ID: 404275
Cookbook: urldownload.jbs
Time: 21:22:50
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

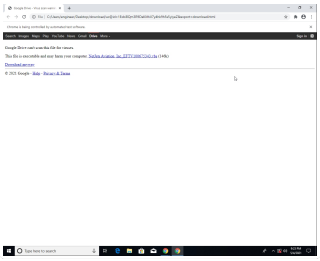
Analysis Report https://drive.google.com//uc?id=1ExbiB…

Overview

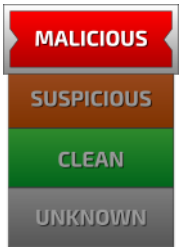
General Information

Sample URL:	http://https://drive.google.com//uc?id=1ExbiBQm3R9DeKMtJJ7y4hk9h5s5yiyeZ&export=download
Analysis ID:	404275
Infos:	

Most interesting Screenshot:



Detection

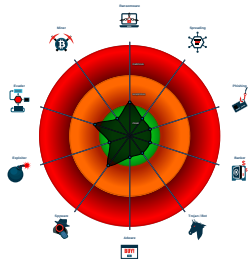


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Snort IDS alert for network traffic (e.…
- Queries the volume information (nam…
- Uses code obfuscation techniques (…

Classification



Startup

- **System is w10x64**
- cmd.exe (PID: 6404 cmdline: C:\Windows\system32\cmd.exe /c wget -t 2 -v -T 60 -P 'C:\Users\user\Desktop\download' --no-check-certificate --content-disposition --user-agent='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko' 'https://drive.google.com//uc?id=1ExbiBQm3R9DeKMtJJ7y4hk9h5s5yiyeZ&export=download' > cmdline.out 2>&1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 6420 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - wget.exe (PID: 6452 cmdline: wget -t 2 -v -T 60 -P 'C:\Users\user\Desktop\download' --no-check-certificate --content-disposition --user-agent='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko' 'https://drive.google.com//uc?id=1ExbiBQm3R9DeKMtJJ7y4hk9h5s5yiyeZ&export=download' MD5: 3DADB6E2ECE9C4B3E1E322E617658B60)
- chrome.exe (PID: 6800 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation -- 'C:\Users\user\Desktop\download\uc@id=1ExbiBQm3R9DeKMtJJ7y4hk9h5s5yiyeZ&export=download.html' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 7000 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1644,12290585205416118591,770383313206273744,131072 --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

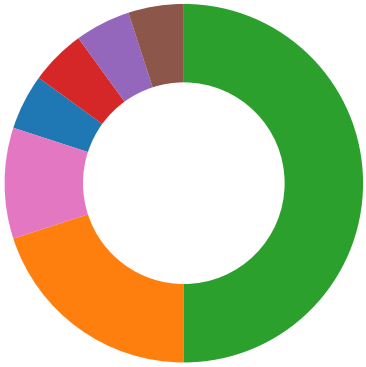
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

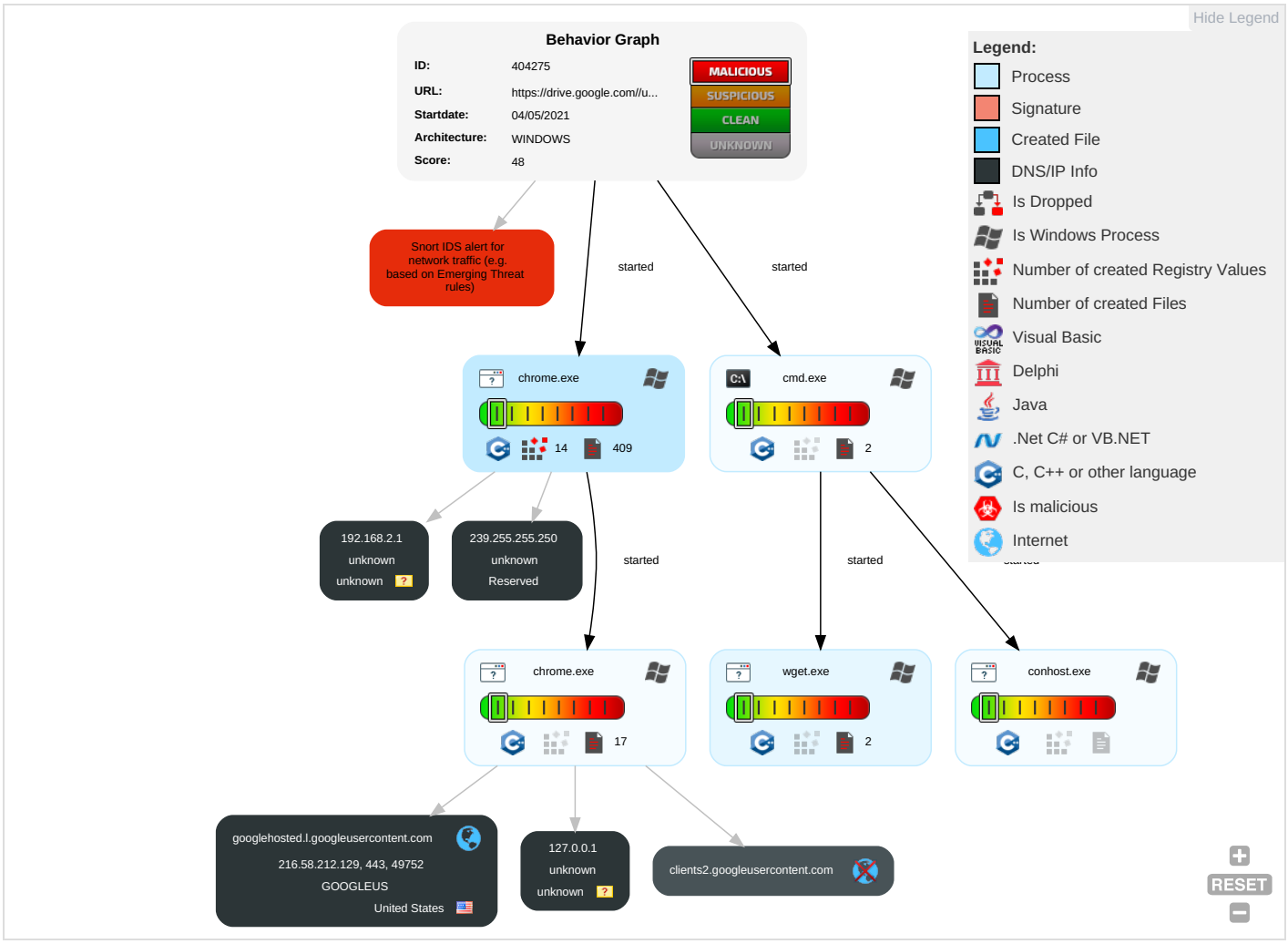
Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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	Im
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 3	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mo Sy Pa
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	System Information Discovery 1 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	De Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Remote System Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	De De Da

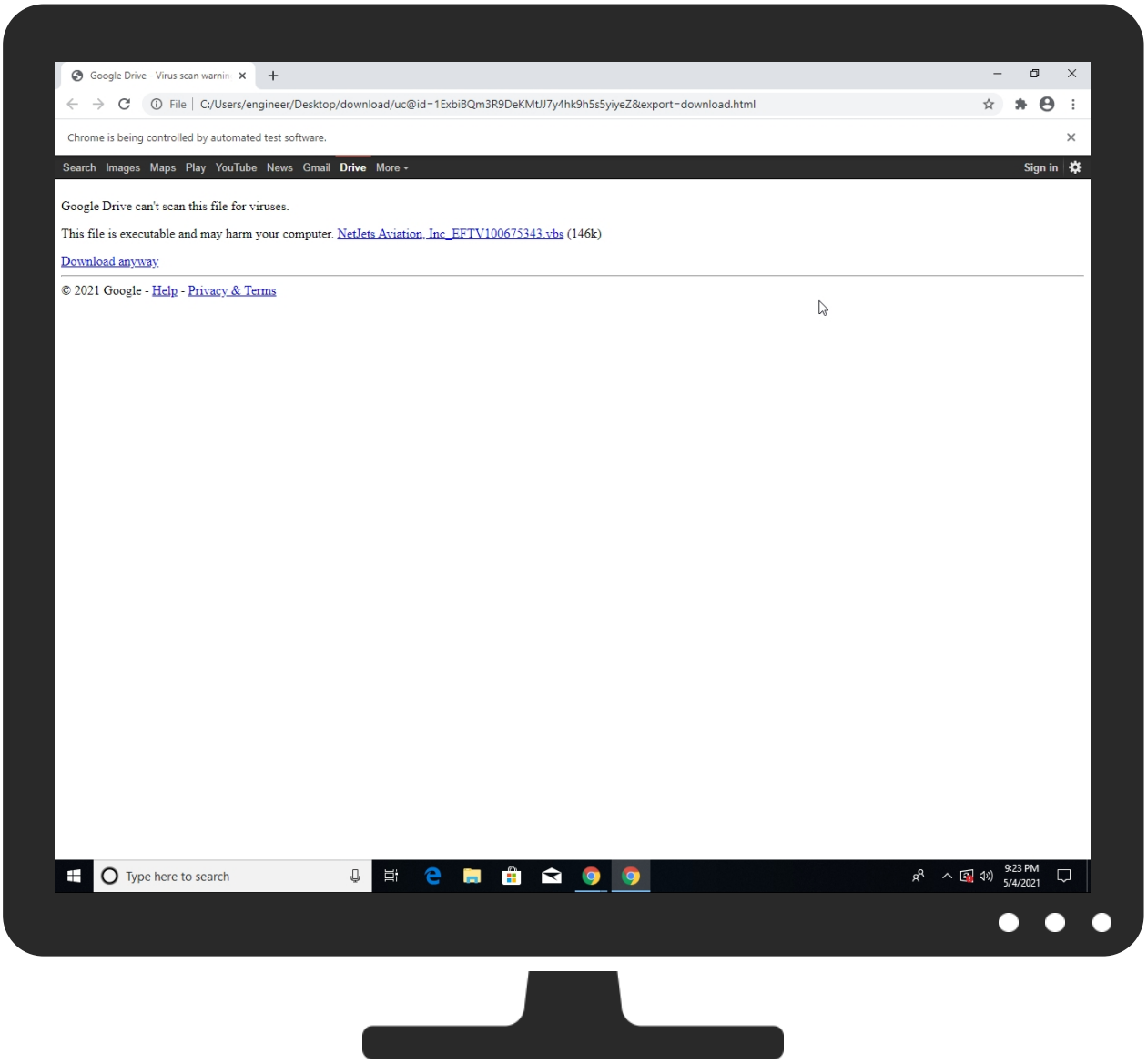
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://drive.google.com//uc?id=1ExbiBQm3R9DeKMtJJ7y4hk9h5s5yiyeZ&export=download	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://pki.goog/gsr1/gsr1.crt	0%	Virustotal		Browse
http://pki.goog/gsr1/gsr1.crt	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	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://crl.pki.goog/gsr1/gsr1.crl0;	0%	Avira URL Cloud	safe	
http://crl.pki.goog/gtsr1/gtsr1.crl-	0%	Avira URL Cloud	safe	
http://crl.pki.goog/gsr1/gsr1.crl	0%	Avira URL Cloud	safe	
http://crls.pki.goog/gts1c3/QqFxbi9M48c.crl	0%	Avira URL Cloud	safe	
http://crl.pki.goog/gtsr1/gtsr1.crl0W	0%	Avira URL Cloud	safe	
http://pki.goog/gsr1/gsr1.crt02	0%	Avira URL Cloud	safe	
http://pki.goog/repo/certs/gts1c3.der	0%	Avira URL Cloud	safe	
http://crl.pki.goog/gtsr1/gtsr1.crly	0%	Avira URL Cloud	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://crls.pki.goog/gts1c3/QqFxbi9M48c.crl0	0%	Avira URL Cloud	safe	
http://pki.goog/repo/certs/gtsr1.der	0%	Avira URL Cloud	safe	
http://crl.pki.goog/gtsr1/gtsr1.crl	0%	Avira URL Cloud	safe	
http://crls.pki.g	0%	Avira URL Cloud	safe	
http://pki.goog/repo/certs/gts1c3.der0	0%	Avira URL Cloud	safe	
http://pki.goog/repo/certs/gtsr1.der04	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

