ID: 383999
Cookbook: browseurl.jbs
Time: 13:54:41
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

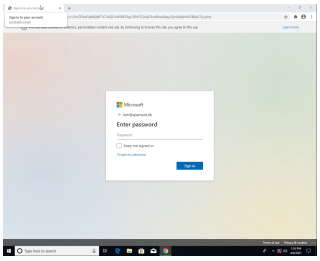
Analysis Report http://www.ztzusl.vibz.co.uk./#jrschnell....

Overview

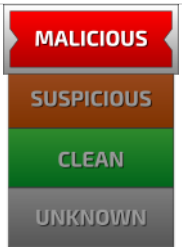
General Information

Sample URL:	http://www.ztzusl.vibz.co.uk./#jrschnell.com.br/site/z1/bGFtQHNwYXJub3JkLmRr
Analysis ID:	383999
Infos:	

Most interesting Screenshot:



Detection



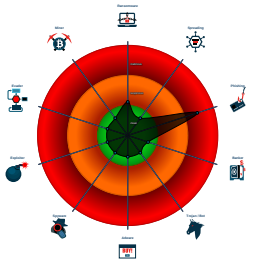
HTMLPhisher

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

Signatures

- Yara detected HtmlPhish10
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- Invalid 'forgot password' link found

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 5056 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'http://www.ztzusl.vibz.co.uk./#jrschnell.com.br/site/z1/bGFtQHNwYXJub3JkLmRr' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 4884 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1496,6792534671230322255,6132008020722060178,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1728 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

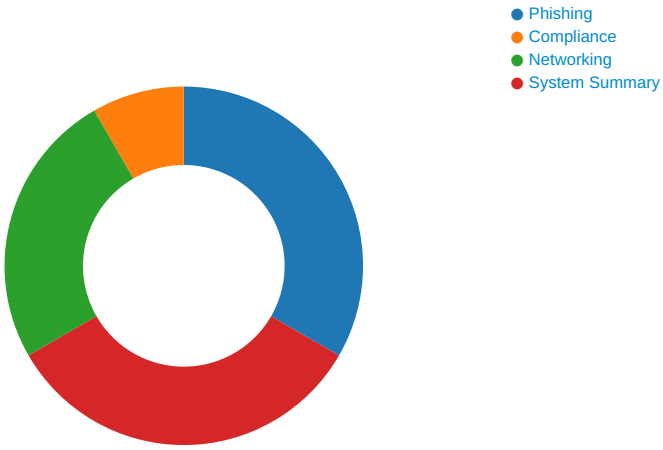
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

Phishing:

Yara detected HtmlPhish10

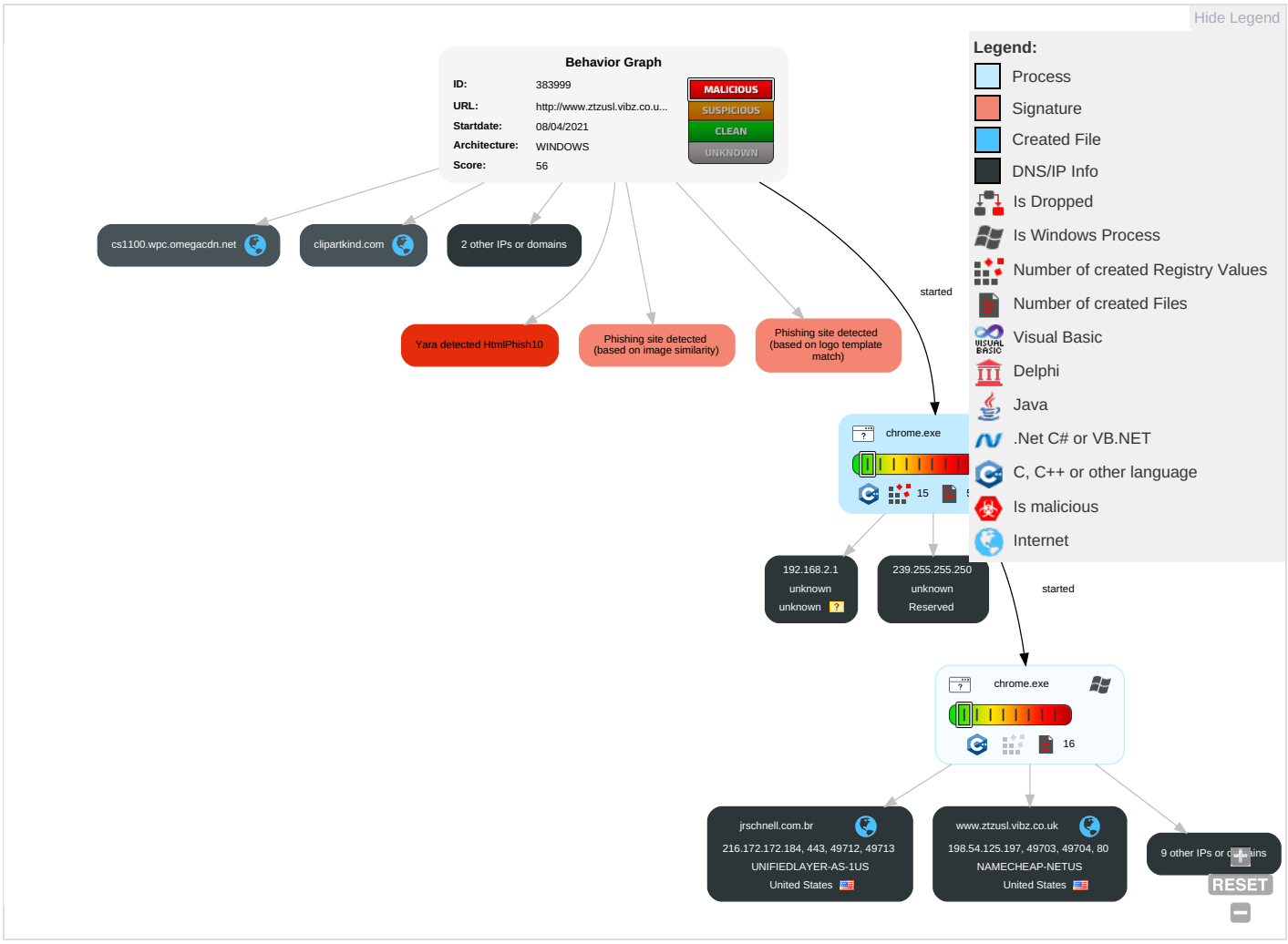
Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 3	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 4	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 2	SIM Card Swap		Carri Billing Fraud

