ID: 324354
Cookbook: browseurl.jbs
Time: 14:21:07
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Analysis Report http://Testgvbgjbhjb.com

Overview

General Information

Sample URL:	http://Testgvbgjbhjb.com
Analysis ID:	324354

Most interesting Screenshot:

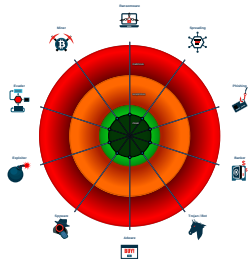
Detection

Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

No high impact signatures.

Classification



Analysis Advice

Some HTTP requests failed (404). It is likely the sample will exhibit less behavior

Uses HTTPS for network communication, use the 'Proxy HTTPS (port 443) to read its encrypted data' cookbook for further analysis

Startup

- **System is w10x64**
- chrome.exe (PID: 1304 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'http://Testgvbgjbhjb.com' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 1564 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1572,738224861734345709 0,8884663749363792362,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1708 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

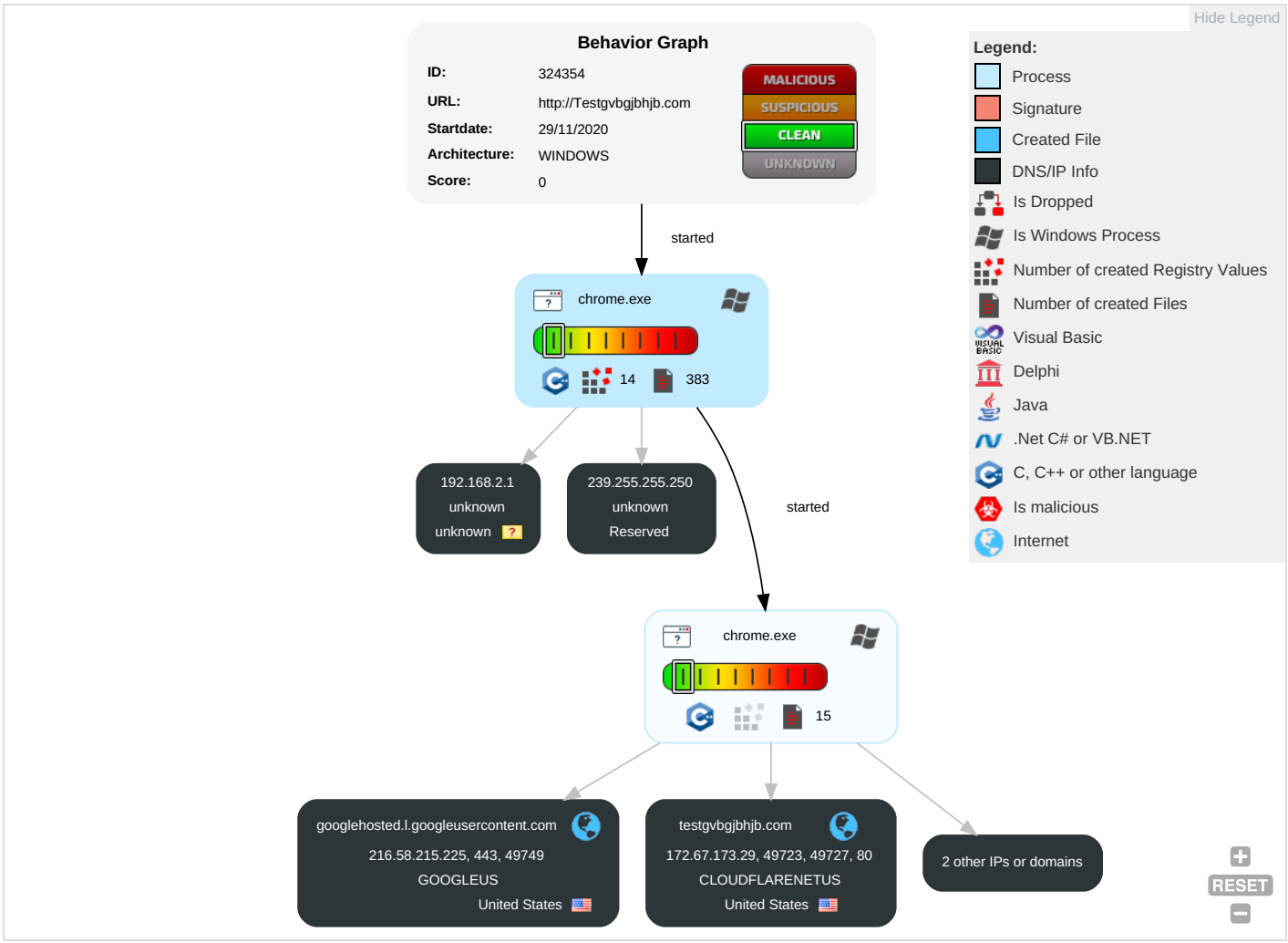
Click to jump to signature section

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 3	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
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	Application Layer Protocol 4	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic 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	Ingress Tool Transfer 3	SIM Card Swap		Carri Billing Fraud

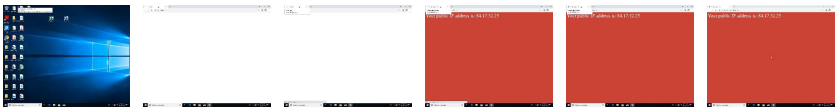
Behavior Graph

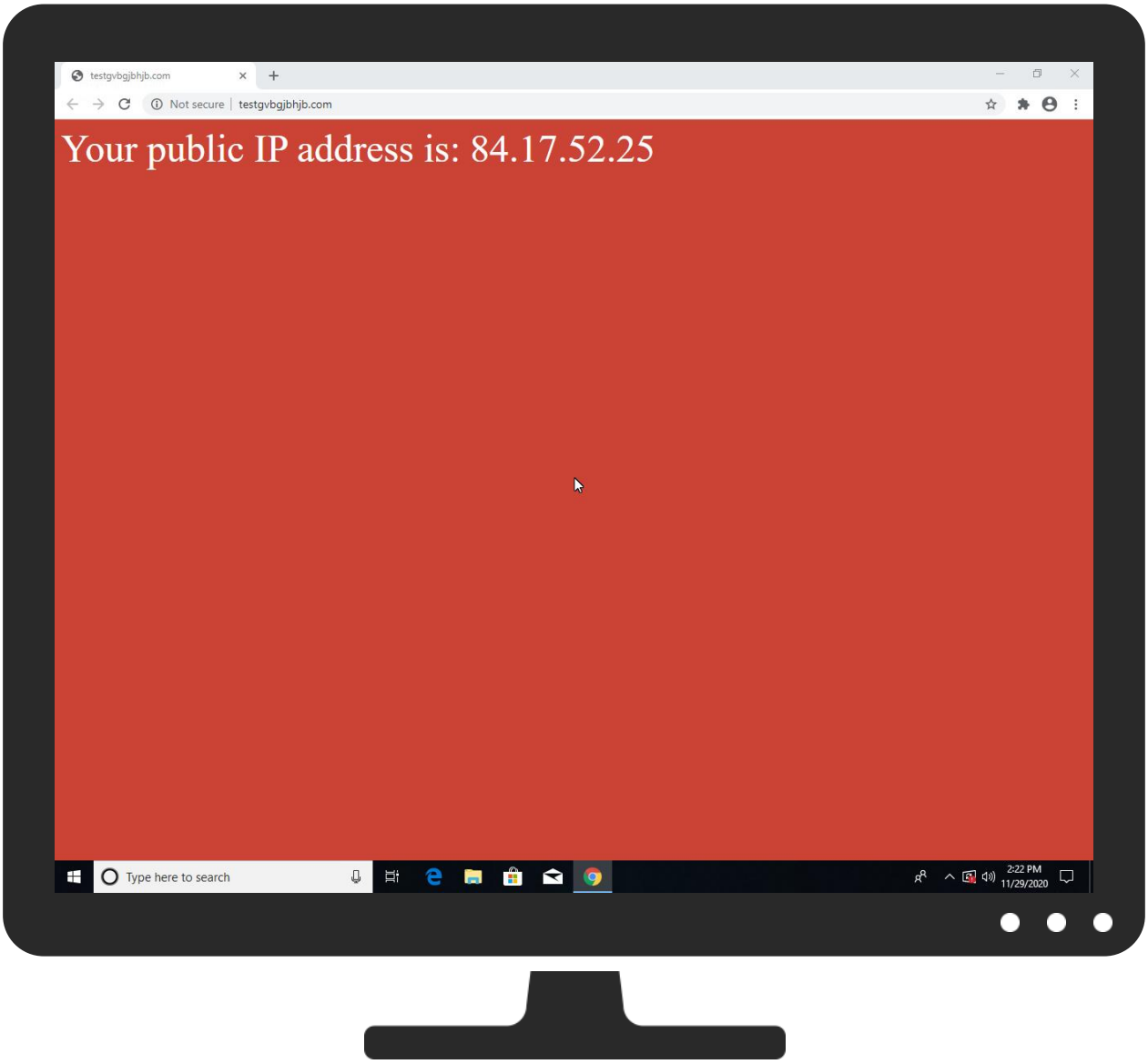


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

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

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
testgvbgjbhjb.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://testgvbgjbhjb.com/favicon.ico	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://testgvbgjbhjb.com/2:	0%	Avira URL Cloud	safe	
http://testgvbgjbhjb.com/	0%	Virustotal		Browse
http://testgvbgjbhjb.com/	0%	Avira URL Cloud	safe	
http://testgvbgjbhjb.com/PY	0%	Avira URL Cloud	safe	
http://testgvbgjbhjb.com/2	0%	Avira URL Cloud	safe	
http://testgvbgjbhjb.com//	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
testgvbgjbhjb.com	172.67.173.29	true	false	• 0%, Virustotal, Browse	unknown
googlehosted.l.googleusercontent.com	216.58.215.225	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high

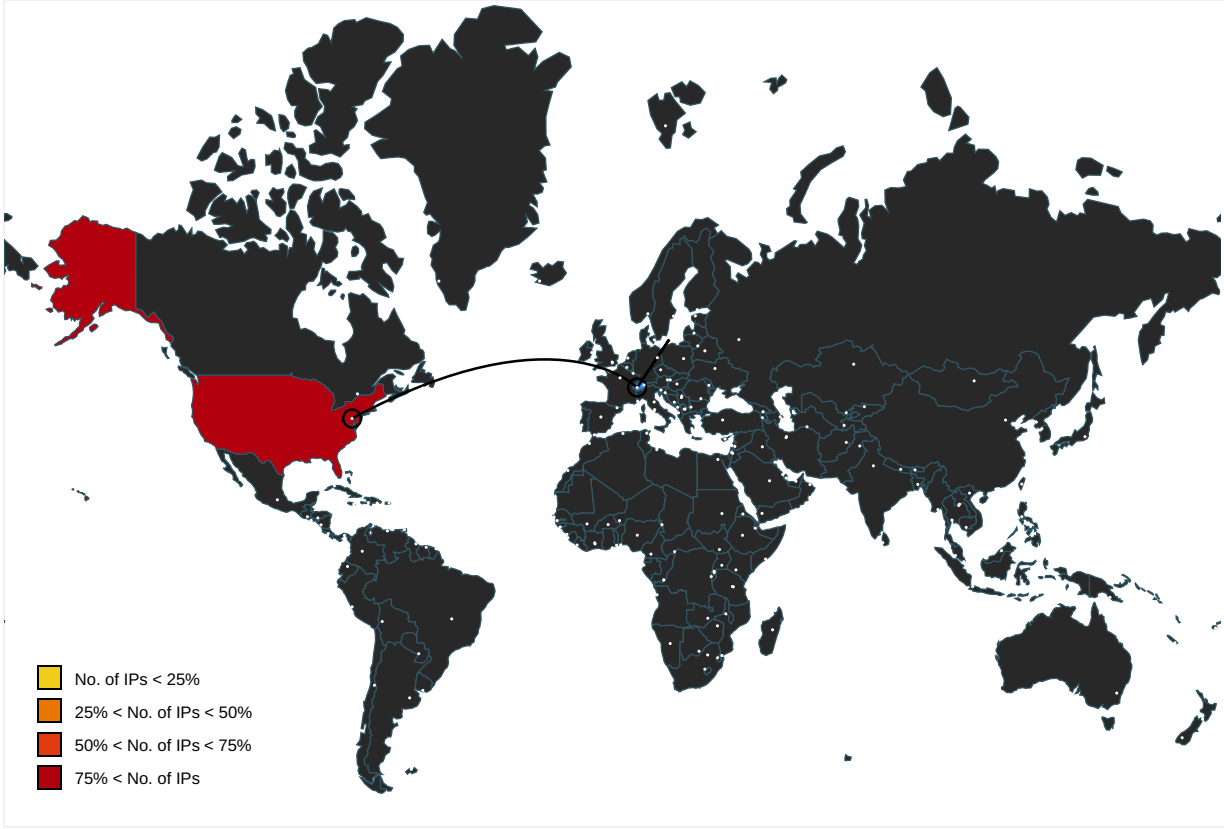
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://testgvbgjbhjb.com/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://testgvbgjbhjb.com/	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	b8d229a8-52f8-4859-a422-641633 47a644.tmp.1.dr, 71335062-4421-479c-8abe-dc7d7f44a2af.tmp.1.dr, 5ffb6394-d0e3-4d94-adc1-fdf7fcba924a.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://testgvbgjbhjb.com/2:	History Provider Cache.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients2.googleusercontent.com	71335062-4421-479c-8abe-dc7d7f 44a2af.tmp.1.dr	false		high
http://testgvbgjbhjb.com/PY	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://testgvbgjbhjb.com/2	History Provider Cache.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://testgvbgjbhjb.com//	History.0.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.215.225	unknown	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.67.173.29	unknown	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324354
Start date:	29.11.2020
Start time:	14:21:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://Testgvbgjbhjb.com
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	13
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@27/160@2/5
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 52.147.198.201, 172.217.168.14, 172.217.168.45, 172.217.168.67, 172.217.168.78, 173.194.187.8, 173.194.182.74, 204.79.197.200, 13.107.21.200, 172.217.168.42, 172.217.168.74, 216.58.215.234, 172.217.168.10, 93.184.220.29, 51.11.168.160, 92.122.144.200, 20.54.26.129, 205.185.216.10, 205.185.216.42 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, arc.msn.com.nsatc.net, r3---sn-4g5e6ns6.gvt1.com, clientservices.googleapis.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, clients2.google.com, redirector.gvt1.com, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, accounts.google.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, www.googleapis.com, r5.sn-4g5e6ns7.gvt1.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, blobcollector.events.data.trafficmanager.net, clients.l.google.com, r5---sn-4g5e6ns7.gvt1.com, r3.sn-4g5e6ns6.gvt1.com • 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 NtQueryVolumeInformationFile 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