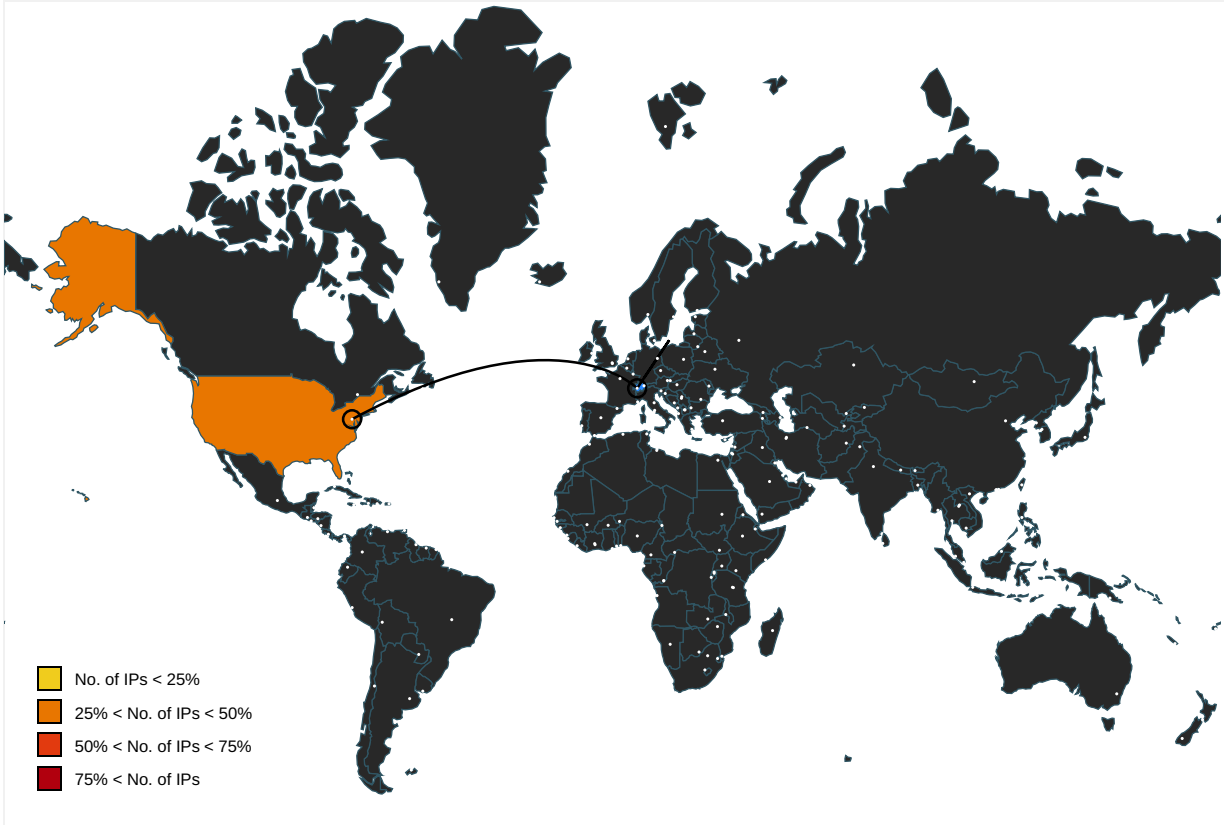
Name	IP	Active	Malicious	Antivirus Detection	Reputation
googlehosted.l.googleusercontent.com	216.58.212.129	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://pki.goog/gsr1/gsr1.crt	wget.exe, 00000002.00000002.332803027.0000000002B50000.00000004.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dns.google	4aa2863d-4eb1-42bb-8dc0-6a1e3ddabf97.tmp.7.dr, 88b21d77-c83a-436a-91cc-853cdfec67e8.tmp.7.dr, 1cea85ae-7fa5-4fe6-937e-4b41c395b45e.tmp.7.dr, 891c2c1c-ee3e-40ce-8f20-dc7bb71ce0bf.tmp.7.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.goog/gsr1/gsr1.crl0;	wget.exe, 00000002.00000003.332054258.0000000002B89000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pki.goog/gtsr1/gtsr1.crl-	wget.exe, 00000002.00000002.332803027.0000000002B50000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://lh3.googleusercontent.com/ogw/default-user=s96	uc@id=1ExbiBQm3R9DeKMtJJ7y4hk9h5s5yiyeZ&export=download.2.dr	false		high
http://https://lh3.googleusercontent.com/ogw/default-user=s24	uc@id=1ExbiBQm3R9DeKMtJJ7y4hk9h5s5yiyeZ&export=download.2.dr	false		high
http://crl.pki.goog/gsr1/gsr1.crl	wget.exe, 00000002.00000002.332803027.0000000002B50000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crls.pki.goog/gts1c3/QqFxbi9M48c.crl	wget.exe, 00000002.00000002.332803027.0000000002B50000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pki.goog/gtsr1/gtsr1.crl0W	wget.exe, 00000002.00000003.332054258.0000000002B89000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://clients2.googleusercontent.com	4aa2863d-4eb1-42bb-8dc0-6a1e3ddabf97.tmp.7.dr, 891c2c1c-ee3e-40ce-8f20-dc7bb71ce0bf.tmp.7.dr	false		high
http://pki.goog/gsr1/gsr1.crt02	wget.exe, 00000002.00000003.332054258.0000000002B89000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki.goog/repo/certs/gts1c3.der	wget.exe, 00000002.00000003.332054258.0000000002B89000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.pki.goog/gtsr1/gtsr1.crly	wget.exe, 00000002.00000002.33 2803027.0000000002B50000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://pki.goog/repository/0	wget.exe, 00000002.00000003.33 2054258.0000000002B89000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crls.pki.goog/gts1c3/QqFxbi9M48c.crl0	wget.exe, 00000002.00000003.33 2054258.0000000002B89000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki.goog/repo/certs/gtsr1.der	wget.exe, 00000002.00000003.33 2054258.0000000002B89000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pki.goog/gtsr1/gtsr1.crl	wget.exe, 00000002.00000002.33 2803027.0000000002B50000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://feedback.googleusercontent.com	manifest.json0.5.dr	false		high
http://crls.pki.g	wget.exe, 00000002.00000003.33 2054258.0000000002B89000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki.goog/repo/certs/gts1c3.der0	wget.exe, 00000002.00000003.33 2054258.0000000002B89000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki.goog/repo/certs/gtsr1.der04	wget.exe, 00000002.00000003.33 2054258.0000000002B89000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.212.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404275
Start date:	04.05.2021
Start time:	21:22:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	urldownload.jbs
Sample URL:	http://https://drive.google.com//uc?id=1ExbiBQm3R9DeKMtJJ7y4hk9h5s5yiyeZ&export=download
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:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.win@36/169@1/4
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 104.43.139.144, 52.255.188.83, 23.54.113.53, 104.42.151.234, 2.23.155.128, 2.23.155.153, 142.250.185.78, 142.250.186.131, 216.58.212.142, 142.250.185.206, 142.250.184.195, 216.58.212.173, 95.168.222.146, 142.250.185.99, 95.168.222.141, 142.250.184.234, 172.217.18.106, 172.217.23.106, 216.58.212.138, 142.250.185.74, 172.217.16.138, 142.250.185.106, 142.250.185.138, 142.250.185.170, 142.250.185.202, 142.250.185.234, 142.250.181.234, 216.58.212.170, 142.250.74.202, 142.250.186.42, 142.250.186.74, 104.43.193.48, 20.82.210.154, 92.122.213.194, 92.122.213.247, 2.20.143.16, 2.20.142.209, 93.184.221.240, 40.64.100.89, 20.54.26.129, 52.155.217.156, 172.217.23.99, 142.250.185.67, 23.57.80.111, 34.104.35.123 • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded domains from analysis (whitelisted): mw1eap.displaycatalog.md.mp.microsoft.com.akadns.net, ssl.gstatic.com, displaycatalog-rp-uswest.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, clientservices.googleapis.com, a767.dspw65.akamai.net, fs-wildcard.microsoft.com.edgekey.net, clients2.google.com, audownload.windowsupdate.nsatc.net, hlb.apr-52dd2-0.edgecastdns.net, update.googleapis.com, drive.google.com, watson.telemetry.microsoft.com, www.gstatic.com, au-bg-shim.trafficmanager.net, consumerrp-displaycatalog-aks2eap-uswest.md.mp.microsoft.com.akadns.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus16.cloudapp.net,

www.googleapis.com, displaycatalog-uswesteap.md.mp.microsoft.com.akadns.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, edgedl.me.gvt1.com, store-images.s-microsoft.com, r2.sn-n02xgoxufvg3-2gbs.gvt1.com, blobcollector.events.data.trafficmanager.net, clients.l.google.com, au.download.windowsupdate.com.edgesuite.net, 2-01-3cf7-0009.cdx.cedexis.net, r2---sn-n02xgoxufvg3-2gbs.gvt1.com, store-images.s-microsoft.com-c.edgekey.net, wu-fg-shim.trafficmanager.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, wu.azureedge.net, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, redirector.gvt1.com, cs11.wpc.v0cdn.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, wu.wpc.apr-52dd2.edgecastdns.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, accounts.google.com, wu.ec.azureedge.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, download.windowsupdate.com, a767.dscg3.akamai.net, download.windowsupdate.com.edgesuite.net, skypedataprdcoleus17.cloudapp.net, r7.sn-n02xgoxufvg3-2gbs.gvt1.com, r7---sn-n02xgoxufvg3-2gbs.gvt1.com, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Execution Graph export aborted for target wget.exe, PID 6452 because there are no executed function
- 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 NtQueryValueKey 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\19548808-9026-4350-9007-074347203bfc.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7489200208885074
Encrypted:	false
SSDEEP:	384:BHdySsPZkvMSVn521NKr/v+G3tGkZH0tGRYrzQSUxb5IIQbrD6xmvbpzgq2WVOgF:t6mRxCE89Qef8u0s/DWmKs2WBJ
MD5:	ABA8C108ED3459E556FE087A4A4998B6
SHA1:	70917A83147F261CA831FBBB77EA02C444EBEC53
SHA-256:	DF6B40775F62FCE5DC245DAB2586A4F32C72222B86DFF59AF6845B0009B430A9
SHA-512:	D6E8FD3A67060D855AFAD81F4B69EA3DE8E137123DA1C95D903A664AA59C57A0B684FF1A9F1037AB031B1ADB037078E35108505A2EC7E781575B197FF7D2500
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....98.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\1a941a08-5a40-4357-91bf-5d4fc2b0fb6c.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):	363005
Entropy (8bit):	6.028428010407517
Encrypted:	false
SSDEEP:	6144:oEr/NOXZG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinC:37NOJGNPUZ+w7wJHyEtAWv
MD5:	01AE843A1222A0C31F08D3ADBD4E79E6
SHA1:	37ACF51BBDC94BFCE6A4E3C106207EC947B20C17

C:\Users\user\AppData\Local\Google\Chrome\User Data\1a941a08-5a40-4357-91bf-5d4fc2b0fb6c.tmp	
SHA-256:	ACC36052C2792CD9D8E56CDA5D3C48D1B71FB273F7D274ECA4E49DA0E7FDAB4F
SHA-512:	EC9E7F9BD93DA7D83A8401AD521C953D9861910328AA3B0378AA285BAEC481339A525C0F965119F8F4CA1F1B4BEA8F1A63013616B9B6F2FF7E73774DA06D181(
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":1.620188628273524e+12,"network":1.62015623e+12,"ticks":161240991.0,"uncertainty":4906379.0}},"os_crypt":{"encrypted_key":"RFB BUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5i S+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488960180"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\21994c25-2a5f-4560-a566-891198456391.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7489562423803466
Encrypted:	false
SSDEEP:	384:RHdySsPZkvMSVn521NKr/v+G3tGkZH0tGRYrzQSUxb5IIQbrD6xmvUzgq2WVOgE2:d6mRxCEF9Qef8u0s/DWmKs2WBR
MD5:	9D9EE2D847A0307EF735D63C40FB9D46
SHA1:	214019E8B1E69BA7215D57653AB56BE06231536D
SHA-256:	776F91663D6E6249B662647D60A1996A21CCFC68BDF3F12A9219F686CD0912D0
SHA-512:	E48DDAB8AC51B0000BBF241D47BE2060D9952BF5B5E6E9D4B6C430934E7ACDEC8B391F14155221B8E91D8ABC1EF06F448E24512D2470915C7AFE435318B63C3 3
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....98.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\25482a5d-9881-4775-aeb9-175bb983abb0.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):	371482
Entropy (8bit):	6.0498259969030554
Encrypted:	false
SSDEEP:	6144:sEr/NOXZG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinC:77NOJGNPUZ+w7wJHyEtAWv
MD5:	F8562F6D07B1152A0DDA0440AF8A706A
SHA1:	B4AEC5133A4D2687027996D3301239EFE55E570B
SHA-256:	71C6CFC2AA66EEC427C179603FA2F66B49966E1A83D822A7B26DDD730E39FFED
SHA-512:	6340A90D1F0044AAB041DFB21C56E225566D1858E4B73531B6D02714F6E3F0667AD1B0A20B3AC9FC791C6775DE1836E1569FC6D7D91CEA77338D8CD360300811
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":1.620188628273524e+12,"network":1.62015623e+12,"ticks":161240991.0,"uncertainty":4906379.0}},"os_crypt":{"encrypted_key":"RFB BUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5i S+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\48f7f3bf-900c-4fb1-a751-fb1d2f201828.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	363005
Entropy (8bit):	6.028428010407517
Encrypted:	false
SSDEEP:	6144:oEr/NOXZG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinC:37NOJGNPUZ+w7wJHyEtAWv
MD5:	01AE843A1222A0C31F08D3ADBD4E79E6
SHA1:	37ACF51BBDC94BFCE6A4E3C106207EC947B20C17
SHA-256:	ACC36052C2792CD9D8E56CDA5D3C48D1B71FB273F7D274ECA4E49DA0E7FDAB4F

C:\Users\user\AppData\Local\Google\Chrome\User Data\48f7f3bf-900c-4fb1-a751-fb1d2f201828.tmp	
SHA-512:	EC9E7F9BD93DA7D83A8401AD521C953D9861910328AA3B0378AA285BAEC481339A525C0F965119F8F4CA1F1B4BEA8F1A63013616B9B6F2FF7E73774DA06D181
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":1.620188628273524e+12,"network":1.62015623e+12,"ticks":161240991.0,"uncertainty":4906379.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488960180"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\91236d06-e52f-408f-98cd-6fcbf3acf767.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):	363005
Entropy (8bit):	6.028428010407517
Encrypted:	false
SSDEEP:	6144:oEr/NOXZG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinC:37NOJGNPUZ+w7wJHyEtAWv
MD5:	01AE843A1222A0C31F08D3ADBD4E79E6
SHA1:	37ACF51BBDC94BFCE6A4E3C106207EC947B20C17
SHA-256:	ACC36052C2792CD9D8E56CDA5D3C48D1B71FB273F7D274ECA4E49DA0E7FDAB4F
SHA-512:	EC9E7F9BD93DA7D83A8401AD521C953D9861910328AA3B0378AA285BAEC481339A525C0F965119F8F4CA1F1B4BEA8F1A63013616B9B6F2FF7E73774DA06D181
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":1.620188628273524e+12,"network":1.62015623e+12,"ticks":161240991.0,"uncertainty":4906379.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488960180"},"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):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXEwozZHGftEwozZHGftEwozZHn:+EwozZHGVEwozZHGVEwozZHn
MD5:	4829695F153A750ADF50C6E979E8E8F3
SHA1:	2F697EF207460D03671E4B59670BC73328D60D6E
SHA-256:	1AACF1304FD42C84FF41DDD2F2252E5C0EDE7362352661B7957648F2EA4C2683
SHA-512:	6D16A6EF4BB20B25B1B14757C475E9F8C3A40D6181F718D563A628BA41DA9426E1B586C472D4F8729FD65FCA014151B7D46FBFAAE171BFF9A6D937DB7A7A2C02
Malicious:	false
Reputation:	low
Preview:	sdPC.....y3..M.Y.NbD.sdPC.....y3..M.Y.NbD.sdPC.....y3..M.Y.NbD.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0748d439-1798-4cf8-a982-28c10c22d939.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):	5458
Entropy (8bit):	5.165612586058926
Encrypted:	false
SSDEEP:	96:nVXbd8PDMfp+QO/yaAVVaxk0JCKL8robOTQVuwn:nVXbUMfp+b/y9XS4Ksa
MD5:	88455C4C0D8AE7B6D4C0D320B337396E
SHA1:	5AE8F7B24C5B769AD2EBA7D917DEA66E7AA282A6
SHA-256:	B16352812525821410A612E791213F3E1F5C46ADA6DB0106751A72535B20B59D
SHA-512:	3E632FB20B56C87B2D5D5E03102735F9630509045159642052B2C3B66AA31A664506B430B2C3ADA1BCA347FF3C0AF6818F6EA6F2B41332B0BD6C62D166647E7F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0748d439-1798-4cf8-a982-28c10c22d939.tmp

Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13264662225298495","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0d123d0d-fb01-4b8b-b62e-440db238fc80.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):	22595
Entropy (8bit):	5.53604080796896
Encrypted:	false
SSDEEP:	384:poUtOLl1PXx1kXqKf/pUZNCgVLH2HfDSrUQHGUdnT5mAjf5JYS40:0Lltx1kXqKf/pUZNCgVLH2HfOrUUGyn5
MD5:	EBCFC4547D920493EA3C777C9863B6B6
SHA1:	8178ADAF957D2427D6EFF056E1410AFA92B9E0F9
SHA-256:	6512D83F3B82C05EBAC93B2E8DA410EF1CDBD0F1AF991165D16CD20BCE458B0D
SHA-512:	E2D34D75A7F866B2741EBF1D39C534FD2BF346DEC877CC9EBB9DAD36412CA41FEA63C7130568D601996433DADA30E9D0B0EE766ABE541BDF6D6B9532C74E199
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":"13264662224961565","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\11d6aa61-131f-47d6-87e5-b02c372c24dd.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):	16745
Entropy (8bit):	5.577262756033701
Encrypted:	false
SSDEEP:	384:poUtTLl1PXx1kXqKf/pUZNCgVLH2HfDSrUBBfHYS4qh:JLltx1kXqKf/pUZNCgVLH2HfOrUBdZZ
MD5:	D4BE540F55C69C1AAF8302479BDC9B75
SHA1:	75AA8D272B21C59655FA251EA3CDB6553512A4A9
SHA-256:	70335D9A4A0EC06D943C9A73132F458A7F119A1310C8140B33F44A4BF429D80C
SHA-512:	015EE1FB9676CC311B0279A9248C4DF28345E3A0FE947A6289EB9565584C057C5F5D8D008B83D19DA4A59A4A564BCF09DFA2441806670DD4A730FE119A8C6BA
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":"13264662224961565","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\4aa2863d-4eb1-42bb-8dc0-6a1e3ddabf97.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	2347
Entropy (8bit):	4.90969952861867
Encrypted:	false
SSDEEP:	48:YALteBdpNnTCXDHz5sCORLsClTsC8tFsuuDs8yKsJ3zsM5MHiYhbG:2lNnTCXDHzxOplv8mxAZGHhS
MD5:	79320DB8E0171D06E21A4D5ECCFD3655
SHA1:	748A9C624DF5F6EA70E92DEF0620098BD981575B
SHA-256:	120345F1164266C1525B8A777095972B34E177F6073AD051E31A9A6B84B35113
SHA-512:	5E615341729E40F0E4AA743FCE7B8DD5FD7585690E3D46DC090935AC6C38EF395A587B3CCED37979AF8D4E24668732BE506EA61AB456A7CF9DDC71C6DC0BB6C9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4aa2863d-4eb1-42bb-8dc0-6a1e3ddabf97.tmp	
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13267254230059496","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13267254230061159","port":443,"protocol_s