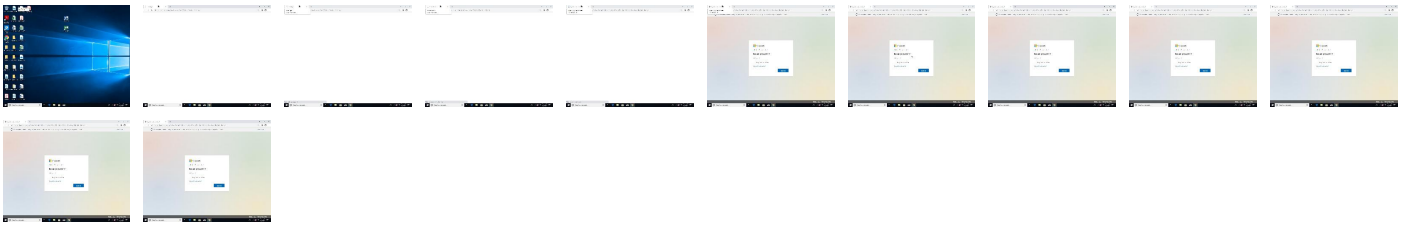
Behavior Graph

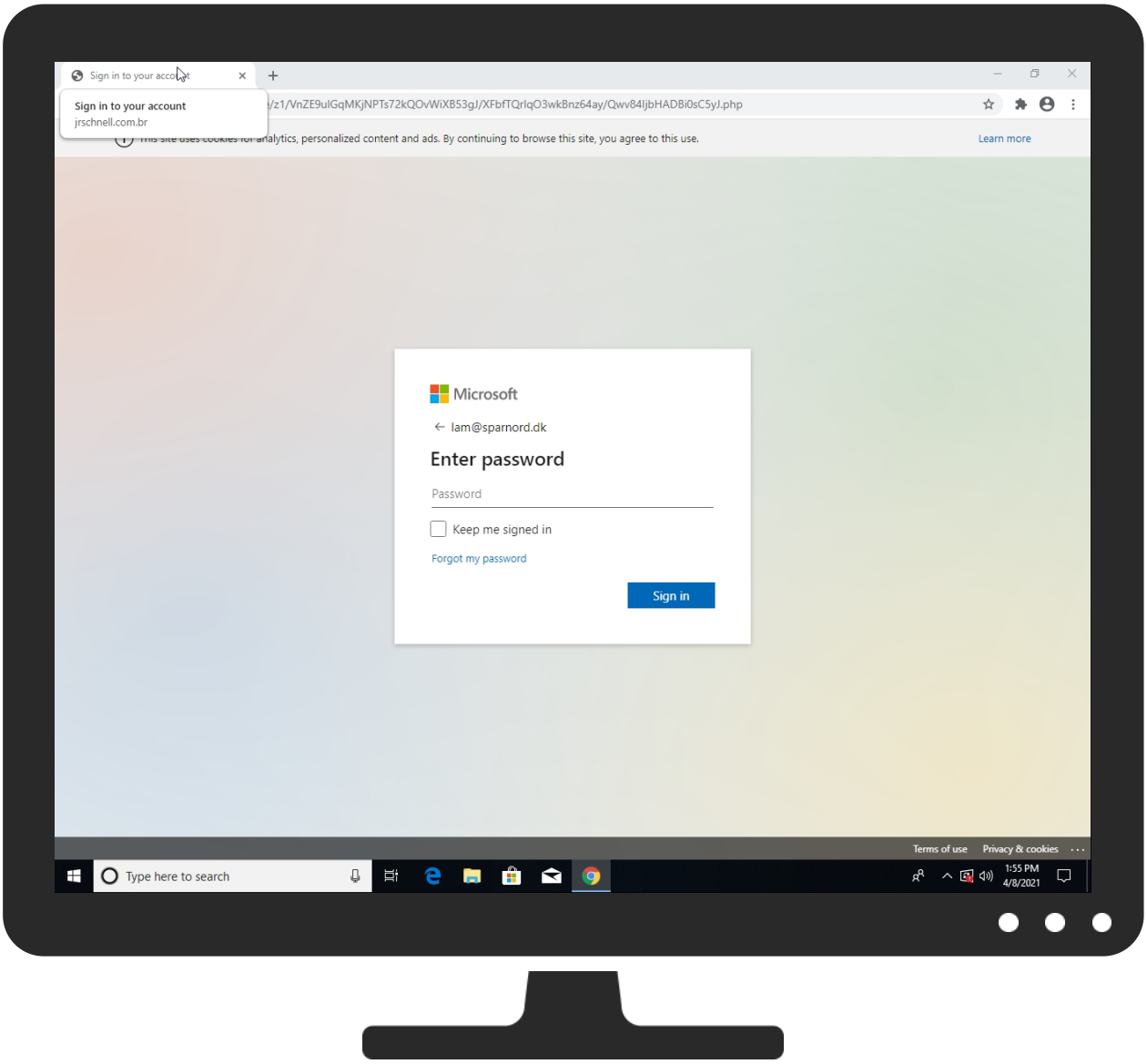


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://www.ztzusl.vibz.co.uk./#jrschnell.com.br/site/z1/bGFtQHNwYXJub3JkLmRr	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cdn.clipart.email	0%	Virustotal		Browse
clipartkind.com	0%	Virustotal		Browse
cs1100.wpc.omegacdn.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://jrschnell.com.br/site/z1/bGFtQHNwYXJub3JkLmRr/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://jrschnell.com.br	0%	Avira URL Cloud	safe	
http://https://jrschnell.com.br/site/z1/VnZE9ulGqMKjNPTs72kQOvWiXB53gJ/XFbfTQrlqO3wkBnz64ay/Qwv84IjbHADBi0s	0%	Avira URL Cloud	safe	
http://https://jrschnell.com.br/site/z1/bGFtQHNwYXJub3JkLmRr2	0%	Avira URL Cloud	safe	
http://https://jrschnell.com.br/site/z1/bGFtQHNwYXJub3JkLmRrQ	0%	Avira URL Cloud	safe	
http://https://jrschnell.com.br/favicon.ico	0%	Avira URL Cloud	safe	
http://https://jrschnell.com.br/site/z1/bGFtQHNwYXJub3JkLmRr2:	0%	Avira URL Cloud	safe	
http://www.ztzusl.vibz.co.uk./	0%	Avira URL Cloud	safe	
http://www.ztzusl.vibz.co.uk./#jrschnell.com.br/site/z1/bGFtQHNwYXJub3JkLmRrPlease	0%	Avira URL Cloud	safe	
http://https://jrschnell.com.br/site/z1/bGFtQHNwYXJub3JkLmRr	0%	Avira URL Cloud	safe	
http://www.ztzusl.vibz.co.uk./#jrschnell.com.br/site/z1/bGFtQHNwYXJub3JkLmRr2	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn.clipart.email	104.21.52.8	true	false	• 0%, Virustotal, Browse	unknown
clipartkind.com	104.21.69.231	true	false	• 0%, Virustotal, Browse	unknown
a.nel.cloudflare.com	35.190.80.1	true	false		high
cs1100.wpc.omegacdn.net	152.199.23.37	true	false	• 0%, Virustotal, Browse	unknown
www.ztzusl.vibz.co.uk	198.54.125.197	true	false		unknown
jrschnell.com.br	216.172.172.184	true	false		unknown
googlehosted.l.googleusercontent.com	172.217.168.33	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
aadcdn.msftauth.net	unknown	unknown	false		unknown
aadcdn.msauth.net	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.ztzusl.vibz.co.uk./	false	• Avira URL Cloud: safe	unknown
http://https://jrschnell.com.br/site/z1/VnZE9ulGqMKjNPTs72kQOvWiXB53gJ/XFbfTQrlqO3wkBnz64ay/Qwv84IjbHADBi0sC5yJ.php	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://jrschnell.com.br/site/z1/bGFtQHNwYXJub3JkLmRr/	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dns.google	8f522560-96a5-408f-8ea6-b71e615dc657.tmp.1.dr, 70d3da1d-19eb-44fe-ae07-c2744b7fb99b.tmp.1.dr, 43662394-a73f-491b-b25d-dadf65d899f7.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://jrschnell.com.br	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://jrschnell.com.br/site/z1/VnZE9ulGqMKjNPTs72kQOvWiXB53gJ/XFbfTQrlqO3wkBnz64ay/Qwv84IjbHADBi0s	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://a.nel.cloudflare.com/report?s=zVuCYb4T5%2BCu2V1YcvmWp6nX75rMO5L0ohPHNJ1QMyQ5%2FZlOjURxxTTQ%2	Reporting and NEL.1.dr	false		high
http://https://jrschnell.com.br/site/z1/bGFtQHNwYXJub3JkLmRr2	History Provider Cache.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://jrschnell.com.br/site/z1/bGFtQHNwYXJub3JkLmRrQ	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://jrschnell.com.br/favicon.ico	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.ztzusl.vibz.co.uk./#jrschnell.com.br/site/z1/bGFtQHNwYXJub3JkLmRr	Favicons.0.dr	false		unknown