ASN

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:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\0760addf-7ba5-4eaf-8871-0614a402d9a5.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):	162521
Entropy (8bit):	6.082393509096706
Encrypted:	false
SSDEEP:	3072:ciGCAPHKb1o/hF5RzweKvf14PnpqISFcbXafIB0u1GOJmA3iuRG:Df4HW1oZF5BtK1engzaqfIlUOoSiuRG
MD5:	5B874D668E6A0B744C306DB50B8959A8
SHA1:	7E807B7D9BDB1FD3C40E34DEFDF8188DA64013BE
SHA-256:	D3558C22C4C15948352BDCCAEA09366D8CA4602FB00D8A3694483ABA3A17290D
SHA-512:	00000B0DBCBB228429382AAC250D0D26E86FEC9E86C9C377BC6FFBD1337285EFA1A890A76D09C41DE9A435FB5CF0FA53CEB57C7A43FFD5664C6E50A44F9B9162
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":1.606688516213298e+12,"network":1.606656118e+12,"ticks":96199933.0,"uncertainty":4543822.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016400774"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\5d074ac6-a505-4333-bdbf-7d73836d43dd.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Google\Chrome\User Data\5d074ac6-a505-4333-bdbf-7d73836d43dd.tmp	
Category:	dropped
Size (bytes):	162521
Entropy (8bit):	6.082392809137779
Encrypted:	false
SSDEEP:	3072:/z7CAPHKb1o/hF5RzweKvf14PnpqISFcbXafIB0u1GOJmA3iuRG:bW4HW1oZF5BtK1engzaqfllUOoSiuRG
MD5:	FB5F6AAC5F2055516FE7E99FF55721BC
SHA1:	E12CFB403B4154810FD56C8D7DBA4D1258EE0345
SHA-256:	4B7092E11459DF9138B7C3ABFA3077E10067F118164564B309D9575A2AC9A0C3
SHA-512:	FA023424B31C7DC375486DA0526BA01D7B5DF3A82FF24CECCEB9F01FEC788CD32B60E5E3A1DCE5A706964638D5FA1769241D0AE0E0F978D6DFE8C69D741F8E9
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":1.606688516213298e+12,"network":1.606656118e+12,"ticks":96199933.0,"uncertainty":4543822.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftlE1G1mkftlE1G1mkftlE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D021294256372C916B8155AC
Malicious:	false
Reputation:	low
Preview:	sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4043373b-6e91-4b2d-b046-6879991ef053.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):	22613
Entropy (8bit):	5.534783113008988
Encrypted:	false
SSDEEP:	384:+n6t4LlgtBX+1kXqKf/pUZNCgVLH2HfD8rULHGVnTorT47:0LlSF+1kXqKf/pUZNCgVLH2HforUbGVV
MD5:	5A600CE752C477C749776293CE7A7231
SHA1:	3FC8EA1AD556540FFC010C37B0AFA902629690AA
SHA-256:	3CE4A07B701DA5CACA5872B4D2DCA5E44225147603B623D7EDB4B8556E9A1137
SHA-512:	0D94100ADB879C39F4626D731A39815E6F36E258A31E4009A34ED6E53FB1B47E7C5374BF3DBA8253E039C2A24B105A7B470C487B3D90135806A499E0BF3F9199
Malicious:	false
Reputation:	low
Preview:	{"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":"13251162113371682","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_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\41455c34-56b7-41c9-ae59-1e63522d49d4.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):	16763
Entropy (8bit):	5.576990950642255
Encrypted:	false
SSDEEP:	384:+n6thLlgtBX+1kXqKf/pUZNCgVLH2HfD8rUgaT4g:FLlSF+1kXqKf/pUZNCgVLH2HforUlTH

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\41455c34-56b7-41c9-ae59-1e63522d49d4.tmp	
MD5:	6BE3CBF1E07561B332034D6B3ECD061B
SHA1:	6F34E5E0E8F1BB9E2845B2796FB5230FD122B734
SHA-256:	A9613C4D7C5139D491E727B5F8B20B9E43BFFE6F7D73FEC689817C541B8DCACA
SHA-512:	40A3B2E2437BA035AA84C2E344210264647D532BE38F3B54898306930EB8A75DCE90A051505CD58AC50AB8710AE6B9669840C4D6D225C0BF74F4B386F7F5A012
Malicious:	false
Reputation:	low
Preview:	{"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":"13251162113371682","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_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\532d36d3-28db-465f-b20c-795c26359b40.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:	modified
Size (bytes):	22614
Entropy (8bit):	5.53475927590787
Encrypted:	false
SSDEEP:	384:+n6t4LlgtBX+1kXqKf/pUZNCgVLH2HfD8rULHGMnTobT4v:0LlSF+1kXqKf/pUZNCgVLH2HforUbGM9
MD5:	F2AB48FBB1E24CE8947D8C3D0F4A485F
SHA1:	1F9E3EAED2CD98F2BC945465BB8402A7DF3FDE0B
SHA-256:	77B09E32E1942EC52498C8098B612E029329F38D23255B532A6E4EED1075CBF5
SHA-512:	18FED51682DC0BF7CCC4EBA0FDD5362A41BD3A167DE4C465F2C11E66255075DC7AA892BB520D568B5B0ACB8CAE647BAFDA5739B4B8DB87B9DEBD3EC2462D 5412
Malicious:	false
Reputation:	low
Preview:	{"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":"13251162113371682","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_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\54097b86-df99-4f49-9b75-2516ee5e2fd5.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):	5031
Entropy (8bit):	4.9763775740426475
Encrypted:	false
SSDEEP:	48:YcNqUkPklwHjQcNqA8RqTlYqlQuoTw0XxqbH3CH3G/s8C1Nfct/9BhUJo3KhmeSI:n8b8X4pcV6Bok0JCKL8Vk91NbOTQVuwn
MD5:	5AFC254DB3485D7963990F3EA2155920
SHA1:	65DE02C6EAE2675038A4B81AAA126F532FDDC5E5
SHA-256:	0D65590D765AF6FCC80D8605895D3D47123DF3D4863CB2D09108D3381147DDE5
SHA-512:	88DF3F8F2FADB424901A6DB8698FB7111D85EDA33250298DB459734051E55C45A2418DA6F718B939698C330FCAFAD59CA9CE6C68808A008C0CA37A063547EDE
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13251162113608288","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\71335062-4421-479c-8abe-dc7d7f44a2af.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\71335062-4421-479c-8abe-dc7d7f44a2af.tmp	
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.19843786690121
Encrypted:	false
SSDEEP:	6:o/hnFlL+q2PWXp+N23iKKdK9RXXTZIFUtwH/hG1ZmwyH/ht9LVkwOWXp+N23iKKU:eVjyva5Kk7XT2FUtwfa/yf5R5f5Kk7XH
MD5:	238F59119F5A1A1ACAF914B67542E048
SHA1:	61F2F62E92A901D01CCC2BBFCB11E56EA1117505
SHA-256:	99B52E4F19ECBDCF2468898E39D271CEBECB9B342E5A14DAE061000CC1777444
SHA-512:	AECA40F58546167CCED3CF10B3E518A1C2C8E5D0D9EBF6FDC8276338D401D9216F99052B690CA9624BE9327EA6439E4B80D41BFE80AECFCB7D62B2DF9A2663C8
Malicious:	false
Reputation:	low
Preview:	2020/11/29-14:22:10.505 1a38 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2020/11/29-14:22:10.508 1a38 Recovering log #3.2020/11/29-14:22:10.509 1a38 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.17079271770699
Encrypted:	false
SSDEEP:	6:o/RFL+q2PWXp+N23iKKdKyDZIFUtwH/hFOz1ZmwyH/hFOlLVkwOWXp+N23iKKdKy:eRFyva5Kk02FUtwf/OZ/yf/OlR5f5Kky
MD5:	9CEEE31A6CFBA594BED0BD4A1ADA899D
SHA1:	1609E589C65249B37B85B7FB3DCDF16802E5CDEC
SHA-256:	8075124F72F1DC1C8D4C257D9880BC8E818DDDB43B016457F8827291D24E1C12
SHA-512:	B547A840DBF3B79462DFF5407379E68C59CA82EB0EB4A81A6C908B3CF5922B2BFF7260FA4D1D360BED0DA5D01DBA867AEBD4F37230CF7DC174BC36073C6FE5C
Malicious:	false
Reputation:	low
Preview:	2020/11/29-14:22:10.499 1a38 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2020/11/29-14:22:10.500 1a38 Recovering log #3.2020/11/29-14:22:10.500 1a38 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	12288
Entropy (8bit):	1.1423783327518777
Encrypted:	false
SSDEEP:	24:TLyqJLbXaFpEO5bNmISHn06UwQwuU9seCrcsgAZOZD/Fy7Dwm:TekLLOpEO5J/Kn7U8ums1IsNOZRm
MD5:	C3F90145150AD0DD68DFC41165E2D1C7
SHA1:	A455ED5CBCE039B62598AAE5945BF6DD8CBC7EF0
SHA-256:	725A01325BB4268ED9F5570C0612B622537F199065C0025FB0D195D5B30C9595
SHA-512:	FC5EE3AD5D345F475BF29C4845356F607D93481CBA350CB42DFA6A4D85254F5021A27BAA2DC1EBE8093F2E3A9A859CF8DE99C5350DC2EF0D1B9E82270DCA1602
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Preview:	SQLite format 3.....@ .....C..... ..g... .8.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.968134091634045
Encrypted:	false
SSDEEP:	24:icLgAZOZD/JHqLbJLbXaFpEO5bNmISHn06Uwr8:i8NOZJHq5LLOpEO5J/Kn7UM8
MD5:	5EDCA7FA3107997BFCDFB57BD10E0BEA
SHA1:	4A9EBFF17C12B7E8020703B26438F7760CE5E6F6
SHA-256:	C18384F847D812DDE8ECE0E15167E3392E591FBDA033AF139F5DE094F6394164
SHA-512:	2C7F7F64165426B4A56BABABB4CF2B14DDA435F19C95A6FA5D88AFF105EBA3687A02E82C1513A505C2DDAD92FD2C996396741B5F7352AE36A2C2EBACC873C1 0B
Malicious:	false
Reputation:	low
Preview:	.....%.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	899
Entropy (8bit):	3.088606747783559
Encrypted:	false
SSDEEP:	12:3olydJhcr407W6PlpxlpN8kIyTrlwzPlHi/Yn7lc9iczPlH+Plpl:34SSrAQlrlAElwzFich6NzF+PlL
MD5:	E3144F90A287B14A22204A2727C364F1
SHA1:	C300FF646CC326FBFD00E7ED81746CE926CE74BC
SHA-256:	FC3B113F2C6F264FEB4843BBA43B931FDA9EDAD2BF12FB4667C2A1DC5589771B
SHA-512:	7AAAC2AC45DF036B7A54A56A4B5EBC98D0DF9EA80A29F1D7EB0069544CB956028852EF41E89A5712F266C56A3F4557CDA97D17178B2279FE6CE36AA72D2F7D C
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...caa3cc41_93ad_4ca9_b127_de2c13832645.....k..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....!.....http://testgvbgjbhjb.com/.....x.....h..... ..`...../<bRF...0<bRF.....:.....h.t.t.p.:./.t.e.s.t.g.v.b.g.j.b.h.j.b...c.o.m./.....8.....0.....8..... ....http://testgvbgjbhjb.com/.....PY.../.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	1.8112781244591325
Encrypted:	false
SSDEEP:	3:3Dtn:3h
MD5:	0686D6159557E1162D04C44240103333
SHA1:	053E9DB58E20A67D1E158E407094359BF61D0639
SHA-256:	3303D5EED881951B0BB52CF1C6BFA758770034D0120C197F9F7A3520B92A86FB
SHA-512:	884C0D3594390E2FC0AEAB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C
Malicious:	false
Reputation:	low
Preview:	SNSS....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491A
Malicious:	false
Reputation:	low
Preview:	.f.5................i.Wd...............Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F..................F................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.238585854488298
Encrypted:	false
SSDEEP:	6:omLjM+q2PWXp+N23iKKdK8aPrqIFUtwHmL7xZmwyHmL7kMVkwOWXp+N23iKKdK8h:zM+va5KkL3FUtwmx/ymkMV5f5KkQJ
MD5:	E4EE30D5FDEC1D46E651E358EE8C21A2
SHA1:	27A7D360A69DED840AE6BCEB3B6AEDB42758AE01
SHA-256:	41045C9DF8AB3179266233B75698DC9C23E471DB9F5680D21A6A97E2CCEED25E
SHA-512:	E082450C4055CC61DE75147A6E1969F2DC75EABC9DB7AB0F4263D0F72967102E1617B8DCEEA66F1703670B699BCC099F87AD0069000F0958DAB912A37B34103
Malicious:	false
Reputation:	low
Preview:	2020/11/29-14:21:53.612 c6c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2020/11/29-14:21:53.613 c6c Recovering log #3.2020/11/29-14:21:53.613 c6c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D951
Malicious:	false
Reputation:	low
Preview:	.f.5................f.5..............f.5................f.5................f.5...............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.264491624020361
Encrypted:	false
SSDEEP:	6:ogLxt+q2PWXp+N23iKKdK8NIFUtwHgLh3JZmwyHgLh39VkwOWXp+N23iKKdK8+ed:FLCva5KkpFUtwALhJ/yALhD5f5KkqJ
MD5:	182933C9DFB33B4C794B37ED693AB26E
SHA1:	F10F674103E69FD2A454015104A274E3C7105A6D
SHA-256:	BCC4D43E6C914696C010B2067901775051972B800765838A257BF042DE4F05B0
SHA-512:	671CAAB6F0B08B00AEA4BE319F80D61951BFD59EDB60CE7859C7277FDFC012281ACDD40986303A8302C31ACD8F56B3FBE895285E82A48874CEE348BA4A9236B
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Reputation:	low
Preview:	2020/11/29-14:21:55.639 c58 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2020/11/29-14:21:55.640 c58 Recovering log #3.2020/11/29-14:21:55.640 c58 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_1_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):	17938
Entropy (8bit):	6.061511031838911
Encrypted:	false
SSDEEP:	384:ahlZ97TC4hNLFkQF/4H/vo3c93yaM5ZAVGnLMeP3rrBsuzfccHyfXRH0MVEPT:ahlvS2Fk5ooNM5Zg+YePRgpXRHLVA
MD5:	58E0F46E53B12F255C9DCFD2FC198362
SHA1:	24E3904DED013ED70FFC033CFA4855FBB6C41C19
SHA-256:	F82EEF4F80D86F5DEF0F40F91FFB6453E1706CA5FD8A7172EDB19C4B17E2F330
SHA-512:	1AC83CDFF124E4C0281FBBFC0A919AA177F1524AB85434D82E5A87DDDF7CAC26A761C5E6249566626054C62D6B0F46A51AAC1F6E64C260F50832AE1D5F0A49IC
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["vyABSKu1ssLnoQtj8Nqw6CjEthL33alh0QYBLzRg9+E=","DGWrOFQ2mF53Fk3FM5jLCV5sKg1DgRTF750mXhpKaoM=","f8vmSL13lL5/sEk/UBo2z9BTE1au+kMnftvxebWlLfQ=","g6BagkGM3fYVfhX6pe9v+WIhrxb6KJyr1H8KEdf3iQc=","6GdjKPovCi9TAL74Kj/R6GzGC1RVsWCb0lMtrG41ElU=","vttVT0ok78296FZBpoJgEIMmZmATBpKLrC5wr6RiPIg=","5dwwmOMAg6GXh2x6hn99MsZgiXJCxgTnwFdiMmcl2/0=","lQFxytI8i5cYLqNLbSnc45XXd/jEIuKwO1nAvNh5/WE=","qETF6aAOXwVcduPggf/FGrY8l2ALwdIswKxFJWG2JpQ=","+fjs95t/ESSgtcK9SzZOIcY/aemUr2I/yYI07esfjbk=","H+r4m51qI4G0z8YtAibc3/AGYvPK9qT14BbGvmM4/y4=","Qz4vtomAqVrAeKIcJ/zbVi5yDpFiY+F7tP/FTdoAKwU=","k110zqa69JMO5T4RH/nBdkCVX9I/98Gd7K2dnRuyFyg=","+QrRx4Pz8wbz4ef9ch1Q2aAQDZbv0r64NMyj9z0qaaE=","6q/tcYekY7TN66ZdPx4ALLcteRLQJqFy0wgcIqL6fFU=","djipPPtOAFsToDpKDbadLJLGQiCzTkN2qsRbzvKijBo=","uHEm1DVxHADroGNWHjmdfpdNUgtHXDQ0zfTmdqtJgYo=","1C2E0Gz2nqKFG3ghcQEVyiTYI4rTYNnrpsHQY9J7BfI=","swYZ8T85/4tzx26dfC0RKxMiHwnjqJoxtn0Mb8NdcjI=","AuXwavx8SOtkgFhnRlnM4rolw243Ryh2ktL0QZRDLoE=","oG0S5XUkjBtAHts9X+uQt5MTsf