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\53aec719-e121-419c-bf30-b536fb366d4a.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\891c2c1c-ee3e-40ce-8f20-dc7bb71ce0bf.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2825
Entropy (8bit):	4.86435102445835
Encrypted:	false
SSDEEP:	48:YALtdpBeMsNMHK5sJDysACs37sHWsd5/sSYMHCKs/MHCzsSOMHwsSJtFsX3RLs9D:HQxGKWDS1i/5vYGmGqOGKJ03QshS
MD5:	95488A82D5073BDAAFC1480073FF801F
SHA1:	E2E979B6D4A3EE16A815115C414D0A98E1DFA93F
SHA-256:	C091AE68AFCD5EC632B2C324B983D70F722463CB4D05A3CE8D52E07AA7E5A5D6
SHA-512:	D536466352320C5D394130A59B605617580050CDF325C4B3392D87D384C246E9D8C54FC16A247FF4B379F162536304E0D312D7781FFE245C643C5081B8BE08CD
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952675493","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":32613},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952813644","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952748754","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952634896","port":443,"protocol_str":"quic"}],"isolation":[],"server"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	340
Entropy (8bit):	5.235912166200197
Encrypted:	false
SSDEEP:	6:mLnW9+q2PN723iKKdK9RXXTZIFUtpEMQJZmwPElW9VkwON723iKKdK9RXX5LJ:j9+vVa5Kk7XT2FUtpNQJ/P+W9V5Oa5KU
MD5:	A5E230FC5439999B7DABA874EF099FC5
SHA1:	82F301D10F8E35619E75D989194E7260152E6C72
SHA-256:	01EF538E6EC1A5E11AAE40EDE1FFD06DA32AD7ABE8AFEE8806B7BC8E516B9FC1
SHA-512:	C0E66D804A97E34D95458DFD9296E1C263052A40CAC76DF92ED0447FC4BB3304218EAAB08B2610CB2D5CD49C5C9D518061F40E61C77E2205F18BF8CA1E9492D
Malicious:	false
Reputation:	low
Preview:	2021/05/04-21:23:58.535 194c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/05/04-21:23:58.536 194c Recovering log #3.2021/05/04-21:23:58.537 194c 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.197802759507333
Encrypted:	false
SSDEEP:	6:mLtgE9+q2PN723iKKdKyDZIFUtpEmQJZmwPEmQ9VkwON723iKKdKyJLJ:GJ9+vVa5Kk02FUtpMJ/PM9V5Oa5KkWJ
MD5:	FA5012670AA5E8FCFFF78646443DA12D
SHA1:	9A124DFEE39B33A54CB03B10C8893AC1AAA94525
SHA-256:	6909796A6C55D4612B819CB70E6F66715E6073C4A7798CA088AA9F480CEFFD8C
SHA-512:	1BF4D24ED991BD60E4EDC93C24293BB5E463B6E055BB81B830742540AA72A531EBC32E6D3447833C370500BE3DDC854314D6865C284A8E739DFD8A2118753FC
Malicious:	false
Reputation:	low
Preview:	2021/05/04-21:23:58.529 194c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/05/04-21:23:58.530 194c Recovering log #3.2021/05/04-21:23:58.530 194c 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:	dropped
Size (bytes):	12288
Entropy (8bit):	0.6863571317626186
Encrypted:	false
SSDEEP:	12:TLyen4ufFdbXGwcFOaOndOtJRbGMNmt2SH/+eVpUHFxOUwae6:TLyqJLbXaFpEO5bNmISHn06Uwd
MD5:	1C0EAEEE6463CAE33B7A7CD9D9DF4DA5
SHA1:	FBC6A28A1501E40154FDC0A9D0C2F34A5F88AA65
SHA-256:	ED8AE7C5E6885874A39F4E86258F552670352A18D29BE1FF4D372A2F4CD06C8A
SHA-512:	355D19828609971998B09B36E7C7D304B7FB88C7A726670BEBF5CF2E2710F8E71B0F9DEF6FE9712B484C1EB122AEEEFDECF31D13E02C4539C399DFB86EC7619F
Malicious:	false
Reputation:	low
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):	0.9651333845102764
Encrypted:	false
SSDEEP:	24:8CpIvJn2QOYiUG3PaVDqLbJLbXaFpEO5bNmISHn06Uw11t8:8CpIvZXC/ahq5LLOpEO5J/Kn7U28
MD5:	5C608E3F1B51242E6DE9409FCA4EBB5B
SHA1:	8417D54AE037DB5383FFC5D0E3FDB1C1E0660FF3
SHA-256:	2F772AB6964CB9D7ED95BFF33B5901E033696169C7D0C8681A26456A0164931B
SHA-512:	83BB0FC4F3AA8ADF58CD3B3C8F10D47DA861B87E75B291812A26C3F8C95B2A5FECC97A643B56D9EDDC5BEB76C9267065B41F0E5FC7654CD850064AC7726F3BA5
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):	1176
Entropy (8bit):	3.8592984810340063
Encrypted:	false
SSDEEP:	24:34SNt6njrxslrlo6ktVkEk4ajjAzCCc5rptVkEx:34cGrKxo6cdmvAWC8pdx
MD5:	0B6D521CFBCAEB9D5F67FC54DFEC21BB

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
SHA1:	8E98E450F0A7B180DF6EEA6651211F156872D5D6
SHA-256:	B8B1946272BD0D993E9D55946A56A9017D102EDEEA9D8F6684B7AA8519AE63B9
SHA-512:	81774E2FD54D8B20DBF059E1FD77EBE5EC080F9C6912DDF4209B38A522036959EC140821ACF5E76831890C36B5AC5C0F028BC14A20269A0D02A23FA9C1E618A
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...7bc5ce11_4d1a_4f46_8ec7_75a0e09e9b0e.....m..... .....5..0.....&...{68ADBCFB-ED3C-4AA1-B80C-ADD502B6FA85}.....Q..L.....g...file:///C:/Users/user/Desktop/download/uc@id=1ExbiBQm3R9 DeKMtJJ7y4hk9h5s5yiyeZ&export=download.html.....h.....`.....8.....@.....8.....7e.....8e.....x..... g...f.i.l.e.:././.C.:./.U.s.e.r.s./.e.n.g.i.n.e.e.r./.D.e.s.k.t.o.p./.d.o.w.n.l.o.a.d./.u.c.@.i.d.=.1.E.x.b.i.B.Q.m.3.R.9.D.e.K.M.t.J.J.7.y.4.h.k.9.h.5.s.5.y.i.y.e.Z.&.e.x.p.o.r.t.=.d.o.w. n.l.o.a.d...h.t.m.l.....8.....0.....8..... .....

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
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):	326
Entropy (8bit):	5.193874407072734
Encrypted:	false
SSDEEP:	6:mLAQyq2PN723iKKdK8aPrqIFUtpEdG1ZmwPEhSQRkwON723iKKdK8amLJ:DVvVa5KkL3FUtpOG1/PkSI5Oa5KkQJ
MD5:	D2AAABE7D93BBF56ABEE3F45AA86E7CB
SHA1:	39E7A772CA1C90E9513D55EDC9521782223D1C6A
SHA-256:	41E2BE280F666D4FDEC261237F0FAC7E6372762B163FC2D6FE72D04E045322FD
SHA-512:	836BC03BC113F392569FF852065F3D011E91310F3418851234A794F79DE918734EE05477F3BA47079785878C85ACAC2DD7E6574ECB61FF0FBE985A36993EC140
Malicious:	false
Reputation:	low
Preview:	2021/05/04-21:23:45.335 1b70 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/05/04-21:23:45.338 1b70 Recovering log #3.2021/05/04-21:23:45.339 1b70 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Reputation:	low
Preview:	.f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f. 5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....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):	326
Entropy (8bit):	5.2344721901659215
Encrypted:	false
SSDEEP:	6:mLEeZL+q2PN723iKKdK8NIFUtpEGU2G1KWZmwPEDr+LVkwON723iKKdK8+eLJ:BeR+vVa5KkpFUtpxoKW/PEriV5Oa5Kk2
MD5:	C73BA9FF5AB2133FD5439B7FE978263B
SHA1:	F0E3387D0F57BCC0E40F3FA1B26C80064DD5DD13
SHA-256:	1E6B5A61CD777B4E3C47D636E6CECECE2B1203C246906195B5AC9B940CFC4C24
SHA-512:	CF98DB54025423F5DB7C357718AF87D8A696089490CC5DF3BE62A933C78FAEDBB97EEBA5824A37AAA4F6CEBE0DF97BF01F100896264208C03D671BB92578A7 2
Malicious:	false
Reputation:	low
Preview:	2021/05/04-21:23:47.486 1b3c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/05/04-2 1:23:47.488 1b3c Recovering log #3.2021/05/04-21:23:47.489 1b3c 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\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXltmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZ rQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMB N2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FF FY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=", "yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWE vYCs40NI=","3mBGNAiRITANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclJ5 n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAF Mms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+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
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):	378
Entropy (8bit):	5.233657708537807
Encrypted:	false
SSDEEP:	6:mLNFS9+q2PN723iKKdK25+Xqx8chI+IFUtpEnUDNJZmwPEbgE9VkwON723iKKdKI:X9+vVa5KkTXfchI3FUtpGSNJ/PcJ9V5Y
MD5:	74E3A2DA959BEA2E7BFEEE53FB396916
SHA1:	5474FB75C5DB08C72174A6BA98E4B7F50CA2C382
SHA-256:	79E090F886CA245F5E53B6F2C15B8A847B174878AC8B9E2F65001DB2875BFD2E
SHA-512:	312E9F68D7DF2B05385B254897B847928BACB5A7454598424470A4BAB5145D2295380FA83629B4E1847C0F1713B4674E58723141F352F0A8744BE4A0C3195215
Malicious:	false
Reputation:	low
Preview:	2021/05/04-21:23:58.481 194c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/05/04-21:23:58.483 194c Recovering log #3.2021/05/04-21:23:58.484 194c 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):	364
Entropy (8bit):	5.217889143366002
Encrypted:	false
SSDEEP:	6:mL79+q2PN723iKKdK25+XuoIFUtpE1mJZmwPE1CQ9VkwON723iKKdK25+XuxWLJ:G9+vVa5KkTXYFUtpkmJ/Pk59V5Oa5Kkl
MD5:	EB6BD0489FE09D509A250DC0B649059F
SHA1:	CD13E1F05ED5605E8C6F2443FF03673058EE9313
SHA-256:	6A54D3FE10563B0F76B05FC359C59885FB41B397C5C01FDD8490B3883BB50199
SHA-512:	B1A7915419A6875CF99365A0516D670FA8F9FD6F1774B7991F23883A78758DE9629953EBA61E1ECA70C09B3730EFC4242902BFEBC1FC46F4F3B04DCB0E1CBA3

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Malicious:	false
Reputation:	low
Preview:	2021/05/04-21:23:58.468 194c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/05/04-21:23:58.472 194c Recovering log #3.2021/05/04-21:23:58.473 194c 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):	336
Entropy (8bit):	5.224879757637445
Encrypted:	false
SSDEEP:	6:mLhRE9+q2PN723iKKdKWT5g1IdqIFUtpEGJZmwPEr9VkwON723iKKdKWT5g1I3Ud:cS9+vVa5Kkg5gSRFUtp3J/PC9V5Oa5Kg
MD5:	D1066E5F0938E18D73F7220711549895
SHA1:	B57AD1539C98F9FD05D500F78C6B5821E0FDF564
SHA-256:	B2156EE082EBA396785C2EBBCEFD06BED337B3F593D603ABCDBC1827B3348218
SHA-512:	19E272627BBC24BC72DA664123EB3C05528E9FD8537616A38025BA5DD82A56F6920039F85F0A6D436D41E5F67F4CB58408630003ECB5F5A63FE801DE0DFC9EE
Malicious:	false
Reputation:	low
Preview:	2021/05/04-21:23:58.443 194c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/05/04-21:23:58.445 194c Recovering log #3.2021/05/04-21:23:58.446 194c 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
Entropy (8bit):	0.16353769386677283
Encrypted:	false
SSDEEP:	12:TL+A/ZFBvVKuFGDVSoaHNuQDgGI/E+NBvVKuFGDQ:TLxftVk5uu6gtVkE
MD5:	54DD159A195653D33DC0675EA88A0B6F
SHA1:	09E6B1D3774057269338D0E2E9F5923ED573856D
SHA-256:	93D76C36FB1D88F7437E344C5503CBC8B4CE747BDFFA2FFE07EA80AB498C5BC5
SHA-512:	FB1A585F101650326E1E0968CB9F68CA299C1C83CFB3BD7672BEFA73A64A8B92633F42AD96C7A1246D6E20B3CD996C74040A31070E54EBE38672E92C82C6D55
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):	1070
Entropy (8bit):	5.5277180321690835
Encrypted:	false
SSDEEP:	24:8MV/vZrdCbMV2P2q2CS0+bh489T0kUY78BJgskfa9yBDOxo7nAUJ9btVkasbNkfL:8Mtvpd4Mi2JBdDQNUsA3zsBUL
MD5:	25AAA076BB840AD88FC0C37318CF223B
SHA1:	5D6790A97B0D18CDD158B14691F701CED67461F8
SHA-256:	AE15B7CCE8ED12DD2FF3EE705CF3DE9822C982146D6A56C96EB315DD7E0196CB
SHA-512:	ACEC2524DB669844BB7C5B8BF01395491FB48C98ABEAEA2C6A3CF5059F139916D17A4C7E0E9D65434C9A881CD38A21AB939B316EB1BFE3FB032A716920E6CA5A
Malicious:	false
Reputation:	low
Preview:	....."....!1exbibqm3r9dekmtjj7y4hk9h5s5yiyez..c..desktop..download..drive..user..export..file..google..html..id..scan..uc..users..virus..warning*.....%.!1exbibqm3r9dekmtjj7y4hk9h5s5yiyez.....c.....desktop.....download.....drive.....user.....export.....file.....google.....html.....id.....scan.....uc.....users.....virus.....warning..2... .....1.....3.....4.....5.....7.....9.....a.....b.....c.....d.....e.....f.....g.....h.....i.....j.....k.....l.....m.....n.....o.....p.....q.....r.....s.....t.....u.....v.....w.....x.....y.....z...:.....B..... .....*gfile:///C:/Users/user/Desktop/download/uc@id=1ExbiBQm3R9DeKMtJJ7y4hk9h5s5yiyeZ&export=download.html2!Google Dr