http://https://jrschnell.com.br/site/z1/bGFtQHNwYXJub3JkLmRr2:	History Provider Cache.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ztzusl.vibz.co.uk./#jrschnell.com.br/site/z1/bGFtQHNwYXJub3JkLmRrPlease	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://a.nel.cloudflare.com/report?s=yEANLvrb3gjrgKSDVW66NfiDAFiP5z138blbV%2BydPALy8Kpx4QDFTFv2qvQV	Reporting and NEL.1.dr	false		high
http://https://clients2.googleusercontent.com	43662394-a73f-491b-b25d-dadf65d899f7.tmp.1.dr	false		high
http://https://jrschnell.com.br/site/z1/bGFtQHNwYXJub3JkLmRr	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.ztzusl.vibz.co.uk./#jrschnell.com.br/site/z1/bGFtQHNwYXJub3JkLmRr2	History Provider Cache.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.52.8	cdn.clipart.email	United States		13335	CLOUDFLARENETUS	false
104.21.69.231	clipartkind.com	United States		13335	CLOUDFLARENETUS	false
198.54.125.197	www.ztzusl.vibz.co.uk	United States		22612	NAMECHEAP-NETUS	false
216.172.172.184	jrschnell.com.br	United States		46606	UNIFIEDLAYER-AS-1US	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.217.168.33	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
35.190.80.1	a.nel.cloudflare.com	United States		15169	GOOGLEUS	false
152.199.23.37	cs1100.wpc.omegacdn.net	United States		15133	EDGECASTUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383999
Start date:	08.04.2021
Start time:	13:54:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://www.ztzusl.vibz.co.uk./#jrschnell.com.br/site/z1/bGFtQHNwYXJub3JkLmRr
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:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.phis.win@34/215@11/10
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.147.198.201, 104.42.151.234, 168.61.161.212, 23.54.113.53, 104.43.139.144, 13.64.90.137, 172.217.168.13, 216.58.215.238, 172.217.168.35, 172.217.168.78, 173.194.160.74, 74.125.173.166, 172.217.168.42, 13.107.246.19, 13.107.213.19, 142.250.34.2, 52.255.188.83, 172.217.168.74, 216.58.215.234, 172.217.168.10, 95.100.54.203, 40.88.32.150, 20.82.209.183, 23.10.249.26, 23.10.249.43, 23.0.174.200, 23.0.174.185 • Excluded domains from analysis (whitelisted): standard.t-0009.t-msedge.net, arc.msn.com.nsatc.net, r5.sn-1gi7znes.gvt1.com, clientservices.googleapis.com, fs-wildcard.microsoft.com.edgekey.net, skypedataprdcoleus15.cloudapp.net, clients2.google.com, audownload.windowsupdate.nsatc.net, update.googleapis.com, watson.telemetry.microsoft.com, www.gstatic.com, au-bg-shim.trafficmanager.net, fs.microsoft.com, content-autofill.googleapis.com, aadcdnoriginwus2.azureedge.net, aadcdnoriginneu.azureedge.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, www.googleapis.com, r1---sn-1gieen7e.gvt1.com, store-images.s-microsoft.com, t-0009.t-msedge.net, blobcollector.events.data.trafficmanager.net, aadcdnoriginwus2.afd.azureedge.net, clients.l.google.com, au.download.windowsupdate.com.edgesuite.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, r1.sn-1gieen7e.gvt1.com, e12564.dspb.akamaiedge.net, redirector.gvt1.com, dual.t-0009.t-msedge.net, Edge-Prod-ZRH.ctrl.t-0009.t-msedge.net, arc.trafficmanager.net, edgedl.gvt1.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, accounts.google.com, r5---sn-1gi7znes.gvt1.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, star-azureedge-prod.trafficmanager.net, aadcdnoriginneu.ec.azureedge.net, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, skypedataprdcolwus16.cloudapp.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtQueryVolumeInformationFile calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\017a9d03-b27e-4e10-846c-3af8a4c00f9a.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):	164081
Entropy (8bit):	6.08157434298651