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_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):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

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):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Reputation:	low
Preview:	.f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.270291473335702
Encrypted:	false
SSDEEP:	6:o/6FL+q2PWXp+N23iKKdK25+Xqx8chI+IFUtwH/adWdFz1ZmwyH/QLVkwOWXp+Nl:euyva5KkTXfchI3FUtwfaA/yfQR5f5KN
MD5:	7F3C2142615F8498BE42B724E0841F27
SHA1:	75389DA4530CA9C62AD8634B8197AA536021D040
SHA-256:	1D86927224C6E512639F9E0604F2C3AD77418CFC95ADB64FE63CFF697A9B433D
SHA-512:	788B63FD189F4A7393890BBE6F520B318461E33240E0B0269182A061169A7BE79101A7A28CBF62F06B878525E9D6FD103C02B7DAC907ACF1919BE886025BBDA2
Malicious:	false
Reputation:	low
Preview:	2020/11/29-14:22:10.474 1a38 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2020/11/29-14:22:10.475 1a38 Recovering log #3.2020/11/29-14:22:10.476 1a38 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\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.223427019247524
Encrypted:	false
SSDEEP:	6:o/GFlL+q2PWXp+N23iKKdK25+XuoIFUtwH/l1ZmwyH/Y9LVkwOWXp+N23iKKdK28:e+yva5KkTXYFUtwfH/yfY9R5f5KkTXHJ
MD5:	95167C910AD40F6D2BD4BFE4D3F2D37A
SHA1:	1DC0D271E0392BCF12B86E0DF5B2449425504DCC
SHA-256:	D5D54F78D0A6F61EA162C48BDB0950EB447232A62D547A838BBF20CCFA0BA23B
SHA-512:	6667FBD1CB0F91EF8E3FE66E66B2F81DE0BDB630C1AE960B5A5A401FCB88BF3E17761F916CB1CE84665D8FC53DD3016B1DE2D74ACF760626BD78B1FEC03DA68
Malicious:	false
Reputation:	low
Preview:	2020/11/29-14:22:10.467 1a38 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2020/11/29-14:22:10.468 1a38 Recovering log #3.2020/11/29-14:22:10.469 1a38 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.256272273974404
Encrypted:	false
SSDEEP:	6:o/wKSQL+q2PWXp+N23iKKdKWT5g1IdqIFUtwH/IG1ZmwyH/LQLVkwOWXp+N23iKN:ewKSVva5Kkg5gSRFUtwfIG1/yfLI5f5N
MD5:	AC201CED0656F9C0625A53418540E030
SHA1:	B6028AA4C6D1FD83B3F64BE16F0C839DE10ADA36
SHA-256:	CCDB2DE87DFD2C8A7B32E084E26A334A9D9B3042AE2B65DFEDCE133AC7CB4CCC
SHA-512:	2BF7393D0D216ABB703741C6B498D86CA94ABAE9B315D15CFEEC7960EB0C906708A5EEE84ED60DE19996CA8A3D4294FE79C14A6F14ABD83DF8868EC2A21F92C
Malicious:	false
Reputation:	low
Preview:	2020/11/29-14:22:10.391 16c8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2020/11/29-14:22:10.395 16c8 Recovering log #3.2020/11/29-14:22:10.396 16c8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	32768

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Entropy (8bit):	0.0866953924397253
Encrypted:	false
SSDEEP:	6:l9bNFlqQCNa/lvuNsRRnPlyZ0WHOo/lCxthiLXGCxC+/erlk0nPlyG:TL+A/tbPla1HNuQLXGI/fqPlt
MD5:	69C5BB8A1DABBFC7F3A12301B4626F60
SHA1:	87497973EF84A6232DB08D476047233DF223B16F
SHA-256:	3F2F8D24645D7AE68CE78F46BBBEF2D67B638FDAE54F29AF2AF47361B4EEF709
SHA-512:	92B0D43BB963FE8CD1A12896855A0B6B9278C715FEC43BBB62DA196130DAD9A385B752DFC4ECD08B87388A6680C96CBEA83A6D18E0F8CE520198A0C4CCEFA05
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

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):	310
Entropy (8bit):	4.976028538503648
Encrypted:	false
SSDEEP:	6:0s4KFgPlOvi2PlKpeXpsEG/ceoEMwxWG/4eUMBk7scY3YkF3nPlyCFDDGW4w:VJaPlcRPlLCEG/XMwxJ/ZBk7v43Pl3DB
MD5:	56FC2E54F78117702456E8DB1626DB12
SHA1:	1C1C5B234BDEC0BBF13A0AEC96D45925502D2A99
SHA-256:	EE89509AF5F974719493FCDF4A95003A968D29A8044430AC799AFF170B4FB895
SHA-512:	AC84C84638CD6026AD81B92109B0CC05CA5AEF777A48913D6EAC13F2A482680F8A0A608035F2CDAD0065C1931589816975E1D069E9BE9745FD88B8B8D7D2154
Malicious:	false
Reputation:	low
Preview:	.....".....com..http..testgvbgjbhjb*(.....com.....http.....testgvbgjbhjb..2p.....b.....c.....e.....g.....h.....j.....m.....o.....p.....s.....t.....v...:..... BA...=..... .....*.http://testgvbgjbhjb.com/2.:.....J.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	33356
Entropy (8bit):	0.04761656801783403
Encrypted:	false
SSDEEP:	6:HSgyv1t3vxGB1xaXvg9bNFlWCj/lx0E/l3n:ypJcsqLBj/bz3n
MD5:	9382A8544F9D3DA5DF46637AF5AB0BA7
SHA1:	BC194D34DB65E2CE8137FBA3B22BB6CBD5685133
SHA-256:	29A38A044A60587E41C1E7700131E6D376DF968C6BEB7191B6C2B34C909ABB9A
SHA-512:	EABAC199CC0781267B774930E500305666DA11AF31490A8B2F2128CF14CE44694BC9EE32815E81932028A70B77CA3723365C03258CBA0303E6E061E9B9DA9E2C
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.451112901777451
Encrypted:	false
SSDEEP:	48:8QtGXV56Aa7YAME38db8yUTkT9bQSefgGXNrS0U9RdiN9R5:aa71MTdbHeu9bQ5fgGdrS0b5
MD5:	CEFB4066FE092AA7F24D1EAB19D5F76E
SHA1:	7B374FD056D89707976DB09F3FDB970228070B1E
SHA-256:	F9CB199FCA8882D05CDEA8EFEDA1FC88664BDB2959AD8BFC6B72E5606557A0CD
SHA-512:	6D85C783751BE03FA0E5D34087E08DB7412F99A0DFB322C2947C8DED3A0E3B0A0034CE7D2D79A49FA2D3DAEEB39552F8C8BE7945D870991788F345A134C868A2
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Reputation:	low
Preview:	50=....*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..731522000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2020-11-29 14:22:11.31][INFO][mr.Init] MR instance ID: f9ad20db-a886-4fcf-8f4c-b1ce704b2257\n","[2020-11-29 14:22:11.31][INFO][mr.Init] Native Cast MRP is disabled.\n","[2020-11-29 14:22:11.31][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2020-11-29 14:22:11.31][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2020-11-29 14:22:11.31][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2020-11-29 14:22:11.31][INFO][mr.CastProvider] Query enabled: true\n","[2020-11-29 14:22:11.31][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.193955796394593
Encrypted:	false
SSDEEP:	6:omLyF39+q2PWXp+N23iKKdK8a2jMGIFUtwHmLvB3JZmwyHmL/39VkwOWXp+N23iP:COva5Kk8EFUtwwZ/yGz5f5Kk8bJ
MD5:	33B28341900CF7180344FE959FDC4E83
SHA1:	5736FD2D7C70C89787D8935F1877B80E1BC06B80
SHA-256:	919ECA778B40043423E25D0FFD3B0BCAE3BBF34C0D4596710CE7F6E20F32D345
SHA-512:	DEC56DA2981BB040A6B56B5B149A5EADA989E2BD988528F144AF29FFC5EF0DC6E288287CC6A1826C093C3563551C08CB0F25EFAB7655AD4BAA7825A2F26CC91E
Malicious:	false
Reputation:	low
Preview:	2020/11/29-14:21:53.412 1148 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2020/11/29-14:21:53.415 1148 Recovering log #3.2020/11/29-14:21:53.417 1148 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.247609146945629
Encrypted:	false
SSDEEP:	6:omL0EpM+q2PWXp+N23iKKdKgXz4rRIFUtwHmLdxZmwyHmLOiMVkwOWXp+N23iKK2:LpM+va5KkgXiuFUtwC/yhiMV5f5KkgXS
MD5:	09BC2CECA8801B9790BE7B1A4EC03FE2
SHA1:	06516CD14FCD8D606C4B43C9765157EADA3632C1
SHA-256:	B400C182E08DEF1691CA36A999DD7E455B7EBA1534325EE23409208711326CC6
SHA-512:	05EA650354A5FB1BF17BF436C63FD09DE6AE314C0F5D57C17F18D1416B171DF4E4CC000D1930EB6C11A532A8CF22EEACE491A4FA34085B902BDE3B1101827353B
Malicious:	false
Reputation:	low
Preview:	2020/11/29-14:21:53.632 c6c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2020/11/29-14:21:53.633 c6c Recovering log #3.2020/11/29-14:21:53.634 c6c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljl:5ljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946B
Malicious:	false
Reputation:	low
Preview:	..&f.....&f.....&f.....&f.....&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.2027988430762955
Encrypted:	false
SSDEEP:	6:omLQClM+q2PWXp+N23iKKdKrQMxIFUtwHmLQ3mZmwyHmLQ3pMVkwOWXp+N23iKKS:rM+va5KkCFUtwRm/yRpMV5f5KktJ
MD5:	7B77AA34D5BFC37B8B4D9317DB43D40B
SHA1:	C84673278D913F2A5DE4A70B4F9021743B2B8067
SHA-256:	ECF294708597780E799E8BC5D84078286B27F08E7B658B5E12AEFE3ED8F47B74
SHA-512:	6D71140153B370EA2CBF6C6D1FDFB12397F255017CE4DC7A89DB8569DB458F1A8E416DC9A2DA336D08DFCE00E9EF68256D83B6EC9779029927A6DAF3B1FC87F
Malicious:	false
Reputation:	low
Preview:	2020/11/29-14:21:53.560 c6c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2020/11/29-14:21:53.561 c6c Recovering log #3.2020/11/29-14:21:53.561 c6c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.170689440435213
Encrypted:	false
SSDEEP:	6:omLW/OL+q2PWXp+N23iKKdK7Uh2ghZIFUtwHmLWlYKWZmwyHmLWlOLVkwOWXp+NN:G/S+va5KkIhHh2FUtwnGKW/ynQV5f5KF
MD5:	AF5353CC0F41E9DED529C5549FCB66E3
SHA1:	9F82067854B7A02875B4AC540657B47BE10C6896
SHA-256:	6DB624C09F7FD0454B4D721A4D52C670DB6A076A6C15CB281BC7A48C8EB1E1F7
SHA-512:	ABAA95E4015A181E834FA5021078904CAF0F5BF58AEF5A7CD4B248C35FBF72265BE2E7EA868EDA68995F85D8DD2E7630FBB19E0CAB7B331AA42AFB3AADD76F9B
Malicious:	false
Reputation:	low
Preview:	2020/11/29-14:21:53.355 103c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2020/11/29-14:21:53.357 103c Recovering log #3.2020/11/29-14:21:53.357 103c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Reputation:	low
Preview:	.'..(.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.266701856662096
Encrypted:	false
SSDEEP:	6:omLQhFiM+q2PWXp+N23iKKdKusNpV/2jMGIFUtwHmLZMmZmwyHmLZ3eMMVkwOWX2:OkM+va5KkFFUtwI/yrMMV5f5KkOJ
MD5:	DD2E36C18F107CB21411A4C8E67E0CE3
SHA1:	C37943ECB54FC7C7957FD720FD85AE86F06F364F

