108958E1F4A68E6B3AAAEEBE14C8A23429D6278BEE89F2562DFD911786394A99088A754E1EEA2EFB76ED9F165551E0512B83630D8481DFE234996E3
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}}, "network_time":{"network_time_mapping":{"local":1.658162158299545e+12,"network":1.65816216e+12,"ticks":125270795.0,"uncertainty":5220940.0}},"os_crypt":{"encrypt ted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqI YBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps 4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"}," password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129725653"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\1801910f-cf6c-43b1-8045-4da5fc35d814.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):	206935
Entropy (8bit):	6.043535252576189
Encrypted:	false
SSDEEP:	6144:ENpMpw3nP3OEwkqhGtA/UNm9FaqfIlUOoSiuRa:jw3/ejGtArmox
MD5:	3F02A1787B2B807F49210C344B83F964
SHA1:	D1D641CCA0DAF7330E1CCB9085A7790ACAF8CF7A
SHA-256:	C4C11D72494324FD24681538DD836AE98838B1487002C5D5DCF8414B1305619B
SHA-512:	26AF5156DE94E091B1D37D5B0953BE5F0D2A6E3B831508E4389399B4AA384B8FC8AC874EFBBF9AE5E8FEA8A793D66ABEB0682ACA680A1FF5B2DD004DD0F8FE45
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.658162158299545e+12,"network":1.65816216e+12,"ticks":125270795.0,"uncertainty":5220940.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxl"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129725653"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\3961b5fe-59f9-4443-98f7-faa899da2e12.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.747415097496942
Encrypted:	false
SSDEEP:	384:XRpfux9jU2rDs9YNlr2vpz3SlDCHTeG2ZrUnxdxq3vHurshm8fkjtJ9WODDpNI1k:iKl963i+kefF7T8/bO7KZXdBR
MD5:	BE2AD534FBB70883F9E2869434AC205D
SHA1:	2EE5C7D333CC40E6CAA6B7833AC24E2D0923E9AE
SHA-256:	4B3D944518B1D75E9E34BED3CA1CF9CED18596E4284EFCED8157DBFB3FB7D427
SHA-512:	11030B00F82A88AFAB0090B631A62808701B438157022BDA5982FFBBE6F61A941C5F41F046E7AD2BA6F2E6097A0B0AF3572F38AA5FFB2AF1F749A9D768D29E33
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...Hb8.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\5a54882d-1928-41d1-97be-638fd89dfd86.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):	207027
Entropy (8bit):	6.043784235411766
Encrypted:	false
SSDEEP:	6144:qZpMpw3nP3OEwkqhGtA/UNm9FaqfIlUOoSiuRa:lw3/ejGtArmox
MD5:	D2585A2700C1D3051D07F8788940DA86
SHA1:	210DB5274B02B5B9CF95127521F67D0AB3CF4FEE
SHA-256:	E43267BBACB16AC3FCDD9EB686BA09E204F986BEA2372BFFD4BF9411AD871168
SHA-512:	9ABB0813A72DF27F1C0BB9DD95BAF368F208143E67626CB2FBFA417ECD10AD3CD858AAEDBF9959EC0F682C60C8A03A99807EBB3FA532FBD4D3E0FF2EBCE8A743
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.658162158299545e+12,"network":1.65816216e+12,"ticks":125270795.0,"uncertainty":5220940.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129725653"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\6b6e8037-92ce-4ca4-9844-540dc84d62c9.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.747691955928208
Encrypted:	false
SSDEEP:	384:pRpfux9jU2fsDrVQ29YNlr2vpz3SlDCHTeG2ZrUnxdxq3vHurshm8oakjtJ9WOD7:hqKl963E+kefF7T8/bO7KZXdB7
MD5:	6F95C6C58C47841DCCD9807E28BBEA43
SHA1:	C95DB01DE969D606B779295292BA2458B85AEFDC
SHA-256:	9552C0DA85FA3626EF6C426EE8842534C3DB9E513A3246FE06F065A0576157A4
SHA-512:	7A73DB1F5739A922497F5448E3D330BB51982E7F5A7B7535A5B6F4E9B2AC756C02359666C6F0EEA88CE5B5E6F0C6F5AFA01F982B990348A2A13D195311F0F561
Malicious:	false
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...Hb8.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\6ecda07e-541d-463c-8b9d-cc01c842a9e2.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):	207121
Entropy (8bit):	6.044029905204594
Encrypted:	false
SSDEEP:	6144:qZpMpw3nP3OEwkqhGtA/UNm9FaqfIlUOoSiuRa:lw3/ejGtArmox
MD5:	3AE3478FFBA7B75AF03FC9124B8C713B
SHA1:	A0F6F272E702635405AC5679A5AFA093627C8EC3
SHA-256:	313A754BBBA630E255304E5AE9FE90A5D205AC40D91A847811B03252D43F4F98
SHA-512:	8488FC80F89280BA470E736CC0FB962870022E7FC012E9AE762FEEF69CA7C1BFF7FA7BBB9DEAE272F87339A11E29C152D69FD62DB6ACA3BAD5A05B17CB495EBF
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.658162158299545e+12,"network":1.65816216e+12,"ticks":125270795.0,"uncertainty":5220940.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129725653"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\74b97186-944d-4d7d-bd79-5009d246120d.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):	207224
Entropy (8bit):	6.044295151841472
Encrypted:	false
SSDEEP:	6144:UZpMpw3nP3OEwkqhGtA/UNm9FaqfIlUOoSiuRa:Xw3/ejGtArmox
MD5:	1A338E4411CFDF2269DB6C04A2F49DBD
SHA1:	A0A6778A7F7C2ABC2D2871637A9A9A2693F9507C
SHA-256:	6F00E537D2308977640E1958FDC050DA9B4100EA3C16A5EBA4DA0F3BF033DFCB
SHA-512:	ABCE20D310A8A59E24D0E034CCACE98444EBFB0B6127689324DAB6123DA20872CD26B4DE52FD088CF37345381F8A2FED394D73F76726AE4A5E2E46C79421190
Malicious:	false

Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.658162158299545e+12,"network":1.65816216e+12,"ticks":125270795.0,"uncertainty":5220940.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129725653"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\89363a91-dde3-4075-8cf7-91d666ea2293.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):	215376
Entropy (8bit):	6.071451435167173
Encrypted:	false
SSDEEP:	6144:lUpMpw3nP3OEwkqhGtA/UNm9FaqfIlUOoSiuRa:lNw3/ejGtArmox
MD5:	A6FC4A5FDD73DB2978389664D01D4311
SHA1:	35AF8872E1FAE3E276D30CBABB856905C822874C
SHA-256:	D08EF5F6016784EDC78B6AFC7C4C79618BDBE8398E7EE02EA34B33E9B73F467E
SHA-512:	2484EBF23748777221EB38D13813573266E53A36C764C1F571C91B9448E575E032F7FFDDD06CA5933B860B7C3CF19A3DC6154C55F67EB9C53D054E6E4A076C5A
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.658162158299545e+12,"network":1.65816216e+12,"ticks":125270795.0,"uncertainty":5220940.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129725653"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\8ce8a778-73c1-4ee1-921d-501740badb08.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):	215376
Entropy (8bit):	6.0714513694599255
Encrypted:	false
SSDEEP:	6144:qUpMpw3nP3OEwkqhGtA/UNm9FaqfIlUOoSiuRa:qNw3/ejGtArmox
MD5:	11D1D18EA4968E685268C1FB78453D7A
SHA1:	CAEE7799DD47FD4FF4564121FA4B9B3FAFA9841D
SHA-256:	F5AFE494B402DADEAF2AF39455E1BAB70ADA98D792086BCF666E94FB8B978934
SHA-512:	DF51A67F4DA1C686667FEFAF74069BB9B407B48F03B58BBCB797B54FE481DA4631F286009E90A57A7BB73B07F454E405DE984EA5DD591725241D3D1C685D16EE
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.658162158299545e+12,"network":1.65816216e+12,"ticks":125270795.0,"uncertainty":5220940.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"di

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXwgs0oRLn:+taRLn
MD5:	7AE9008C2AA5ED3E5ED52743E082F5BF
SHA1:	CD90099842F51474494BFC490433578A89C1B539
SHA-256:	94E7D9BF431A0E3F0FD02F0FBA7321F43DD8B523E3D32092AFC474D3FD5ABF62
SHA-512:	596E66D10186ADAD552F4CF7E74CD438AD19AF4C30950D2D6EB80E9F9430CA475D12BB79423EC8D15EAF37ABE0AD1DCCAE459C356A00055A82155C24A35C614
Malicious:	false

Preview:	sdPC....................UO..E.D.Q.o....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\114a658d-ecd8-43cb-9be7-13eba55e017a.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):	4934
Entropy (8bit):	4.9317054507112275
Encrypted:	false
SSDEEP:	48:YcXkKSChkliCcqALciqTlYGlQKHoTw0URkrN4MqM8C1Nfct/9BhUJo3KhmeSnpNv:nPLQBj1pIKIuRk5k0JCKL8bbOTlVuHn
MD5:	61FCBE3E2BD8C21811CB6AC485ED2C51
SHA1:	5EE018D05CB8C6EFBF5D1996F78105A05DE98497
SHA-256:	B03327A3ABFCDCE32FD40ECF899CFEFAC1014010FB97DAC29324FB5883C62596
SHA-512:	BC972F6DEB229A2FAF8981CE411DB810D1083DA904F20EB5C9E85FFC8D690EE6C4B9D80351D2FB188B445E0A9A082ACBA8B2F928761731F62F30B66DA7D21E 2F
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13302635756134417","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\46eeff2e-c4a7-4562-b899-53b19a8d0d59.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):	4961
Entropy (8bit):	4.9369204945350305
Encrypted:	false
SSDEEP:	48:YcXkKSChkliCQbsqALciqTlYGlQKHoTw0URkrN4MqM8C1Nfct/9BhUJo3KhmeSnR:nPLQ6j1pIKIuRk5k0JCKL85bOTlVuHn
MD5:	E4CB3C6AE3F9BE0FD8C7697354551DA3
SHA1:	2429E40D462C851FC96402FB6AD5DDB9B6851380
SHA-256:	6BB0B753CE45444140CA7581FABF46757B2FB76CEEA9A0B852888E9F87989B71
SHA-512:	27CDBEB0D701209E7DC7CBCC25546599DBA69E17A1B21602958EAD61F5B7C4349D886B706B2D87129461B0B434F040EE0207C5D2305A73A6905B515DD5304E(D
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13302635756134417","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\56fe0613-2fa7-48d7-8456-da39dd4152e3.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):	19796
Entropy (8bit):	5.564525079533198
Encrypted:	false
SSDEEP:	384:2P+tvLlDWXE1kXqKf/pUZNCgVLH2HfDBrUSOHGk7B7sS4I:fLlIE1kXqKf/pUZNCgVLH2Hf9rU5Gqsy
MD5:	FB4980C9DB133DF3AF1A901F67823D4D
SHA1:	96E7947B49FBB39F716164DB64E6CDE6D99E7C18
SHA-256:	A1B8C9ADD576FEF965AB792B1E585CE3DB057A44E9ECD71405D05726FB58EAAC
SHA-512:	428CC8C120E9E4F45FF524A855C69EAF7C9EFD166AAAA6CAC56CACB57C6E7CE377B2E8698B1E4D5086D561A50248582F3033384588DCD29CF833E4C9A18C8I 5D
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13302635754717530","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\7d5a61e7-35f3-4e76-8642-dae2ae803399.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):	3473
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhlGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIlyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1C
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607497410","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":27387},"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607318875","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":23359},"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7e67fe26-1e55-4a3a-b912-26f7e5155c82.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):	5.577268628165127
Encrypted:	false
SSDEEP:	384:2P+tvLlDWXE1kXqKf/pUZNCgVLH2HfDBrUB7BJsS44:fLlIE1kXqKf/pUZNCgVLH2Hf9rUtsSD
MD5:	CBEE29AC3928BEE2F7472D00A11637E3
SHA1:	F6866CF684FEABB03AB9CA448B6046DB43370F59
SHA-256:	F99A9330DC0282121ABD1FB9D422EBBD0C3DF1EE009244C24E03D3CA83FA4C94
SHA-512:	D026349A2C262F72CA40538ADEFC3393CDBFB53BA441B2CEAD3CC69F52EAC734EB199CB382F809E4030A31F18C059E834F4AC5B213591FEA21DB29D5995628E5
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13302635754717530","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\9ae7a855-5166-4070-9a01-71c526eb8520.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17529
Entropy (8bit):	5.574697710230317
Encrypted:	false
SSDEEP:	384:2P+teLlDWXE1kXqKf/pUZNCgVLH2HfDBrUz7B1sS4C:uLlIE1kXqKf/pUZNCgVLH2Hf9rUHsS9
MD5:	D66C585E6151F9DB944361FF4DB3AF90
SHA1:	56899AFC06898E2859B17C1AAD7422D71B6DCE98
SHA-256:	AB7C0174A18B56E11AF74A3F7144B3D4D34F566BDF19157F9A003054BB7E8A65
SHA-512:	40FF162C3FC70372F5CE0E57D641EB32513FDB0D77060474D19E83C1DF28E840700393B8C8C608665CB4367760713A591BBD572D8FCD36AF18BBB528C0176A7
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13302635754717530","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\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json