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):	42076
Entropy (8bit):	0.11652928109206337
Encrypted:	false
SSDEEP:	12:Ev9lINLJKdnlMgqLBj/Xt3lu504nMWQfy9LHOBQZ8fOe/:aXqLBXt32ltNHOTft
MD5:	016A4717FE5E153CCF49A2DC961C35E1
SHA1:	97C15F90A6F9963FA5191F22858D601D470B5AB5
SHA-256:	F7A4BA194946E23EB51D797254A030AF0C5ECA5510D084C468AE304DBA833576
SHA-512:	77B041A8F43B26D84C1BA1C7F26B84C19FC59C1D33504761CBCE93A7640F2CFE02DDAB78C61AC44327E2E85C513A00CD874D45D37E30C5E51A8B591217A3D63
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):	5.460268897249595
Encrypted:	false
SSDEEP:	48:QduG5Ta7KMh8dbsbT50cbQSefgGVNrS0U9RdiN9G:Qda7KMidbsbT50cbQ5fgGnrS0l
MD5:	F6F5B4D59AE7A59BB4C7336BA51F68EB
SHA1:	4BA0C141EEC4A8086DDD07423A022A0A9F060652
SHA-256:	402A0B421200E9C58EB51D6A397A591219790318E5AA0BA3C95832481B72D384
SHA-512:	CA8C57F3219CBA189678BA8D467C13F941DD4AD1AAF5D11599B3B9048F174CC40AFAB846A4E62E23032BCB131CD8EF058605127BEF87AC3D58D30739EE0DC097
Malicious:	false
Reputation:	low
Preview:	...U...*.....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..610220000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-05-04 21:24:00.28][INFO][mr.Init] MR instance ID: 34a1fc96-8acb-4341-981a-21794a1c4c09\n","[2021-05-04 21:24:00.28][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-05-04 21:24:00.28][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-05-04 21:24:00.28][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-05-04 21:24:00.28][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-05-04 21:24:00.28][INFO][mr.CastProvider] Query enabled: true\n","[2021-05-04 21:24:00.28][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):	338
Entropy (8bit):	5.151935346590267
Encrypted:	false
SSDEEP:	6:mLp4q2PN723iKKdK8a2jMGIFUtpE0MIdvJZmwPE0IiDkwON723iKKdK8a2jMmLJ:zvVa5Kk8EFUtprh/PD5Oa5Kk8bJ
MD5:	219D5D2FD628C1FC0D61825C0B99B5BE
SHA1:	8BDC2820A70A91770A3282A6AA767B186B73FDA6
SHA-256:	2CFBFC4182078D8D5D6A7B98C4F15EADA1DF7D253B38D19BF71B913995BD59B2
SHA-512:	CCC4BB5A1F61F797FCF59D9611CBD56AEC44B437146B09E08CA51B4F0E69AF7F06C470AF15F5509BC3D9FEE00F6685A67BFE93CF7A09834186301C56084AEC88
Malicious:	false
Reputation:	low
Preview:	2021/05/04-21:23:44.999 1b80 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/05/04-21:23:45.010 1b80 Recovering log #3.2021/05/04-21:23:45.014 1b80 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):	340

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Entropy (8bit):	5.213192461744841
Encrypted:	false
SSDEEP:	6:mLpL+q2PN723iKKdKgXz4rRIFUtpEV4zKWZmwPEnLVkwON723iKKdKgXz4q8LJ:A+vVa5KkgXiuFUtppzKW/PGV5Oa5Kkgi
MD5:	A5AB687A8B82A32C741833FFB40E9D77
SHA1:	AFABA01846CA66AB145F62D5841F968571E182D5
SHA-256:	969E5A0BF87EF77F0566E72DC0FE56997CA8E123F267454DEA7D7A0CA0535459
SHA-512:	00C857D9BC128352CBBECA070ABAB486EF7FCF6B2CCBC2DFEC2C97F2E2541DDE87D9AF67D4C559F57105C4A9CA7C32429563AAD27A6D9286F62C2F02D615BBC
Malicious:	false
Reputation:	low
Preview:	2021/05/04-21:23:45.356 1b3c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/05/04-21:23:45.357 1b3c Recovering log #3.2021/05/04-21:23:45.358 1b3c 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:	3:5ljljljljljl:5ljljljljljl
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):	326
Entropy (8bit):	5.159083117155192
Encrypted:	false
SSDEEP:	6:mL2JeZL+q2PN723iKKdKrQMxIFUtpE2SuTzKWZmwPE2jU2+LVkwON723iKKdKrQq:JMR+vVa5KkCFUtpZSuTzKW/PZjJiV5Om
MD5:	D4641D471C880E85FEF8B9F2246B5DC2
SHA1:	BFC20C985D1D30FCDAD388833089F0C70D5FEF77
SHA-256:	C567E15703EB6B20E2C2CCC9F5B209559F013924319DAA4E6054677617AA006A
SHA-512:	53E297C61A43C2235E918B74130E0C43DB5CA69C2873CCFBBBF8900FA6DE6CABD610996928DF49045209BE862BD44919444FEF16CEF64C0EECC883CF80BA99B
Malicious:	false
Reputation:	low
Preview:	2021/05/04-21:23:45.284 1b3c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/05/04-21:23:45.285 1b3c Recovering log #3.2021/05/04-21:23:45.286 1b3c 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):	354
Entropy (8bit):	5.155093012875424
Encrypted:	false
SSDEEP:	6:mLIq2PN723iKKdK7Uh2ghZIFUtpEK6ZmwPEkUbFkwON723iKKdK7Uh2gnLJ:dvVa5KklhHh2FUtpK/PdKF5Oa5KklhHd
MD5:	149741D9782B180454B9E06D2E0EF971
SHA1:	47641358DAB2B18D82321CBFD01D90EF92903DD3
SHA-256:	472969FE0837C745C4F2C2846C795ED73BDE7B4A7ABC309D330820040B8863CB
SHA-512:	F15B797CAE708AEAEE1DD7240B8DC463DDA1806EB65611BCDB0B14DDDFB4E757DA5515A6D2EA419003405A81E3783C2ED6DEDAD20A1B315A058DA0474B9E4004
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Reputation:	low
Preview:	2021/05/04-21:23:44.957 1b04 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/05/04-21:23:44.964 1b04 Recovering log #3.2021/05/04-21:23:44.966 1b04 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\1cea85ae-7fa5-4fe6-937e-4b41c395b45e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.95629898779197
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5kjxZsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdSZsBdLJlyH7E4f3K33y
MD5:	D5BB2F0F1694209F0C6AE5BA44DAC338
SHA1:	41B2CDE10C8937FC9607E608AF65EDF709033350
SHA-256:	20FC2ED4DA8AC625B83B6B84C1B88B534BC35B18DC8BD7521C66FFDABAB53738
SHA-512:	A713918E0F88AE62AFAC2A6202107CF547B962900BCB779C7C5C2C8A228C140AAC5191A50BDAF5718EAAE91446DB21648CF2A7B967B9029AF16F13E923FD6EE2
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544897343531","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	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):	436
Entropy (8bit):	5.2170631615379355
Encrypted:	false
SSDEEP:	6:mLBQyq2PN723iKKdKusNpV/2jMGIFUtpEnG1ZmwPESJQRkwON723iKKdKusNpV/s:uVvVa5KkFFUtpIG1/PfJI5Oa5KkOJ
MD5:	AB7EC39A543E29C49E972CA3BC17E7C6
SHA1:	A3DF9FC5BE368ABABED3C3E2B420CD1BB2EF6623
SHA-256:	B57A6545354B24E06758069BA14432548E5C7A6B32E4FB6A4314AF3340AF1875
SHA-512:	69A1A06884D657A908AB8B546D41A41676373D4B28B55E78415F28C47708604A8FDF9336B27CAD1A5CC20D8229A6688CEA3ECE35EFC6155240E547DB1BCC01C
Malicious:	false
Reputation:	low
Preview:	2021/05/04-21:23:45.312 1b70 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/05/04-21:23:45.314 1b70 Recovering log #3.2021/05/04-21:23:45.315 1b70 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):	438

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Entropy (8bit):	5.290611162661282
Encrypted:	false
SSDEEP:	6:mL/QQ+q2PN723iKKdKusNpqz4rRIFUtpEYU8dSgZmwPEyfQVkwON723iKKdKusN9:bVvVa5KkmiuFUtpnSg/P5fI5Oa5Kkm2J
MD5:	E05208A65601883D59998537258887C2
SHA1:	642A5645918543EB6DCD7437F72E6416683CD443
SHA-256:	6DFA09D15434FF6F48F0B86BB303873505E4A9479A5559C1F402FF24CBC10C17
SHA-512:	BAF423B515C785CD92BB14BB1AB88CDB89BA552BB68F8AA33A94F7BB7CC0765359F7932C52EE48BE405B846339EA37BE7C053519553BB48CAD50A1913C566F9 D
Malicious:	false
Reputation:	low
Preview:	2021/05/04-21:23:45.360 1b98 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/05/04-21:23:45.361 1b98 Recovering log #3.2021/05/04-21:23:45.362 1b98 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):	424
Entropy (8bit):	5.229629919259242
Encrypted:	false
SSDEEP:	6:mB+q2PN723iKKdKusNpZQMxIFUtpcZmwPtVkwON723iKKdKusNpZQMFLJ:5vVa5KkMFUtpc/PT5Oa5KkTJ
MD5:	218F829AF5112E4D5DE7614BC80F1C21
SHA1:	04A49966E7D606D01338D02286BEF9C2AD173810
SHA-256:	D781F4F89F4C4E7EA38B63C1E8CAF32DE168E6180B87DEF97B58F3651639C9C6
SHA-512:	31BCC86C99A15D7D402F858A35AAFFAE75A3F41807BE9387C706C25821DA065F06BAD60DAF6F23CA9E463009E161C131E9D4504EE54DA915378FE16AB56B7C3 7
Malicious:	false
Reputation:	low
Preview:	2021/05/04-21:24:02.399 1b78 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2021/05/04-21:24:02.401 1b78 Recovering log #3.2021/05/04-21:24:02.402 1b78 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\nmmhkkegccagdldgiimedpiccmgmieda\def\88b21d77-c83a-436a-91cc-853cdfec67e8.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.958114650763609
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV59YIEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdXXEsBdLJlyH7E4f3K33y
MD5:	F08847672DDD58749FE32FEFD1DBBAE9
SHA1:	C4C1750B297311628D53B0D3DD473F3EDD6019E9
SHA-256:	4165A9C7A2CA81E34A969C02FC75FFA899F49A5B04899EBA10E341C44839CC90
SHA-512:	541C4ADF3A92398F61F1E90C9995FD9CCB668FF51F578968C6CCD73AB81AB24668D969A9F98A1B529F631022EF4A3D224D76B4EDCB656ADADB27A7E4065395A 0
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\88b21d77-c83a-436a-91cc-853cdfec67e8.tmp	
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544901990438","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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):	436
Entropy (8bit):	5.164020555712483
Encrypted:	false
SSDEEP:	12:YVvVa5KkkGHArBFUtp0G1/PYAI5Oa5KkkGHAryJ:Y5Va5KkkGgPgCrASOa5KkkGga
MD5:	5F2D0D535EC01C622F6434845770D61B
SHA1:	2CBB41207F9D65396C03A9D9289AC23B54872702
SHA-256:	D52CC103F6EA3A899B4277CFB0BFCCCE2759737298CD0C1E475371C5B4B455AB
SHA-512:	EA210A9658FA68BE7DCAA5471D648E0105294B77CFA5AE81183218052962A0BA10DB5F560FA641EEF96F838034FB6CD0750E3F2157EC9B3AB00B81465E987ED4
Malicious:	false
Reputation:	low
Preview:	2021/05/04-21:23:59.007 1b70 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/05/04-21:23:59.010 1b70 Recovering log #3.2021/05/04-21:23:59.013 1b70 Reusing old log C:\Users\user\AppData\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):	438
Entropy (8bit):	5.201431885214433
Encrypted:	false
SSDEEP:	12:mMM+vVa5KkkGHArqiuFUtpF/PGMV5Oa5KkkGHArq2J:NdVa5KkkGgCgC2Oa5KkkGg7
MD5:	20CC306018A990E37651B50E8D25321D
SHA1:	9C6288FFF6083FA479E25965F677F7C0BC3EA012
SHA-256:	834DF5D72F723EF7B1B369D67A1A8098588BE82082E2601008044EE7A3E9D843
SHA-512:	23BAB43484719850AE58F8DFE5FE6AD9865C0E8AB8BE0A4AA62408BE8455265DDE51EC5D447C74E65FDC4A55B4E302911633A8B71B1CFBDC398BF9867895915B
Malicious:	false
Reputation:	low
Preview:	2021/05/04-21:23:59.008 1b8c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/05/04-21:23:59.012 1b8c Recovering log #3.2021/05/04-21:23:59.014 1b8c 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
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):	424
Entropy (8bit):	5.160366233287373
Encrypted:	false
SSDEEP:	12:W2ax+vVa5KkkGHArAFUtpG2/zKW/PG2/NV5Oa5KkkGHArfJ:FjVa5KkkGgkgT/9Oa5KkkGgV
MD5:	A5AD3BC0ED81AE5C1836A8881570C8D6
SHA1:	DD6518FF96D394C24EECE52E3E8B2E43DB5ECB06
SHA-256:	127CE363238383CC71C84005FD0CF5C2E6680DD51AD8B50DE17617D04A4083F9
SHA-512:	0048B3318204FBC1628738FA55FFAA6D5E8596E9FBA4D1C151781F2E0A6C00AC4BC72176B27A8F1A3AE9EF8F1B2B674326E12EB56B03AC9344C78731C89DA11
Malicious:	false
Reputation:	low
Preview:	2021/05/04-21:24:14.306 1b3c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/05/04-21:24:14.307 1b3c Recovering log #3.2021/05/04-21:24:14.307 1b3c 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
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):	330
Entropy (8bit):	5.227469625900626
Encrypted:	false
SSDEEP:	6:mLYCq2PN723iKKdKpIFUtpEkUyZmwPE3kwON723iKKdKa/WLJ:hCvVa5KkmFUtpdL/Pg5Oa5KkaUJ
MD5:	85F0B18F497C2B362620091ECDFF35F2
SHA1:	342A393B2080A2408BB6166106073935A12F836C
SHA-256:	71EBF7824B84C20108CC9DDCA5EDF14A0250C3D1900428BE0A9A95B2F822602B
SHA-512:	EE8846B483E815BE9DEEDC4E6F59330B1E5644E0E8F37BF8FD4E55378B82BD2835B2398F609A8ECC17BA893C9F02DB7BFEBF3F97B3AC74031A5C8919788E4E0 F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Preview:	2021/05/04-21:23:44.962 1b30 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/05/04-21:23:44.966 1b30 Recovering log #3.2021/05/04-21:23:44.972 1b30 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):	408
Entropy (8bit):	5.282432051810921
Encrypted:	false
SSDEEP:	6:mQ+q2PN723iKKdKks8Y5JKKhdIFUtpiZmwPbVkwON723iKKdKks8Y5JKKTLJ:UvVa5KkkOrsFUtpi/PB5Oa5KkkOrzJ
MD5:	413D9CEC68AB415785E8529AE8455C83
SHA1:	AF5ADDBDBB0DCFA1FD4BDC5B420C8DF9BDBF32E4
SHA-256:	89FDEF92E1D18A27DCC1A99E960A3CDCBBC418FA60E5E665B82145B20D7B71E8
SHA-512:	D1872C448CF34EE57D4669324E4BBA34062FBB754EB6EE3494E80CF127D79D8C5C202329D1724E2306DF342FA7FAA9420D2EE3E9F09C71C2B1B9DEBCB239763 1
Malicious:	false
Reputation:	low
Preview:	2021/05/04-21:24:00.264 1b78 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/05/04-21:24:00.265 1b78 Recovering log #3.2021/05/04-21:24:00.266 1b78 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):	2.9182958340544896
Encrypted:	false
SSDEEP:	3:ylP0/:2PG
MD5:	40208052620C90CD093B526D603A5423
SHA1:	075BE7099C97ACA95A0938DFC7B2730C1BC5674C
SHA-256:	9C3328FB9B445206D6AC90B56585DD00C454757160D4788F0DC6A52307E4812C
SHA-512:	BB6B145919848E2B3C811DEA6BFBF6032B7731DAA9B69AC1800EE98B7D7F309F1D13FCCB642F50F1507454DDB01FD1CF75B9ED3F61964FB6C53911766127E0D
Malicious:	false
Reputation:	low
Preview:	......7..h.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\aa6cacf3-217b-481f-9e23-6616e859d441.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):	22596
Entropy (8bit):	5.535815810715569
Encrypted:	false
SSDEEP:	384:poUtOLl1PXx1kXqKf/pUZNCgVLH2HfDSrUQHGXdnT5mAjf8JYS4tS:0Lltx1kXqKf/pUZNCgVLH2HfOrUUGNn4
MD5:	FA87FAC0365A11795E1C2CAE33857F3B
SHA1:	92B61F69E6E2EE701D935698DF02024A42ADA4B4
SHA-256:	A1CD78D715739A46343C010C8FF976CAEAF05FC7FA4DBAA2A89724701E0C365D
SHA-512:	C31BCCE717A79C786359CC3596ACD0A81C460F33435A86473BA6A200EF07454623E3E003570D0745EBDCD59E28F04CE380CBCD9B8132CF6D4D9498E3EB86FF 3
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":"13264662224961565","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/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cba89b3d-518b-4167-a1a3-a0ac9efd4932.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\cba89b3d-518b-4167-a1a3-a0ac9efd4932.tmp	
Category:	dropped
Size (bytes):	5484
Entropy (8bit):	5.169237586099563
Encrypted:	false
SSDEEP:	96:nVXbd8yDMfp+QO/yaAVVaxk0JCKL8rsbOTQVuwn:nVXbjMfp+b/y9XS4KsW
MD5:	5E0EFD1DD7CBDA6C4ABE1C21288198EE
SHA1:	7A41CAB5B161A2296878C572990D2C97BCB367FB
SHA-256:	06DF7DC15D5236E9171ED83C52ABC288D9AEFE73B880C60167ABB8E8B23700C5
SHA-512:	AE9D07942AB6A72429440C9C0DCE06870632DCEDD45EC2FF99B1C89267DD019DDFBF9C6AF764D8BB2CFB6E2B8C1D55C48789C315E9F40F492AAB64BEA1DB5 60A
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13264662225298495","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
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):	4.454975609103508
Encrypted:	false
SSDEEP:	3:tUKDRIXUAE13F3j1Zmwv39RIXUAgcuHVdFhVV8s9RIXUAhCBVWGv:mLcJZmwPEQLVVvEhCBVtv
MD5:	F1576B46FD74698D7D968822B3B0B5B5
SHA1:	6C1F6043807801B27082244AF605D5D3A68060E2
SHA-256:	06E53D1BFDA50B77248D7B56A7994AD7282148E0D2019EF762C232DB95DC4286
SHA-512:	B00255D9BAF7A3DA9F48289A16094547CD734B2EC6EB11292686EFCFD5DE46EAEAF8535BC7269154073C8ADA91C37C1CBBA817F2C25923A49463F9B1E894981
Malicious:	false
Reputation:	low
Preview:	2021/05/04-21:23:58.029 1b08 Recovering log #3.2021/05/04-21:23:58.209 1b08 Delete type=0 #3.2021/05/04-21:23:58.210 1b08 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
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKIVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF04
Malicious:	false
Reputation:	low
Preview:	V........leveldb.BytewiseComparator...#...........