Encrypted:	false
SSDEEP:	3072:kkOzmnDWVhPFlyU7sCXgcbjHsLA7bV/nYorVcI8XIssElYTRR:7c6Q1sJQHsgbV/njhcI8II6RR
MD5:	3892DDB23EFF30C8866AC94FE6A374A3
SHA1:	394B126C4A2024FE8729F9AB8B571C60BBD951E7
SHA-256:	FACB5AD71F41CEA41C3F075880C44026C7A90987DE359A6E91B55C7F5EF8EB54
SHA-512:	E976B4024FBDC897FEF9B316CAD2C240374F344FAD7BCDEEFE955CCA85B917EB9B179ED1C5D13D91A6F1E790608C9EFCE9EF7675F268FC07667F9AE2301457C9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\017a9d03-b27e-4e10-846c-3af8a4c00f9a.tmp	
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":1.617915332199945e+12,"network":1.617882933e+12,"ticks":107183504.0,"uncertainty":4429299.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909820208"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\842a5274-4f22-4210-87bd-e0791868038f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.746227119522752
Encrypted:	false
SSDEEP:	384:XLOBlbkejbkNgNVrmvZD3CVL6HbWGGJrE3p1xafn3WrEZmkn0Tdxt+O7bhNQ11Ux:yStN63Cm1OePdjzk/LWrKZ3FpR
MD5:	E50508F1277758C11A0BDF1B6E92CC21
SHA1:	4E9427E3401A8471394AA57614DDEBC7B1456F00
SHA-256:	80139B2AC70C91F3F705E3D8C734911BA21F48CCCCF7D92CDB192FF44D942F41
SHA-512:	03FB8ABDBD67E5AA74D44F388062589BF7F5C0F8018DE22124631711315111318C4F95E8C4CB54CD6BE6F28DC4A68B35F2BD0284DEAD8A7CA638AA3BD01C8CF
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....68.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\92dea4d3-1c38-45e3-90bd-f4a469befe3f.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):	164081
Entropy (8bit):	6.0815737854731955
Encrypted:	false
SSDEEP:	3072:kkRzmnDWVhPFlyU7sCXgcbjHsLA7bV/nYorVcI8XIssElYTRR:7R6Q1sJQHsgbV/njhcI8II6RR
MD5:	8577AC2A8B927ABEC8E358D228845C6D
SHA1:	7E473C9A3778C54590A6F495076679D71132C58F
SHA-256:	51289BEDEC9BC201A996EFFC1162E1CF98443BDCFAD25BDBA29BF96236E3BEB0
SHA-512:	5017941E604B806E9E1ABF52DDCC150FEA9DC34816E2CFC5D15381E61C511E4BE3A21A708DCC5657BF23DCF2E6696719E5AB6052FBBAE7A125F82875D39BD53
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":1.617915332199945e+12,"network":1.617882933e+12,"ticks":107183504.0,"uncertainty":4429299.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909820208"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\9aae0cfb-440d-441d-9739-15701c35174e.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):	164081
Entropy (8bit):	6.08157424677735
Encrypted:	false
SSDEEP:	3072:kkpzmnDWVhPFlyU7sCXgcbjHsLA7bV/nYorVcI8XIssElYTRR:756Q1sJQHsgbV/njhcI8II6RR
MD5:	8647155D5E7C2A42857A2D98DC1427EE
SHA1:	2B5ED052D024EEDF661825A3F1CB5C8223FBDFE1
SHA-256:	DBA6BFD77D9FBBCCCE507D268082EB60D661C10C6DAAAF344547788F3958002E
SHA-512:	91510A5465C36AE3932D9BB91A19E2BB74DF38D5D663997C31495411535D86D6177C6D35DFFA80066BA27B1D799866D8CB3E07B0E7924AB893388C91F7E9675E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\9aae0cfb-440d-441d-9739-15701c35174e.tmp	
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":1.617915332199945e+12,"network":1.617882933e+12,"ticks":107183504.0,"uncertainty":4429299.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909820208"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXJFlsz6VVJFlsz6VVJFlsz6I:+rJsrJsrJJ
MD5:	E4C3A0CCEDB71D53052C719DE30FD750
SHA1:	C89D101217D4AA05AD9C6FB24DB2037B3BCC630E
SHA-256:	B9ABED457F567199890198C9CE3B20954C73C458014CEB77C5E4514B1A8D8BF9
SHA-512:	D248EFCFA1BA3BA433A7A8D57B432F13D968DCF82A29535295BF03044982E69F441E6455EE7E6E7E4E902794B6D1B9CDAACBC92050B73062C0FDD33C4058034
Malicious:	false
Reputation:	low
Preview:	sdPC.....@.*.L..nM._bMsdPC.....@.*.L..nM._bMsdPC.....@.*.L..nM._bM