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
SHA-256:	3C8376607709F17987E2A53339B7D71345537B25DA0CCD0A31C2DF6944B30209
SHA-512:	3855B8F10A15CC095518D1B6D752D5F75812D1FA66E693F4FEC73FF82A4B44BF0BF9E18C9C357B9DD538A5064061BB24E269229E25F3F88A60A71C425C51D84C
Malicious:	false
Reputation:	low
Preview:	2020/11/29-14:21:53.595 c6c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2020/11/29-14:21:53.600 c6c Recovering log #3.2020/11/29-14:21:53.601 c6c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.330273016425907
Encrypted:	false
SSDEEP:	6:omLbR9+q2PWXp+N23iKKdKusNpqz4rRIFUtwHmLoZZmwyHmLoNVkwOWXp+N23iKV:Lyva5KkmiuFUtw9/yP5f5Kkm2J
MD5:	FA28B63ED75809A1F2D14526497A8D74
SHA1:	34C4203D4C6232610AB53302CD271AE7D34B6AB6
SHA-256:	110C59FF4C615F3E6B13453813DCB0801CC7814489480B04D05371C34FD2615D
SHA-512:	BF671C0E2BB3469C8E82C3F28120E5178F5CEFC21FB68A8EA3A3012D890E8B9D977D4638E3676292DB19A919937A41CC140B4BF424F286AA3FA4A280FEC0FD0
Malicious:	false
Reputation:	low
Preview:	2020/11/29-14:21:53.635 c58 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2020/11/29-14:21:53.636 c58 Recovering log #3.2020/11/29-14:21:53.636 c58 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5l:5l
MD5:	E556F26DF3E95C19DBAECA8F5DF0C341
SHA1:	247A89F0557FC3666B5173833DB198B188F3AA2E
SHA-256:	B0A7B19404285905663876774A2176939A6ED75EF3904E44283A125824BD0BF3
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Reputation:	low
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.292258594519991
Encrypted:	false
SSDEEP:	6:o/2Tgt+q2PWXp+N23iKKdKusNpZQMxIFUtwH/2TbNJZmwyH/2TFI3VkwOWXp+N2R:eAJva5KkMFUtwfAbNJ/yfAFIF5f5KkTJ
MD5:	F535494D716C89506FF7E27971415E47
SHA1:	083A07769263AA4376309346ED9D20C087F09217
SHA-256:	9AC9765E40832E2741CFBED8AA51C3EAE4D7DA602FF8266730DF1B10FDD74B5A
SHA-512:	83282C4EA2F92996329B7A5D25DB520E5A4D654FB3686C8C3959457D1EFE9488ABC3AEEC6E829A76611C734959AE105B11057B36C0198D125F76D2D61CF4773E
Malicious:	false
Reputation:	low
Preview:	2020/11/29-14:22:09.661 c58 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2020/11/29-14:22:09.662 c58 Recovering log #3.2020/11/29-14:22:09.663 c58 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\b8d229a8-52f8-4859-a422-64163347a644.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\b8d229a8-52f8-4859-a422-64163347a644.tmp	
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\5ffb6394-d0e3-4d94-adc1-fdf7fcba924a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Reputation:	low
Preview:	.'..(..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.182059728973334
Encrypted:	false
SSDEEP:	12:e5M+va5KkkGHArBFUtwff6/yfzkMV5f5KkkGHAryJ:4a5KkkGgPgInL9f5KkkGga
MD5:	AAEE40FC2F8D463D0DDE620810EC1029
SHA1:	D987CE17450739949E1EB1DEEF56E73F502284F7
SHA-256:	EEA5B6FF8DA0091F88DE91EE7A1A57B089EF405BDA9CB834FDE73FAF23CF1066

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
SHA-512:	95886A02717FD05DD80EE84D9ECFF878BECA0795949830EF9623D7A4DE3B3BD879753D906D2047BCB5712A921387FC5736C7BA11EAD7F24FBBC28C4C440E07E 6
Malicious:	false
Reputation:	low
Preview:	2020/11/29-14:22:10.143 c6c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Local Storage\leveldb/MANIFEST-000001.2020/11/29-14:22:10.147 c6c Recovering log #3.2020/11/29-14:22:10.148 c6c Reusing old log C:\Users\user\AppD ata\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.199428699518028
Encrypted:	false
SSDEEP:	12:eQRova5KkkGHArqiuFUtwfa/yfx5f5KkkGHArq2J:fRaa5KkkGgCgW7f5KkkGg7
MD5:	BE09BADA50A20BF0F02FDCB88F4AD339
SHA1:	B53C1B5B2540F2F5E1013A885CD9136E6AF3C2A2
SHA-256:	6D442F6C2B6BE8327A47690A84EC1BE08AA4404CF66B10A1E59828FA20A33AD1
SHA-512:	2459B2E6444B4062EA5E79D79D0A59FF875122F16400CF63244FFE07F474C9E11A70A05A0240A413CFC9260A5179FCF2E9AE377268C0206B5AC0FDD1ED05FC42
Malicious:	false
Reputation:	low
Preview:	2020/11/29-14:22:10.151 1048 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2020/11/29-14:22:10.153 1048 Recovering log #3.2020/11/29-14:22:10.154 1048 Reusing old log C:\Users\user\ AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5l:5l
MD5:	E556F26DF3E95C19DBAECA8F5DF0C341
SHA1:	247A89F0557FC3666B5173833DB198B188F3AA2E
SHA-256:	B0A7B19404285905663876774A2176939A6ED75EF3904E44283A125824BD0BF3
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Reputation:	low
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.203842842925009
Encrypted:	false
SSDEEP:	12:eAi7va5KkkGHArAFUtwfAid/yfAiZ5f5KkkGHArfJ:tiba5KkkGgkg3i4YiLf5KkkGgV
MD5:	04D45051EE8BF9F779A358134E2215C8
SHA1:	8BD0232A96243C0E6E88C0C13972065D4F4B7232
SHA-256:	D471BD70005499EE7D68384E8BA7C132E6A897B005B1BD1B953E2B6FB362D7A1
SHA-512:	F150C48B2980523C804CB7F90BAD6081F28BDDFBBBA273995DA9E5FBA8DEFA02B1C57DE9C139565BA84D9295F1A6F959A0EC9C00F4714161AAAA00FD12875C 6
Malicious:	false
Reputation:	low
Preview:	2020/11/29-14:22:25.388 1048 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2020/11/29-14:22:25.389 1048 Recovering log #3.2020/11/29-14:22:25.390 1048 Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF21 24
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.25487875036225
Encrypted:	false
SSDEEP:	6:omLWPjL+q2PWXp+N23iKKdKpIFUtwHmLW0zKWZmwyHmLW0lLVkwOWXp+N23iKKdk:GP3+va5KkmFUtwneKW/ynYV5f5KkaUJ
MD5:	49C69FEA5022D21B412B3B01CD444A22
SHA1:	BB14EC1F28F1476D570286F7852271E451740F78
SHA-256:	DE1454A28EF943613E9E68AE261A70E83265D72EF8D6640B6780860F42F71758
SHA-512:	29F3D8B3508811A9286C2789C39F649FA2F55BEBA67D990C9DA8BFBB56F88CFC161BCAF0898844FF671AB1DC04738CDA267FCD5E05AFFDCF58867E26A14699 E
Malicious:	false
Reputation:	low
Preview:	2020/11/29-14:21:53.378 103c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2020/11/29-14:21:53.379 103c Recovering log #3.2020/11/29-14:21:53.379 103c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.290434712424679
Encrypted:	false
SSDEEP:	12:eZ/va5KkkOrsFUtwfZr0/yfZr05f5KkkOrzJ:OHa5Kk+gUdxyf5Kkn
MD5:	4091928E35A25FA53CB11F1A085E8842
SHA1:	B186B1921284B36A337DA778762D4AEC5CDA9AC5
SHA-256:	81FDA83DF8D9BBD9828234BEB9AEAE597D956410FD6E98DE6D7727C5A31A91B2
SHA-512:	C4968F645DF22E24F10A90CB4966224E077252EAE84AC7D6729DAFF3B066AD48DCDCC916B492628439A2FE6A05BAC672FAA4944466CCC0D08A29229F52E13CB 1
Malicious:	false
Reputation:	low
Preview:	2020/11/29-14:22:11.312 17a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2020/11/29-14:22:11.314 17a4 Recovering log #3.2020/11/29-14:22:11.314 17a4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12
Entropy (8bit):	3.188721875540867
Encrypted:	false
SSDEEP:	3:DThM:DThM
MD5:	CE40FEBF177FA98D57378F536A52C866
SHA1:	80BC00C6896D714C614ED2071F780F2F1E4631FD
SHA-256:	CF66E718B6934537AD7C18B318D12C943E2E2F05E074CDC7EC45F125D1117F99

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
SHA-512:	C1C535B99C0A3AD1B12002A573A76D89FE96BCEB7A7DFD36BB471743C836E14BF8EED652EE2B22583969343940E641F67E27F10837331D9E00C981BB5BFD2E6E
Malicious:	false
Reputation:	low
Preview:	.....-7W..D)

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b2fd04dc-0ad6-4f4e-802d-8e392aba43fe.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):	5628
Entropy (8bit):	5.180014857216756
Encrypted:	false
SSDEEP:	96:n8bbC4EQiu5cV6Bok0JCKL8Vk91NbOTQVuwn:n8a4gWcf4Kck9T
MD5:	81947F2005222324592EA0EBA10C5565
SHA1:	932481E5839CCA574B528B8B676D700C40FF3410
SHA-256:	06EEA6D5E7C838F0453ABE0BF98697989DCE7A34D8A3AC94F36C24B770831BFE
SHA-512:	DF76F2665D5DDBE0A795DC969C5D33BDE2281D1EA0E265EBC05403ECA24029979115F1C531AC4A991D9CABB804048A8026AED472B318B574CD100CD8DCF7F9E
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13251162113608288","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.473774149886633
Encrypted:	false
SSDEEP:	3:tVPFi/3iDToAGKWZmwvK4i/3lV9Bh7V8n4i/3lV9Bh7WGv:o/SDTdG1ZmwyH/1P7VSH/1P7tv
MD5:	1B56FD4D3155D47D56418B6B88617785
SHA1:	408B3ED6B579C12679C35017E33F1A5043413449
SHA-256:	E02A767277B99A4C4AAC127D254159755C8A81DFE5D3175336BC492FE7C2F6A5
SHA-512:	F68D2B5F35805D7C9E6EEB4AD0D0E2B809FC0B1FFBF4ACC4783F73CB07B7F8D21DFEEF2203FBF17FAB811EC43ACC25A63C0D1BB231B40C7080352731A9CFEA51
Malicious:	false
Reputation:	low
Preview:	2020/11/29-14:22:08.327 16c8 Recovering log #3.2020/11/29-14:22:08.408 16c8 Delete type=0 #3.2020/11/29-14:22:08.408 16c8 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKlVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF04
Malicious:	false
Reputation:	low
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ed1f427f-0c10-4c3e-8f46-70825d81e107.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f9f809e0-ec5d-4591-8cac-a6ca1c76d1be.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):	1039
Entropy (8bit):	5.565135196524143
Encrypted:	false
SSDEEP:	24:YI6H0UhVsTG1KUerkq/HeUeXby2qUeXvy7wUtRUenHQ:YI6UUhVseKUewqPeUer2Uef8wUDUenw
MD5:	7834AA395B547465225029626C2BAE31
SHA1:	70C0ABB1487354E9EB16CB715CB26885D61D151A
SHA-256:	44583FED2AA12E78556C393B0468AA21D574421271BEC01B5A488EF512F0B38C
SHA-512:	D94904F3D00E363096E79468C3872338F63118A598FCCF3A7208D1E1376CA80F39F35FFD4613AAB0C78F6C5B00CBA9CA7593A3BBF263E648D4C4922D646E5AA
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1638224517.861341,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1606688517.861344},{"expiry":1633014077.462534,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.176235889174994
Encrypted:	false
SSDEEP:	6:o/4aXAQ+q2PWXp+N23iKKdKfrzAdIFUtwH/sAgZmwyH/sAQVkwOWXp+N23iKKdKS:e4jva5Kk9FUtwf+/yfy5f5Kk2J
MD5:	D92B25F6D98A4188E6CDBF32B8CDEA9A
SHA1:	045E7D10AE9FDD89ABC44AD1BEFE610CC612CB94

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
SHA-256:	046130C64131F4FA7C6D58A819C535F082F63824B298E335F3D303903B99878B
SHA-512:	0A6F4788812C41FC9962B9DC2AC655BA9979BD0A3723C3A12E7119DB6BA8333372566695AA9F7402487C4843CE0B37C5296FF44C45D12A0F73479F38B38BC156
Malicious:	false
Reputation:	low
Preview:	2020/11/29-14:22:10.613 1048 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.202 0/11/29-14:22:10.614 1048 Recovering log #3.2020/11/29-14:22:10.614 1048 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_prot o_db\metadata/000003.log .