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f96c85a6-a601-49b5-a8bc-08e22ee85cf0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	874
Entropy (8bit):	5.55052453213819
Encrypted:	false
SSDEEP:	12:YmZ6Hk3O+UAnIvcJeJrNgmh4r+UAnIEJScNnYj+UAnIEORflR7N+UAnIbBVWFKOR:Yc6H0Uhc4G1KUe4aUeqb7wUB3RUeHQ
MD5:	DC8B03F3187FE0B2D9822839C0B11A6B
SHA1:	65D15E5A643B81D07C79892AFE57CFC005AF15B2
SHA-256:	D2BFCDB2225B4D9E2D9B8F24B6B8FE1AA357A47559C426E43C6A20E041D3A134
SHA-512:	B3717E8BBE6784F571AF0172E0B25FB347671A9B3FFA17377065042E23558F78090ADA234F94037FF5008F77E82ED98BFD3C4FF0701EBE4FAE4430A2AE191EE5
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633015352.675531,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601479352.675536},{"expiry":1633015352.520557,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601479352.52056},{"expiry":1633015352.455722,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601479352.455726},{"expiry":1651724630.059558,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620188630.059561},{"expiry":1633015352.814139,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601479352.814142}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\fabebae9-01e7-48a5-adf9-ff1c9673ea15.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):	4862
Entropy (8bit):	4.947242544123496
Encrypted:	false
SSDEEP:	96:nVXbd8oqmfpaAVVaxk0JCKL8robOTQVuwn:nVXbSmfp9XS4Ksa
MD5:	8EBE2E78A2F2F37B8CE92F757F727F5E
SHA1:	9FBA7248E7C1348DC4176E3EB7DADD3F2200C7CD
SHA-256:	09520BC6FE24CFC5E094BE8D874A8C5BB801C46D1327E1BD69CCCB719159D460
SHA-512:	DAB321000B37B0586629B6958599D0317AC3086629E6F7C00A85CB0678C9D4B44D8639EABE863E1A9DD31FF01D7613F81354C682A60488746E1DF9DA5A356E92
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13264662225298495","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0","

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):	344
Entropy (8bit):	5.221851786918587
Encrypted:	false
SSDEEP:	6:mLvjq2PN723iKKdKfrzAdIFUtpENXZmwPESkwON723iKKdKfrzILJ:uvVa5Kk9FUtpQ/Pp5Oa5Kk2J
MD5:	1DEA929B85ED8A813A4CC9ECE79361C4
SHA1:	3348D1C04CC6C4119C6D2A636AC5CD1C5709AA0C
SHA-256:	9C4097EE2EE89F4B938B8622CDE88B3531D5C34316FB2B1CF599573A1A1C2559
SHA-512:	23CE603EA9B45CC910D4A5AA8DBF941312969FB3570B4DBEF333B2E7DC82D880C87C3440D4DABA7C9CF61D69FC24F46E8FE85F7B5C593E8AFBF113A1A2B2F0B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Preview:	2021/05/04-21:23:58.634 1b84 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.202 1/05/04-21:23:58.640 1b84 Recovering log #3.2021/05/04-21:23:58.641 1b84 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\ddf0b04d-1b16-46ba-9ec9-d735d1ab0bad.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):	371482
Entropy (8bit):	6.049826236838379
Encrypted:	false
SSDEEP:	6144:YEr/NOXZG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinC:H7NOJGNPUZ+w7wJHyEtAWv
MD5:	1ABDDDCD6E24B67C1126B1BAFF083693
SHA1:	F4737C4CDB3498B86A3296974848B5480E38CF17
SHA-256:	BC96FEA801E08BBCF42A72A262B3E03CF237AD2002176419E3225D371C4A7F3D
SHA-512:	E1392F52B51FA3B271B0CF4D7E3E94BA3719C53A84770ECEC98FE15FBC6C5DCB1318B817CE6330F3BB4C212AC5341AD72EA8F34C383470618CF513AB88B777 4
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":1.620188628273524e+12,"network":1.62015623e+12,"ticks":161240991.0,"uncertainty":4906379.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488960180"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\f8881a1c-3d4f-41fa-9101-4ebc63b43873.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\f8881a1c-3d4f-41fa-9101-4ebc63b43873.tmp	
Size (bytes):	371482
Entropy (8bit):	6.049826193215441
Encrypted:	false
SSDEEP:	6144:+Er/NOXZG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinC:l7NOJGNPUZ+w7wJHyEtAWv
MD5:	0E95424C8A4353CDF19A7D92427E3D47
SHA1:	DF2D64D0095FB2C8B1993768F711D4B41E70705D
SHA-256:	068BC222ECAEA2CD80200FF187AC94BBC948FB6A92D28E3D90E1DDD2BF2E0ED3
SHA-512:	093ED287AD2FA76A49A3D5927EE4492DF4F69579034F87E206796F8C244624FBF3456ECBBFF1ADD1260ADCB52CD4E1160E51899B49E260B580071948883E8951
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":1.620188628273524e+12,"network":1.62015623e+12,"ticks":161240991.0,"uncertainty":4906379.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\f91a24d7-6a3e-40aa-8fb2-4df1736d319d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.748556024810905
Encrypted:	false
SSDEEP:	384:nHdySsPZYMb21NKr/v+G3tGkZH0tGRYrzQSUxb5IlQbrD6xmvUzgq2WVOgEmNQS/:PmRxCEF9Qef8u0s/DWmKs2WBL
MD5:	4BB4A1B85D00742D58934905D3FA11C1
SHA1:	A6355E3D9278B1855ABC50C4B24CFB7F8B36B4F9
SHA-256:	E59FF1504F8CF195B712FB313A7441887A5A18723896A4C1D34551F0E022BA74
SHA-512:	D45DFC8C9F92D5DD41A6180B86D2F90AD70BEB1D0A4DDF8C2B22DA2A9EEE9EFFAABA81FB1CB5B856B79E52592398D36CC08AE1E068B8C402062AEA5378A0C64
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....98.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\0b202f1f-3bb0-46d8-ae4a-c5c64dc25809.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
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.$.....I-m.....m....ni...`..W.....R.p.b.+...+.\k.R$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\107e86bb-2c6a-415f-b8dc-1fcaed3e1d88.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

C:\Users\user\AppData\Local\Temp\107e86bb-2c6a-415f-b8dc-1fcaed3e1d88.tmp	
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\45040fc5-b1d0-4b6a-be95-a5f4e016b916.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\6389ea05-8027-40a2-a1cf-d1647ead34c6.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_dir6800_1086792300\0b202f1f-3bb0-46d8-ae4a-c5c64dc25809.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
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\0b202f1f-3bb0-46d8-ae4a-c5c64dc25809.tmp	
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...l.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\am\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17307
Entropy (8bit):	5.461848619761356
Encrypted:	false
SSDEEP:	384:arfbEVrFvMP4rMhuDopC3vUuFBYZV6uml:aHEVrFvMP4KuFvr6D6uml
MD5:	26330929DF0ED4E86F06C00C03F07CE3
SHA1:	478F3B7E7A7E007BEE182B89C2EF6FFE6045E92C
SHA-256:	621B5139ED199022BB6529AF18ED4DC312AE9F3E90ECAF3B2C9E1D12114F5B22
SHA-512:	0BE6183A1BF12575C0F99960705D4249E79CDB8528C55FF132BE99A111F09494231AD6A36CD61B090A3B34C6971D68A29373BA346888E852C52E05DC14380682
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "1282768764603190 75": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": ".... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "... ...".. },.. "1802762746589457177": {.. "message": "...".. },.. "1850397500312020388": {.. "message": ".$START_LINK$Google Home .....END_LINK ... . Chromecast ....? $START_SPAN$*END_SPAN",.. "placeholde

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\ar\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16809
Entropy (8bit):	5.458147730761559
Encrypted:	false
SSDEEP:	192:0IprKC78JmUjk8RkeryFOYPATxLZ8fsbE3/IFV6c8TEKdl:Jrp8JjA8RkerK0lc3wFV6uml
MD5:	44325A88063573A4C77F6EF943B0FC3E
SHA1:	78908D766F3E7A0E4545E7BD823C8ED47C7164EB
SHA-256:	67A439A08804EF4BEF261BDBADD8F0FEFD51729167D01EDCA99DD4AF57D6108B
SHA-512:	889C02BC986794C58C76022E78F57F867DD1D5217687F12D679A33A2DB9E5A18F3A37CF94D8FE4585E747C78E4662EAB93361FF7D945990774C7CFCACCFB79D
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": ".. .. ..".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "...".. },.. "1636686747687494376": {.. "message": ".....".. },.. "180276746589457177": {.. "message": "..... .....".. },.. "1850397500312020388": {.. "message": "... .... Chromecast .. $START_LINK$..... Google HomeEND_LINK. $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	18086
Entropy (8bit):	5.408731329060678
Encrypted:	false
SSDEEP:	192:4jjpr342SIwPIasR9VhMkACVmrv8evj+3eXivOMbb2vVzCkwRV6V6c8TEKdl:4ZrYo+rxT+qOV6V6uml
MD5:	6911CE87E8C47223F33BEF9488272E40
SHA1:	980398F076BB7D451B18D7FDE2DE09041B1F55AD
SHA-256:	273DEF0F67F0FA080802B85EF6F334DE50A19408F46BDF41F0F099B1F5501EEA
SHA-512:	CDB69405BB553E46DCF02F71B1A394307D0051E7FA662DFFEBA7888F30DD933F13C7FD6E32F1D7AEAEE8746316873B6E1D92029724ABDC75E49DCC092172EA2
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "......".. },.. "1213957982723875920": {.. "message": "... .. ..-..... ....?".. },.. "12827687 6460319075": {.. "message": "..... .. ..".. },.. "1428448869078126731": {.. "message": "..... .. ..".. },.. "1522140683318860351": {.. "message": "..... .. .., ...".. },.. "155090406471082895 8": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "18027627 46589457177": {.. "message": ".... .. ..".. },.. "1850397500312020388": {.. "message": "..... .. .. Chromecast . $START_LINK$..... Google Hom eEND_LINK? $START_SPAN$*END_SPAN",.. "p

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\bn\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19695
Entropy (8bit):	5.315564774032776
Encrypted:	false
SSDEEP:	384:PrUCrcTIOeswIW/Vre/sZn8TFfzheV6uml:lPswlWtoK8xfG6uml
MD5:	F9DDF525C07251282A3BFFCEE9A09ABB
SHA1:	A343A078E804AF400A8F3E1891E3390DA754A5CD
SHA-256:	C69C6C90F7EB8F10685CD815AF1F6F1B87CF30C4E8D95DF1D577DE1105AAD227
SHA-512:	EBD339C37162984672513019D470B92DF8B743DD69D4430361EF12D42FD1C208DBDE818A7BFE20BE8A7D63CD6E02B3F4344DEA1C4AEDB8719D789981A49DA4C
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "..... ...".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... ....".. },.. "1522140683318860351": {.. "message": "..... ... .".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "$START_LINK$ Google

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15518
Entropy (8bit):	5.242542310885
Encrypted:	false
SSDEEP:	384:drGUBKxMF2ayv8FrIccUVFmwf+7d9VKS3V6uml:dCUBKxMFBy0FE3UzmQ+zkSl6uml
MD5:	A90CF7930E7C3BEC61EE252DEFAD574A
SHA1:	F630CA01114A7BDD39607CB84B8280CCE218A5C6
SHA-256:	A533740E17559E2ADF40B4555C60F21EEC84E92C09CDBC19EED033A0B4DD2474
SHA-512:	598F991B344FA6724617D6CE57BB0D6D64EF86B4F5317BF6AD5EDF43E6B0A385094E7885F7A8FA2B107405B31C3D9F76E92315BC1D9BB52ACD4ECAD342917DE1
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Es congela".. },.. "1213957982723875920": {.. "message": "Quina de les opcions.seg.ents descriu millor la vostra xarxa?".. },.. "128276876460319075": {.. "message": "Detecci. de dispositius".. },.. "1428448869078126731": {.. "message": "Flu.desa del v.deo".. },.. "1522140683318860351": {.. "message": "S'ha produ.t un error en la connexi.. Torneu-ho a provar.".. },.. "1550904064710828958": {.. "message": "Correcta".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volum".. },.. "1850397500312020388": {.. "message": "Pots veure el Chromecast a l'$START_LINK$aplicaci. Google.HomeEND_LINK?$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15552
Entropy (8bit):	5.406413558584244
Encrypted:	false
SSDEEP:	192:eVdprJrG5efiTk93ebrxZR1fdc8VDCwT9fTV6c8TEKdl:2rMqiQerxQ88W7V6uml
MD5:	17E753EE877FDED25886D5F7925CA652
SHA1:	8E4EC969777CC0CEB7C12D0C1B9D87EBBB9C4678
SHA-256:	C562FCCFCE374D446BFAC30AC9B18FF17E7A3EF101C919FF857104917F300382
SHA-512:	33D61F6327FC81D7A45AA2CC97922DC527F5F43E54AA1A1638DA6EE407024A2F10CFD82CC5C3C581C2E7B216276987CB26C3FA95198572E139ACF29CC5B7ADB
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Video zamrz.".. },.. "1213957982723875920": {.. "message": "Kter. popis nejl.pe vystihuje va.i s..?".. },.. "128276876460319075": {.. "message": "Zji..ov.n. za..zen.".. },.. "1428448869078126731": {.. "message": "Plynulost videa".. },.. "1522140683318860351": {.. "message": "P.ipojen. se nezda.ilo. Zkuste to pros.m znovu.".. },.. "1550904064710828958": {.. "message": "Plynul.".. },.. "1636686747687494376": {.. "message": "Perfektn.".. },.. "1802762746589457177": {.. "message": "Hlasitost".. },.. "1850397500312020388": {.. "message": "Vid.te sv.j Chromecast v.$START_LINK$aplikaci Google Home END_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\da\messages.json	
Size (bytes):	15340
Entropy (8bit):	5.2479291792849105
Encrypted:	false
SSDEEP:	192:+Upr8XnI1MY2kPuir8j7Rd3kbTWc4QtV6c8TEKdl:FrJ1H9br8h6eZCV6uml
MD5:	F08A313C78454109B629B37521959B33
SHA1:	3D585D52EC8B4399F66D4BE88CED10F4A034FCCC
SHA-256:	23BF7E5EDF70291CA6D8F4A64788C5B86379EECB628E3DFA7DD83344612F7564
SHA-512:	9F2868AEBBF7F6167A7EA120FE65E752F9A65D1DC51072AA2413B2FDE374DA2D169D455A4788E341717F694179E6F1FA80413C080D9CD8CB397C3E84668CBFE
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Fryser".. },.. "1213957982723875920": {.. "message": "Hvilket af f.lgende udsagn beskriver bedst dit netv.rk?".. },.. "128276876460319075": {.. "message": "Enhedsregistrering".. },.. "1428448869078126731": {.. "message": "Videostabilitet".. },.. "152214068331 8860351": {.. "message": "Forbindelsen blev afbrudt. Pr.v igen.".. },.. "1550904064710828958": {.. "message": "Problemfri".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lydstyrke".. },.. "1850397500312020388": {.. "message": "Kan du se din Chromecast i $ START_LINK$ Google Home-appenEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "STAR