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

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

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

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.266149374021937
Encrypted:	false
SSDEEP:	6:6EFL+q2Pwkn23iKKdK25+Xqx8chI+IFUtqV5EW11ZmwYV5E1LklLVkwOwkn23iKG:+vYf5KkTXfchI3FUti11/gz5Jf5KkTM
MD5:	409B77ED55BB67440823F5952B811715
SHA1:	F2FB7525BA3FC5636528DCE3A66553B365441FAF
SHA-256:	021E24BBFB7C3E5EB2893BD2561A8BA3BE3BAFF83752BCFD943FA0F64D8BA1CB
SHA-512:	B8B476B2A70FF3D83C8FA7D4EBE97933AF151BDBC22F46087EC01183847F7FBAA20AD52EB6FB2F0A96DD5F5C31FF5BCC33A9D3F26AF3DAAB47AD7741CFA8DAF2
Malicious:	false
Preview:	2022/07/18-18:36:11.738 1a98 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/07/18-18:36:11.739 1a98 Recovering log #3.2022/07/18-18:36:11.740 1a98 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):	5.266149374021937
Encrypted:	false
SSDEEP:	6:6EFL+q2Pwkn23iKKdK25+Xqx8chI+IFUtqV5EW11ZmwYV5E1LklLVkwOwkn23iKG:+vYf5KkTXfchI3FUti11//gz5Jf5KkTM
MD5:	409B77ED55BB67440823F5952B811715
SHA1:	F2FB7525BA3FC5636528DCE3A66553B365441FAF
SHA-256:	021E24BBFB7C3E5EB2893BD2561A8BA3BE3BAFF83752BCFD943FA0F64D8BA1CB
SHA-512:	B8B476B2A70FF3D83C8FA7D4EBE97933AF151BDBC22F46087EC01183847F7FBAA20AD52EB6FB2F0A96DD5F5C31FF5BCC33A9D3F26AF3DAAB47AD7741CFA8DAF2
Malicious:	false
Preview:	2022/07/18-18:36:11.738 1a98 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/07/18-18:36:11.739 1a98 Recovering log #3.2022/07/18-18:36:11.740 1a98 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	917
Entropy (8bit):	5.4830196660678725
Encrypted:	false
SSDEEP:	24:18ikOGoQqTQ62ToN8j86nTRTq4Y78BJgskfa9yBDOxo7IVpncrAR:CiKoQs2c48ATRU4cy
MD5:	6FE8184496878FEBB0D82A041843B4EB
SHA1:	5DD661209945912CE85D126C0CAF9A1856330CD6
SHA-256:	DD1A14E65DE432CCF2E293B5823EF12FC0966857F1AFBDD8FC4BC7168C73EBC0
SHA-512:	BEDBC106824B9393C893D32243F4D6100AECC0983CB5D75A14F411047CD122A8549E14E6468E397F773D7C246195B64B9B02F1FED5CEBC0936EAE93EC0DE742
Malicious:	false
Preview:	......"b....0..2022..30190..c..cve..day..desktop..exploit..file..generator..hacxx..htm..user..msdt..users*.....0.....2022.....30190.....c.....cve.....day.....desktop.....exploit.....file.....generator.....hacxx.....htm.....user.....msdt.....users..2.....0.....1.....2.....3.....9.....a.....c.....d.....e.....f.....g.....h.....i.....j.....k.....l.....m.....n.....o.....p.....r.....s.....t.....u.....v.....x.....y...:.....B..... .....*^file:///C:/Users/user/Desktop/Hacxx%20MSDT%200-Day%20CVE-2022-30190%20Exploit%20Generator.htm21Hacxx MSDT 0-Day CVE-2022-30190 Exploit Generator:.....J".....%*,049?GQ..... (

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):	1518
Entropy (8bit):	4.811560928410642
Encrypted:	false
SSDEEP:	24:Y26aL3M33ayFGRaXa63aDaaraqavatZa+RdsdydR/RdsdaUdMHRmQYhbG7n/iy:Y2nzM3qyvK6qDHGXCtwWsGRLsnMHVYhM
MD5:	DFD52E3C64F71C443B41CC9934D1CCED
SHA1:	A805D4B4264B41193A2C9002379E60329BAF4FC2
SHA-256:	786508224F112AE902BE532719531FC5BBD08A89F1B66BDB7010EC2DC0949B49
SHA-512:	26B99A10B70023FA43865E1A33ED0515CE66FDD6DB59ABE00F5E570AAEBA1C20F2F555EBD46F93C67C0939936FB20F9A44487934F2F355D8FDBAB92B86B2BE44
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expi

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):	4961
Entropy (8bit):	4.9369204945350305
Encrypted:	false
SSDEEP:	48:YcXkKSChkliCQbsqALciqTlYGlQKHoTw0URkrN4MqM8C1Nfct/9BhUJo3KhmeSnR:nPLQ6j1pIKIuRk5k0JCKL85bOTlVuHn
MD5:	E4CB3C6AE3F9BE0FD8C7697354551DA3

SHA1:	2429E40D462C851FC96402FB6AD5DDB9B6851380
SHA-256:	6BB0B753CE45444140CA7581FABF46757B2FB76CEEA9A0B852888E9F87989B71
SHA-512:	27CDBEB0D701209E7DC7CBCC25546599DBA69E17A1B21602958EAD61F5B7C4349D886B706B2D87129461B0B434F040EE0207C5D2305A73A6905B515DD5304E D
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13302635756134417","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19796
Entropy (8bit):	5.564525079533198
Encrypted:	false
SSDEEP:	384:2P+tvLlDWXE1kXqKf/pUZNCgVLH2HfDBrUSOHGk7B7sS4I:fLlIE1kXqKf/pUZNCgVLH2Hf9rU5Gqsy
MD5:	FB4980C9DB133DF3AF1A901F67823D4D
SHA1:	96E7947B49FBB39F716164DB64E6CDE6D99E7C18
SHA-256:	A1B8C9ADD576FEF965AB792B1E585CE3DB057A44E9ECD71405D05726FB58EAAC
SHA-512:	428CC8C120E9E4F45FF524A855C69EAF7C9EFD166AAAA6CAC56CACB57C6E7CE377B2E8698B1E4D5086D561A50248582F3033384588DCD29CF833E4C9A18C8 5D
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13302635754717530","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\727a27ef-2203-4b69-a8bf-89c988389b14.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

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

SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898D58
Malicious:	false
Preview:	.....

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","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\5fa60e0e-e2b5-4357-988a-4477fd114917.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	325
Entropy (8bit):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2F7ED
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

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

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2 F7ED
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","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\a0c37120-c382-49e4-8883-5472249fbc6b.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):	19795
Entropy (8bit):	5.564600388134185
Encrypted:	false
SSDEEP:	384:2P+tvLlDWXE1kXqKf/pUZNCgVLH2HfDBrUSOHGV7BkEsS4E:fLlIE1kXqKf/pUZNCgVLH2Hf9rU5Gvs6
MD5:	973A16B9B437138E7FF99C53ADEA55D9
SHA1:	363637816F5B62C2223A6946FC5845E0EB14B1C9
SHA-256:	845D5251763E32250E7EDF9A9FC5DDCE45BD703E86825A98E9540F81F0F303A4
SHA-512:	AA426010D09E943F80350BFE86F579F452F178AB974480A9BA2E9397E86B74504099E332EB5A201B14815A4FA130B6B73148B578FA308003772C59582E2CA8D5
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13302635754717530","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\ca173ec6-7f47-4d84-bf32-be41c1efea0a.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):	4934
Entropy (8bit):	4.932413214347104
Encrypted:	false
SSDEEP:	48:YcXkKSChkliCrqAOiqTlYGlQKHoTw0URkrN4MqM8C1Nfct/9BhUJo3KhmeSnpNGC:nPLQGt1pIKIuRk5k0JCKL8bbOTlVuHn
MD5:	55849F4C2B83D0C437409B5656AEB038
SHA1:	5F4DC1BFFE12BF61CBCB3AF63E8571C6459EC800
SHA-256:	76961E62B82340BDBD836B58BD56C558807B3F842B93438F4BAD7397E779C648
SHA-512:	BB1421CC63C230A94F593C252E39FB75B95A625A2C6B651B977EC36520409FF7B615C6A2C40FD429D9E1AE1678C01E22D62B86503AD60A7F693C2C1E6D10A62
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13302635756134417","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

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

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

Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 89
Malicious:	false
Preview:	MANIFEST-000004.