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\aef151f4-7f6d-47c1-bacc-774b8a502f03.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):	162521
Entropy (8bit):	6.082393012548419
Encrypted:	false
SSDEEP:	3072:/iGCAPHKb1o/hF5RzweKvf14PnpqISFcbXafIB0u1GOJmA3iuRG:6f4HW1oZF5BtK1engzaqfIlUOoSiuRG
MD5:	1A530131E0421C2FBB24ED6D8127E832
SHA1:	F297FC6FC74CAD7952FB8B4171C2751B72B398D3
SHA-256:	72F0D6CC5ED0FA0E1EA0BFE0A51C043684434F4C4D2C31B9B1152673274D5F79
SHA-512:	DD0446C9488503B9C5CD9C86138DF8BF0211AE8BD846198D3DA4CF158D6C399F32AF0392DCA8B88AA5A410BAF4EDA2905D98C76737FEFC27A07512CF1732B5 A
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"use r":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time": {"network_time_mapping":{"local":1.606688516213298e+12,"network":1.606656118e+12,"ticks":96199933.0,"uncertainty":4543822.0}},"os_crypt":{"encrypted_key":"RFB BUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr 2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1 vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_mana ger":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\fa0e5b06-b2a2-4401-ab65-1b84138539dc.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7443279481371112
Encrypted:	false
SSDEEP:	384:jbA/zxisVpujqNLrQvnt3AflgH54G8rrWBHjxQFFVUrunmO5CtT3zYO9dXNy1raV:MKFluJkMQevL5JEX7qxKXJj1/
MD5:	2134644A8111DFF458F8E9C4F0AB949D
SHA1:	2DCE2AFB04A40C70580FFAD1CA9B7B5E18F64CB3
SHA-256:	0D031788282A4CFA468CD4819C3504B25DCF8228A2D6FE14125E02283367B2D5
SHA-512:	6BA7751D920A41CDA14A6550135493222C35C651D8397F99991315F38C469D5D2B318767D18F52875357AFB5C37008C6D9FD606BEDADACCA2D9070A82E2C0BF
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...n*8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Temp\1a16bb92-8f5b-4178-82bb-ef2243036074.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	300953
Entropy (8bit):	7.973503294353402
Encrypted:	false
SSDEEP:	6144:0sb1v/4nxPbqqBbWbFsw+wh3bC5NFv++S/hup0XcaxlnJ9:7l/4nxPZbOFsw+y3d+S6WnX
MD5:	1FE8E0AEB768437A23CEEAE6053E5822
SHA1:	5529A275644B729009E22035F6125879450F4ABB
SHA-256:	25A2F515CEC98CF2ACF11B34C59723D76820A4B5734E223D7EBEA55E5A851468
SHA-512:	45C8EEC35301495EB9DCE36B32F1CA2E9A7B167CAB52D3E026E2617134067C38CCE1463DEC18C1657A6984FBB8F342336E29E8BF6280C0533CB67CA56812320
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..''0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n. <Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....L.18..Y.~..%...~._.....O\..p,...eY.0=.!..+.SoZA7...:t.G...VZ<..d....MN.....T..{1\.T...P, ...i...NrD...e.2..u....5.....1.n.Zu.E...!..XR..j.:.E.gUw.-s7:T.c_...(.i..iU.).M=yF<..`.....F...@)..IK.. b.4.o..mC'...N.*@OtT...`.&|.8.M;.....0..0...*.H.....0.....).'..b.*$w\ $.q&.]zF_2..;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.I....{.K@]6.LIP/....](.A.....e..;.<LQ0{^....=m.V.#....a.NL.....%...p.@.4....Q.Fw...dUoCq....R l.G.,2.....[..T'.....''ct.).s#.(/.D..C..4..RKf.W....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...H0F.!...L..\.j.1.d.....==v.....-

C:\Users\user\AppData\Local\Temp\932b9f0f-3394-4b3e-9a74-79849301c0c5.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\a5fbf7a2-fa02-43c3-bd22-257e2f88dcf0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob

C:\Users\user\AppData\Local\Temp\a5fbf7a2-fa02-43c3-bd22-257e2f88dcf0.tmp	
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-I..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\e121ac07-8134-4cf1-8b4e-e9a91097977a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\1a16bb92-8f5b-4178-82bb-ef2243036074.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	300953
Entropy (8bit):	7.973503294353402
Encrypted:	false
SSDEEP:	6144:0sb1v/4nxPbqqBbWbFsw+wh3bC5NFv++S/hup0XcaxlnJ9:7l/4nxPZbOFsw+y3d+S6WnX
MD5:	1FE8E0AEB768437A23CEEAE6053E5822
SHA1:	5529A275644B729009E22035F6125879450F4ABB
SHA-256:	25A2F515CEC98CF2ACF11B34C59723D76820A4B5734E223D7EBEA55E5A851468
SHA-512:	45C8EEC35301495EB9DCE36B32F1CA2E9A7B167CAB52D3E026E2617134067C38CCE1463DEC18C1657A6984FBB8F342336E29E8BF6280C0533CB67CA56812320
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....L.18..Y.~..%...~._.....O\..p,...eY.0=.!..+.SoZA7...:t.G...VZ<..d....MN.....T..{1\.T...P,...i...NrD...e.2..u....5.....1.n.Zu.E...!..XR..j.:.E.gUw.-s7:T.c_...(.i..iU.).M=yF<..`.....F...@)..IK.. b.4.o..mC'...N.*@OtT...`.&|.8.M;.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.I....{.K@]6.LIP/....](.A.....e..;.<LQ0{^....=m.V.#....a.NL.....%...p.@.4....Q.Fw...dUoCq....RI.G.,2.....[..T'....."ct.).s#.(/.D..C..4..RKf.W....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-I..`.Q.{...H0F.!...L..\.j.1.d.....==v.....-

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	886
Entropy (8bit):	4.799570700992651
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyIDEK:1HE7n4gn8WYpYrbhz8ZpotHOPjsrdaD
MD5:	0F604F138A921EE7270C45E520621C30
SHA1:	E2BA940AF44609BEAC49B603EB1C379E43F4AAEB
SHA-256:	A149D52858570C9544E33B183915556230B7F66CF4ABAD4DDB00B1409476FBE1
SHA-512:	D87C8C7D0C998B37E34B7E4E6F5212FF4A0588C15F1273A55CD36B4A6FB13B7FDAE4F3B23EA469E7ACAF22B8BF53EB67476D897B96CA5C15C113EC078071A6D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\CRX_INSTALL_locales\bg\messages.json	
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": "..... .. .., ...-.....".. },.. "please_sign_in": {.. "message": "...., ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	705
Entropy (8bit):	4.576619033098666
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyFJKtOi2V2Te:1HE5baib6WYpm31Lt0Z8Zp8pxOaKtwVl
MD5:	DDD77BA67108D8D88D66E35AA72A8048
SHA1:	F9C217728E756728B788C969F5101484D0557065
SHA-256:	3DB4D2B1586C020EC679C09148DB226DBB23857D326BECBB6CC48976036C391F
SHA-512:	6CA88083CECF6166503A1441BE8BB726CF08DEA8CFD61F1E81A970FE623284039FB9A530990E8E2008A4B1128399022AFE4F517E85CC7B069B670F5BA659F4F6
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "C onnecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "No s'ha pogut completar la transacci.. Torneu-ho a provar m.s tard.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	663
Entropy (8bit):	4.771803710371731
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyN+/sFfmSYWc:1HEl4G8WYpdt8Zpq5TOT0FfmR
MD5:	B587AF92ECD087AAE3EF210364960844
SHA1:	AD78B31888863D3F0EC0D8CDCA316EDE9EBD7543
SHA-256:	9796A230BA459EF31E3D102B02575B73D6F1C812BF11F4D1E55B17C17891D2C5
SHA-512:	D2771ABB1174C3B6AF70BA1640837DE1B28137319307841B12A7D03C0A605AAECFC93069026A3906B289BAE12D33F4457FB54D7D27ABC5DC674C5C4C1E9F7CE 1
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "Transakci nebylo mo.n. dokon.it. Zkuste to znovu pozd.ji.".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	642
Entropy (8bit):	4.533570611298554
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyNz31m8tbYzD:1HErMKfqMKVWYpM6lL8ZpDNOOQ84D
MD5:	639CEF5231701AE13F81DBB67730BB95
SHA1:	E249FE0C70B0F85B033730719B6D1B30F0B04431
SHA-256:	6C71F9D37006245D0E2E956D6D2C1815FFEB43236DD3D427A02F8DD348AC93C5
SHA-512:	D040D25ADD9666050544F9173EF61E044F7EBBAE8C528FC4077880734141205AAE60566668E6854D0B9C8D59924E22D1665D2C93085ED7F7E1F4DA91B951F09E
Malicious:	false
Reputation:	low
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": "Transaktionen kunne ikke gennemf.res. Pr.v igen senere.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\CRX_INSTALL_locales\de\messages.json	
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	701
Entropy (8bit):	4.598783840405771
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603Oy91Lj8SYJ6K:1HEzWWYp3Bewv8Zp7k4OALIhj
MD5:	6E1B49ABC0AA5C1E2764E48EB1EA256A
SHA1:	604E76C89D4763C002C51908CEFE8C11AF7CBBE5
SHA-256:	B692DB1A249223E62E62DE9725334039419B5942AF715669F0F0F4BDEDAC5733
SHA-512:	EE527D48178D09D66120C0D1EA2584A7397404109A074AC09487D6AE8507A593193B31D3197C2418A162BB3E7DCC46FA5844D4951BB09650FC2A4AA10EAB811(
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_una vailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "Die Trans aktion konnte nicht abgeschlossen werden. Bitte versuchen Sie es sp.ter erneut.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	875
Entropy (8bit):	4.920210350678433
Encrypted:	false
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWlOBINZXD:WguYpCZnpEZb6fD
MD5:	41BB0DB6EC99E4664C6E2247EC704151
SHA1:	BF2268F9A77218384F1F73951F98829296318452
SHA-256:	90FC75C419D7359C2241F54562177252655526F3074E7E419E36F5C473843842
SHA-512:	738F7C254825E0D00D4BDF909FA6957D5A6027BCBCDF76F1385210FA5F908C2C94C038B6DF4309C68774C96B84447079AAF514F46519E60876BE4A8F4ABC9E6(
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavail able": {.. "message": ". ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": ".. ....".. },.. "jwt_retrieve_failed": {.. "message": "... ....".. },.. "please_sign_in": {.. "message": "..... ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	617
Entropy (8bit):	4.481995064086158
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOtiCsHTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOthFD
MD5:	64CBD0878A320F70E8F9DC2AD540C8DE
SHA1:	E95BC23E053C078BA4C269B2F75C22159450C2F2
SHA-256:	E99F26D0540E2C71802716B24668D9B4611E9BC429CD681606963E095D18EDFD
SHA-512:	10BAF5423314EF0352FD56D3649CF73713BE8D5EE8A2E21E7E02AAA46EE92635A1EEF87DC62D3E999A1B3704720C51D3281FB28CB9523395EB5A21C4AB3C6D(A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unava ilable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed. Please try again later.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	617
Entropy (8bit):	4.481995064086158
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOtiCsHTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOthFD
MD5:	64CBD0878A320F70E8F9DC2AD540C8DE