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15555
Entropy (8bit):	5.258022363187752
Encrypted:	false
SSDEEP:	192:AJprM71A4qyJSwlk5KR5rtXsmvL0xhVw921YV6c8TEKdl:2re3jJS5A5rt8msA2KV6uml
MD5:	980FB419ED6ED94AD75686AFFB4E4C2E
SHA1:	871BFBCA6BCBA9197811883A93C50C0716562D57
SHA-256:	585C7814AFD2453232BC940252D4AE821D6E6CBCFD74A793F78E5DB8BA5342F1
SHA-512:	1681FA9C3BA882250A5005FB807D759EB8A634F1AA011725B1C865C0028BE7AB7BC16DC821A7F5BBFBA84C91E7D663ADE715284798E7E84E8FFF2D254488882
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "H.ngenbleiben".. },.. "1213957982723875920": {.. "message": "Welche dieser Aussagen beschreibt dein Netzwerk am besten?".. },.. "128276876460319075": {.. "message": "Ger.teerkennung".. },.. "1428448869078126731": {.. "message": "Videowiedergabequalit.t".. },.. "1522140683318860351": {.. "message": "Fehler beim Herstellen der Verbindung. Bitte versuche es noch einmal.".. },.. "1550904064710828958": {.. "message": "St.rungsfrei".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lautst.rke".. },.. "18503975003 12020388": {.. "message": "Siehst du deinen Chromecast in der $START_LINK$Google Home AppEND_LINK? $START_SPAN$*END_SPAN",.. "placeholde rs": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17941
Entropy (8bit):	5.465343004010711
Encrypted:	false
SSDEEP:	384:S0rDuhLh41cZrP3TzDBknbpgo6djIV6uml:S0fuBh46ZD3TzDinbpgoUK6uml
MD5:	40EB778339005A24FF9DA775D56E02B7
SHA1:	B00561CC7020F7FE717B5F692884253C689A7C61
SHA-256:	F56BF7C171AA20038EE30B754478B69A98F3014C89362779B0A8788C7B9BEEE1
SHA-512:	8BED281A33EC1E4E88A9F9D62BB13FE0266C0FAF8856D1DC2A843D26DD3CE5E7D1400FD3325ABD783B0364EC4FB1188AD941D56AEB9073BC365BE0D12DE6C 013
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "......".. },.. "1213957982723875920": {.. "message": ".... ... .;".. },.. "1282768 76460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": "..... ....".. },.. "1850397500312020388": {.. "message": "..... .. .. Chromecast .... $START_LINK$..... Google HomeEND_LINK; $START_SPAN $*$END_SPAN$",.. "placeholders": {.. "END_LINK": {.. "content

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	14897
Entropy (8bit):	5.197356586852831
Encrypted:	false

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\en\messages.json	
SSDEEP:	96:2MKUOp5N7GTNMRuv6M0blt3FXGkW6/5NkkQ9NJKJhnH3t9F410sUA+ISN6cGDSyR:VKzprogudTGkWqrKcJhdIR+V6c8TEKdl
MD5:	8351AF4EA9BDD9C09019BC85D25B0016
SHA1:	F6EC1FFD291C8632758E01C9EE837B1AD18D4DCF
SHA-256:	F41C82D8A4F0E9B645656D630C882BE94A0FB7F8CEC0FE864B57298F0312B212
SHA-512:	75672B57F21F38F97341AD76A199AD764E9FBAB2384D701BF6EB06CEFDE6C4F20F047F9051A4E30D99621E5C1FBBDB9E38E8D2B47470806704B38DA130A146C
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": "Freezes".. },.. "12139579827238759 20": {.. "message": "Which of the following best describes your network?".. },.. "12827687646031907 5": {.. "message": "Device Discovery".. },.. "14284488690781267 31": {.. "message": "Video Smoothness".. },.. "15221406833188603 51": {.. "message": "Connection failed. Please try again.".. },.. "15509040647108289 58": {.. "message": "Smooth".. },.. "16366867476874943 76": {.. "message": "Perfect".. },.. "18027627465894571 77": {.. "message": "Volume".. },.. "18503975003120203 88": {.. "message": "Are you able to see your Chrom ecast in the $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "START

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15560
Entropy (8bit):	5.236752363299121
Encrypted:	false
SSDEEP:	192:NAgprfy1pTCukFr+1DIyDRoanvV6c8TEKdl:KMrq6FrmvV6uml
MD5:	8A70C18BB1090AA4D500DE9E8E4A00EF
SHA1:	8AFC097FA956C1317DB0835348B2DA19F0789669
SHA-256:	FF173D1CEF665B1234E02F11070ABD2B65230318150734579A03C7F31B4AE3F4
SHA-512:	140BAF40A4ABE9B8AF0855B0EBB7DFDF17869EDFC4EE1037C5EA7FDD8EDEBD4850E055B6A4D7B8782657618BCE1517813779BA01BA993CC838BB43E0BE71E EEE
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": "Congelaci.n de im.genes".. },.. "12139579827238759 20": {.. "message": ".Cu.l de las siguientes respuestas descr ibe mejor tu red?".. },.. "12827687646031907 5": {.. "message": "Detecci.n de dispositivo".. },.. "14284488690781267 31": {.. "message": "Fluidez del v.deo".. },.. "15221406833188603 51": {.. "message": "Error en la conexi.n. Vuelve a intentarlo.".. },.. "15509040647108289 58": {.. "message": "V.deo fluido".. },.. "16366867476874943 76": {.. "message": "Perfecta".. },.. "18027627465894571 77": {.. "message": "Volumen".. },.. "18503975003120203 88": {.. "message": ".Puedes ver tu Chromecast en la $START_LINK$aplicaci.n Google.HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\et\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15139
Entropy (8bit):	5.228213017029721
Encrypted:	false
SSDEEP:	96:Z48bxhWYp5Ny5M63niwAKD4rrJSJ2RkPXh9P5NFP2+NBMU01jewUEVez3QOiSevy:ikxprot3lYkf/rHBc0KsUV6c8TEKdl
MD5:	A62F12BCBA6D2C579212CA2FF90F8266
SHA1:	F7E964A2D9BBDA364252BCE5CFBA3FD34FDD825E
SHA-256:	3EB3EB0B3B4A8E5A477D1B3C3A3891CCC7DC6B8879ECE243A7BD7C478068273D
SHA-512:	E300201245C00ADEC8F39D586875F8FA4607AB203572BF3CE353C1CA7CDCA05B8786810CA0CEE27E4EA54A5EFD53690F1EA7AA4148CFF472A66BB1120272356 6
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": "Hangub".. },.. "12139579827238759 20": {.. "message": "Milline j.rgmistest v.idetest kirjeldab k.ige paremini teie v.rku?".. },.. "12827687646031907 5": {.. "message": "Seadme tuvastamine".. },.. "14284488690781267 31": {.. "message": "Video sujuvus".. },.. "152 2140683318860351": {.. "message": ".hendamine eba.nnestus. Proovige uuesti.".. },.. "15509040647108289 58": {.. "message": ".htlane".. },.. "16366867476 87494376": {.. "message": "T.iuslik".. },.. "18027627465894571 77": {.. "message": "Helitugevus".. },.. "18503975003120203 88": {.. "message": "Kas n.ete oma Chromecasti $START_LINK$rakenduses Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "conte nt": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\fa\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17004
Entropy (8bit):	5.485874780010479
Encrypted:	false
SSDEEP:	192:rngaIprIX/t9wkjTJrs3hqaXxRQdiIMDnD+LhfHdoltV6c8TEKdl:4rin5rU1X7Qd0M9CtV6uml
MD5:	852BD3CFF960F1BC3A2AAB3CB3874EF9

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\fa\messages.json	
SHA1:	C9F6F3C776542889FE3B67971D65ACFE048A3A0A
SHA-256:	D87597B6C10364501B98AA42524843F109009CCEF022D8E0170440D7F144F4C6
SHA-512:	2A7AE4D70E33E53EE31831CE2E61DD8DF103C4170EC483BDA14B8788E5DD536EEE84DBA340CACBDF16889C7E6465B48D82C4714E746E8A7B372D12CBDF371 95
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".... ... .".. },.. "1213957982723875920": {.. "message": ".... .. ..".. },.. "128 276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "....".. },.. "1802762746589457177": {.. "message": "..... ....".. },.. "1850397500312020388": {.. "message": ".... .... Chromecast ... . $START_LINK$ ..... Google HomeEND_LINK ..... $START_SPA N$*END_SPAN",.. "placeholders": {.. "END_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\fi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15268
Entropy (8bit):	5.268402902466895
Encrypted:	false
SSDEEP:	192:efMprYXiYUNpj5Coik1tXxrUhvUzSPWV6c8TEKdl:eIrjbjosdrU5WV6uml
MD5:	3902581B6170D0CEA9B1ECF6CC82D669
SHA1:	C8208AC2B1DD6D4F8BDAAE01C8BD71FFFA5A732B
SHA-256:	D2A8180225A83A423BB6E17343DFA8F636D517154944002ED9240411B8C0C5E1
SHA-512:	612FDD8A3C5051F0A4F1E11E50B5D124B337C77D62D987D35C2AF9E08AFC6AFCEBAEE8D40FDFBCD1E1889F39758B96FAECBF6C6D1CF146C741A5261952050 21
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Pys.htyy".. },.. "1213957982723875920": {.. "message": "Mik. seuraavista kuvaa parhaiten verkkoasi?".. },.. "128276876460319075": {.. "message": "Laitteiden tunnistaminen".. },.. "1428448869078126731": {.. "message": "Videon tasaisuus".. },.. "152214068331886 0351": {.. "message": "Yhteys ep.onnistui. Yrit. uudelleen.".. },.. "1550904064710828958": {.. "message": "Tasainen".. },.. "1636686747687494376": {.. "message": "T.ydellinen".. },.. "1802762746589457177": {.. "message": "..nenvoimakkuus".. },.. "1850397500312020388": {.. "message": "N.etk. Chromecastisi $START_LINK$Google Home .sovelluksessaEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },..

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\fil\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15570
Entropy (8bit):	5.1924418176212646
Encrypted:	false
SSDEEP:	192:+esprzAsQp68wIJYkMyr2k0jR1/7Rr1uV6c8TEKdl:Gr78JDMyrR0tJuV6uml
MD5:	59483AD798347B291363327D446FA107
SHA1:	C069F29BB68FA7BA2631B0BF5BBF313346AC6736
SHA-256:	DD47530EAE96346CD4DC3267A0BB1091BB17B704803A93CDA2E3E81551B94F12
SHA-512:	091595CA135E965ED3DE376873541117F0E7A8EBDEB4714833EFDD6C820234373891BE5DEC437BA85CCB79CCCA053D407E6ADA17EBDAE7D313324A48775C00 0
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Hindi gumagalaw".. },.. "1213957982723875920": {.. "message": "Alin sa sumusunod ang pinakamahusay na naglalarawan sa iyong network?".. },.. "12827687646031907 5": {.. "message": "Pagtuklas ng Device".. },.. "1428448869078126731": {.. "message": "Pagka-s mooth ng Video".. },.. "1522140683318860351": {.. "message": "Hindi nakakonekta. Pakisubukang muli.".. },.. "1550904064710828958": {.. "message": "Smoot h".. },.. "1636686747687494376": {.. "message": "Perpekto".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Nakikita mo ba ang iyong Chromecast sa $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\fr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15826
Entropy (8bit):	5.277877116547859
Encrypted:	false
SSDEEP:	192:nLZprAZg3EkV3sjrICe8L/1Va7lt1rlxLAkoYHHavV6c8TEKdl:vrW+2jrI7TdLAk3MV6uml
MD5:	9B416146FE4F1403C2AACAC4DCF1A5C3
SHA1:	616F055C9FAD4CE972DF82EC8A9B2F4EDA3E7FAD
SHA-256:	7C7F5758F54008190ACCDDBD1761CBD980FB5FE0847E992874498228D2571DBC

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\fr\messages.json	
SHA-512:	6E8E70380A8C6E2C0587ADFF6AE36963EC76694904841CE1DFE4EEE215B917AD3E8AF727555627FBDF6B8BA6A4A0674D2B90AC4E9331B6628A32F4C4348FB51B
Malicious:	false
Reputation:	low
Preview:	{.. "10198456148852051 7": {.. "message": "Se fige".. },.. "12139579827238759 20": {.. "message": "Parmi les propositions suivantes, laquelle d.crit le mieux votre r.seau.?".. },.. "128276876460319075": {.. "message": "D.tection d'appareils".. },.. "14284488690781267 31": {.. "message": "Fluidit. de la vid.o".. },.. "15221406833188603 51": {.. "message": ".chec de la connexion. Veuillez r.essayer.".. },.. "15509040647108289 58": {.. "message": "Fluide".. },.. "1636686747687494376": {.. "message": "Parfaite".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Votre Chromecast est-il visible dans l'$START_LINK$application Google.HomeEND_LINK.? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\gu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19255
Entropy (8bit):	5.32628732852814
Encrypted:	false
SSDEEP:	384:Hq2Mr+qPlJKYMdzKgXr3dGsGF+yAK37Wf7Cy/V6uml:KxzTVgX7ykj6uml
MD5:	68B03519786F71A426BAC24DECA2DD52
SHA1:	B8E6608932EC5CEC4BC3C5475BFC3E312D2E2E7D
SHA-256:	C77A4D27E9E6CA25B9290056D93A656E3EBE975957E4C2EE9F0FB11B133D5CD4
SHA-512:	5FFE06A10774877AF25E05BA07F3032CC52F874896D67E320F4EF9D524A22E40B462CC6206700E9557EB354FA2730172DC6912EBCA49C671FB0EF155B17F9EFF
Malicious:	false
Reputation:	low
Preview:	{.. "10198456148852051 7": {.. "message": ".....".. },.. "12139579827238759 20": {.. "message": "..... ....?".. },.. "128276876460319075": {.. "message": "..... ...".. },.. "14284488690781267 31": {.. "message": "..... .....".. },.. "15221406833188603 51": {.. "message": "..... ....".. },.. "15509040647108289 58": {.. "message": "....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "... ... $START_LINK$ Google Home ..END_LINK... Chromecast..