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e8e1b108-9b2b-438d-a725-5f2576c66354.tmp

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f8a16519-1264-457e-bd0e-0d7479d9eb2b.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):	1518
Entropy (8bit):	4.811560928410642
Encrypted:	false
SSDEEP:	24:Y26aL3M33ayFGRaXa63aDaaraqavatZa+RdsdydR/RdsdaUdMHRmQYhbG7n/iy:Y2nzM3qyvK6qDHGXCtwWsGRLsnMHVYhM
MD5:	DFD52E3C64F71C443B41CC9934D1CCED
SHA1:	A805D4B4264B41193A2C9002379E60329BAF4FC2
SHA-256:	786508224F112AE902BE532719531FC5BBD08A89F1B66BDB7010EC2DC0949B49
SHA-512:	26B99A10B70023FA43865E1A33ED0515CE66FDD6DB59ABE00F5E570AAEBA1C20F2F555EBD46F93C67C0939936FB20F9A44487934F2F355D8FDBAB92B86B2BE 44
Malicious:	false

Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expi

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

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

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

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

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	207483
Entropy (8bit):	6.044823884945142
Encrypted:	false
SSDEEP:	6144:pCpMpw3nP3OEwkqhGtA/UNm9FaqfIlUOoSiuRa:pw3/ejGtArmox
MD5:	A313F6C250AD3B68156DEBE85E698917
SHA1:	7356DA767C7C6A407C605CC19178B3D5301B5200
SHA-256:	BB7FB9A132D4014488040F37F0D99786811DD123C17EF615249206DDC331EE4A
SHA-512:	F03059E4E83D5EE54293A1D0747B672E88142F6CBC3215C63C74BB1585FA59996BA555C9E135F33335DB013B423C3B494904FDA735D3D30B57606B7258215286
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.658162158299545e+12,"network":1.65816216e+12,"ticks":125270795.0,"uncertainty":5220940.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129725653"},"plugins":{"metadata":{"adobe-flash-player":{"di

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):	3.747691955928208
Encrypted:	false
SSDEEP:	384:pRpfux9jU2fsDrVQ29YNlr2vpz3SlDCHTeG2ZrUnxdxq3vHurshm8oakjtJ9WOD7:hqKl963E+kefF7T8/bO7KZXdB7
MD5:	6F95C6C58C47841DCCD9807E28BBEA43
SHA1:	C95DB01DE969D606B779295292BA2458B85AEFDC
SHA-256:	9552C0DA85FA3626EF6C426EE8842534C3DB9E513A3246FE06F065A0576157A4
SHA-512:	7A73DB1F5739A922497F5448E3D330BB51982E7F5A7B7535A5B6F4E9B2AC756C02359666C6F0EEA88CE5B5E6F0C6F5AFA01F982B990348A2A13D195311F0F561
Malicious:	false
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6..*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...Hb8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir3628_360129491\Ruleset Data

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	150056
Entropy (8bit):	4.8588214550289095
Encrypted:	false
SSDEEP:	3072:P8C4uHgjBz+BZKEZZ3F0Sl03PzpDL7Ul09QEwNyfe:P8C5go1U6lYeH
MD5:	C56FF16BF9B9FC0002C0128DD0BD763D
SHA1:	5048CFDBAC5D7AAAD345BAE08E66E8C4E803CA02
SHA-256:	404AA48D274C3A8FEC3145858E00279D01E0C37A5304218E191C0156E4DE00FF
SHA-512:	D993A324F5D9A1FC4FB3131252F48679750081D996295C994E2DCA4E84F2DECF7E90AF6766EFEDC2CEFC6B66194FFF38181C9E9CE45346BEEB8B3A09CE66BB 73
Malicious:	false
Preview:	.....[..... ...X...l...h...d...0.....X...T...P...L...H.....@...<.....4...0...,.....|...`...D..... .....'.....ozama.....*...'.....g.bat.....&.. .'.....onwod.....`....'.....ennab.....'.....nozam.....(.....geips.....P...((.....rekoj.....@(.....lgoog.....X(.....uotpo.....+..p(.....lreko.....d...h(.....Y..... .....Y...Y..pY..TY..8Y...Y...Y...Y...Y...Y...X...Y...Y...Y...Y...X..|Y..xY...X..pY..xX..hY..XX..`Y..\Y..4X..TY..PY..LY..HY..DY..@Y...X..8Y...W..0Y...W..(Y...W.. Y...Y...Y.. .Y...Y...Y...Y...Y...Y...X...X...X...X..PW..4W...X...X...X...X...W...X...X...X...X...V...X...V...V...X...X...X..xV...X...X...X...X...X...X...X...X...X..|X..4V..tX..pX..lX..hX..dX...V...U..XX ...U..PX..LX...U..DX..@X..<X..8X..xU..\U..@U..(X..$X.. X...X...X...X...U...X...X...X...T...T...T...T...W...W...W...W...W...W...W...W...W...LT...W...W...W...W.. T...W..

C:\Users\user\AppData\Local\Google\Chrome\User Data\b2c0e852-f021-448f-9c08-e38b954f106c.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):	206935
Entropy (8bit):	6.043534054291697
Encrypted:	false
SSDEEP:	6144:RZpMpw3nP3OEwkqhGtA/UNm9FaqfIlUOoSiuRa:Sw3/ejGtArmox
MD5:	7B78E5B5B96FBB0F51836A98E3A17DFE
SHA1:	AD1D038E790B95D8DFB08CFE5EDEE7C34BA29737
SHA-256:	CADA5FE33F21E2CF2EF439DE3AFB3F2C271593ACE82AA30E5525496E1767655D
SHA-512:	3AB37DF31BFA3CDC6311E6A0F67492F356AC8DC1CFF4C40455BD2BE7662251BD01046C18C8AA4743D2E63B8CB9D9E5A92A3F4BBEA0781E97970D85D4B00A6 21
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground": {}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}}, "network_time":{"network_time_mapping":{"local":1.658162158299545e+12,"network":1.65816216e+12,"ticks":125270795.0,"uncertainty":5220940.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqI YBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps 4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129725653"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\bca37c47-d014-4f7a-b1d6-5f2c7b48d818.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):	215376

Entropy (8bit):	6.0714513694599255
Encrypted:	false
SSDEEP:	6144:qUpMpw3nP3OEwkqhGtA/UNm9FaqfllUOoSiuRa:qNw3/ejGtArmox
MD5:	11D1D18EA4968E685268C1FB78453D7A
SHA1:	CAEE7799DD47FD4FF4564121FA4B9B3FAFA9841D
SHA-256:	F5AFE494B402DADEAF2AF39455E1BAB70ADA98D792086BCF666E94FB8B978934
SHA-512:	DF51A67F4DA1C686667FEFAF74069BB9B407B48F03B58BBCB797B54FE481DA4631F286009E90A57A7BB73B07F454E405DE984EA5DD591725241D3D1C685D16E E
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground": {}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}}, "network_time":{"network_time_mapping":{"local":1.658162158299545e+12,"network":1.65816216e+12,"ticks":125270795.0,"uncertainty":5220940.0}},"os_crypt":{"encryp ted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPql YBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps 4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"}," password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\c5c88fb3-f819-4ba0-bf6a-a459b9a5cc93.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):	207400
Entropy (8bit):	6.044678241980226
Encrypted:	false
SSDEEP:	6144:KCpMpw3nP3OEwkqhGtA/UNm9FaqfllUOoSiuRa:mw3/ejGtArmox
MD5:	3C476CA19288C64B63972E0501A8DBFB
SHA1:	5550C5E85A9330E377FD3A64B6B763CB6C12A683
SHA-256:	EA07A6AF8E8ABF42C02D7E8D4A0604ACE3F27867861353CBF91ACF2C3A1EE704
SHA-512:	1C16B53F11A33EF5C19EBFE8B4B71EA8A7548DD38CB02835E4FD0E7DAC795D757CD22370A791DBAC6E4DF325B576097934B45430CFC69D46576D4DC4C9571 A6
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground": {}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}}, "network_time":{"network_time_mapping":{"local":1.658162158299545e+12,"network":1.65816216e+12,"ticks":125270795.0,"uncertainty":5220940.0}},"os_crypt":{"encryp ted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPql YBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps 4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"}," password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129725653"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\cecc145c-6e1c-4fe2-8378-812c8c4b9c09.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	207483
Entropy (8bit):	6.044823884945142
Encrypted:	false
SSDEEP:	6144:pCpMpw3nP3OEwkqhGtA/UNm9FaqfllUOoSiuRa:pw3/ejGtArmox
MD5:	A313F6C250AD3B68156DEBE85E698917
SHA1:	7356DA767C7C6A407C605CC19178B3D5301B5200
SHA-256:	BB7FB9A132D4014488040F37F0D99786811DD123C17EF615249206DDC331EE4A
SHA-512:	F03059E4E83D5EE54293A1D0747B672E88142F6CBC3215C63C74BB1585FA59996BA555C9E135F33335DB013B423C3B494904FDA735D3D30B57606B7258215286
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground": {}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}}, "network_time":{"network_time_mapping":{"local":1.658162158299545e+12,"network":1.65816216e+12,"ticks":125270795.0,"uncertainty":5220940.0}},"os_crypt":{"encryp ted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPql YBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps 4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"}," password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129725653"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\d5b172b1-5595-4dae-853a-723d6f31977d.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):	207121

Entropy (8bit):	6.044029905204594
Encrypted:	false
SSDEEP:	6144:qZpMpw3nP3OEwkqhGtA/UNm9FaqfIlUOoSiuRa:lw3/ejGtArmox
MD5:	3AE3478FFBA7B75AF03FC9124B8C713B
SHA1:	A0F6F272E702635405AC5679A5AFA093627C8EC3
SHA-256:	313A754BBBA630E255304E5AE9FE90A5D205AC40D91A847811B03252D43F4F98
SHA-512:	8488FC80F89280BA470E736CC0FB962870022E7FC012E9AE762FEEF69CA7C1BFF7FA7BBB9DEAE272F87339A11E29C152D69FD62DB6ACA3BAD5A05B17CB495EBF
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.658162158299545e+12,"network":1.65816216e+12,"ticks":125270795.0,"uncertainty":5220940.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129725653"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Temp\3628_1040151320\LICENSE

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

C:\Users\user\AppData\Local\Temp\3628_1040151320_metadata\verified_contents.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1511
Entropy (8bit):	5.970539470066976
Encrypted:	false
SSDEEP:	24:pZRj/flTU3YThgA9PjoYzM67aoXPXy+/ip/yKeF7koX0o+0tudn5kVh9J0ho2pTs:p/hUICy+67akPCT/2kkCAK5kVLJ0Ts
MD5:	C7C3AB14499E6EC12051CF70E20F0E78
SHA1:	9D8D67E8EA1A96A8848472A3CA526D7B236FE39F
SHA-256:	B3F070CA7725A2E82E53D8C564D573A0B78541508F7D8E6DEF451816CEC80D8D
SHA-512:	F42BC7704DF0DB2AF9E1800B8C5F0009DFCFB9F5A08A103D0D863228D65E6C5F877F3DE9E41B1BEAB149BC0A90A99F83089D83EA8B7C4D72639A4170C199583
Malicious:	false
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJMSUNFTlNFIiwicm9vdF9oYXNoIjoiUGIwc2tBVUxaUzFqWldTQnctV0hIRkltRlhVcExiZDlUcVkwR2ZHSHBWcyJ9LHsicGF0aCI6ImNybC1zZXQiLCJyb290X2hhc2giOiJBRV9DS2xGM2pSRU9sWVpRMjZTMURfRU5yVGJlOF9LakRlcTdXMlZoZnpRIn0seyJwYXRoIjoibWFuaWZlc3QuanNvbiIsInJvb3RfaGFzaCI6IndWX2hWV0NkU1U4RW1VWmdfX0hMbzlXSUQ4bmhHWk5BbU55SG12YVZaTWcifV0sImZvcm1hdCI6InRyZWVoYXNoIiwiaGFzaF9ibG9ja19zaXplIjo0MDk2fV0sIml0ZW1faWQiOiJoZm5rcGltbGhoZ2llYWRkZ2ZlbWpob2ZtZmJsbW5pYiIsIml0ZW1fdmVyc2lvbiI6NjYiLCJwcm90b2NvbF92ZXJzaW9uIjoxfQ","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"N0ZgnxUpdaD5lUNUstfnVOMqjRbq3uYTW4Qdkzm3Kc0J6S3gdrngzc1GAaNGdewlGfiR-q-Ju8puFuPVLDhIl1JWMqn8eFDsdwyqkrQz9Bl52w8YgoyjnLTh4nCsVXh0EshyasCBom0faehzW6LgVAtQhZ9cXEdKs9K6ACf3-X4hxbRUkvcReLI5Sv_3Kdy_TZS03eru8hTilub1SwgJ_12P-kQth0RLcMY1MEDHD8xbZwqcl9vehesNVPOcJ7Gs6gY