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\CRX_INSTALL_locales\en_GB\messages.json	
SHA1:	E95BC23E053C078BA4C269B2F75C22159450C2F2
SHA-256:	E99F26D0540E2C71802716B24668D9B4611E9BC429CD681606963E095D18EDFD
SHA-512:	10BAF5423314EF0352FD56D3649CF73713BE8D5EE8A2E21E7E02AAA46EE92635A1EEF87DC62D3E999A1B3704720C51D3281FB28CB9523395EB5A21C4AB3C6D0A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed. Please try again later.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	696
Entropy (8bit):	4.469493700399435
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyFJhwtOLLY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OahwtyD
MD5:	B4B479436878DA0B032F1B656B310637
SHA1:	F525EDB5B376CE665280DB32EFE3684CE6DC10DC
SHA-256:	3B3DEB56AD7A5F85ED5AB944172B715A5F5F49E3C5A0F7915DB879BF8ACCFEE0
SHA-512:	56C5CCA31DFF155E608723EFEBE01B421DFA3AB43EDFB586778BD76C6EB1AAF57CF904BDE0EA0FB5E912CCB445788136DE319653A882DC2E844046847D201B0D
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "Los pagos en la aplicaci.n no est.n disponibles en este momento.".. },.. "jwt_retrieve_failed": {.. "message": "No se ha podido completar la transacci.n. Vuelve a intentarlo m.s tarde.".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	667
Entropy (8bit):	4.49547663693789
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34GLO03OyFJ2tOLLYiJD:1HEvaC6WYpcDeEFxq8Zp4LlOa2t4D
MD5:	807730218B74CA040AD8DD01E5B2E0D8
SHA1:	ADA0042296C448DCD5C2B22F520C9304526FE9AD
SHA-256:	2823F6DDBF6905D9F4459091A85073644E64B5F7AAAA7FC435495C50DC5ECE68
SHA-512:	5ED86C91A0A435417CB0EDF984AA4DF2177BE37C27D0C805147CEB11ABF75C642416443DB88049A538F63BED9CCCBA95973DAC795498A1A7E022DD6ED362042
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "En este momento, Pagos En-Apps no est. disponible.".. },.. "jwt_retrieve_failed": {.. "message": "No se pudo completar la transacci.n. Vuelve a intentarlo m.s tarde.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	609
Entropy (8bit):	4.483029436148137
Encrypted:	false
SSDEEP:	12:1HEJfPGGGfPG+WYpU34Ze7z+dgrW9O8ZpU34ZwZz03OyQQUe1YgoLIR:1HEdvqlWYpTeObk8ZpT/O3QU1LIR
MD5:	B5DF9CEA0A2FEAE9816F8D41470D744E
SHA1:	65C86CD677A68FF7E11A789EAB078FB932A9E157
SHA-256:	AD75B59775C8F6688FFA9F0453868999996E04B9EE9645721765D1C731D04578
SHA-512:	10C30393C29829FFC535559C57B31EBDCC370ABB5C2ED2A6F04E9CC5590FB8587DAB330E4E9367F3E762314EFE913802B98821136D17E9B9A437B56885F259F8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\CRX_INSTALL_locales\et\messages.json	
Preview:	{.. "app_description": {.. "message": "Chrome'i veebipoe maksed".. },.. "app_name": {.. "message": "Chrome'i veebipoe maksed".. },.. "craw_app_unavail able": {.. "message": "Rakendus pole praegu saadaval.".. },.. "craw_connect_to_network": {.. "message": "Looge .hendus v.rguga.".. },.. "iap_unavailable": {.. "message": "Rakendusesisesed maksed ei ole praegu saadaval.".. },.. "jwt_retrieve_failed": {.. "message": "Tehingut ei saa l.pule viia. Proovige hiljem uuesti.".. },.. "please_sign_in": {.. "message": "Logige Chrome'i sisse.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	673
Entropy (8bit):	4.6221501785662396
Encrypted:	false
SSDEEP:	12:1HEJRuzGGRuz+WYpU34ujSBu+dgYO8ZpU34J+Bu03Oy0EyOxAxWeY5HN:1HEFcWYpPNa8ZpD+FO4zxAWHN
MD5:	50EF678CECF0C82675B9DF64CC3CF72E
SHA1:	F9D9A994530C86C1A99B6D104E86666AB56AD4DA
SHA-256:	7F5B921E0D0B01D8D3287D3293729BFFF07ABC7DBCB1227134823A404DF29E83
SHA-512:	62A96C70F496CEA0FF0765E4ED7E014F1A2C7B394F7438C887C094C62885F5B9CD2822B0A9BB83C45471076CA5CF47954C0D5C46D4B45AA7AD5910D57CD2AF
Malicious:	false
Reputation:	low
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": "Tapahtumaa ei voi suorittaa loppuun. Yrit. my.hemmin uudelleen.".. },.. "please_sign_in": {.. "message": "Kirjaudu sis..n Chromeen.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	692
Entropy (8bit):	4.519947404204655
Encrypted:	false
SSDEEP:	12:1HEJADlbGGADlb+WYpU34hTUT+dgHfZAFFZO8ZpU34hTjzeT03OytnmHQnJvYHf9:1HEYah6WYp7TUSoxOS8Zp7TOsO4wXX2w
MD5:	0CA8EE1D816E684D781E7DF18C18455D
SHA1:	F711596B4049CBAA99296AD3755CCC0E79D47051
SHA-256:	CA9739F4FA8514C8669AE6221842B1F5D148BD80492888CECBA7410CB32225A8
SHA-512:	3BE7CA9E781E0D0BF17F3E894FD75CF7FCCCB0BEEB9A0FC7C17D3F5BC142B662ACFDC7254AA75D2AF9933D0FB70057297E29E8A5815F29469906F9DC8F3390 2E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "app_name": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Kasalukuyang hindi available ang app.".. },.. "craw_connect_to_network": {.. "message": "Mangyaring kumonekta sa isang network.".. },.. "iap_unavailable": {.. "message": "Kasalukuyang hindi available ang Mga Pagbabayad na In-App.".. },.. "jwt_retrieve_failed": {.. "message": "Hindi makumpleto ang transaksyon. Pakisubukang muli sa ibang pagkakataon.".. },.. "please_sign_in": {.. "message": "Mangyaring mag-sign in sa Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	708
Entropy (8bit):	4.573921094123133
Encrypted:	false
SSDEEP:	12:1HEJALf/nbGGALf/nb+WYpU34Owdgbyb+dgdQjO8ZpU34ITQpGnbyb03Oynha3Gg:1HE4Hna1Hn6WYpNdgpY8ZpSTQwnBOshi
MD5:	BE3C2C2BF4551641D84A60EC9F1E6E15
SHA1:	AAB0C8097A5B35FA40F2B137E1889677CB105B40
SHA-256:	DDDDAA9A83C34BF2874CBBE0214351C15E2620C0DC3863B2B79C4ACF9C2A4637
SHA-512:	4F263F78B61075525FA94493FB5C6297A53395F61E630E2DE81F14393BD2D5B3E687F35BF321C1009C0AF9A230A0C49D188F68AA7F2E4F61F3358596A86A6C2D
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "app_name": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "craw_app_unavailable": {.. "message": "Application indisponible pour le moment.".. },.. "craw_connect_to_network": {.. "message": "Veuillez vous connecter . un r.seau.".. },.. "iap_unavailable": {.. "message": "Les paiements via l'application ne sont pas disponibles pour le moment.".. },.. "jwt_retrieve_failed": {.. "message": "Impossible de finaliser la transaction. Veuillez r.essayer plus tard.".. },.. "please_sign_in": {.. "message": "Veuillez vous connecter . Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\CRX_INSTALL_locales\hi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\CRX_INSTALL_locales\hi\messages.json	
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	955
Entropy (8bit):	4.664681647654927
Encrypted:	false
SSDEEP:	24:1HEs07J0JWYp9vnCSVLP8Zp6CsOjSvzdlmLzSLm:Wh7qgYp1CMLUph1jSv3mLzSLm
MD5:	8CFF82EB516A180F2BFA22DA0B18D9E7
SHA1:	87053836FFDB4103302D17D221BC76C8DB842A28
SHA-256:	EA0020B530B3E047559248C076B54E90EFEF6A233DA130D5F43445C25BCB2008
SHA-512:	DEADC807AE4F254A4A73D31A12C2BC274D0E2E25413A36DCEF565B155BA72037BD3A14B5067A8B0325A86CB126C3B223A7DDFC66D5981CB48F1975E962AFBE E6
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome ... .".. },.. "app_name": {.. "message": "Chrome ... .".. },.. "craw_app_unavailable": {.. "messa ge": "..... .. ..".. },.. "craw_connect_to_network": {.. "message": "..... ....".. },.. "iap_unavailable": {.. "message": "..-.. ....".. },.. "jwt_retrieve_failed": {.. "message": "...-... ....".. },.. "please_sign_in": {.. "message": "..... Chrome ... .".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	633
Entropy (8bit):	4.602004893403632
Encrypted:	false
SSDEEP:	12:1HEJGiimxmbZGGGiimxmbZ+WYpU34OBOEuhopIO+dgcapZO8ZpU34GiiZrMrQphc:1HE4H4TH8WYpNjTta28ZpQVLP0SOv3XD
MD5:	5A777479C6072C009FF6EEEDD167B205
SHA1:	D4B509E3AD07A7EABEB32E7EF06166D5A60D4B54
SHA-256:	1650A45BF772FA06F99EB68015FD356B8BCC1DD4AEE0A4213C626BA2216D9D43
SHA-512:	8E13AD3DF747E6F082D813E4BC5321F1AB1A6D8C203EB9E0A01EF8B5B496DE74F5FCAE956239C85A18DD26399847177325FAADD84C60AC507818E9F26BBB53 D
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "app_name": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "craw _app_unavailable": {.. "message": "Aplikacija trenuta.no nije dostupna.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se s mre.om.".. },.. "iap_unavailable": {.. "message": "Pla.anje u aplikaciji trenuta.no nije dostupno.".. },.. "jwt_retrieve_failed": {.. "message": "Transakcija nije dovr.ena. Poku.ajte ponovo kasnije.".. },.. "please_sign_in": {.. "message": "Prijavite se na Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	710
Entropy (8bit):	4.727128297637916
Encrypted:	false
SSDEEP:	12:1HEJVJiGGVJi+WYpU34Hpo9O+dgMmfgijO8ZpU34Huo9O03OyeFRLpzS0suYBIAd:1HEVrk5WYpQzTUg/8ZpwoXODpFGIAd
MD5:	C3AD6A15FC6370A3D3E18A313AB22237
SHA1:	E1FB9248DA5E0607882DBCC1819DE5B67F8614F5
SHA-256:	F895E3D151B52E817531C21F877689109B92EC2DA5F0F1A677CC8219A6315373
SHA-512:	F3DEDD20971FCAC9FED5C403E6452C0562148BFD08F81128161F83459A2686127590E997B584F89FA250666C9A82EB3F0C561DA0CCFA1444DC1796DA4404AA0
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. },.. "app_name": {.. "message": "Chrome Internetes .ruh.z Fizet.si r endszere".. },.. "craw_app_unavailable": {.. "message": "Az alkalmaz.s jelenleg nem .rhet. el.".. },.. "craw_connect_to_network": {.. "message": "K.rj.k, csatlako zzon egy h.l.zathoz.".. },.. "iap_unavailable": {.. "message": "Az alkalmaz.son bel.li fizet.s jelenleg nem .rhet. el.".. },.. "jwt_retrieve_failed": {.. "message": "A tranzakci.t nem siker.lt befejezni. Pr.b.lja .jra k.s.bb.".. },.. "please_sign_in": {.. "message": "Jelentkezzen be a Chrome-ba.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	617
Entropy (8bit):	4.445455113766944
Encrypted:	false
SSDEEP:	12:1HEJs25bGGs25b+WYpU34ORBHAeSJ+dgkmO8ZpU34s22C/SzFAs03OyN4KolFYjt:1HEBaA6WYpaHFH8ZptOYODhuD
MD5:	8B27E83CA394C9D73B58C33910881F01

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\CRX_INSTALL_locales\id\messages.json	
SHA1:	007F3DFA6CACB4D96D5C057930A8D45241F9908F
SHA-256:	EE050F8DE5EC6F49D4B8E5CE1A432BDE43B4EAFA0963C045D8A097AB622D96E8
SHA-512:	EF1ACFADA29E971E6468804D63AE490C7046B20B946B39F572BC1FF5BAB480C93F97C85E5DC3484EC1A0C3A4CA35FBBF3C217102A9EA269B7AE353C17C5CFF BA
Malicious:	false
Reputation:	low
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": "Transaksi tidak dapat diselesai kan. Coba lagi nanti.".. },.. "please_sign_in": {.. "message": "Harap masuk ke Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	622
Entropy (8bit):	4.505455493845955
Encrypted:	false
SSDEEP:	12:1HEJsqd/bGGsqd/b+WYpU34OcX4+dgUvIO8ZpU34vq703OynjbeQfL6CYsD:1HEXd/aKd/6WYpZrv58ZpskOsjhDD
MD5:	DCA488BB7ACBBDC0FF63246899F85933
SHA1:	9408CEF9B8C2EB24E66700E7CD6405A232803EDE
SHA-256:	43267C5F695BCD2A31360D6B03699EFD27D9F53215479042642F42F8612EB7BB
SHA-512:	484793E3F366EBBCC59625BDA5BEAF4B4A0FB58E9CAEB9700BC5A7B74F7ED13B51E72AF46ACD609C137AF84E776FEC3ECF9B256C58F7B5731C8871D3DCD0A CDB
Malicious:	false
Reputation:	low
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": "Impossibile completare la transazione. Riprova pi. tardi.".. },.. "please_sign_in": {.. "message": "Accedi a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	778
Entropy (8bit):	5.228857160227492
Encrypted:	false
SSDEEP:	12:1HEJ07uGG07u+WYpU34DB+dgnsVztO8ZpU34MwiB03Oypv/Ik589dwttYmSH:1HEcnDNWYp1kxU8Zp2wiqOoIk589QnSH
MD5:	5FB01096BE49765965AE2148455ADD74
SHA1:	BA73186A0A0D81A20D2830432DEDA52A0527C9A1
SHA-256:	C6BE17C57BB3500A02F98F8A218B120F63D4F29BAE2A960210DC14656D37CBE3
SHA-512:	4A365178D73EA46C9FC6E7A28D1EF13FD89F8E42239231D9DDFE9BF2CA68713C015FC4C76AE25A6497D9287EF693E4A317596AF5A4063B863828F0C13BD1504
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome ....."".. },.. "app_name": {.. "message": "Chrome ....."".. },.. "craw_app_unavailable": {.. "message": "....." ....."".. },.. "craw_connect_to_network": {.. "message": "....."".. },.. "iap_unavailable": {.. "message": "....."".. },.. "jwt_retrieve_failed": {.. "message": "....."".. },.. "please_sign_in": {.. "message": "Chrome ....."".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	669
Entropy (8bit):	5.2871011966880666
Encrypted:	false
SSDEEP:	12:1HEJ1GG1+WYpU34K3aT+dgh8d0HTO8ZpU34KaNkaT03OyhMcg/QeHTY/YeHx:1HEajWYpc3aSl0Hq8Zpc6kasOeMcgIeY
MD5:	087B93BE3016C3C7CBB1753C38E337EF
SHA1:	01F9EAB9C8E614DDAC5AE7CAEB564E4803586753
SHA-256:	F49A563FD4545BE61DBB720325E4DF86E2C6674F9EBC53C24E190F291E44E364
SHA-512:	4B9301150BD8601D1D70DD6F4403762D7D7D538DD97E088B73A5281820D017987F8607385DFD1D14DF49E68F99F399B1A700D39BFB71CBFA1265E1033F84F752
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\CRX_INSTALL_locales\ko\messages.json	
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": "... ....".. },.. "please_sign_in": {.. "message": "Chrome. .....".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	686
Entropy (8bit):	4.727132438660756
Encrypted:	false
SSDEEP:	12:1HEJpqHnkGGpqHnk+WYpU346M+dgV6O8ZpU34WzSWz03OyFMm/FYx:1HELqHtKqHPWYpM3A8ZpwGzOCu
MD5:	FC774504DD2DCE69B8DD55AFC02AF58D
SHA1:	1D31DC3F3DA200AC24026B2F542BB30B52CE6B16
SHA-256:	6F976F9ED367A7B85CE9B1DE0CB3B228E9E983E3FBBA4D3CD35A59BCA58EDBBC
SHA-512:	8A832DFCB0326D731FDC7D0D33F59724239A1BAB6E9780C8032925E411C184062F71710D217B9F4FA079D5247BED051897EBA12AE2A7AEE148C903B445D736D
Malicious:	false
Reputation:	low
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": "Nepavyko u.baigti operacijos. V.liau bandykite dar kart..".. },.. "please_sign_in": {.. "message": "Prisijunkite prie .Chrome..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	699
Entropy (8bit):	4.685697694118083
Encrypted:	false
SSDEEP:	12:1HEJFhVbGGFhVb+WYpU34wDoz+dgGedBO8ZpU34wF03OyNrEuIjYGYID:1HENQkkWYp2Doy/em8Zp2WOZuIBYID
MD5:	4FDBF2298A69836E8F76B3374E20DDA7
SHA1:	445DFC32C1D748D3B100D1211D2A2ABCD26C5834
SHA-256:	5E3FEFF17B28742EE0D5882D94C7A31D13CDB1D9C1524FE69F045AB109B2A173
SHA-512:	5058F9AE32F655DE90BB4FEA9FA2D75494D3E11E7AB6EA54F6A78D8AF12CC386B1CC789DB9C1308C716DFBBCC04697676D57CBC5922125532E0555D765E7A17
Malicious:	false
Reputation:	low
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": "Transakciju n evar.ja pabeigt. L.dzu, v.l.k m..iniet v.lreiz.".. },.. "please_sign_in": {.. "message": "L.dzu, pierakstieties p.rl.k. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	644
Entropy (8bit):	4.587522520391651
Encrypted:	false
SSDEEP:	12:1HEJhiOGGhiO+WYpU34OHSN+dgFjdGFZO8ZpU34JgdN03OyN3L8AebYiD:1HEDiHIitWYpCYJ8ZpD1OcL8TD
MD5:	8DF502C935CB5F2C61F7B9EFD6426CF5
SHA1:	31D25CF9B1DC6CDBA07203C107AA1233987D6FFF
SHA-256:	AB56E763119222142A2A69B694238E7C2069F03D909623B7DA25BEAB87494A8A
SHA-512:	3E3F4C956863355282B2C6F31419950A325490027FC839D3881897B7B102DE35953DDD33F417AD8BD89544801A1B378D436C871A592F428DE236BA9B682F5B5B
Malicious:	false
Reputation:	low
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": "Transaksjonen kunne ikke fullf.res. Pr.v p. nytt senere.".. },.. "please_sign_in": {.. "message": "Du m. logge p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\CRX_INSTALL_locales\nl\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\CRX_INSTALL_locales\nl\messages.json	
Category:	dropped
Size (bytes):	642
Entropy (8bit):	4.477340419637416
Encrypted:	false
SSDEEP:	12:1HEJJQGkbGGJQGkb+WYpU34OQKJT+dgiXUmvFZO8ZpU34g7JT03OyjnpSglzYMD:1HErxkaqxk6WYptndXI8ZpTOQ7D
MD5:	F7739EB95F617BFC907FD1D245B49329
SHA1:	D7E6850E8EE0743726BB9CBFE0CDC68F2272D188
SHA-256:	D614E1F67703BC80B0DBEB0896C87E31466E3E3E668A41364EEA7478A8049CB2
SHA-512:	F3E5386F3A70FE8E55FF4CD64F4A6B988F9B3890A6155EBAFCCB09DE128A538DCC1083A3B3CD83977A87B7C20CBCFDA15E072591631784196B004C18917231B
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalingen via Chrome Web Store".. },.. "app_name": {.. "message": "Betalingen via Chrome Web Store".. },.. "cr aw_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": "De transactie kan niet worden voltooid. Probeer het later opnieuw.".. },.. "please_sign_in": {.. "message": "Log in bij Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	666
Entropy (8bit):	4.731175547924324
Encrypted:	false
SSDEEP:	12:1HEJbiVbGGbiVb+WYpU34OBHlBi9+dgQUg6O8ZpU34bdbfiIu03OyFLQz9NnuOYk:1HE5iVauiV6WYpIAYr8ZpxFiaOEt50D
MD5:	B0329570F687126C3D9D26FD4279A107
SHA1:	DCF852F8E558C9445AE3598B814226D8C756932B
SHA-256:	9A50EB2C558B250F198F3D1EED232056D3BF8C4463DCEFF37D99579381C84118
SHA-512:	CFB4EC0E5FFD21EC85F7EB47F9B2D394C7C7F59B7BA425B8B0FC8C38D9B844AFA12E3003FED3A588BF694547B4316A891FA26C5EB75CBD473FBE57759F37B9 ED
Malicious:	false
Reputation:	low
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": "Nie uda.o si. zrealizowa. transakcji. Spr.buj ponownie p..niej.".. },.. "please_sign_in": {.. "message": "Zaloguj si. w Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	667
Entropy (8bit):	4.5430939640446315
Encrypted:	false
SSDEEP:	12:1HEJsc/bGGsc/b+WYpU34OLw+dgn/KzO8ZpU34FjIBMwGRO03OyFK46XEn6IkYNX:1HEb/a8/6WYp4mZ8Zp7cKlOZ46U6IptD
MD5:	F39681D5543FB19D168EEBE59277C73B
SHA1:	B279538A6B837A0930CD4CD86200792B58E10454
SHA-256:	619631AA6317854DF7FE928288E3A13B2AEAEFAB2F2B46F019F68856E1B02B1E
SHA-512:	E4F93BC1FEC189B3CFC7BC9B68DD2E4CBF54495D98C58053FCBCCD31CB6951AA4D5C008B9044EF98CD5040518918A810ED22D200FA267D1AB34564DA021B3 3C
Malicious:	false
Reputation:	low
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": "N.o foi poss.vel concluir a transa..o. Tente novamente mais tarde.".. },.. "please_sign_in": {.. "message": "Fa.a login no Google Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	661
Entropy (8bit):	4.57627334449273
Encrypted:	false
SSDEEP:	12:1HEJsZUkbGGsZUkb+WYpU34OAE+dgqxKzO8ZpU34rEpBPPO03OyFK46XEn6IkYLD:1HEmUka5Uk6WYpFvdxZ8ZpSTPPlOZ46I
MD5:	EFCAC911642CA7FAF70B8807891387D4