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1205099d-b56d-4bac-a252-3be3abb988bf.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\43662394-a73f-491b-b25d-dadf65d899f7.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):	2724
Entropy (8bit):	4.858441642519087
Encrypted:	false
SSDEEP:	48:YXsPMHi5s7MHgKsSMH/zs8MHIs51tFsL6zsbWsdCshDysuMHCLsKMH9swIMHlYhj:XGiQGBGFGJ12LLHDwGyGkGihj
MD5:	9E0C31BCE1C83C78981EB86A29E2879B
SHA1:	3973E5D4DA1BC0BB99B78D1DFA7BEA045C85E173
SHA-256:	3D1BDA968D1CFF79DBD0C4B9D2A22367E9D9B8374622CD4263BD39137D8FE584
SHA-512:	D196B2993F4A46AFFD38DBA59866B048221D5CF6EAB1574846D1799B748BD71B09BE28D8154B16D97AEA300C7EE13719DC2E5034EC9D8913C6A6B399BDEBC2E
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544495618845","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31528},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345624305","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":26637},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345531701","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":53820},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345601356","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":36228},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\479c5188-37ae-4362-9aea-46946c17be33.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\479c5188-37ae-4362-9aea-46946c17be33.tmp

File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	24055
Entropy (8bit):	5.53337791733268
Encrypted:	false
SSDEEP:	384:TjRtJLl+4XQ1kXqKf/pUZNCgVLH2HfD5rUfHGjHG/nTr1Vg4pq:dLltQ1kXqKf/pUZNCgVLH2HfNrUPGDGg
MD5:	916881921E4D342962BD04F1623A77B1
SHA1:	957E204A6BC7B7E3FCAD6C83C9584F3C69158521
SHA-256:	DBDD3E1171552CA5FA4420AC9BFA5C2609E7F365274271B4D4BE8E7DC546C3EC
SHA-512:	6DEBDE33140E1527EC4C890D63F1EA7684C78BD43BE56C40CA97D5BE9373F3164FD95CEC3D22270BECFA8367B3A5919D67BFFD2C5BE7BAC3334F947FB6486 9B
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":"13262388929229385","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\7ee5ee20-5778-441f-9f1a-60961cabb3ef.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):	6103
Entropy (8bit):	5.20419972731985
Encrypted:	false
SSDEEP:	96:nR15aGzWfTNFIyYVeKik0JCkRWL81k/1LkJIhmbOTQVuwn:n/xWfTXIyYIKk4kYUk/hkJIO
MD5:	25A0127A352B2065B37C79C4FDCBF0F9
SHA1:	99005AC5453367031126DEDB16F451B53DE069B9
SHA-256:	269CBBAE4A86D87A1C655556B5D942A83B0002E0806E3E05E668B74D09465072
SHA-512:	18F81BE709A80A71874540D01877AA09B251851A49FC583F1B04AC1DCEC0FC5972119B2E613044491F5288E773FDE0835DB9D6BB651D2AEEA22FFA5F33A636D
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13262388929457555","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	342
Entropy (8bit):	5.268032202921885
Encrypted:	false
SSDEEP:	6:m1nkgF3cM+q2PcNwi23iKKdK9RXXTZIFUtpknkoIJZmwPknkxocMVkwOcNwi23ie:vHM+vLZ5Kk7XT2FUtp/oa/P/7MV54Z51
MD5:	84F8E6D69A380172873FEDD02FD74367
SHA1:	7AF1701A23486AAC8D3A34B7B6BE664BC1F9C6B0
SHA-256:	30395AE4AF96CD598CD11BF84CA75BE182B5F442818E71C905609885CBADC9FB
SHA-512:	DD4E48DE2CED80B743D131CF1A1762947D32A8A15C945C84CC26C3139A74FA4E1B95543F61BCA51FB65DC2393902EA672C3104D9214663C63E3590D59FB703
Malicious:	false
Reputation:	low
Preview:	2021/04/08-13:55:38.901 1b6c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/04/08-13:55:38.904 1b6c Recovering log #3.2021/04/08-13:55:38.905 1b6c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	326
Entropy (8bit):	5.27862248438849

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Encrypted:	false
SSDEEP:	6:m1nitcM+q2PcNwi23iKKdKyDZIFUtpkn8tJZmwPknke3cMVkwOcNwi23iKKdKyJd:cM+vLZ5Kk02FUtpL3/P+MMV54Z5KkWJ
MD5:	640EA3856D8768816E71B23BBA1F5254
SHA1:	BD47EB1EE8CC5CC2B2417089A3A2A06F65B0B1C8
SHA-256:	A04BCEA3DEC6E5F092232C637C0B696E5E5F2ED517603CACD503014D5DA22C00
SHA-512:	A309EB8CE3134CBC1F9B08B0CEE731B883C38C6BE90FEB58E7C144CF665F452DD3F57AA7B10786F53366641F9412A59FD73415F40519CD3982915EC02ED7B04
Malicious:	false
Reputation:	low
Preview:	2021/04/08-13:55:38.865 1b6c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/04/08-13:55:38.867 1b6c Recovering log #3.2021/04/08-13:55:38.868 1b6c 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):	0.967648752068229
Encrypted:	false
SSDEEP:	24:22+tYeFky/pqLbJLbXaFpEO5bNmISHn06Uw68:22UYeT/pq5LLOpEO5J/Kn7Ut8
MD5:	804229063FAFA2F614A753FD82DCB23B
SHA1:	CACA3DBA93DE4F49FCE409025FF6C47F9486BEF3
SHA-256:	B9DF291A82F889355229A5CA4EF9D2A2A594A340453E90D21725D89BC18549F1
SHA-512:	3BC08A3F79A4BB0A8CAA148CD1EA33B0CD193917BA43599293D207F9BAAD37113D23C0A1804DD0BD3C694CB845E7358D62D2B548EB549914B95E7530D4C3B35
Malicious:	false
Reputation:	low
Preview:	.....>.Gt..... ....

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):	3799
Entropy (8bit):	3.94793381350084
Encrypted:	false
SSDEEP:	48:34Txqtob0L7euiWPCBUL7euiWnzL72XBXCB1Rr:34E5iUh5iG2XBXE
MD5:	4D21C6CE6B1FFFD85F0DC3E951D6BDCD
SHA1:	6490A6110024A625CC7BA1432AC297D1107618FC
SHA-256:	BD257710096761D92C51E80310818DD11C705553E058A88C1C53B36BA284A839
SHA-512:	48E47BAF5C53F189688E2348D98BC9EA691F43E802C5B256F7E7312282E2DF55F7E48096DB5273F929EE1B2111726EDFBC422FFC6A20E2F280346AB4C2602E0B
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...a2ded5c6_9839_4c7b_b7f3_dd02cb63e4e2.....|.8..... .....5..0.....&...{C578CEAF-A17C-4AAB-9284-A5059F1242C7}.....l...https://jrschnell.com.br/site/z1/VnZE 9ulGqMKjNPTs72kQOvWiXB53gJ/XFbfTQrlqO3wkBnz64ay/Qwv84IjbHADBi0sC5yJ.php.....h.....`.....H.....X.. D|...Y..D|.....l...h.t.t.p.s.:././.j.r.s.c.h.n.e.l.l...c.o.m...b.r./.s.i.t.e./.z.1./.V.n.Z.E.9.u.l.G.q.M.K.j.N.P.T.s.7.2.k.Q.O.v.W.i.X.B.5.3.g.J./.X.F.b.f.T.Q .r.l.q.O.3.w.k.B.n.z.6.4.a.y./.Q.w.v.8.4.I.j.b.H.A.D.B.i.0.s.C.5.y.J...p.h.p.....r...5...h.t.t.p.s.:././.j.r.s.c.h.n.e.l.l...c.o.m...b.r./.s.i.t.e./.z.1./.b.G.F.t.Q.H.N