C:\Users\user\AppData\Local\Temp\3628_1040151320\crl-set

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

Size (bytes):	22887
Entropy (8bit):	7.83801346554205
Encrypted:	false
SSDEEP:	384:T26XPKcVeWcURWVPODJc4m8kWxmXYoBZsTQ4k5bYTaQzsvFvatr4G9h96/HDufBr:Tf38ZVGDJJuW0XYozmQ4+YTaSKCr4G0u
MD5:	A0FADBD777E88DC09B7B65D38D0D2E85
SHA1:	2BFCF628429FD5E07E86DB2203007BFFCE10CE30
SHA-256:	FEC5BDA618A63AE22FC447D5B1E6745C12985895DE78B589573155F23E06748A
SHA-512:	E155C619AD0717943958548A874AC5B3556598FDEAA5973738F1602CBCF6CA7E893DDF85CDF0FDDB23F40772EE8C8BC5D6AA67F1DC3E2A4A6EC57069EFA2E1B
Malicious:	false
Preview:	".{"Version":0,"ContentType":"CRLSet","Sequence":7466,"DeltaFrom":0,"NumParents":193,"BlockedSPKIs":["Jdoa1Yu/z7In2HI7GFfUwY57qnQXtPnv+TZrXoafizk=","Ii5LVLuYp+5dX+uWM/mR08MwDpUU2t57DU+CjHlPjoc=","yP3cdcsb27WMB7TqhHKH9iZIndZrwQomrdm1dbOgo40=","BN3pqpp59hSYaCMl+ghwJ2cH+5ypU4QSC0aJMmhJT8k=","tbqN1/iVZMKInT1kU8hJmMd4JJGbZOoINapimGWRvlA=","wO0gU0a7veButWD1zuAqNjTiR0p+ds+PvvVjuxF90OM=","eBpM8ukkUvPuAdDDgaQhTzkEFlw5CtvWH80RJE4Jstw=","/NdsyiNH5c1bOTR/Uc9DZUtpor/JBzZwpr5H2HAebg4=","lo26afv/Fb83YgiUMa3lp+rUt+rxvnACaBC8V9HGT24=","fNKVt1VEgIq9lAlGbwg3xarcAuM7YVDGZE3goJZZ8jw=","9Sk9R+041MMbLULe47WzrOl8omyirANl42Iu6AlTH7s=","nFmjzK6kaZhCsGjPxSz5RdtRmGlXyDLNsYynOEn7ue4=","OUz/WJ5okxLPwHHuC8Gf5MYGIWzlQ0Kd5tti5C27O8E=","NuqWEoyJg5+2IfitDh7gucIgb2Kre02ixnZYk8m3ztI=","pqyh7JgJzFtIIf+dKcXr5lGWC5Gx8ZzIm1Xvh4GKlQk=","MO/kE4JHbDOA8C9+I+ZrovhnsFnuHqaHlrRBuFtdElY=","r1kVGOLmxg67/AkHr6pJvEBR1F5/IUq/7nUS7gD2Ye0=","6EnHF2yT32X2S2FpgjZuVmMReBK2+ivAyPqK6u5Bgcw=","0x7DkoW3pTGdAVfbQg7YfHQ+Mzu8d/h3H3BGT0NqYEk=","h7/Yr

C:\Users\user\AppData\Local\Temp\3628_1040151320\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):	3.9585645296198466
Encrypted:	false
SSDEEP:	3:S7NlUB5AUgBUROG2DG17UYV4jHX:SxOBeUgBG2iFPaj3
MD5:	DED47DD360493C1555D9849B082DFF50
SHA1:	F72B12344BDA162DE96923BA086EA9AFC049ED36
SHA-256:	6E55B58EF3568A1B31F0F08A752C3E10B2A497B112E3015A1A06CCB3507B62EF
SHA-512:	7522011281ED8BA4F6AD7439339F385EDD5F88204C20C2D1D5ECA301DB8D54AA0B4400A35718C127A4A08CD5BCD383548084F6E2ACB9FF1A068741398E5EC092
Malicious:	false
Preview:	1.d9ef474c1dab4d5de1e54cf8f2a86f756e7bcf23a8013c743161007f22ba1220

C:\Users\user\AppData\Local\Temp\3628_1040151320\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	192
Entropy (8bit):	4.808430356468707
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFJRevSlLC4FgS1mz9JEeSWU4pv/8F/FxLj2RF2fcTZTotL:F6VlMYSKS1mwWfB0NpK4aotL
MD5:	1A435BCBD2BB2B600CF880F2F0C5423D
SHA1:	81503CE661F0F65A112067CDF8FBF0D0D597FD03
SHA-256:	C15FE155609D494F04994660FFF1CBA3D5880FC9E119934098DC879AF69564C8
SHA-512:	84E7BD00AF1F61A1AC0B7ECE54E9DBC47ACB5C0FDE54E359FDC43C7845C98F4F2B864E3825E6BA0647125C5CBFDF7A53AF3F8DA490E793F1683183599073C274
Malicious:	false
Preview:	{. "manifest_version": 2,. "name": "crl-set-10890505766058335453.data",. "version": "7466",. "imageName": "image.squash",. "squash": true,. "fsType": "squashfs",. "isRemovable": false.}

C:\Users\user\AppData\Local\Temp\3628_1290221689\Recovery.crx3

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	145035
Entropy (8bit):	**7.995615725071868**
Encrypted:	**true**
SSDEEP:	3072:TdgEhmDf+E8VY0x81Rkc6L2oqzqkPEu30gZlc3G2ZknF:TyEhmDf+/+Fnkj6lEukgZyyF
MD5:	EA1C1FFD3EA54D1FB117BFDBB3569C60
SHA1:	10958B0F690AE8F5240E1528B1CCFFFF28A33272

SHA-256:	7C3A6A7D16AC44C3200F572A764BCE7D8FA84B9572DD028B15C59BDCCBC0A77D
SHA-512:	6C30728CAC9EAC53F0B27B7DBE2222DA83225C3B63617D6B271A6CFEDF18E8F0A8DFFA1053E1CBC4C5E16625F4BBC0D03AA306A946C9D72FAA4CEB779F8FF CAF
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.| 1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....S'.....2.{.....'....+.'..''..Y.x.ISa...)....H.&92..?!..~..F.5."...n,.B.-|\.)..(.....]G..j.-M)... .C.....o&L..0.K.....UtP.&.N...;..^w/a{)v...~KG;...?.1...k.c..D.U.....J.6.`.G.5.x.k..[...i.A.@I^..I.<A. J...j.'.G.`.$q.N..Tdq]2]p.OF..#.#.....'....8.3.....0.."0...*.H.....0.....O..(...':19..O/.>....=.....m.n\.z..q.....JW..F.....+H.Z+KGO.9....8....U...&.y....,$...?.Eo.....\f/.Z..+M8...B.3'..Y.r...X.AS?.~..k..n..... Z...&.G....."n.....l.0v.x#<....Lx,-.w..-..d.....J.pT..(' e~*{%kQ.Q.....rI.....Z....v.N.....J.d_.....rX.....w@.b.[.c../V.'c...!.~.k..}z...U.S..nC.....@.....Y..#.D.z.....5&.1O...X=p..2.F..P.6yP..>{.....HBX.*.E5....y..

C:\Users\user\AppData\Local\Temp\3628_1290221689_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:	BCBE40CAFAA4B14566D91E361D8FB7F0288D5C459FA478AA4C575444DA4D406E1076FC0B3A31D4A9E5EE034F0FE15A0EFE8A8A52B838DE94B96D3E488D28F0 FE
Malicious:	false
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiO lt7InBhdGgiOiJSZWNvdmVyeS5jcngzIiwicm9vdF9oYXNoIjoiaGdCR051SzhNR2NKaDlfNmZQaFdEWmpVYUFKeklzeDlJS21DUEZvb0dfUSJ9LHsicGF0aCI6Im1hbml mZXN0Lmpzb24iLCJyb290X2hhc2giOiIwYXduVFBFQmdDRHkyV05hVVk3Um9mSWN3c3ZwNHFRNUxzZVMxVXRiVXY0In1dLCJmb3JtYXQiOiJ0cmVlaGFzaCI sImhhc2hfYmxvY2tfc2l6ZSI6NDA5Nn1dLCJpdGVtX2lkIjoiaWhubGNlbm9jZWhnZGFlZ2RtaGJpZGpobmhkY2hmbW0iLCJpdGVtX3ZlcnNpb24iOilxLjMuMzYuMTQxI iwicHJvdG9jb2xfdmVyc2lvbiI6MX0","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"iFuMX_kOZ-zJ7KVu6Lxb3rHWZg QvkZhv25x_SGlBiDV_okALrGbj6rUOWyNNNsHXMnT118XZmA696XR8qkr4dwT5Gvez-9gi-WYBY7XBkgo7v6NspGgJF89BNCeI-P9k-zBHOGgrf-fCEiAcoM7xCx9_f8ql Ry7nhQPyjOIHn5eEJEir0uSu6gdqR9afnVZ3UoR-VOLdOBt7fA4ee38MP2ut5qWU50F5dvIezfKkTVDMHwztvcLCy6R9SVkdSYv6jwWGccYRl-aclvkkHu6SnbZGI7fmDZ dkcBAxBHYEZZMmvb76ro4SO15GDyEVAo_Qf4trdrY_GyN_Bm73imCTjgtoGc

C:\Users\user\AppData\Local\Temp\3628_1290221689\manifest.fingerprint

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.7900469623255675
Encrypted:	false
SSDEEP:	3:SpOXzxlQ4BdPWfDL9c:SpOjDQFfVc
MD5:	2AE14F91312C4E8034366B09D49D5B18
SHA1:	AD4933A5D838D0FA0B960C327A5039A9E8249642
SHA-256:	4F122332EF0F2BB490EF59619D3602C1A7277C0A7A19C132202DB4803A09BFA2
SHA-512:	FB0CC467A4B8463F6A3BF42CDC11C23B34EB94A9397644B68714DCB819EE326BAE05022D59D23DC9907DF1E6928064D853FD0900BB6083417892D4D5A9BA771
Malicious:	false
Preview:	1.aeedb246d19256a956fedaa89fb62423ae5bd8855a2a1f3189161cf045645a19

C:\Users\user\AppData\Local\Temp\3628_1290221689\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	195
Entropy (8bit):	4.682333395896383
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFJ9LAG9Xg0XTFHqS1wP/pEeSWU4pv/8F/FxLj2RF2fcTZTotL:F6VlM90ggITgS1wnuWfB0NpK4aotL
MD5:	7A8E3A0B6417948DF4D49F3915428D7A
SHA1:	4FC084AABDB13483567D5C417C7ED8FD16726A80
SHA-256:	D1AC274CF1018020F2D9635A518ED1A1F21CC2CBE9E2A4392EC792D54B5B52FE
SHA-512:	064D84A57B28C19AD10742859DA493D0826B47ADC632F6C623DFB4DE36D72A9D29BE98518061A9FFD42D99FCF01F27DE39CE74782B3A5ACBBE11DFDDEEAB5 9A1
Malicious:	false