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\hi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19381
Entropy (8bit):	5.328912995891658
Encrypted:	false
SSDEEP:	384:zrGrSmhKy7KyY+bNEDqlQdrMEPxtShJV6uml:zBqG6QdwEPrW6uml
MD5:	20C86E04B1833EA7F21C07361061420A
SHA1:	617C0D70E162CF380005E9780B61F650B7A39F9B
SHA-256:	C2C27CA242DBDE600BA3AA7782156BC2B190A64D8A1B51EDC8007BDECA139553
SHA-512:	9FB91AA8E0226519E298B1136E8A1A3C1879DB7F0E6052AF1BFD55921CD698346278D04602510680A9695A76DD5C96D9665380580044C50D81392BB2CB3E8E95
Malicious:	false
Reputation:	low
Preview:	{.. "10198456148852051 7": {.. "message": ".....".. },.. "12139579827238759 20": {.. "message": "..... ... .?".. },.. "128276876460319075": {.. "message": "..... ...".. },.. "14284488690781267 31": {.. "message": "..... .....".. },.. "15221406833188603 51": {.. "message": "..... ....".. },.. "15509040647108289 58": {.. "message": "....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": ".... .. $START_LINK$ Google Home .....END_LINK ... . Ch

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\hr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15507
Entropy (8bit):	5.290847699527565
Encrypted:	false
SSDEEP:	192:Pdapr6h85tRwVQgkvJryLkla5Kfndg/V6c8TEKdl:Arwot2Q7BryVce/V6uml
MD5:	3ED90E66789927D80B42346BB431431E
SHA1:	2B061E3271DF4255B1FFC47BDB207CDEC0D9724F
SHA-256:	0B41E3C42414F72C9A12C05F8772597F9685115366A774C66018467AD4B71A74
SHA-512:	92BE43F1FFC8EFBF5BBC50573AC4C65F6104416A5B6CD04404C3A9854CA3DCF2A43A4044C168590CDF83887D234495843572331ADCD5B020D2E48A3956F3C16
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\hr\messages.json	
Preview:	{.. "1019845614885205 17": {.. "message": "Zamrzavanje".. },.. "1213957982723875920": {.. "message": "Koje od sljede.eg najbolje opisuje va.u mre.u?".. },.. "128276876460319075": {.. "message": "Otkrivanje ure.aja".. },.. "142844869078126731": {.. "message": "Ujedna.enost videoreprodukcije".. },.. "1522140683318860351": {.. "message": "Povezivanje nije uspjelo. Poku.ajte ponovo.".. },.. "1550904064710828958": {.. "message": "Glatko".. },.. "1636686747687494376": {.. "message": "Savr.ena".. },.. "1802762746589457177": {.. "message": "Glasno.a".. },.. "1850397500312020388": {.. "message": "Vidite li svoj Chromecast u $START_LINK$aplikaciji Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "co ntent": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\hu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15682
Entropy (8bit):	5.354505633120392
Encrypted:	false
SSDEEP:	192:CCEAproS9fZv+JwkDMrC2NSxoSgbV6c8TEKdl:5r5VZv+RDMrazoV6uml
MD5:	8E9FF7E49473C5734A2F6F0812E12EB3
SHA1:	A4F10DDD1580582533D5EB59EDF6D8048F887C81
SHA-256:	6CDD2FB39ADECE00E88B989E464B05ED1414092D0492F6D0AE58D549BFD1A46A
SHA-512:	E9A4AF31B1A276F395599BB620A3164CABF3459F3C102DD3F57DFEA734510BD985DE65CB409E1975559ACCC615075439A08E1DEBE22C90A0ABCAA3CAFEE79AC7
Malicious:	false
Reputation:	low
Preview:	{.. "1019845614885205 17": {.. "message": "Lefagy".. },.. "1213957982723875920": {.. "message": "Az al.bbiak k.z.l melyik jellemzi legjobban h.l.zat.t?".. },.. "128276876460319075": {.. "message": "Eszk.zfelfedez.s".. },.. "1428448869078126731": {.. "message": "Vide. folyamatoss.ga".. },.. "1522140683318860351": {.. "message": "Sikertelen kapcsol.d.s. K.rj.k, pr.b.lja .jra.".. },.. "1550904064710828958": {.. "message": "Folyamatos".. },.. "1636686747687494376": {.. "message": "T.k.letes".. },.. "1802762746589457177": {.. "message": "Hanger.".. },.. "1850397500312020388": {.. "message": "L.tja a Chromecastot a $START_LINK$Google Home alkalmaz.sbanEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content":

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\id\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15070
Entropy (8bit):	5.190057470347349
Encrypted:	false
SSDEEP:	192:GsprMtChjkWfrEWL0KRCnEOWV6c8TEKdl:9rtAEr3LTRuWV6uml
MD5:	7ADF9F2048944821F93879336EB61A78
SHA1:	C3DA74FB544684D5B250767BB0CB66FFB7C58963
SHA-256:	3630947E1075E3663AD3E4824D0BE42CB47C0D615D8053E83B9595047C8BA9BE
SHA-512:	1F28BB80E1839C5581106BEA3AE2501C7618249D7E3115819F5A9A87771D59F5DE346C1B9C87F7FFC390604D5B9888CE738E25F2F04A094002A0FB3B22CBEC95
Malicious:	false
Reputation:	low
Preview:	{.. "1019845614885205 17": {.. "message": "Membeku".. },.. "1213957982723875920": {.. "message": "Dari berikut ini, manakah yang paling mendeskripsikan jaringan Anda?".. },.. "128276876460319075": {.. "message": "Penemuan Perangkat".. },.. "1428448869078126731": {.. "message": "Kelancaran Video".. },.. "1522140683318860351": {.. "message": "Sambungan gagal. Coba lagi.".. },.. "1550904064710828958": {.. "message": "Lancar".. },.. "1636686747687494376": {.. "message": "Sempurna".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Bisakah Anda melihat Chromecast di $START_LINK$aplikasi Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": " $1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },..

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\it\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15256
Entropy (8bit):	5.210663765771143
Encrypted:	false
SSDEEP:	192:lYprk52dAaykVza8rE0QWBKD9+vq0hKEV6c8TEKdl:qrlA8r6DalV6uml
MD5:	BB3041A2B485B900F623E57459AE698A
SHA1:	502F5EA89F9FB0287E864B240EA39889D72053A4
SHA-256:	025737EF8FA06706B3F26D0F52B4844244A6D33DAE1D82FEF2931A14C003D57E
SHA-512:	BA51784073BEF82F3A116B33DA406FDB10EC823B9EE74375C46036DAD8BDCB4141F60845DE141ABE42CEEF9251572F6AB287CA5FC7669C60E4F68071D5AB8CD
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\it\messages.json	
Preview:	{.. "1018984561488520517": {.. "message": "Si blocca".. },.. "1213957982723875920": {.. "message": "Quale delle seguenti definizioni descrive meglio la tua rete?".. },.. "128276876460319075": {.. "message": "Rilevamento dispositivi".. },.. "1428448869078126731": {.. "message": "Uniformit. video".. },.. "1522140683318860351": {.. "message": "Connessione non riuscita. Riprova.".. },.. "1550904064710828958": {.. "message": "Fluido".. },.. "1636686747687494376": {.. "message": "Perfetta".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Riesci a vedere il tuo dispositivo Chromecast nell'$START_LINK$app Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\ja\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16519
Entropy (8bit):	5.675556017051063
Encrypted:	false
SSDEEP:	192:nkprPhQdxkRWrZe1wYpMR5wnAV6c8TEKdl:YrLRWri65wAV6uml
MD5:	6F2CC1A6B258DF45F519BA24149FABDC
SHA1:	8A58C7880C6D22765DCBB6BCE22A192C1B109AE1
SHA-256:	42ECFEE727CFC4F2845FEFDACE5EDC2E0A40AFAD69973A3B950CE653A7633342
SHA-512:	F7454F0E14301C59CC54361ACC0A1C6D072EF9BDF5DEA60646FB90B1CE47612785938C784A4CF1DE3E62648A14420374933B5F5DA43907BC00D3799FF163A3D
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "...".. },.. "1213957982723875920": {.. "message": "................................".. },.. "128276876460319075": {.. "message": "......".. },.. "1428448869078126731": {.. "message": ".......".. },.. "1522140683318860351": {.. "message": ".......................".. },.. "1550904064710828958": {.. "message": "...".. },.. "1636686747687494376": {.. "message": "....".. },.. "1802762746589457177": {.. "message": "..".. },.. "1850397500312020388": {.. "message": "$START_LINK$Google Home ...END_LINK. Chromecast ....$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\kn\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	20406
Entropy (8bit):	5.312117131662377
Encrypted:	false
SSDEEP:	384:a6C5rBSzvrZreGnla9ZBHRUDYr9yRwEcAa4rSeD5BSz0hJz8qbbM3gbr//Hkr44c:a6C5rBSzvFreGnla9ZBHRUDYr9yRwEcC
MD5:	2E3239FC277287810BC88D93A6691B09
SHA1:	FC5D585DA00ADC90BF79109C7377BD55E6653569
SHA-256:	5FC705AD19761204D8604EA069936A23731B055D51E7836CAAF16AC7719FBEEA
SHA-512:	DF8BC9E577D3ECB0E6C303E1D2C9E9A4A8317CAE810A9DFC88D91B373A4B665722C5A9AB5A589BB947FDA4C7CD9A6DF39DDD13EA47FE9EFF7E0AC43E49FF 3479
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "....... ....".. },.. "1213957982723875920": {.. "message": "...... ....?".. },.. "128276876460319075": {.. "message": "..... ....".. },.. "1428448869078126731": {.. "message": "........ ....".. },.. "1522140683318860351": {.. "message": "...... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": "........".. },.. "1850397500312020388": {.. "message": ".... $

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\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):	15480
Entropy (8bit):	5.617756574352461
Encrypted:	false
SSDEEP:	192:kWprGvSQtkxWffrnl5JuFBWVZV6c8TEKdl:TrkuxKfrlT4YVZV6uml
MD5:	E303CD63AD00EB3154431DED78E871C4
SHA1:	3B1E5B8E2CF5EBDF5D33656EF80A46563F751783
SHA-256:	FDE602BFDB1AFD282682DA5338C4F91D8A2F6CB5411DB8F62F4583D629CE67A6
SHA-512:	18BA1D5A25FBC1829AD957A531B0CC490AFCBD20AC22181021363AA3CFB916270B8732E824463C9B0897220E8AE86EB1BE561D6540E6C625F08F228F61DDFFA
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "...".. },.. "1213957982723875920": {.. "message": ".. . .. .?".. },.. "128276876460319075": {.. "message": ".. ..".. },.. "1428448869078126731": {.. "message": "... ..".. },.. "1522140683318860351": {.. "message": ".... ....".. },.. "1550904064710828958": {.. "message": "...".. },.. "1636686747687494376": {.. "message": "...".. },.. "1802762746589457177": {.. "message": "..".. },.. "1850397500312020388": {.. "message": "$START_LINK$Google Home .END_LINK. Chromecast. .....? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\lt\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15802
Entropy (8bit):	5.354550839818046
Encrypted:	false
SSDEEP:	192:lGxSprfkiRR+2zJckS1khrnPI85+80p3DWReV6c8TEKdl:lG4rlq0OkSmhrwbpIeV6uml
MD5:	93BBBE82F024FBCB7FB18E203F253429
SHA1:	83F4D80F64FA2ADCE6C515C5F663BD38A76C51DB
SHA-256:	E7A8570922CCC4F2CA3721C4E61F426158C4E7BC90274FBC8BE4040FF8B6CA9B
SHA-512:	B7E7878106B466CE95069141DF1DE387E847348B62E9C4D548006452F3E164B3AD842E9673A56DC011A5ECC3346B5863E2034EE477A9D1F3E0ABD76B2D0F640A
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Stringa".. },.. "1213957982723875920": {.. "message": "Kuris i. toliau pateikt. teigini. geriausiai apib.dina j.s. tinkl. ?".. },.. "128276876460319075": {.. "message": ".renginio suradimas".. },.. "1428488869078126731": {.. "message": "Vaizdo .ra.o sklandumas".. },.. " 1522140683318860351": {.. "message": ".vyko ry.io klaida. Bandykite dar kart..".. },.. "1550904064710828958": {.. "message": "Leid.iama skland.iai".. },.. "1636686747687494376": {.. "message": "Puiki".. },.. "1802762746589457177": {.. "message": "Garsumas".. },.. "1850397500312020388": {.. "message": "Ar .Chromecast. rodomas $START_LINK$programoje .Google Home.END_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6800_1086792300\CRX_INSTALL_locales\lv\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15891
Entropy (8bit):	5.36794040601742
Encrypted:	false
SSDEEP:	192:y18prUkm15wkLDG2raqhnZDuvyI762V6c8TEKdl:RrAL7rte62V6uml
MD5:	388590CE5E144AE5467FD6585073BD11
SHA1:	61228673A400A98D5834389C06127589F19D3A30
SHA-256:	05CA14196CA5D90B228C0F03684E03EBE403A3E7B513AE0A059244AE12B51164
SHA-512:	BF83AC90BC56CEB1CA12DCB47BCE542FB8CFE0BC14E34DE4FE1A84F7CDB4B54E36C125CEA7EE06EA6244F7795A0957A8A20DB30CA4C60FC6E96EF2A73544 8521
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".Iesald.ts. att.ls".. },.. "1213957982723875920": {.. "message": "Kur. no t.l.k min.tajiem apgalvojumiem vislab.k raksturo j.su t.klu?".. },.. "128276876460319075": {.. "message": "Ier.ces atra.ana".. },.. "1428448869078126731": {.. "message": "Video vienm.r.ba".. },.. "1522140683318860351": {.. "message": "Neizdev.s izveidot savienojumu. L.dzu, m..iniet v.lreiz.".. },.. "1550904064710828958": {.. "message": "Vienm.r.gs a tt.ls".. },.. "1636686747687494376": {.. "message": "Nevainojama".. },.. "1802762746589457177": {.. "message": "Ska.ums".. },.. "1850397500312020388": {.. "message": "Vai j.su Chromecast ier.ce ir redzama $START_LINK$lietotn. Google.HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2"..