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\CRX_INSTALL_locales\pt_PT\messages.json	
SHA1:	9F603B7AE7A06D83540B4C6B2EF5955C8ECB7C26
SHA-256:	0327B23F28CEC110209093E1305FF1EFE550C04AE977C31A3E1D5AFB2098BD7F
SHA-512:	72F337AE3BBB1B53C75CB0BD10A2322DF520A9F02E69B641EC6DB50907EFD89BE16576D3FA891BB1C100195522C19C1DB947C7ABB1B2974B2759D52E36E895(1
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamentos via Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos via Chrome Web Store".. },.. "cr aw_app_unavailable": {.. "message": "Aplica..o atualmente indispon.vel.".. },.. "craw_connect_to_network": {.. "message": "Ligue-se a uma rede.".. },.. "iap_unavailable": {.. "message": "Os Pagamentos na Aplica..o est.o atualmente indispon.veis.".. },.. "jwt_retrieve_failed": {.. "message": "N.o foi poss.vel concluir a transa..o. Tente novamente mais tarde.".. },.. "please_sign_in": {.. "message": "Inicie sess.o no Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	668
Entropy (8bit):	4.650567255288544
Encrypted:	false
SSDEEP:	12:1HEJqJrJZGGqJrJZ+WYpU344HIx2Z+dgrVPlZO8ZpU34qT7hI3O03Oy/r6rjJSZR:1HEC4D8WYpKow8WV68ZpKhoOWr6rj8CY
MD5:	AC696B33EC1AFDAE3A4A3E2029E92CCB
SHA1:	2B1D6F49C25A082C876E98C71DF96CAF4D1A1681
SHA-256:	E7829B9A2FC8F518340A97A09C537608DB005EB265B670581682728E0FB0DA41
SHA-512:	A4CCFF6C003083889C3305C4A3E466E76D242746543367E5555A694A6921C93017494BF55E8D09BB693A6EB540E8B12A1773E8A5EB6A3C0FFD97188BB712B4A7
Malicious:	false
Reputation:	low
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": "Tranzac.ia nu s-a putut finaliza. .ncearc. din nou mai t.rziu.".. },.. "please_sign_in": {.. "message": "Conecteaz.-te la Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\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):	783
Entropy (8bit):	4.868660175371157
Encrypted:	false
SSDEEP:	24:1HElOJHZMq4uOJHZMq8WYpdWJ/YGHq8ZptNWgOIF5x07ZqD:WlT7uTgYp6hvptNe85e7UD
MD5:	7A151C71B963B0547E30005DF632B5A2
SHA1:	AB9D0B08786AF05AEAE7DAD971934B82C21D38D5
SHA-256:	6FE9E5A1B0C425766582273747F85911C40D8EE125CD609209BA1E3C706EF6E8
SHA-512:	37699BF04408A5EC4FED3321188B6FECC04D1D713305DABE1BE826D131DA180D1B92C138428BA2411E551B01F75B3A4C2597BB83DB4C59782C169642A5BE6F1
Malicious:	false
Reputation:	low
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": "..... ....".. },.. "please_sign_in": {.. "message": "..... . Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\CRX_INSTALL_locales\sk\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):	4.731089071117101
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34ORO+dgmmCO8ZpU34yH7u2Z03OyNnSyfuoCTYCUAi0D:1HEl4G8WYpetPmD8ZpcH7aO0bf72UeD
MD5:	C3DC2B3DC1DFF033F0687C6FF017BA39
SHA1:	E50BBB328E2A500BED3590DBBC1F7378443A7C03
SHA-256:	E2CD4F04332E33D5C733CACEADE0512ADDC1401A0EC36549FC53B066BB99A220
SHA-512:	52938FC8450D5B59241434ADBEEE982C12613DBCF9AF44371784B6A6FB78B9E0D01D1095692F3A1EAE5B042A193092B5D75631261FC2BF28014E42AB0DB6DC8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\CRX_INSTALL_locales\sk\messages.json	
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplik.cia moment.lne nie je dostupn..".. },.. "craw_connect_to_network": {.. "message": "Pripojte sa k sieti.".. },.. "iap_unavailable": {.. "message": "Platby v aplik.cii moment.lne nie s. k dispoz.cii.".. },.. "jwt_retrieve_failed": {.. "message": "Transakciu nebolo mo.n. dokon.i.. Sk.ste to znova nesk.r.".. },.. "please_sign_in": {.. "message": "Prihl.ste sa do prehliada.a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\CRX_INSTALL_locales\sl\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):	642
Entropy (8bit):	4.54448147529131
Encrypted:	false
SSDEEP:	12:1HEJGcyvmbZGGGcyvmbZ+WYpU34OBOEtf+dgca1ZO8ZpU34GcQArERff03OyNrzo:1HE4cyY4TcyY8WYpNoWa1w8ZpQcQ6Af9
MD5:	E9FD187A41491AB6CB1A62D1FB704C31
SHA1:	F158189AB73A614C84FA42C0CA21595591A1D418
SHA-256:	744BE9A108C755A6FBCADF571F8A319B75E9076F47BA0C62A1354134DD78DDFE
SHA-512:	AE05D6AE24CF4687C3F3A1E185386D945BFEFD1FB1A383D34204738F07E6ED910CE4C5F22CFE800FC2C45B16829EDEB6669B4257620730AC5C77D443B6E61E4B
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pla.ila v spletni trgovini Chrome".. },.. "app_name": {.. "message": "Pla.ila v spletni trgovini Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikacija trenutno ni na voljo.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se z omre.jem.".. },.. "iap_unavailable": {.. "message": "Pla.ila v aplikacijah trenutno niso na voljo.".. },.. "jwt_retrieve_failed": {.. "message": "Transakcije ni bilo mogo.e dokon.ati. Poskusite znova pozneje.".. },.. "please_sign_in": {.. "message": "Prijavite se v Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\CRX_INSTALL_locales\sr\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):	812
Entropy (8bit):	4.85495461699779
Encrypted:	false
SSDEEP:	24:1HEKsb59sbTWYplx4Xud8Zpy1mNOM4YDYD:WKu59uyYplOuSpyYkM4JD
MD5:	903D486DA74BB1A637D94C8ABF8A3462
SHA1:	4036AEDC1823F9EC05BF3B0CBC5594C86AC26065
SHA-256:	0EF65E44921254DDEEEB7DC1DDC8A9ED8A9E0F5B7B8152EE9A0121E2023932D4
SHA-512:	4B6166335370284E1E69572A34C79838C887A8174A35C29B066DEF8FFAF8C450AAFBC7E0E0AE6F26D742B6D367893E224D693799501A6E95102DF26960FAB7B4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... . Chrome ...-.....".. },.. "app_name": {.. "message": "..... . Chrome ...-.....".. },.. "craw_app_unavailable": {.. "message": "..... .. ..".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": "..... . ...".. },.. "jwt_retrieve_failed": {.. "message": ".... ....".. },.. "please_sign_in": {.. "message": "..... .. . Chrome.".. }..}..

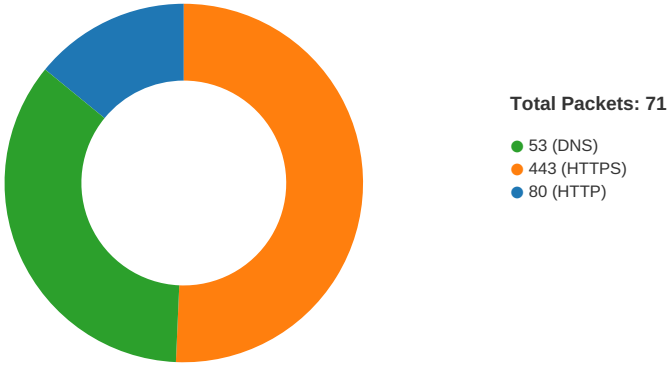
C:\Users\user\AppData\Local\Temp\scoped_dir1304_1913289536\CRX_INSTALL_locales\sv\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	649
Entropy (8bit):	4.551181507608622
Encrypted:	false
SSDEEP:	12:1HEJJMkbGGJMkb+WYpU34OACwz+dgNPGFZO8ZpU34JgpXLSb03OyNzfUzVYLdID:1HErMkaqMk6WYpTOcb8ZpDgdZOOfOKID
MD5:	79733424BB4B9547D18D8395A4221CBF
SHA1:	28B49907E1DB3D1FB5850DA4167A010E2288D082
SHA-256:	401FF6EE0C8B1EB757F78890D00456054C844609C4C5E5F02489AF731199AB9F
SHA-512:	A4AE283BEDF5750798724D232FEC3737EA04F456E1C87532602D7048BB5E7E5A7042F0A08C4FCEB6466D68EFD8BEE9DDD7D6D78789B7ED46B2A917167EC30ED
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalning via Chrome Web Store".. },.. "app_name": {.. "message": "Betalning via Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Appen .r inte tillg.nglig f.r tillf.llet.".. },.. "craw_connect_to_network": {.. "message": "Anslut till ett n.tverk.".. },.. "iap_unavailable": {.. "message": "Betalning i appen .r inte tillg.ngligt f.r n.rvarande.".. },.. "jwt_retrieve_failed": {.. "message": "Transaktionen kunde inte slutf.ras. F.rs.k igen senare.".. },.. "please_sign_in": {.. "message": "Logga in i Chrome.".. }..}..