Preview:	{. "manifest_version": 2,. "name": "ImprovedRecoveryComponentInner",. "version": "1.3.36.141",. "imageName": "image.squash",. "squash": true,. "fsType": "squashfs",. "isRemovable": false.}

C:\Users\user\AppData\Local\Temp\3628_1783822598_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):	6.016932513650603
Encrypted:	false
SSDEEP:	48:p/hKAGj0FnAp7XgNGIaku9E5tPJXaWqkbszesM:R5Gj0FAlsaBmfPsRD3M
MD5:	6D1D175F88B64546105E3E7C31D1129A
SHA1:	75A1B56F55BB62B05365A0FDBFC7941DE77CBFAF
SHA-256:	A0BC246E8E160A9BB32FA60F4E7A04D148A17125F426509466031E07731FDF81
SHA-512:	5C80908331E30C7EAD67F7F6C5AB064B07626FD9C58925A0D2124D66B25C5AE2F218BDACFB68AFCB332E88EB297CFB7E0A7A9E5E1E54C9B7A510FEF095F9B54F
Malicious:	false
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJtYW5pZmVzdC5qc29uIiwicm9vdF9oYXNoIjoiSUxrUllPSmhIVEZaclllLRmN5UC12SkJrVjNWbWVLdHo4d1hEb2VPWjBZMCJ9LHsicGF0aCI6InNzbF9lcnJvcl9hc3Npc3RhbnQucGIiLCJyb290X2hhc2giOiJyRFZLUnlPcXBQQnI3RGhkM2VTazBKZzYxUlJXOVNzeHFBYU95WDFiWHFjIn1dLCJmb3JtYXQiOiJ0cmVlaGFzaCIsImhhc2hfYmxvY2tfc2l6ZSI6NDA5Nn1dLCJpdGVtX2lkIjoiZ2lla2NtbWxua2xlbmxhb21wcGtwaGtuam1ubnBuZWgiLCJpdGVtX3ZlcnNpb24iOiI3IiwicHJvdG9jb2xfdmVyc2lvbiI6MX0","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"nBdNk-7bgnEftAs4hWaHwF1Lk9pt7Eh6pcqe2gyNsE7VnVRp-H27tm1RFAF4htCUlXNJxX6YY-MUiK2DqJpQ3c73KDaFV8DcnadQfcXO3Lbrw7jLYSUaSdzujPkTyhuFcq_BhK0KWiIJ0aJgh7nVOBfAa5AbE6oFlLKMB2Ls0gmzS1-a5hUIu4rw2h9r9jkr6gLYbein5Jk2hdwW3u-1GNjyki4dftG2iZNAI8VhUf5gnCiF4AHCnYSGJsM0RGkmO_HJlzgwpQpP3RDsG2ioeKgxL-kcHhjXWOj3uVGyxpp1FkyHGkeGuqpFZMAxx3CEBiOtFj7i3iQxkgEW-E3uMKI3yA

C:\Users\user\AppData\Local\Temp\3628_1783822598\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):	3.9570514164363635
Encrypted:	false
SSDEEP:	3:SVCBGERJd9WaHpYx4eiXoA:SVCwERJdVMiXd
MD5:	C6ABF42CB5AF869629971C2E42A87FD5
SHA1:	6EB0FAE28D9466E76FA12E31FE6CDADD3ACCE4D1
SHA-256:	D281AFDA759075F4CB7D7CEEC4A3CB2AF135213B4D691F27090E13F238486AD1
SHA-512:	EDDF7E4883E82718743C589E8F2E48BEAD948428E730231FEFADAD380853343332BC56C9DC61C963B3F537CD4865B06FF330CEF012B152CEA35F8A0AA2C7B5D
Malicious:	false
Preview:	1.fd515ec0dc30d25a09641b8b83729234bc50f4511e35ce17d24fd996252eaace

C:\Users\user\AppData\Local\Temp\3628_1783822598\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	76
Entropy (8bit):	4.169145448714876
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFY8Wypv/KS1f:F6VlMQyBSS1f
MD5:	4AAA0ED8099ECC1DA778A9BC39393808
SHA1:	0E4A733A5AF337F101CFA6BEA5EBC153380F7B05
SHA-256:	20B91160E2611D3159AD82857323FEBC906457756678AB73F305C3A1E399D18D
SHA-512:	DFA942C35E1E5F62DD8840C97693CDBFD6D71A1FD2F42E26CB75B98BB6A1818395ECDF552D46F07DFF1E9C74F1493A39E05B14E3409963EFF1ADA8889715289
Malicious:	false
Preview:	{. "manifest_version": 2,. "name": "sslErrorAssistant",. "version": "7".}

C:\Users\user\AppData\Local\Temp\3628_1783822598\ssl_error_assistant.pb

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

Category:	dropped
Size (bytes):	2816
Entropy (8bit):	6.108955364911366
Encrypted:	false
SSDEEP:	48:jkbh6AW2Bfc3osI6Hc3+XgU+EVeY55J4gXM/QDH4yq2dxckdfmkM:jkbhM2a3pntgQVb8Ylq2di
MD5:	E2F792C9E2DD86F39E8286B2EAD2FC70
SHA1:	8A32867614D2A23E473ED642056DED8E566687F9
SHA-256:	AC354A4723AAA4F06BEC385DDDE4A4D0983AD51456F52B31A8068EC97D5B5EA7
SHA-512:	6A7AF0CA1EFA65A89A9CA3B8DF0D2E24F21D91673C60CDFEEB02D33647442B01D535497249542F40E66E0D2DD3E9F8ED1F4A201FD97138D07A2B71366737E58 0
Malicious:	false
Preview:	...5.3sha256/fjZPHewEHTrMDX3l1ecEIeoy3WFxHyGplOLv28klbtI=.5.3sha256/m/nBiLhStttu1YmOz7Y3D2u1iB1dV2CbIfFa3R2YW5M=.5.3sha256/8Iuf4xR bVCmCMQTJn3rxlgIIO1IOKoyuSUgmXyfaIKs=.5.3sha256/8IHdrS+r6IWzSMcRcD/GA6mBxk1ECX8tGRW0rtGWILE=.5.3sha256/k/2eeJTznE32mblA/du19wpVDSI ReFX44M8wXa2JY30=.5.3sha256/urWd7jMwR6DJgvWhp6xfRHF5b/cba3iG0ggXtTR6AfM=.5.3sha256/IJPCDSE5tM9H3nuD5m6RU2i9KDdPXVn4qmC/ULlcZzc=.5. 3sha256/0Gy8RMdbxHNWR2GQJ62QKDXORYf5JmMmnr1FJFPYpzM=.5.3sha256/8tTICtyaxIQrdbYYDdgZhTN0OpM9kYndvoImtw1Ys5E=.5.3sha256/F7HIlsaG0bpJ W8CzYekRbtFqLVTTGqwvuwPDqnlLct0=.5.3sha256/zaV2Aw1A742R1+WpXWvL5atsJbGmeSS6dzZOfe6f1Yw=.5.3sha256/UwOkRGMlP0K/mKNJdpQ0sTg2ean9Tje8 UTOvFYzt1GE=.5.3sha256/w7KUXE4/BAo1YVZdO3mBsrMpu4IQuN0mhUXUI//agVU=.5.3sha256/JnPvGqEn36FjHQlBXtG1uWwNtdMj1o2ojR/asqyypNk=.5.3sha2 56/AUSXlKDCf1X30WhWeAWbjToABfBkJrKWPL6KwEi5VH0=.5.3sha256/zSyVjjFJMIeXK0ktVTIjewwr6U5OePRqyY/nEXTI4P8=.5.3sha256/9dcHlrXN2WV/ehbEd MxMZ8IV4qvGejCtNC5r6nfTviM=.5.3sha256/E+0WZLGSIe5nddlVKZ5fYzaNHHCE3hNqi/OWZD3iKgA=.5.3sha2

C:\Users\user\AppData\Local\Temp\3628_2036087933_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:	37048EF8FADF62A26CAEC6EE90AC192429AB1E99424E5C68FACA90C0DAD68642C761FDCAC03FC38FA930841F91FA145A6943EC7F168D4F2FA426F1F092C2F5 02
Malicious:	false
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiO lt7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY19wbmFjbF9qc29uIiwicm9vdF9oYXNoIjoiVkNUSHNJVHNUSXVncWNhV2ctWHVpTU1 sdWloV1FSTE1sQnpTTGprdGhETSJ9LHsicGF0aCI6Il9wbGF0Zm9ybV9zcGVjaWZpYy94ODZfNjQvcG5hY2xfcHVibGljX3g4Nl82NF9jcnRiZWdpbl9mb3JfZWhfbyIs nJvb3RfaGFzaCI6ImxINWt2a1BvSVZZczZKVHhyOHc5Q2MxXzloVEJCX3lVSlF6VDZseVVNd0kifSx7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWN sX3B1YmxpY194ODZfNjRfY3J0YmVnaW5fbyIsInJvb3RfaGFzaCI6IkVuLVFQTW1HUm1xbG9Ud1gzOTAzckpsMkw0R25sQmdET1FhZlNKaHJ4Nk0ifSx7InBhdGgiOiJfc GxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY194ODZfNjRfY3J0ZW5kX28iLCJyb290X2hhc2giOiJkT2lJVzRmdEdGNW9FY0k1UXYyYjBmd XNrUlYyaUVtdmxhbmV6MlpFc3VvIn0seyJwYXRoIjoiX3BsYXRmb3JtX3NwZWNpZmljL3g4Nl82NC9wbmFjbF9wdWJsaWNfeDg2XzY0X2xkX25leGUiLCJyb290X2hhc2g iOiIzNEU5QU9EMmpqLWNoMzZQZ0NVV0YtMUpYWVhVdlNGY1I4bks1aWppcWNjIn0seyJwYXRoIjoiX3B

C:\Users\user\AppData\Local\Temp\3628_2036087933_platform_specific\x86_64\pnacl_public_pnacl_json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	507
Entropy (8bit):	4.68252584617246
Encrypted:	false
SSDEEP:	12:TjLJ7qaVgPPd8bdzQBXefosmc5T9+n6e1Cetm1JXcAwA:TJ7jViPOd8wfHmZ6RP15
MD5:	35D5F285F255682477F4C50E93299146
SHA1:	FB58813C4D785412F05962CD379434669DE79C2B
SHA-256:	5424C7B084EC4C8BA0A9C69683E5EE88C325BA28564112CC941CD22E392D8433
SHA-512:	59DF2D5F2684FACC80C72F9C4B7E280F705776076C9D843534F772D5A3D578BEE04289AEE81320F23FB4D743F3969EDF5BA53FEBBAC8A4D27F3BC53BCF271C E
Malicious:	false
Preview:	{. "COMMENT": [. "This file serves as a template for the resource info description used by ", . "the NaCl Chrome plugin. It is kept in the NaCl repository to prevent ", . "hard-coding of NaCl-specific information inside the Chrome repository.".], . "abi-version": 1, . "pnacl-arch": "x86-64", . "pnacl-ld-name": "ld.nexe", . "pnacl-llc-name": "pnacl-llc.nexe", . "pnacl-sz-name": "pnacl-sz.nexe", . "pnacl-version": "5dfe030a71ca66e72c5719ef5034c2ed24706c43".}

C:\Users\user\AppData\Local\Temp\3628_2036087933_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_for_eh_o