Static File Info

No static file info

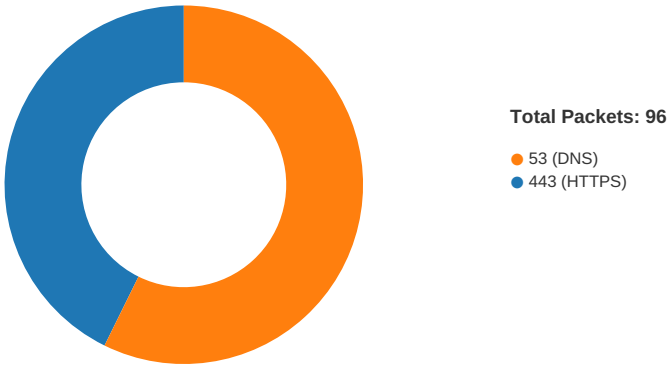
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-21:23:39.800715	ICMP	384	ICMP PING			192.168.2.6	2.23.155.128
05/04/21-21:23:39.835730	ICMP	449	ICMP Time-To-Live Exceeded in Transit			84.17.52.126	192.168.2.6
05/04/21-21:23:39.837229	ICMP	384	ICMP PING			192.168.2.6	2.23.155.128
05/04/21-21:23:39.873266	ICMP	449	ICMP Time-To-Live Exceeded in Transit			149.11.89.129	192.168.2.6

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-21:23:39.873872	ICMP	384	ICMP PING			192.168.2.6	2.23.155.128
05/04/21-21:23:39.909715	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.49.165	192.168.2.6
05/04/21-21:23:39.910155	ICMP	384	ICMP PING			192.168.2.6	2.23.155.128
05/04/21-21:23:39.951386	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.0.18	192.168.2.6
05/04/21-21:23:39.951769	ICMP	384	ICMP PING			192.168.2.6	2.23.155.128
05/04/21-21:23:39.998847	ICMP	449	ICMP Time-To-Live Exceeded in Transit			154.54.36.53	192.168.2.6
05/04/21-21:23:39.999288	ICMP	384	ICMP PING			192.168.2.6	2.23.155.128
05/04/21-21:23:40.046008	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.15.66	192.168.2.6
05/04/21-21:23:40.047594	ICMP	384	ICMP PING			192.168.2.6	2.23.155.128
05/04/21-21:23:40.113521	ICMP	449	ICMP Time-To-Live Exceeded in Transit			195.22.208.79	192.168.2.6
05/04/21-21:23:40.114051	ICMP	384	ICMP PING			192.168.2.6	2.23.155.128
05/04/21-21:23:40.167239	ICMP	449	ICMP Time-To-Live Exceeded in Transit			93.186.128.39	192.168.2.6
05/04/21-21:23:40.167725	ICMP	384	ICMP PING			192.168.2.6	2.23.155.128
05/04/21-21:23:40.220388	ICMP	408	ICMP Echo Reply			2.23.155.128	192.168.2.6
05/04/21-21:23:54.531968	ICMP	466	ICMP L3retriever Ping			192.168.2.6	142.250.185.99
05/04/21-21:23:54.531968	ICMP	384	ICMP PING			192.168.2.6	142.250.185.99
05/04/21-21:23:54.582247	ICMP	408	ICMP Echo Reply			142.250.185.99	192.168.2.6

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:23:59.348965883 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.391496897 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.391632080 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.392076969 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.434967995 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.442230940 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.442262888 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.442286968 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.442311049 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.442337036 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.442358017 CEST	443	49752	216.58.212.129	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:23:59.442397118 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.442461967 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.493545055 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.493733883 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.493904114 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.536881924 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.537166119 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.537283897 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.539336920 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.539390087 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.539462090 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.539494991 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.540755033 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.540811062 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.540855885 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.540882111 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.543806076 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.543845892 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.543870926 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.543927908 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.546794891 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.546874046 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.546905994 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.546936035 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.549771070 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.549823999 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.549894094 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.549922943 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.552838087 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.552889109 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.552927971 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.552949905 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.555767059 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.555794954 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.555882931 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.579845905 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.579884052 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.579922915 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.579956055 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.581244946 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.581269979 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.581321001 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.581355095 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.584280014 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.584307909 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.584379911 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.587312937 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.587342024 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.587542057 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.590256929 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.590284109 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.590337038 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.593267918 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.593296051 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.593362093 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.596312046 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.596343994 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.596394062 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.599270105 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.599309921 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.599378109 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.602230072 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.602262974 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.602344036 CEST	49752	443	192.168.2.6	216.58.212.129

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:23:59.605081081 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.605114937 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.605164051 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.607712030 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.607754946 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.607834101 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.610312939 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.610346079 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.610423088 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.612957001 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.612982988 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.613048077 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.615557909 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.615600109 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.615658045 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.618166924 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.618262053 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.618289948 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.620846033 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.620898962 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.620955944 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.623398066 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.623445034 CEST	443	49752	216.58.212.129	192.168.2.6
May 4, 2021 21:23:59.623490095 CEST	49752	443	192.168.2.6	216.58.212.129
May 4, 2021 21:23:59.625372887 CEST	443	49752	216.58.212.129	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:23:34.404161930 CEST	62044	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:34.454766989 CEST	53	62044	8.8.8.8	192.168.2.6
May 4, 2021 21:23:35.289118052 CEST	63791	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:35.337825060 CEST	53	63791	8.8.8.8	192.168.2.6
May 4, 2021 21:23:35.373644114 CEST	64267	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:35.433132887 CEST	53	64267	8.8.8.8	192.168.2.6
May 4, 2021 21:23:36.110426903 CEST	49448	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:36.167826891 CEST	53	49448	8.8.8.8	192.168.2.6
May 4, 2021 21:23:37.845711946 CEST	60342	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:37.897291899 CEST	53	60342	8.8.8.8	192.168.2.6
May 4, 2021 21:23:38.801798105 CEST	61346	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:38.859132051 CEST	53	61346	8.8.8.8	192.168.2.6
May 4, 2021 21:23:39.722641945 CEST	51774	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:39.762536049 CEST	56023	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:39.785690069 CEST	53	51774	8.8.8.8	192.168.2.6
May 4, 2021 21:23:39.819776058 CEST	53	56023	8.8.8.8	192.168.2.6
May 4, 2021 21:23:41.475569963 CEST	58384	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:41.527493954 CEST	53	58384	8.8.8.8	192.168.2.6
May 4, 2021 21:23:41.740204096 CEST	60261	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:41.809022903 CEST	53	60261	8.8.8.8	192.168.2.6
May 4, 2021 21:23:42.655859947 CEST	56061	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:42.705559969 CEST	53	56061	8.8.8.8	192.168.2.6
May 4, 2021 21:23:44.243753910 CEST	58336	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:44.292351961 CEST	53	58336	8.8.8.8	192.168.2.6
May 4, 2021 21:23:46.629151106 CEST	53781	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:46.681042910 CEST	53	53781	8.8.8.8	192.168.2.6
May 4, 2021 21:23:48.670080900 CEST	50055	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:48.719012976 CEST	53	50055	8.8.8.8	192.168.2.6
May 4, 2021 21:23:50.271428108 CEST	49694	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:50.320264101 CEST	53	49694	8.8.8.8	192.168.2.6
May 4, 2021 21:23:50.562489986 CEST	54982	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:50.563563108 CEST	50010	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:50.564785957 CEST	63718	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:50.567405939 CEST	62116	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:50.568345070 CEST	63816	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:23:50.618938923 CEST	53	62116	8.8.8.8	192.168.2.6
May 4, 2021 21:23:50.619664907 CEST	53	54982	8.8.8.8	192.168.2.6
May 4, 2021 21:23:50.624283075 CEST	53	63718	8.8.8.8	192.168.2.6
May 4, 2021 21:23:50.625308990 CEST	53	63816	8.8.8.8	192.168.2.6
May 4, 2021 21:23:50.625837088 CEST	53	50010	8.8.8.8	192.168.2.6
May 4, 2021 21:23:50.986568928 CEST	55014	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:51.051619053 CEST	53	55014	8.8.8.8	192.168.2.6
May 4, 2021 21:23:51.052618980 CEST	62208	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:51.122730017 CEST	53	62208	8.8.8.8	192.168.2.6
May 4, 2021 21:23:51.178469896 CEST	57574	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:51.244358063 CEST	53	57574	8.8.8.8	192.168.2.6
May 4, 2021 21:23:51.387073040 CEST	51818	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:51.435554981 CEST	53	51818	8.8.8.8	192.168.2.6
May 4, 2021 21:23:52.489985943 CEST	56628	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:52.544291973 CEST	53	56628	8.8.8.8	192.168.2.6
May 4, 2021 21:23:54.471270084 CEST	59329	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:54.530730009 CEST	53	59329	8.8.8.8	192.168.2.6
May 4, 2021 21:23:55.828300953 CEST	64021	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:55.879772902 CEST	53	64021	8.8.8.8	192.168.2.6
May 4, 2021 21:23:58.900094986 CEST	54069	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:58.950372934 CEST	53	54069	8.8.8.8	192.168.2.6
May 4, 2021 21:23:59.286995888 CEST	61178	53	192.168.2.6	8.8.8.8
May 4, 2021 21:23:59.343893051 CEST	53	61178	8.8.8.8	192.168.2.6
May 4, 2021 21:24:00.924599886 CEST	57017	53	192.168.2.6	8.8.8.8
May 4, 2021 21:24:00.976058006 CEST	53	57017	8.8.8.8	192.168.2.6
May 4, 2021 21:24:01.535099030 CEST	56327	53	192.168.2.6	8.8.8.8
May 4, 2021 21:24:01.583785057 CEST	53	56327	8.8.8.8	192.168.2.6
May 4, 2021 21:24:09.766881943 CEST	50243	53	192.168.2.6	8.8.8.8
May 4, 2021 21:24:09.817344904 CEST	53	50243	8.8.8.8	192.168.2.6
May 4, 2021 21:24:13.664134026 CEST	62055	53	192.168.2.6	8.8.8.8
May 4, 2021 21:24:13.731594086 CEST	53	62055	8.8.8.8	192.168.2.6
May 4, 2021 21:24:27.970784903 CEST	61249	53	192.168.2.6	8.8.8.8
May 4, 2021 21:24:28.033479929 CEST	53	61249	8.8.8.8	192.168.2.6
May 4, 2021 21:24:28.137527943 CEST	65252	53	192.168.2.6	8.8.8.8
May 4, 2021 21:24:28.194905043 CEST	53	65252	8.8.8.8	192.168.2.6
May 4, 2021 21:24:30.531959057 CEST	64367	53	192.168.2.6	8.8.8.8
May 4, 2021 21:24:30.660861015 CEST	53	64367	8.8.8.8	192.168.2.6
May 4, 2021 21:24:31.874494076 CEST	55066	53	192.168.2.6	8.8.8.8
May 4, 2021 21:24:31.931581020 CEST	53	55066	8.8.8.8	192.168.2.6
May 4, 2021 21:24:32.322668076 CEST	60211	53	192.168.2.6	8.8.8.8
May 4, 2021 21:24:32.387996912 CEST	53	60211	8.8.8.8	192.168.2.6
May 4, 2021 21:24:33.219073057 CEST	56570	53	192.168.2.6	8.8.8.8
May 4, 2021 21:24:33.421406031 CEST	53	56570	8.8.8.8	192.168.2.6
May 4, 2021 21:24:33.883904934 CEST	58454	53	192.168.2.6	8.8.8.8
May 4, 2021 21:24:33.943922043 CEST	53	58454	8.8.8.8	192.168.2.6
May 4, 2021 21:24:35.202299118 CEST	55180	53	192.168.2.6	8.8.8.8
May 4, 2021 21:24:35.251553059 CEST	53	55180	8.8.8.8	192.168.2.6
May 4, 2021 21:24:36.559959888 CEST	58721	53	192.168.2.6	8.8.8.8
May 4, 2021 21:24:36.622653961 CEST	53	58721	8.8.8.8	192.168.2.6
May 4, 2021 21:24:37.146917105 CEST	57691	53	192.168.2.6	8.8.8.8
May 4, 2021 21:24:37.255454063 CEST	53	57691	8.8.8.8	192.168.2.6
May 4, 2021 21:24:38.067958117 CEST	52943	53	192.168.2.6	8.8.8.8
May 4, 2021 21:24:38.127331972 CEST	53	52943	8.8.8.8	192.168.2.6
May 4, 2021 21:24:39.893980026 CEST	59489	53	192.168.2.6	8.8.8.8
May 4, 2021 21:24:39.952121973 CEST	53	59489	8.8.8.8	192.168.2.6
May 4, 2021 21:24:41.033915997 CEST	64022	53	192.168.2.6	8.8.8.8
May 4, 2021 21:24:41.082778931 CEST	53	64022	8.8.8.8	192.168.2.6
May 4, 2021 21:24:45.735785007 CEST	60023	53	192.168.2.6	8.8.8.8
May 4, 2021 21:24:45.796885014 CEST	53	60023	8.8.8.8	192.168.2.6
May 4, 2021 21:24:46.298001051 CEST	57193	53	192.168.2.6	8.8.8.8
May 4, 2021 21:24:46.355007887 CEST	53	57193	8.8.8.8	192.168.2.6
May 4, 2021 21:24:47.334894896 CEST	64413	53	192.168.2.6	8.8.8.8
May 4, 2021 21:24:47.392038107 CEST	53	64413	8.8.8.8	192.168.2.6
May 4, 2021 21:25:11.360723019 CEST	60429	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:25:11.422792912 CEST	53	60429	8.8.8.8	192.168.2.6
May 4, 2021 21:25:11.494430065 CEST	60345	53	192.168.2.6	8.8.8.8
May 4, 2021 21:25:11.552438021 CEST	53	60345	8.8.8.8	192.168.2.6
May 4, 2021 21:25:11.764453888 CEST	58730	53	192.168.2.6	8.8.8.8
May 4, 2021 21:25:11.826052904 CEST	53	58730	8.8.8.8	192.168.2.6
May 4, 2021 21:25:20.280563116 CEST	53830	53	192.168.2.6	8.8.8.8
May 4, 2021 21:25:20.332158089 CEST	53	53830	8.8.8.8	192.168.2.6
May 4, 2021 21:25:22.807085037 CEST	57226	53	192.168.2.6	8.8.8.8
May 4, 2021 21:25:22.876555920 CEST	53	57226	8.8.8.8	192.168.2.6
May 4, 2021 21:25:48.257555008 CEST	57880	53	192.168.2.6	8.8.8.8
May 4, 2021 21:25:48.317651987 CEST	53	57880	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 21:23:59.286995888 CEST	192.168.2.6	8.8.8.8	0x542d	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)

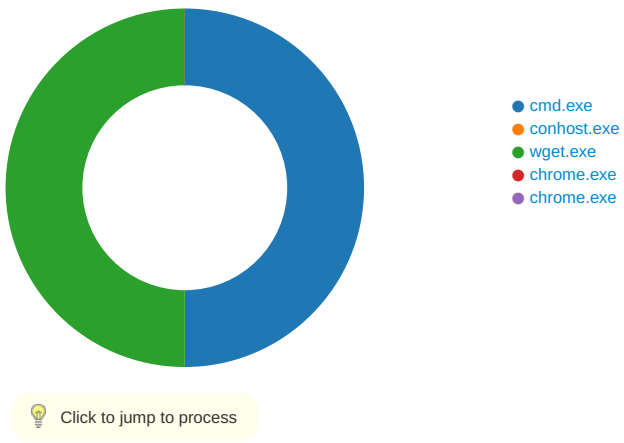
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 21:23:59.343893051 CEST	8.8.8.8	192.168.2.6	0x542d	No error (0)	clients2.google.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:23:59.343893051 CEST	8.8.8.8	192.168.2.6	0x542d	No error (0)	googlehosted.l.googleusercontent.com		216.58.212.129	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: cmd.exe PID: 6404 Parent PID: 4876

General

Start time:	21:23:38
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c wget -t 2 -v -T 60 -P 'C:\Users\user\Desktop\download' --no-check-certificate --content-disposition --user-agent='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko' 'https://drive.google.com//uc?id=1ExbiBQm3R9DeKMtJJ7y4hk9h5s5yiyeZ&export=download' > cmdline.out 2>&1
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\cmdline.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2AD194	CreateFileW

Analysis Process: conhost.exe PID: 6420 Parent PID: 6404

General

Start time:	21:23:39
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: wget.exe PID: 6452 Parent PID: 6404

General

Start time:	21:23:40
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\wget.exe
Wow64 process (32bit):	true
Commandline:	wget -t 2 -v -T 60 -P 'C:\Users\user\Desktop\download' --no-check-certificate --content-disposition --user-agent='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko' 'https://drive.google.com//uc?id=1ExbiBQm3R9DeKMtJJ7y4hk9h5s5yiyeZ&export=download'
Imagebase:	0x400000
File size:	3895184 bytes
MD5 hash:	3DADB6E2ECE9C4B3E1E322E617658B60
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\download\uc@id=1ExbiBQm3R9DeKMtJJ7y4hk9h5s5yiyeZ&export=download	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	46596C	fopen

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: 6800 Parent PID: 5844

General

Start time:	21:23:43
Start date:	04/05/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation -- 'C:\Users\user\Desktop\download\uc@id=1ExbiBQm3R9DeKMtJJ7y4hk9h5s5yiyeZ&export=download.html'
Imagebase:	0x7ff7c15e0000
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: 7000 Parent PID: 6800

General

Start time:	21:23:45
Start date:	04/05/2021
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=1644,12290585205416118591,7703833132062737 44,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1708 /prefetch:8
Imagebase:	0x7ff7c15e0000
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

Code Analysis