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):	183
Entropy (8bit):	4.267376444120917
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+GgGg:qT5z/t2qoEwhXeLKBt
MD5:	7FA0F874EABF1EED31988230680AD210
SHA1:	E71B360F1E8D5C278A051AD03DFB9027ACCF38C3
SHA-256:	09E15F8939364145E710C314EBD93FD19BF60C2B6B20BF8023315D617B6B141B
SHA-512:	AF4C2E595AA0B1FD96474A0E73530B38BE5F2906B10BE1DEFC0A9221129A3E5BB8D0816777550863AD426C5C836ECA1F0C384986C2A1108E2E4CA20EF10A782
Malicious:	false
Reputation:	low
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....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):	325
Entropy (8bit):	5.267294237917558
Encrypted:	false
SSDEEP:	6:m1z6+q2PcNwi23iKKdK8aPrqIFUtpkzU4ZmwPkzUlVkwOcNwi23iKKdK8amLJ:ebvLZ5KkL3FUtpuU4/PuUg54Z5KkQJ
MD5:	E210EF03C0951A8B9778C751C1734A53
SHA1:	30FC8F98B8FD21EEF7F1057A0C9394DD4EE62C8A
SHA-256:	275A117BA6C1C57EA4BD102238CA1F5504513786C4C6CFA2DC2A95C2AD81F9BE
SHA-512:	EDB508ADD82F33A929EB9075561AC82C996DC52F0697FC77C3346FE2106E118BE1E086BA850576CBC6EF563D5DF682F236C2235F6D13D31D31C64DA92558CCI A
Malicious:	false
Reputation:	low
Preview:	2021/04/08-13:55:29.482 168 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/04/08-13 :55:29.483 168 Recovering log #3.2021/04/08-13:55:29.483 168 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003. log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	627
Entropy (8bit):	1.8784775129881184

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Encrypted:	false
SSDEEP:	12:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW:
MD5:	9D7435EA49A80FDD66E4915F513017F9
SHA1:	469F6C6E4B19B85CC1BE497812B2F20864F4FF2C
SHA-256:	409D4C47E940688527D730B996E8991E010988C7671565467ED69D640D0947F3
SHA-512:	0561CD632D4219AEF4686DE40EC092921384CA89755D354801E0EAEC8645A8630A180807AF518AC8FCF01F71EB3D10FAA9CE1E62C7A7226A274975BDCB7EEB4C
Malicious:	false
Reputation:	low
Preview:	.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):	325
Entropy (8bit):	5.187974033731729
Encrypted:	false
SSDEEP:	6:m1D34q2PcNwi23iKKdK8NIFUtpkWZmwPkRkwOcNwi23iKKdK8+eLJ:FvLZ5KkpFUtpT/PC54Z5KkqJ
MD5:	24BDE97F05D073408A72C2CEED2F7B6B
SHA1:	31E66F492F206090CEAE9CF82D67E9531FE58CFA
SHA-256:	529BA38065B3509C88D0020A2DAF92D1DA7AA3CAA60F42181391D163498E8A9C
SHA-512:	4FADA99F2B59D13B136768026D5FFE6A0C33EDC59D8CCD772FDA63B9F7FCFEC436C113E07A8771F7527BDBE015EB9632EEFA3CAD9361382EB8888FF616B1301
Malicious:	false
Reputation:	low
Preview:	2021/04/08-13:55:31.703 2a0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/04/08-13:55:31.704 2a0 Recovering log #3.2021/04/08-13:55:31.705 2a0 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:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUscllJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkIjEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_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):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_1_metadata\computed_hashes.json	
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkIjEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","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
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["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=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
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):	20480
Entropy (8bit):	2.050220007879475
Encrypted:	false
SSDEEP:	96:0BCNRmUsTDqAAzqOHXN3pMQAtBvKiW47H+cDtje:m8RmU22JzqO3BpMQIBvKiW4achq
MD5:	016BA6C50300E14C80FC776F9285859B
SHA1:	92FB2D03179EFB53686FCE6E5E61F949F42FDE9F
SHA-256:	BC4121718633F34CD0B8D0FECCA382CF3314EBA138E7095CDC68024D7F57BAAB
SHA-512:	089679E9EBD4C4DC481840D6B430F6A16480E3E00011FF1BE5884DBBA3533C5F93EC1D682C324175455F7D8B618AB0AF9BF7BF01F3B1B339EBD87F9803A8FD6
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16972
Entropy (8bit):	0.7780991369728646
Encrypted:	false
SSDEEP:	24:se3FcWyLiXxh0GY/l1rWR1PmCx9fZjsBX+T6UwDhyWh3n:DdBmw6fU8p3n
MD5:	D723B44A3EFD981F3CC998ABF741410A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
SHA1:	6C8923A0E054D9EBB3000B34705F41B7DEFB54E5
SHA-256:	E2E0A3A344AA9A932C20E115AA8D70219D4E656DAE9925A7C863D604A770AF56
SHA-512:	E294878570311E364FC7F31701D5C944D6C39E974E51CE964B654D5A6421620304B48E0D3384AA0D7380EBA02E190F424DD203B7C989CA8D53888F8D44C9B47B
Malicious:	false
Reputation:	low
Preview:	....