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped

Size (bytes):	2712
Entropy (8bit):	3.4025803725190906
Encrypted:	false
SSDEEP:	48:b/5D5V5PK82aTS6aTTw0Do1DttoyDNsEA:b/hbVic1ZtLDNsE
MD5:	604FF8F351A88E7A1DBD7C836378AE86
SHA1:	9D8D89AE9F13D6306E619A4EAAD51EDE91A5F9F3
SHA-256:	947E64BE43E821562CE894F1AFCC3D09CD7FF614C107FC94250CD3EA5C943302
SHA-512:	85B1EDA4C473E00034EE627B7ABB894A77E521BC6A91A91A4A3744CA7511CB0AF10B9723D9ECC2CE3378DD70B659DF842D8C11875958CB77070CF01EC0A158 40
Malicious:	false
Preview:	.ELF.....>.....@.....@.....PH.....,$J.l=....J.$<A[..@.A...M..A..ffffff.....PH.....,$J.l=....J.$<A[..D..A...M..A..ffffff..... ....PH..1..,$J.l=....J.$<A[.....A...M..A..ffffff.....PH..SP..h.....fff.....h.....fff.....J.$<[.,$J.l=....J.$<.....f..... .....NaCl....x86-64.....zR..x.....@....C....C.....8.....@....C....C.....T.....@....C....C .....p.....`....C....C..B..... .....<.....@.....X.....t.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl- clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pna

C:\Users\user\AppData\Local\Temp\3628_2036087933_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_o

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

C:\Users\user\AppData\Local\Temp\3628_2036087933_platform_specific\x86_64\pnacl_public_x86_64_crtend_o

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

C:\Users\user\AppData\Local\Temp\3628_2036087933_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:HPHonlwYZJ0ykwVO7Owf31yJKzCtxO8RSV4lY+PbeHVxCtjFV4lBNeSAmfGqa+A7:HvSMRwf3SKmlY+PyPvnM2Gq+

MD5:	0BB967D2E99BE65C05A646BC67734833
SHA1:	220A41A326F85081A74C4BB7C5F4E115D1B4B960
SHA-256:	C6C2D0C2FC3E38A9BFA19C78066439C2F745393F1FD1C49C3C6777F697222C76
SHA-512:	8EF8689E00E4B210A30444D18ED6247F364995ABEB2FD272064C3AF671EEDB4D9B8B67CA56F72FEBF8F56896D4EA7EC4B10CB445FFA1C710C1F312E9DA0E4896
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	.ELF.....>.... .....@.....!.....@.8...@.....{.....W.....@.....@.....P.td.....h.....h.....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\3628_2036087933_platform_specific\x86_64\pnacl_public_x86_64_libcrt_platform_a

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

C:\Users\user\AppData\Local\Temp\3628_2036087933_platform_specific\x86_64\pnacl_public_x86_64_libgcc_a

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

C:\Users\user\AppData\Local\Temp\3628_2036087933_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_a

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	13514
Entropy (8bit):	3.8217211433441904
Encrypted:	false
SSDEEP:	192:uU9v4pXizdrEuxwk3vp20tprpdSGFwDqO:P9v4palvvc0tpFdSGFwmO

MD5:	4E8BEDA73EB7BD99528BF62B7835A3FA
SHA1:	DC0F263A7B2A649D11FF7B56FE9CFAC44F946036
SHA-256:	6B835FD48DF505EB336FF6518CE7B93BB0ED854DADAA5C1EEED48D420291F62C
SHA-512:	46116B8BABC719676D68FD40D2AC82F38A3D13D8A482ADFC6FC32A99170AC3420E52CC33242CCD0FA723ABF4FA5EDBB9CE16A09C729BF04AE4AFBB2F67A1E 38B
Malicious:	false
Preview:	!<arch>./ 0 0 0 0 94 `....._pnacl_wrapper_start.__pnacl_real_irt_query_func.__pnacl_wrap_irt_query_func..shim_entry.o/ 0 0 0 644 7392 `..ELF.....>..... .....@.....@.....NaCl....x86-64.....A.L....A.L...D.....D....A.....t+.. u..t"..A.D..... .....A... .....A.D.....f..D..<.....Q.....V.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163f dd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f).../../ ppapi/native_client/src/untrusted/pnacl_irt_shim/shim_entry.c./mnt/data/b/build/slave/sdk/build/src/out_pnacl/x64.NACL_STARTUP_FINI.NACL_STARTUP_ENVC. NACL_STARTUP_ARGC.NACL_STARTUP_ARGV.NaClStartupInfoIndex.unsigned int.size_t.char.TYPE_na

C:\Users\user\AppData\Local\Temp\3628_2036087933_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_dummy_a

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

C:\Users\user\AppData\Local\Temp\3628_2036087933_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=309d6d3d463e6b1b0690f39eb226b1e4c469b2ce, stripped
Category:	dropped
Size (bytes):	14091416
Entropy (8bit):	5.928868737447095
Encrypted:	false
SSDEEP:	196608:tKVqXp3Qev4dg6ilfHM8KLM2J3jqjnkZ:uqufB
MD5:	9B159191C29E766EBBF799FA951C581B
SHA1:	D1D4BBC63AB5FC1E4A54EB7B82095A6F2CE535EE
SHA-256:	2F4A3A0730142C5EE4FA2C05D27A5DEFC18886A382D45F5DB254B61B28ED642B
SHA-512:	0B4FF60B5428F81B8B1BCF3328CF80CBD88D8CE5E8BDBC236B06D5A54E7CF26168A3ABB348D87423DA613AB3F0B4D9B37CB5180804839F1CA158EC2B315DD 00
Malicious:	false
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\3628_2036087933_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
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.....$@.....@.....@`...`.....@..... .`.....0...0...2..`4.. 6...7...9...~...~...z...{...{..

C:\Users\user\AppData\Local\Temp\3628_2036087933\manifest.fingerprint

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

C:\Users\user\AppData\Local\Temp\3628_2036087933\manifest.json

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

C:\Users\user\AppData\Local\Temp\3628_2095119410_metadata\verified_contents.json

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

C:\Users\user\AppData\Local\Temp\3628_2095119410\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.947126840193127
Encrypted:	false
SSDEEP:	3:SuOcV6oDkEoVavUd1iSiXn:SBCDk5svU6SiX
MD5:	072D0D7C824A2889BEB0B9CEF0FD2197
SHA1:	985C0EC750CFFBBAE6B2F079E77149E434E9D517
SHA-256:	BF69E3FA772C505E6E75E2A5086FF0396248246F319024745B80FC0FB39D93E7
SHA-512:	A397B48EE93B964A38501846F876ABF2C29AF2150786DCF6E37BAA0EADF48DEE2F8601953F8AB7D4AD76CB5586D669CB1F11FF5A8FDE5B638F0B91413B358C 3
Malicious:	false
Preview:	1.ab8d70a60ce0fba1355fad4edab88fd4d1bccc566b230998180183d1d776992b

C:\Users\user\AppData\Local\Temp\3628_2095119410\manifest.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	300
Entropy (8bit):	4.716626192856269
Encrypted:	false
SSDEEP:	6:zeXC6WQpVyTJCAEIfd26VO9bIA6VDHs/C6wrhKXk7Vm01LwyAGl/zqSkhY:0eTJCAEQLO9hQADgK0711LqGika
MD5:	9569E205D5815A3D9E14DEE93B7717C3
SHA1:	020BD6A07EF64A304B07E3ADFDA4C4D5397534CD
SHA-256:	79B7618620E50A91C4F46F4560AD054823F115A03DA55D5651CECE8843896582
SHA-512:	BE5EB17E769203E6A064326F227D21FFC1E8AA3F2684BD9786FAA4D0EAC944E4343608B1AEA25FDA15FFF88D9C41487907037FEF75DC4D1615A27C7041FC0F9 C
Malicious:	false
Preview:	{. "description" : "Origin Trials public key updates and disabled features list",. "manifest_version" : 2,. "minimum_chrome_version" : "55",. "name" : "Origin Trials Updates",. "origin-trials" : null,. "update_url" : "https://clients2.google.com/service/update2/crx",. "version" : "1.0.0.13".}

C:\Users\user\AppData\Local\Temp\3628_562390067\Filtering Rules	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97968
Entropy (8bit):	5.489893397464442
Encrypted:	false
SSDEEP:	1536:ojHlFMJw9iI9Yh9FHc6cPC3CpBHTrDo630a8Q78xRAQudDv4NZ/p2GuN+BO1:6FMJw9v9efHc6cPCURDR30EYnAQuJANw
MD5:	3846A25BC9191585763E06550798BAB1
SHA1:	F43D903B13AB969E2276E304795CE164F22F893C
SHA-256:	C7D5D133E8F995D3E4D5B68F28BE0D7B1F290DFBD1502E0EC260142325FA8F88
SHA-512:	6B1E1776DE4B4B7D7BD7E6252F555AD84CC689EFE1F3920B3ACFE23DE65212254FC219E0A530037A5EA819894BC2F5B85ECFC0ADDEE9AF3163393AA32F97BA 44
Malicious:	false
Preview:	.....0.8.@.R.-728x90.....0.8.@.R.adtdp.com^.....0.8.@.R.yomeno.xyz^.:.....*...adcore.com.au..*...adcore.ch..0.8.@.R./adcore_.....0.8.@.R.uwoapte e.com^.8.....*...safeway.com0.8.@.R.fwcdn2.com/js/embed-feed.js.....0.8.@.R._468_60..3.....0.8.@.R#/wp-content/plugins/wp-super-popup/.9.....0.8.@.R)bancodevenezuela.com/imagenes/publicidad/.....0.8.@.R..adbutler-.....0.8.@.R.adrecover.com^.....0.8.@.R.hdbcode.com^.?.....*...google.com0.8.@.R!develo pers.google.com/google-ads/.-.....*...konograma.com..0.8.@.R./adserver.....*...vk.com0.8.@.R.vk.me/css/al/ads.css.,.....0.8.@.R.mysmth.net/nForum/*/ADAgent_.. .....0.8.@.R.indoleads.com^.%.....0.8.@.R.discordapp.com/banners/.E.....*...daum.net0.8.@.R)daumcdn.net/adfit/static/ad-native.min.js.(.....0.8.@.R.looker.com/a pi/internal/.#.....0.8.@.R.broadstreetads.com^.....0.8.@.R./banner.cgi?.....*...thefreedictionary.com*...downloads.codefi.re*...windows7themes.net

C:\Users\user\AppData\Local\Temp\3628_562390067\LICENSE.txt	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	24623
Entropy (8bit):	4.588307081140814