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 14:21:58.634113073 CET	49723	80	192.168.2.3	172.67.173.29
Nov 29, 2020 14:21:58.636959076 CET	49727	80	192.168.2.3	172.67.173.29
Nov 29, 2020 14:21:58.656642914 CET	80	49723	172.67.173.29	192.168.2.3
Nov 29, 2020 14:21:58.656810999 CET	49723	80	192.168.2.3	172.67.173.29
Nov 29, 2020 14:21:58.659064054 CET	80	49727	172.67.173.29	192.168.2.3
Nov 29, 2020 14:21:58.659148932 CET	49723	80	192.168.2.3	172.67.173.29
Nov 29, 2020 14:21:58.659178972 CET	49727	80	192.168.2.3	172.67.173.29
Nov 29, 2020 14:21:58.681417942 CET	80	49723	172.67.173.29	192.168.2.3
Nov 29, 2020 14:21:59.087512016 CET	80	49723	172.67.173.29	192.168.2.3
Nov 29, 2020 14:21:59.087554932 CET	80	49723	172.67.173.29	192.168.2.3
Nov 29, 2020 14:21:59.087622881 CET	49723	80	192.168.2.3	172.67.173.29
Nov 29, 2020 14:21:59.287894011 CET	49723	80	192.168.2.3	172.67.173.29
Nov 29, 2020 14:21:59.310188055 CET	80	49723	172.67.173.29	192.168.2.3
Nov 29, 2020 14:21:59.642565012 CET	80	49723	172.67.173.29	192.168.2.3
Nov 29, 2020 14:21:59.642615080 CET	80	49723	172.67.173.29	192.168.2.3
Nov 29, 2020 14:21:59.642687082 CET	49723	80	192.168.2.3	172.67.173.29
Nov 29, 2020 14:22:09.540688992 CET	49727	80	192.168.2.3	172.67.173.29
Nov 29, 2020 14:22:09.563008070 CET	80	49727	172.67.173.29	192.168.2.3
Nov 29, 2020 14:22:09.563122034 CET	49727	80	192.168.2.3	172.67.173.29
Nov 29, 2020 14:22:09.620093107 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:09.641242981 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:09.641376972 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:09.641593933 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:09.662645102 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:09.675898075 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:09.675952911 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:09.675992966 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:09.676031113 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:09.676104069 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:09.676147938 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.320321083 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.320431948 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.320557117 CET	49749	443	192.168.2.3	216.58.215.225

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 14:22:10.341854095 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.342169046 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.342245102 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.342292070 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.342339993 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.342355967 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.342381001 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.342422009 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.342461109 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.342489004 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.342519999 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.342525005 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.342529058 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.343405008 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.343460083 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.343482971 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.343549013 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.344367981 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.344413996 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.344489098 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.344511032 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.345448971 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.345489025 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.345534086 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.346453905 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.346492052 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.346518040 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.346560001 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.346569061 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.347568035 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.347605944 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.347635984 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.347687960 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.348628044 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.348704100 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.348705053 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.348762989 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.349664927 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.349729061 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.363399982 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.363445044 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.363496065 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.363919020 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.363960028 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.364000082 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.364945889 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.364986897 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.365031958 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.365995884 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.366038084 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.366079092 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.367089033 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.367130995 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.367176056 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.368144035 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.368184090 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.368227959 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.369188070 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.369266987 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.369268894 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.370265961 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.370307922 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.370341063 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.371290922 CET	443	49749	216.58.215.225	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 14:22:10.371367931 CET	49749	443	192.168.2.3	216.58.215.225
Nov 29, 2020 14:22:10.371830940 CET	443	49749	216.58.215.225	192.168.2.3
Nov 29, 2020 14:22:10.371870995 CET	443	49749	216.58.215.225	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 14:21:49.414350986 CET	60100	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:21:49.441704988 CET	53	60100	8.8.8.8	192.168.2.3
Nov 29, 2020 14:21:50.231637001 CET	53195	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:21:50.258872032 CET	53	53195	8.8.8.8	192.168.2.3
Nov 29, 2020 14:21:51.092600107 CET	50141	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:21:51.128005981 CET	53	50141	8.8.8.8	192.168.2.3
Nov 29, 2020 14:21:52.110296011 CET	53023	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:21:52.145659924 CET	53	53023	8.8.8.8	192.168.2.3
Nov 29, 2020 14:21:52.999906063 CET	49563	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:21:53.035552979 CET	53	49563	8.8.8.8	192.168.2.3
Nov 29, 2020 14:21:55.143125057 CET	51352	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:21:55.170461893 CET	53	51352	8.8.8.8	192.168.2.3
Nov 29, 2020 14:21:56.286946058 CET	57084	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:21:56.314045906 CET	53	57084	8.8.8.8	192.168.2.3
Nov 29, 2020 14:21:58.286062956 CET	50540	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:21:58.313415051 CET	53	50540	8.8.8.8	192.168.2.3
Nov 29, 2020 14:21:58.581155062 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:21:58.582144976 CET	53034	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:21:58.585942984 CET	57762	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:21:58.588864088 CET	55435	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:21:58.590046883 CET	50713	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:21:58.621284008 CET	53	57762	8.8.8.8	192.168.2.3
Nov 29, 2020 14:21:58.624855042 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 14:21:58.625786066 CET	53	53034	8.8.8.8	192.168.2.3
Nov 29, 2020 14:21:58.632030010 CET	53	55435	8.8.8.8	192.168.2.3
Nov 29, 2020 14:21:58.634228945 CET	53	50713	8.8.8.8	192.168.2.3
Nov 29, 2020 14:21:58.943850994 CET	56132	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:21:58.989294052 CET	53	56132	8.8.8.8	192.168.2.3
Nov 29, 2020 14:21:59.057256937 CET	58987	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:21:59.094723940 CET	53	58987	8.8.8.8	192.168.2.3
Nov 29, 2020 14:21:59.103957891 CET	56579	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:21:59.147209883 CET	53	56579	8.8.8.8	192.168.2.3
Nov 29, 2020 14:21:59.974337101 CET	60633	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:22:00.001672029 CET	53	60633	8.8.8.8	192.168.2.3
Nov 29, 2020 14:22:09.543011904 CET	56130	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:22:09.586488962 CET	53	56130	8.8.8.8	192.168.2.3
Nov 29, 2020 14:22:10.767261982 CET	56338	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:22:10.794440031 CET	53	56338	8.8.8.8	192.168.2.3
Nov 29, 2020 14:22:12.242819071 CET	59420	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:22:12.278793097 CET	53	59420	8.8.8.8	192.168.2.3
Nov 29, 2020 14:22:19.029025078 CET	58784	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:22:19.056257010 CET	53	58784	8.8.8.8	192.168.2.3
Nov 29, 2020 14:22:19.504502058 CET	63978	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:22:19.531569958 CET	53	63978	8.8.8.8	192.168.2.3
Nov 29, 2020 14:22:24.083975077 CET	62938	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:22:24.145689011 CET	53	62938	8.8.8.8	192.168.2.3
Nov 29, 2020 14:22:33.250294924 CET	55708	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:22:33.294101954 CET	53	55708	8.8.8.8	192.168.2.3
Nov 29, 2020 14:22:38.873694897 CET	56803	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:22:38.900836945 CET	53	56803	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 29, 2020 14:21:58.585942984 CET	192.168.2.3	8.8.8.8	0x53f	Standard query (0)	testgvbgjb hjb.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 29, 2020 14:22:09.543011904 CET	192.168.2.3	8.8.8.8	0x13ef	Standard query (0)	clients2.google usercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 29, 2020 14:21:58.621284008 CET	8.8.8.8	192.168.2.3	0x53f	No error (0)	testgvbgjbhjb.com		172.67.173.29	A (IP address)	IN (0x0001)
Nov 29, 2020 14:21:58.621284008 CET	8.8.8.8	192.168.2.3	0x53f	No error (0)	testgvbgjbhjb.com		104.27.128.199	A (IP address)	IN (0x0001)
Nov 29, 2020 14:21:58.621284008 CET	8.8.8.8	192.168.2.3	0x53f	No error (0)	testgvbgjbhjb.com		104.27.129.199	A (IP address)	IN (0x0001)
Nov 29, 2020 14:22:09.586488962 CET	8.8.8.8	192.168.2.3	0x13ef	No error (0)	clients2.google usercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Nov 29, 2020 14:22:09.586488962 CET	8.8.8.8	192.168.2.3	0x13ef	No error (0)	googlehosted.l.googleusercontent.com		216.58.215.225	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- testgvbgjbhjb.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49723	172.67.173.29	80	C:\Program Files\Google\Chrome\Application\chrome.exe

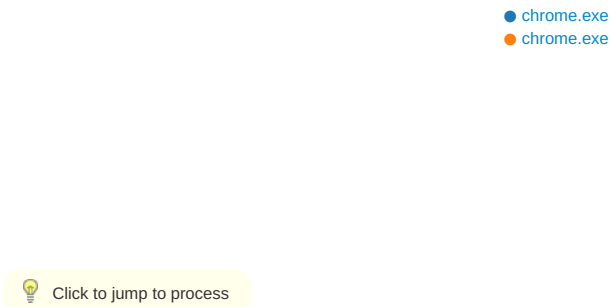
Timestamp	kBytes transferred	Direction	Data
Nov 29, 2020 14:21:58.659148932 CET	105	OUT	GET / HTTP/1.1 Host: testgvbgjbhjb.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Nov 29, 2020 14:21:59.087512016 CET	224	IN	HTTP/1.1 200 OK Date: Sun, 29 Nov 2020 13:21:59 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=de8754fdbb4b9ddc0f8b959b98791b7db1606656118; expires=Tue, 29-Dec-20 13:21:58 GMT; path=/; domain=.testgvbgjbhjb.com; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 06b5c3e78f00000c85df2ed000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=RRA9NfnxvEfFT0lwP8JW8xR2%2Bk32nkWGCy8NRt7IAJawZ%2B82GWdgPXFXAgPnhrKUto2ecIX2l2G3Yx5CNM0%2BD9rLeWVz8U6jab8mw0WOPf41oQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5f9ca285bfb10c85-AMS Content-Encoding: gzip Data Raw: 32 30 35 0d 0a 1f 8b 08 00 00 00 00 00 00 03 5c 53 5d 8b 14 31 10 7c cf af 28 f7 49 e1 76 ee db 13 99 5b d0 3b d1 7b 11 c1 03 f1 b1 27 d3 3b 09 9b 49 cf a5 93 59 d6 5f 2f 99 5b f5 30 10 42 d2 49 55 75 75 a7 75 79 0c 1b d3 be 5a af 1f 1d a3 97 91 7c 44 f0 71 e7 e3 80 83 14 38 4e 0c af c8 4e ca e0 32 b2 c0 d1 cc e8 98 23 94 33 ca 04 52 4c 94 32 64 0b c2 48 61 e6 94 bd 56 04 4b e3 44 7e 88 8d f9 22 7b 9e 39 9d 20 3b c6 c4 49 25 62 ef 04 53 49 d6 91 72 bf 04 8e 02 b2 0c 43 60 c5 fd d7 ef 48 6c 25 f5 8a 8e f3 be 72 9e 5f dc 34 67 cd 59 73 8e d7 a4 20 a8 8f 3b 27 81 df 18 8a 3d 74 62 eb b7 de e2 e1 9b 62 a4 48 03 f7 e8 0e 2f c1 65 1f 39 35 c0 fd 8b 2d c4 5a 52 2f 91 42 38 a0 28 d7 84 bd fe d3 03 f5 63 09 94 d9 38 3f 38 cc 12 ca c8 5a 33 fe fc e9 11 89 9f 0a 6b d6 7a 31 b3 66 cc 94 bc 14 85 0d 52 7a 28 a7 d9 5b d6 c6 98 0f 8a 20 71 a8 96 bd 24 48 6c d9 cf ac f8 1f bd 3a f0 54 38 f9 45 11 c3 96 94 38 e6 a3 ea bd 0f 01 15 20 ff cd 44 9d 9f aa 8c 29 f1 cc 31 9b 91 82 b7 8b 16 b2 59 92 62 9b 64 44 59 aa 53 33 73 8c 6d c9 25 71 63 cc c3 76 29 39 25 86 95 68 39 45 ee 41 9d 94 fc 2c 96 6c f6 b3 cf 87 fa f0 20 25 21 72 de 4b da 9d a0 0b 64 77 c1 6b 7e 61 b4 a2 4b 3e 0e 7f 1a a9 5a 53 41 7e 70 37 d1 c0 0d 70 47 ca d5 21 e5 be 31 eb f5 c6 b4 8e a9 df 98 36 fb 1c 78 d3 9e 3e af a6 3d 3d 9e 77 d2 1f d0 0d 56 82 a4 db d5 dd c7 ab cb cb eb d5 c6 b4 5b 89 19 ea 7f f1 ed ea f2 ed 0a c7 f8 76 19 35 3e 3d cf 9f 55 f2 54 ba b0 b4 07 a8 ef 13 ab c2 eb 7b f3 ee aa 39 bf 69 ae 2f 9a 8b eb f6 b4 c2 55 d6 4a b7 b0 2f 7f e4 37 00 00 00 ff ff 03 00 e7 11 66 1c 2b 03 00 00 0d 0a Data Ascii: 205\S]1|(lv[;{';lY_/[0BlUuuuyZ|Dq8NN2#3RL2dHaVKD~"{9 ;l%bSIrC`Hl%r_4gYs ;'=tbbH/e95-ZR/B8(c8?8Z3kz 1fRz([q$Hl:T8E8 D)1YbdDYS3sm%qcv)9%h9EA,l %!rKdwk~aK>ZSA~p7pG!16x>==wV[v5>=UT{9i/UJ/7f+

Timestamp	kBytes transferred	Direction	Data
Nov 29, 2020 14:21:59.287894011 CET	927	OUT	GET /favicon.ico HTTP/1.1 Host: testgvbgjbhjb.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Referer: http://testgvbgjbhjb.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: __cfduid=de8754fdbb4b9ddc0f8b959b98791b7db1606656118
Nov 29, 2020 14:21:59.642565012 CET	1001	IN	HTTP/1.1 404 Not Found Date: Sun, 29 Nov 2020 13:21:59 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=14400 CF-Cache-Status: MISS cf-request-id: 06b5c3ea0500000c85619c8000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=ki9ATEH%2F4I0%2BNqBoJbbly%2FMu%2FLQtf0VXof46Nxc6GdKO7HLbAw%2B15MiPfe5i6MaWlzMVg3qb8kYbukLXi%2FyNPGJMcPuKA9s2Zd7%2FeFuGc8qHaQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Vary: Accept-Encoding Server: cloudflare CF-RAY: 5f9ca289aa200c85-AMS Content-Encoding: gzip Data Raw: 65 39 0d 0a 1f 8b 08 00 00 00 00 00 03 4d 8f 41 4f c2 40 14 84 ef fb 2b 9e 9c f4 60 5f c1 1e 38 bc 6c a2 b4 44 92 8a 0d 96 83 c7 2d fb 64 4b a0 5b 77 1f 18 ff bd 69 09 89 d7 99 6f 26 33 74 97 bf 2f ea cf aa 80 d7 fa ad 84 6a fb 52 ae 16 30 79 44 5c 15 f5 12 31 af f3 ab 33 4b 52 c4 62 3d d1 8a 9c 9c 8e 9a 1c 1b ab 15 49 2b 47 d6 59 9a c1 da 0b 2c fd b9 b3 84 57 51 11 8e 10 35 de fe 0e b9 a9 fe c7 b8 a9 56 d4 eb da 31 04 fe 3e 73 14 b6 b0 dd 94 f0 63 22 74 5e e0 6b e0 c0 77 20 ae 8d 10 39 5c 38 24 84 fd d0 14 b4 22 63 6d e0 18 f5 73 6f 76 8e 71 96 64 c9 d3 1c ee 73 6e 5a d3 3d c0 c7 18 00 23 20 1c 65 7f 69 f6 87 c6 1d 9a 64 e7 4f 50 f9 20 30 4f 09 6f 1d 8a 70 1c 49 38 9e 53 7f 4b e5 23 b7 17 01 00 00 0d 0a Data Ascii: e9MAO@+`_8lD-dK[wio&3t/jR0yD\13KRb=I+GY,WQ5V1>sc"t^kw 9\8$"cmsovqdsnZ=# eidOP 0OopI8SK#

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 1304 Parent PID: 4716

General

Start time:	14:21:52
Start date:	29/11/2020
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'http://Testgvbgjbhjb.com'
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: chrome.exe PID: 1564 Parent PID: 1304

General

Start time:	14:21:53
Start date:	29/11/2020
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=1572,7382248617343457090,8884663749363792362,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1708 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Disassembly