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):	380
Entropy (8bit):	5.298734261704423
Encrypted:	false
SSDEEP:	6:m1nVcM+q2PcNwi23iKKdK25+Xqx8chI+IFUtpknaS3JZmwPknbtcMVkwOcNwi23U:vM+vLZ5KkTXfchI3FUtpCZ/PDMV54Z5G
MD5:	D4739F03ED06CEDFD14D1939A832A795
SHA1:	19D2EEECD4FD6C725AFC81C82BD80172B7D25064
SHA-256:	A7E59693F513D214D027E91737677CA594CD83509B3D6BF5F0B19B6CDCD9AECF
SHA-512:	D10F196C1BA2AA803143922BD2FBD66611172D98DFB4B7AEC22282FC40E3A992DC3A73AF5C272C1440031159BE81D57C26EC0ECCD4F0F083F62EF434B66D09
Malicious:	false
Reputation:	low
Preview:	2021/04/08-13:55:38.336 1b6c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/04/08-13:55:38.338 1b6c Recovering log #3.2021/04/08-13:55:38.376 1b6c 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):	366
Entropy (8bit):	5.254491450531076
Encrypted:	false
SSDEEP:	6:m1nH3cM+q2PcNwi23iKKdK25+XuoIFUtpknSPJZmwPknYL3cMVkwOcNwi23iKKdQ:CMM+vLZ5KkTXYFUtpb/PyMV54Z5KkTXp
MD5:	D50F3291A586C62A605899862C69FB8C
SHA1:	71E8BB064CDD69B2103FFC876A5055ED973D3B7B
SHA-256:	FBD521D016B6E3D8DFF7C2C9311F29809A45FA2BFD141373F7932A7D596A9167
SHA-512:	184557AA23AC12406F17EEDFEE834099C8F5396D7BD2C30F1AAB4538DB3CA2CB57E2681AA71795F26B661166D478E2DA729C818751B190D37D3CB63541EF91F
Malicious:	false
Reputation:	low
Preview:	2021/04/08-13:55:38.248 1b6c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/04/08-13:55:38.306 1b6c Recovering log #3.2021/04/08-13:55:38.311 1b6c 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.287375188026852
Encrypted:	false
SSDEEP:	6:m1nr3cM+q2PcNwi23iKKdKWT5g1IdqIFUtpknSJZmwPknXDcMVkwOcNwi23iKKd6:FM+vLZ5Kkg5gSRFUtpv/P1MV54Z5Kkgk
MD5:	3CB03FDF3ACA8680C546F8DA9DF51FBF
SHA1:	75DA48CA9E2A73A54411F60019D3CDFEA57D0F40
SHA-256:	CEF0988FC8A8BC00CECFA32F774416599ABE84851A43B54653C8371C425E6B88
SHA-512:	E7FF56BE65437DB1137A5940BAEC76C0063C7684E5B5761BD8BE2B2C41AF965AF4A40E887D86C3102639CB84B1A21CF812FB45BB02C7539241962CB61868D1F
Malicious:	false
Reputation:	low
Preview:	2021/04/08-13:55:38.033 1b6c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/04/08-13:55:38.045 1b6c Recovering log #3.2021/04/08-13:55:38.046 1b6c 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):	0.32551881176966463
Encrypted:	false
SSDEEP:	24:TLxQIwIiFFBIiCmqNIiCF3+3RBdzIiFeIiCsNIiCM:TFLEFcH5sEM
MD5:	F0E81D69218B94BE5F04269E38834254
SHA1:	BBD82D70A2CA865EE4DBF235C451149499658AB6
SHA-256:	7EF58E7AD88CBDC5A2C002FD4D678FA7E5F3FAD26F35B62DCCC7827E8D73CDF5
SHA-512:	A9FEB610A402C69C658222D20EF9C6E2B88C6EC33D3FF6993B7741690E16AA0993D1AE2817BBFF383E6122DA037DEEC0433C9299C07B22F82A4398DA039E4C2
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:	zlib compressed data
Category:	dropped
Size (bytes):	1674
Entropy (8bit):	5.943766432679931
Encrypted:	false
SSDEEP:	48:tP8XS549DOr09zd4jzbyBWFEwk97tgsEUjr:tPoSulOkOaB8udXP
MD5:	B876F5CCDEB5BB1516487196283D664E
SHA1:	3BF8FD8A8B4C2480EAAD19CACE1CC86BE27E44F0
SHA-256:	323748C73C3A74B8B6B4ECF8CA97AED5DC10FD304BB13F6DED973A964094F282
SHA-512:	046FCFFE48023F4C17D32954596E70787AE12F9C3DF7149083D547CECCCE5C8A5732A357391E61BDE85DCDEB873C50A1CE4E02088240E268A2CC54BE15014FD
Malicious:	false
Reputation:	low
Preview:	....."......account..br..com..https..in..jrschnell..php..qwv84ijbhadbi0sc5yj..sign..site..to..vnze9ulgqmkjnpts72kqovwixb53gj..xfbftqrlqo3wkbnz64ay..your..z1..bgftqhnwyxjub3jklmrr..co..http..please..uk..vibz..wait..www..ztzusl*.....account.....bgftqhnwyxjub3jklmrr.....br.....co.....com.....http.....https.....in.....jrschnell.....php.....please.....qwv84ijbhadbi0sc5yj.....sign.....site.....to.....uk.....vibz..."..vnze9ulgqmkjnpts72kqovwixb53gj.....wait.....www.....xfbftqrlqo3wkbnz64ay.....your.....z1.....ztzusl..2...$.....0.....1.....2.....3.....4.....5.....6.....7.....8.....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.....:

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	33356
Entropy (8bit):	0.047324706358956733
Encrypted:	false
SSDEEP:	3:C6l93llu/fllijo/NlliiotfllitvNlliuvltFlivvtflliholtFllim2QMRgm:pl9iP4ivXGl9Wg9bNFlWCj/lAl3n
MD5:	5EAF8F3AA5E44749A9B5FEC1A435AB9B