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

C:\Users\user\AppData\Local\Temp\3628_562390067_metadata\verified_contents.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1529
Entropy (8bit):	5.993915630498445
Encrypted:	false
SSDEEP:	24:pZRj/flTHYfcl5kYbKqLjeT3azkaoX1pF/kSYYRVHbo0doXxOB6G6QL3foQ3QL5D:p/h4ElBbKdTakak1pFcSfRV7o0dkx8L4
MD5:	6B2EDD2D0C16E5D77BD2C3E4AE88C95F
SHA1:	BC82982FA8A04FA6FD9F17DA03D443A57E0F78D4
SHA-256:	CA0F5F75FC56FBEDA7522B2C83707A451D01760F417C497A37C70554E290B737
SHA-512:	533026A33030795ABF24B6E78D26763734D98CA74BFA4FAC2073EFAD0BB5CA1C38E7036BEAF17E6ABBFE56CF968E80EB3CA3CFD23AEEC10CE1280E8DB1C4078C
Malicious:	false
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJGaWx0ZXJpbmcgUnVsZXMiLCJyb290X2hhc2giOiJMTF90X0NkWWRYUnpMSHJBZ3hmUW5tcENTaXlkWEtzVVlJZnZjLTR0czRBIn0seyJwYXRoIjoiTElDRU5TRS50eHQiLCJyb290X2hhc2giOiIyaWswNmk0TFlCdVNHNWphRGFIS253NE9pdnVSRzZsQ0JKMVk0TGtzRFJJln0seyJwYXRoIjoibWFuaWZlc3QuanNvbiIsInJvb3RfaGFzaCI6Imo4MmhRZGhaa0MwMjFWOEZ1MHUtMExvMnVJdXl5SzdFem5JcHE3WHd2YlkifV0sImZvcm1hdCI6InRyZWVoYXNoIiwiaGFzaF9ibG9ja19zaXplIjo0MDk2fV0sIml0ZW1faWQiOiJnY21qa21nZGxnbmtrY29jbW9laW1pbmFpam1tam5paSIsIml0ZW1fdmVyc2lvbiI6IjkuMCIsInByb3RvY29sX3ZlcnNpb24iOjF9","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"VM_rIA1uXuXjbhz_uZ8uQp9F3FfgEgGTjCXL08Q_jrGXXH-Yty1DqAw4yzWsadeOjVRozUf_7kBrYJ2U8Y8slircdLRbrqJejQeyyrJx4HFT8qgZEb60YHdsOd76C57YzF5dXErpjT7_FkWA41lTxLQvdWbACMO0DE7uOHO9mZx5pM98Ni9GsM_yxJbRSyDZWa8BdPHErfMuO6YE6D8tbnYTr2tXcMV9p2ZEAFMiso2B-6DSr

C:\Users\user\AppData\Local\Temp\3628_562390067\manifest.fingerprint

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

C:\Users\user\AppData\Local\Temp\3628_562390067\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	115
Entropy (8bit):	4.563301657145084
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFHXG7LGMdv5HcDKhtUJKS1Avn:F6VlMZWuMt5SKPS1Avn
MD5:	47B89067C397B3EABBD04E6FC4008B71
SHA1:	7B4E623806D7EA8BFCD2FE6836A21E50C9F9340E

SHA-256:	8FCDA141D859902D36D55F05BB4BBED0BA36B88BABF4AEC4CE7229ABB5F0BDB6
SHA-512:	FDA1CE8EB24A05F65E8132248EEF96C422E5AA2D3254B590FBFD3FCB2016E3B7F6E4B53702D88E1695D4BEC0175F72EB4256CDAA2FF72DDF4390D480D04BA373
Malicious:	false
Preview:	{. "manifest_version": 2,. "name": "Subresource Filtering Rules",. "ruleset_format": 1,. "version": "9.36.0".}.

C:\Users\user\AppData\Local\Temp\73a88e6c-8bc8-4e75-af96-e80b0ef97d01.tmp

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

C:\Users\user\AppData\Local\Temp\83e2d3a3-c39c-4d02-ac9e-2cb5ac7dc711.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F332688
Malicious:	false
Preview:	Cr24.....0.."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.| 1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u.. ..k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2.. ;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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_dir3628_1255938956\83e2d3a3-c39c-4d02-ac9e-2cb5ac7dc711.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F332688
Malicious:	false
Preview:	Cr24.....0.."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.| 1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u.. ..k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2.. ;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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_dir3628_1255938956\CRX_INSTALL_locales\bg\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F770C
Malicious:	false
Preview:	{.. "app_description": {.. "message": "..... . ... Chrome".. },.. "app_name": {.. "message": "..... . ... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "...., ...".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "...., ... Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\ca\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CB4
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "Connecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\cs\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D8488SCB
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\da\messages.json

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

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

C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\de\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\el\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\en\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC

SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\en_GB\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\es\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	661
Entropy (8bit):	4.450938335136508
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyZnLAOfTY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OGAOffD
MD5:	82719BD3999AD66193A9B0BB525F97CD
SHA1:	41194D511F1ACC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE0128
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "Los pagos en la aplicaci.n no est.n disponibles en este momento.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\es_419\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	637
Entropy (8bit):	4.47253983486615
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34GLO03OyZnLAOfTYiJD:1HEvaC6WYpcDeEFxq8Zp4LlOGAOfvD
MD5:	6B2583D8D1C147E36A69A88009CBEBC7
SHA1:	4D4DEEB4BE6AA0181825F3371A761ABC5B4D5937
SHA-256:	6659BC3705311D7641A73995DCFEA80C7734F2F4EBBC3787B3892A240348324F
SHA-512:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA53
Malicious:	false

Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "En este momento, Pagos En-Apps no est. disponible.".. },.. "jwt_retrieve_failed": {.. "message": "The tr ansaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\et\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\fi\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\fil\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	658
Entropy (8bit):	4.5231229502550745
Encrypted:	false
SSDEEP:	12:1HEJADlbGGADlb+WYpU34hTUT+dgHfZAFFZO8ZpU34hTjzeT03OyZnLAOfTYHfvF:1HEYah6WYp7TUSoxOS8Zp7TOsOGAOfqV
MD5:	57AF5B654270A945BDA8053A83353A06
SHA1:	EEEF7A4F869F97CF471A05D345E74F982D15E167
SHA-256:	EC002ED92359F67818B49455DFC579E140368E6A004080AF022FD4F57F6B03F2
SHA-512:	5F0AE839FCF3F4EA48FF41A76655AE0F3821564AFD5D42FBB9FBB9A38E8D8F7BB5E9B6F71064588CD441261F644095A44A755C134CE546D506D9A21E488BAF5 2
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "app_name": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Kasalukuyang hindi available ang app.".. },.. "craw_connect_to_network": {.. "message": "Mangyaring kumonekta sa isang network.".. },.. "iap_unavailable": {.. "message": "Kasalukuyang hindi available ang Mga Pagbabayad na In-App.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Mangyaring mag-sign in sa Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3628_1255938956\CRX_INSTALL_locales\fr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	677
Entropy (8bit):	4.552569602149629
Encrypted:	false
SSDEEP:	12:1HEJALf/nbGGALf/nb+WYpU34Owdgbyb+dgdQjO8ZpU34ITQpGnbyb03OyZnLAO8:1HE4Hna1Hn6WYpNdgpY8ZpSTQwnBOGAh
MD5:	8D11C90F44A6585B57B933AB38D1FFF8
SHA1:	3F9D44EA8807069A32AACA2AAAD02FD892E6CC90
SHA-256:	599491F8C52B945C16C441ADF45BFD45AFAE046DA07757D97C56AF4DE75ED3B5
SHA-512:	D7EF7F5AD7EF1A1595825D79B69E2B1E988AD3CF1F3881496FCCD30F241E4E9C6E457F9F5D0F855DE3536DB7A40C3E1C55946B50D3F556F4A35285066A0CD6F7
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "app_name": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "craw_app_unavailable": {.. "message": "Application indisponible pour le moment.".. },.. "craw_connect_to_network": {.. "message": "Veuillez vous connecter . unr.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_dir3628_1255938956\CRX_INSTALL_locales\hi\messages.json

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

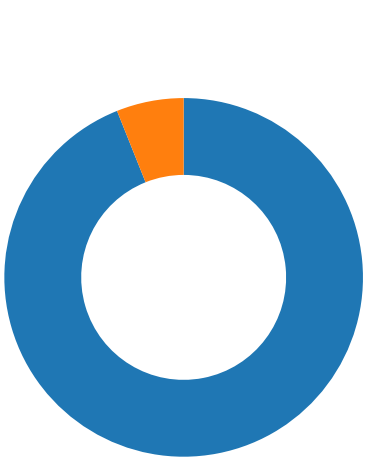
Static File Info

General

File type:	HTML document, ISO-8859 text, with very long lines, with CRLF line terminators
Entropy (8bit):	3.5802684601635977
TrID:	• HyperText Markup Language (6006/1) 100.00%
File name:	Hacxx MSDT 0-Day CVE-2022-30190 Exploit Generator.htm
File size:	10690
MD5:	944593b21badb2add4c954e7ea09bc53
SHA1:	737ec2a8778af5404d5c57824f705a5fb1897b10
SHA256:	b2743f7047a7119794a28840403def40e27ff7f9575ef060c458ab4fe3e9aeb9
SHA512:	814fdd37b9f6dfbdc444a9a555ce5fe528f620f82a67d67a125f5e7b41441b791918a325f75fb2764745a1860b492c87d0d191b905ceb79066313c2672cd6989
SSDEEP:	96:/lW7qbTQGwXZkYjxac0O44oObbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb/:/lWOnaNv0O44opUP6PNQYNWOOh
TLSH:	CA220975E6A5248E09AA7AF290177DC7CD6612CF030B45B0FC05D6A36A8FE4441BFB9C
File Content Preview:	<html>..<title>Hacxx MSDT 0-Day CVE-2022-30190 Exploit Generator</title>..<body bgColor=#5e717f> ..<table style="background: #bed5e2;" cellspacing=0 cellpadding=0 align=center>.. <tr>.. <td style="border-right: #d8d8d8 0.75pt solid; padding-right:

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 18, 2022 18:35:59.302963018 CEST	49731	443	192.168.2.4	142.250.180.141
Jul 18, 2022 18:35:59.303004026 CEST	443	49731	142.250.180.141	192.168.2.4
Jul 18, 2022 18:35:59.303070068 CEST	49731	443	192.168.2.4	142.250.180.141
Jul 18, 2022 18:35:59.305084944 CEST	49732	443	192.168.2.4	216.58.209.46
Jul 18, 2022 18:35:59.305133104 CEST	443	49732	216.58.209.46	192.168.2.4
Jul 18, 2022 18:35:59.305218935 CEST	49732	443	192.168.2.4	216.58.209.46
Jul 18, 2022 18:35:59.305763960 CEST	49731	443	192.168.2.4	142.250.180.141
Jul 18, 2022 18:35:59.305784941 CEST	443	49731	142.250.180.141	192.168.2.4
Jul 18, 2022 18:35:59.306067944 CEST	49732	443	192.168.2.4	216.58.209.46
Jul 18, 2022 18:35:59.306094885 CEST	443	49732	216.58.209.46	192.168.2.4
Jul 18, 2022 18:35:59.377578974 CEST	443	49731	142.250.180.141	192.168.2.4
Jul 18, 2022 18:35:59.378220081 CEST	49731	443	192.168.2.4	142.250.180.141
Jul 18, 2022 18:35:59.378247023 CEST	443	49731	142.250.180.141	192.168.2.4
Jul 18, 2022 18:35:59.379836082 CEST	443	49731	142.250.180.141	192.168.2.4
Jul 18, 2022 18:35:59.379970074 CEST	49731	443	192.168.2.4	142.250.180.141
Jul 18, 2022 18:35:59.381275892 CEST	443	49732	216.58.209.46	192.168.2.4
Jul 18, 2022 18:35:59.384994984 CEST	49732	443	192.168.2.4	216.58.209.46
Jul 18, 2022 18:35:59.385083914 CEST	443	49732	216.58.209.46	192.168.2.4
Jul 18, 2022 18:35:59.385464907 CEST	443	49732	216.58.209.46	192.168.2.4
Jul 18, 2022 18:35:59.385617018 CEST	49732	443	192.168.2.4	216.58.209.46
Jul 18, 2022 18:35:59.386256933 CEST	443	49732	216.58.209.46	192.168.2.4
Jul 18, 2022 18:35:59.386354923 CEST	49732	443	192.168.2.4	216.58.209.46
Jul 18, 2022 18:36:00.792655945 CEST	49732	443	192.168.2.4	216.58.209.46
Jul 18, 2022 18:36:00.792900085 CEST	443	49732	216.58.209.46	192.168.2.4
Jul 18, 2022 18:36:00.795753956 CEST	49731	443	192.168.2.4	142.250.180.141
Jul 18, 2022 18:36:00.795999050 CEST	443	49731	142.250.180.141	192.168.2.4
Jul 18, 2022 18:36:00.797179937 CEST	49732	443	192.168.2.4	216.58.209.46
Jul 18, 2022 18:36:00.797228098 CEST	443	49732	216.58.209.46	192.168.2.4
Jul 18, 2022 18:36:00.797348022 CEST	49731	443	192.168.2.4	142.250.180.141
Jul 18, 2022 18:36:00.797383070 CEST	443	49731	142.250.180.141	192.168.2.4
Jul 18, 2022 18:36:00.841388941 CEST	443	49732	216.58.209.46	192.168.2.4
Jul 18, 2022 18:36:00.841495037 CEST	443	49732	216.58.209.46	192.168.2.4
Jul 18, 2022 18:36:00.841497898 CEST	49732	443	192.168.2.4	216.58.209.46
Jul 18, 2022 18:36:00.841551065 CEST	49732	443	192.168.2.4	216.58.209.46
Jul 18, 2022 18:36:00.842266083 CEST	49731	443	192.168.2.4	142.250.180.141
Jul 18, 2022 18:36:00.847155094 CEST	49732	443	192.168.2.4	216.58.209.46
Jul 18, 2022 18:36:00.847196102 CEST	443	49732	216.58.209.46	192.168.2.4
Jul 18, 2022 18:36:00.870641947 CEST	443	49731	142.250.180.141	192.168.2.4
Jul 18, 2022 18:36:00.870745897 CEST	49731	443	192.168.2.4	142.250.180.141
Jul 18, 2022 18:36:00.870769978 CEST	443	49731	142.250.180.141	192.168.2.4
Jul 18, 2022 18:36:00.870795012 CEST	443	49731	142.250.180.141	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 18, 2022 18:36:00.870842934 CEST	49731	443	192.168.2.4	142.250.180.141
Jul 18, 2022 18:36:00.925939083 CEST	49731	443	192.168.2.4	142.250.180.141
Jul 18, 2022 18:36:00.925992012 CEST	443	49731	142.250.180.141	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 18, 2022 18:35:59.247416019 CEST	64454	53	192.168.2.4	8.8.8.8
Jul 18, 2022 18:35:59.249737978 CEST	60506	53	192.168.2.4	8.8.8.8
Jul 18, 2022 18:35:59.275964975 CEST	53	64454	8.8.8.8	192.168.2.4
Jul 18, 2022 18:35:59.277240992 CEST	53	60506	8.8.8.8	192.168.2.4
Jul 18, 2022 18:36:06.177706957 CEST	58172	443	192.168.2.4	216.58.209.46
Jul 18, 2022 18:36:06.213860989 CEST	443	58172	216.58.209.46	192.168.2.4
Jul 18, 2022 18:36:06.214525938 CEST	58172	443	192.168.2.4	216.58.209.46
Jul 18, 2022 18:36:06.250947952 CEST	443	58172	216.58.209.46	192.168.2.4
Jul 18, 2022 18:36:06.250984907 CEST	443	58172	216.58.209.46	192.168.2.4
Jul 18, 2022 18:36:06.251008034 CEST	443	58172	216.58.209.46	192.168.2.4
Jul 18, 2022 18:36:06.251029968 CEST	443	58172	216.58.209.46	192.168.2.4
Jul 18, 2022 18:36:06.252291918 CEST	58172	443	192.168.2.4	216.58.209.46
Jul 18, 2022 18:36:06.253855944 CEST	58172	443	192.168.2.4	216.58.209.46
Jul 18, 2022 18:36:06.325710058 CEST	58172	443	192.168.2.4	216.58.209.46
Jul 18, 2022 18:36:06.326303005 CEST	58172	443	192.168.2.4	216.58.209.46
Jul 18, 2022 18:36:06.371828079 CEST	443	58172	216.58.209.46	192.168.2.4
Jul 18, 2022 18:36:06.377638102 CEST	443	58172	216.58.209.46	192.168.2.4
Jul 18, 2022 18:36:06.377965927 CEST	443	58172	216.58.209.46	192.168.2.4
Jul 18, 2022 18:36:06.392889023 CEST	58172	443	192.168.2.4	216.58.209.46
Jul 18, 2022 18:36:06.398607969 CEST	443	58172	216.58.209.46	192.168.2.4
Jul 18, 2022 18:36:06.398663998 CEST	443	58172	216.58.209.46	192.168.2.4
Jul 18, 2022 18:36:06.403971910 CEST	58172	443	192.168.2.4	216.58.209.46
Jul 18, 2022 18:36:06.408965111 CEST	443	58172	216.58.209.46	192.168.2.4
Jul 18, 2022 18:36:06.439575911 CEST	58172	443	192.168.2.4	216.58.209.46

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 18, 2022 18:35:59.247416019 CEST	192.168.2.4	8.8.8.8	0x16d5	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jul 18, 2022 18:35:59.249737978 CEST	192.168.2.4	8.8.8.8	0x470d	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 18, 2022 18:35:59.275964975 CEST	8.8.8.8	192.168.2.4	0x16d5	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 18, 2022 18:35:59.275964975 CEST	8.8.8.8	192.168.2.4	0x16d5	No error (0)	clients.l.google.com		216.58.209.46	A (IP address)	IN (0x0001)
Jul 18, 2022 18:35:59.277240992 CEST	8.8.8.8	192.168.2.4	0x470d	No error (0)	accounts.google.com		142.250.180.141	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49732	216.58.209.46	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-18 16:36:00 UTC	0	OUT	GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel= &prodversion=85.0.4183.121&lang=en-GB&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v% 3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelp bcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1 HTTP/1.1 Host: clients2.google.com Connection: keep-alive X-Goog-Update-Interactivity: fg X-Goog-Update-AppId: nmmhkkegccagdldgiimedpiccmgmieda,pkedcjkdefgpdelpbcmbmeomcjbeemfm X-Goog-Update-Updater: chromecrx-85.0.4183.121 Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183. 121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-07-18 16:36:00 UTC	1	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-lCO18ugU3sEMn3ynzbdDBQ' 'unsafe-inline' 'strict-dynamic' http s: http:;object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/clientupdate-aus/1 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Mon, 18 Jul 2022 16:36:00 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5677 X-Daystart: 34560 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; m a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-07-18 16:36:00 UTC	2	IN	Data Raw: 33 31 62 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 67 75 70 64 61 74 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 75 70 64 61 74 65 32 2f 72 65 73 70 6f 6e 73 65 22 20 70 72 6f 74 6f 63 6f 6c 3d 22 32 2e 30 22 20 73 65 72 76 65 72 3d 22 70 72 6f 64 22 3e 3c 64 61 79 73 74 61 72 74 20 65 6c 61 70 73 65 64 5f 64 61 79 73 3d 22 35 36 37 37 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 33 34 35 36 30 22 2f 3e 3c 61 70 70 20 61 70 70 69 64 3d 22 6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 22 20 63 6f 68 6f 72 74 3d 22 31 3a 3a 22 20 63 6f 68 6f 72 74 6e 61 6d 65 3d 22 22 Data Ascii: 31b<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" p rotocol="2.0" server="prod"><daystart elapsed_days="5677" elapsed_seconds="34560"/><app appid="nmmhkkegccagdld giimedpiccmgmieda" cohort="1::" cohortname=""
2022-07-18 16:36:00 UTC	2	IN	Data Raw: 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 7a 65 3d 22 32 34 38 35 33 31 22 20 73 74 61 74 75 73 3d 22 6f 6b 22 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 2e 30 2e 36 22 2f 3e 3c 2f 61 70 70 3e 3c 61 Data Ascii: mmhkkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5 450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" size="248531" status="ok" version="1.0.0.6"/></app><a
2022-07-18 16:36:00 UTC	2	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

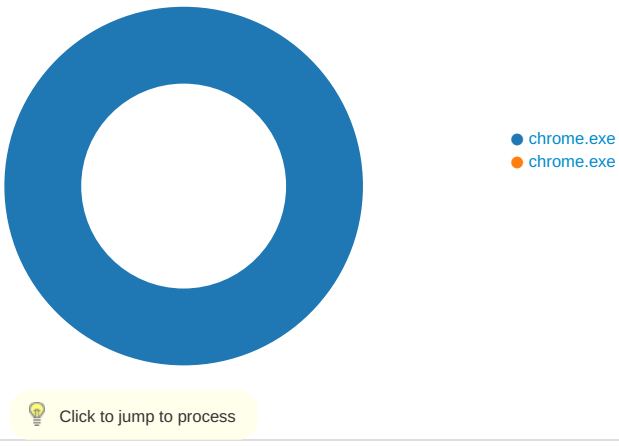
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49731	142.250.180.141	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-07-18 16:36:00 UTC	0	OUT	POST /ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard HTTP/1.1 Host: accounts.google.com Connection: keep-alive Content-Length: 1 Origin: https://www.google.com Content-Type: application/x-www-form-urlencoded Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-07-18 16:36:00 UTC	1	OUT	Data Raw: 20 Data Ascii:
2022-07-18 16:36:00 UTC	2	IN	HTTP/1.1 200 OK Content-Type: application/json; charset=utf-8 Access-Control-Allow-Origin: https://www.google.com Access-Control-Allow-Credentials: true X-Content-Type-Options: nosniff Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Mon, 18 Jul 2022 16:36:00 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Cross-Origin-Opener-Policy: same-origin; report-to="IdentityListAccountsHttp" Content-Security-Policy: script-src 'report-sample' 'nonce--fIK6Zya6HIj9lwiTsA7YA' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'nonce--fIK6Zya6HIj9lwiTsA7YA' 'self' https://apis.google.com https://ssl.gstatic.com https://www.google.com https://www.gstatic.com https://www.google-analytics.com;report-uri /_/IdentityListAccountsHttp/cspreport Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport Report-To: {"group":"IdentityListAccountsHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external"}]} Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Server: ESF X-XSS-Protection: 0 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-07-18 16:36:00 UTC	4	IN	Data Raw: 31 31 0d 0a 5b 22 67 61 69 61 2e 6c 2e 61 2e 72 22 2c 5b 5d 5d 0d 0a Data Ascii: 11["gaia.l.a.r",[]]
2022-07-18 16:36:00 UTC	4	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **3628**, Parent PID: **1636**

General

Target ID:	0
Start time:	18:35:52
Start date:	18/07/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "C:\Users\user\Desktop\Hacxx MSDT 0-Day CVE-2022-30190 Exploit Generator.htm
Imagebase:	0x7ff7964c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}	dr	unicode	0	1	success or wait	1	7FF7964FFC4B	RegSetValueExW

Analysis Process: chrome.exe PID: **3372**, Parent PID: **3628**

General

Target ID:	1
Start time:	18:35:54
Start date:	18/07/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1592,17218383300859783571,9943285069256131307,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1928 /prefetch:8
Imagebase:	0x7ff7964c0000

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

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Disassembly

No disassembly