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
SHA1:	DAEC4EF08CAF421678D6EDB9B9C0817C3AD91C95
SHA-256:	951A2A3EC45400B5F799EA73370334340E3BBDF140E81DDD1AC7D1C901DDC931
SHA-512:	77CD9E873FB51B3C01E454D373CBC5A1327BE18EA7021C2BEA76AFA37E83088C003B40EBD53EC06966137C627ABC356E8C826F11AFBE0CFEDA13BAF781484045
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):	5.48458215300414
Encrypted:	false
SSDEEP:	48:MUDO+GaQWMeBa7BBMFQ8db9XVwlw5nbQSefgGWNrS0U9RdiN9K:Mqa7rMJdbBC2pbQ5fgGKrS0I
MD5:	A5D603F78FACD44C693052C819555ADC
SHA1:	BFE32A603E65D22BADDACF784C2AE960179E7486
SHA-256:	8F2DDB76062A2CDCAA5FB8E75E6D64C6D5A694DAECF41896607C6CDFDBCA15BE
SHA-512:	047C71A6F6A42C20185D542D5F5D934BAEF25508961BE0E0877D4CD1E1B96FFC6ECD126B037B99A2727955756BC04558E6E409A5F7471D10A4F74CAB3183F45E
Malicious:	false
Reputation:	low
Preview:	..:...*.....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..876879000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-04-08 13:55:40.18][INFO][mr.Init] MR instance ID: 44f8c46e-17b9-473e-963f-6306361e056e\n","[2021-04-08 13:55:40.18][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-04-08 13:55:40.18][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-04-08 13:55:40.18][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-04-08 13:55:40.18][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-04-08 13:55:40.18][INFO][mr.CastProvider] Query enabled: true\n","[2021-04-08 13:55:40.18][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):	337
Entropy (8bit):	5.215885931017665
Encrypted:	false
SSDEEP:	6:m11aLN+q2PcNwi23iKKdK8a2jMGIFUtpk1BHZmwPk1EVkwOcNwi23iKKdK8a2jM4:JN+vLZ5Kk8EFUtp6H/PPV54Z5Kk8bJ
MD5:	D5D3F6EB7D451411C8FE041BA0534285
SHA1:	73E0B1573095606F1DC7BBC19B95A555DED17ADA
SHA-256:	3404F51A77E93EAE5D2D57C2DA5C98DA3573A4F02DF1E42B4B5C1388B88F285A
SHA-512:	845C03508F5F09FD603602F1067FDF168525DE345DD9E30C1E0CFF56E0D5E4BC75F2F4745731C49BAF1AB98E4A0D2B5583E06E46B51C60C856C81EBA2D38E51
Malicious:	false
Reputation:	low
Preview:	2021/04/08-13:55:29.238 29c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/04/08-13:55:29.239 29c Recovering log #3.2021/04/08-13:55:29.241 29c 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):	339
Entropy (8bit):	5.19276654953644
Encrypted:	false
SSDEEP:	6:m1HHAq2PcNwi23iKKdKgXz4rRIFUtpkNZmwPkUvDkwOcNwi23iKKdKgXz4q8LJ:AAvLZ5KkgXiuFUtpo/Pb754Z5KkgX2J
MD5:	CB1B9C316923AD578CAD96D3C296F963
SHA1:	A12A78A824F6B0E7C842CF499A10FFC2930A4A60
SHA-256:	399DA14215F7AA7780FED14C3158329F2AD5DA02D4B794F6708608EF2606CDFE
SHA-512:	7EBC869BAE7A024674D134C3F9C5ADB87713A6CF4DDA8A057EE1CBFF046875736E129BEBA3ACE795D87A97BA9D5C326F102E60C4FEA7260C050C8A3512FC554D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Preview:	2021/04/08-13:55:29.515 2a0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/04/08-13:55:29.520 2a0 Recovering log #3.2021/04/08-13:55:29.521 2a0 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\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	28672
Entropy (8bit):	1.0548486147390597
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGU3bVKh2okMT6i4:wIElwQF8mpcSbBKwok/5klKYk/
MD5:	17C9505E5F1A6090BFEAF07A66127073
SHA1:	4918CD85A9C303C30651C0A61BB2981D7A05D2EC
SHA-256:	5A49CFBA4480F76AC3B9A71B67D21A72164040EBF48E714110C4B0A7DDA4EB8D
SHA-512:	3CC278D0B8A73EBFC32FA92D61DBCA0E8D802A6C320AF79E8D890DA4AA8189952525E131A0CF100D4C12163C3BF770EB00E1FD15E8FCAFA97AC512AD9771E41
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g...^.....j..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	29252
Entropy (8bit):	0.6278690398329302
Encrypted:	false
SSDEEP:	48:QwqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUR4:QwhIElwQF8mpcSC
MD5:	85D4E8B320D45EB589E772F6E18198DE
SHA1:	140854FEF7F09EEFB0F1FDBCD67753B5F9A7124E
SHA-256:	8685C31C98CDFADAA801AD05407DED59C36AF1C8209977FD774186DC4FE0A5E3
SHA-512:	1DEBB90E39E68AADC7947F0CEC214D21F777FC63759881B99AB48AA842912E25769D73375AB6DA8E18720235760A3A6D81C2D6B03B880ADC80E2646BF232CCD3
Malicious:	false
Reputation:	low
Preview:	.....PG..... ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Size (bytes):	328
Entropy (8bit):	5.191224071774345
Encrypted:	false
SSDEEP:	6:m1zBq2PcNwi23iKKdKrQMxIFUtpkzpZmwPkzUFkwOcNwi23iKKdKrQMFLJ:eBvLZ5KkCFUtpup/Pu454Z5KktJ
MD5:	A64D536DFA9D9A5C950E748AD8D3A1B0
SHA1:	EA1FF97C64F603F7314392133C7457D6C759A9E3
SHA-256:	4D01E0CF4FC20804757E4775988D3A26F47EB1EF3040BB19EA3F7763730512E0
SHA-512:	A1AEA1E4D7FCB8AC034DBD798D45AC19B354CD932E7C8F98E81CE5531FFF3D791A3022026DAE2CDA3C0A09154704B4481548F50BDAEB9C390E4E92B8469ED2B
Malicious:	false
Reputation:	low
Preview:	2021/04/08-13:55:29.432 1520 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/04/08-13:55:29.435 1520 Recovering log #3.2021/04/08-13:55:29.436 1520 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):	353
Entropy (8bit):	5.184390310594404
Encrypted:	false
SSDEEP:	6:m11m+q2PcNwi23iKKdK7Uh2ghZIFUtpk1SuGNJZmwPk1l3VkwOcNwi23iKKdK7UT:Z+vLZ5KkIhHh2FUtpLX/P+3V54Z5KkIT
MD5:	0A8224CF29B07767CC5D70420DD80344
SHA1:	5FC7ECE38F2409337F4572AACA2FC1756DAD5069
SHA-256:	61F0402040E88CD8D528824644C793B7A78A8737EDA49A6023AA1C0BA4846045
SHA-512:	0836F355E19041ADB34DE304B52BE991460A259BC1FC6E139DD5D08B7DAFD974B0EBF6A59383E7B8D3A75E83FFD4C2B4F9F431F9FF3BC2BDFD935477A0847FE
Malicious:	false
Reputation:	low
Preview:	2021/04/08-13:55:29.229 29c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/04/08-13:55:29.230 29c Recovering log #3.2021/04/08-13:55:29.231 29c 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\70d3da1d-19eb-44fe-ae07-c2744b7fb99b.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):	4.957371343316884
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5hsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sd7sBdLJlyH7E4f3K33y
MD5:	363D9EBEDB5030036B53B6B28E8A8EA5
SHA1:	1C7C9012156AC8295EB465BC774430A866096832
SHA-256:	466FE09323B709A587648157D77298132B29F7CD916CD68EF6B28A0FC5EE355B
SHA-512:	9C9A230BAF627B8A9856C0AC66E4EA262C304BBC2272662F4213EB617297DFE222E0CCC4FC0F22B04FAFB3125D55D774174700B381EA3FF90B8C3D11926E023
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544335120983","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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
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):	435
Entropy (8bit):	5.304834395568993
Encrypted:	false
SSDEEP:	6:m1zh+q2PcNwi23iKKdKusNpV/2jMGIFUtpkz1ZZmwPkz1NVkwOcNwi23iKKdKusO:esvLZ5KkFFUtpu1Z/Pu1z54Z5KkOJ
MD5:	EF0175B1253A2E13B0D92949A0FBEDF2
SHA1:	54B5D74F16F1157276DE0A0B478BF7E1333E435A
SHA-256:	2B48BBB6D9BC741FA2D5BE9D654E98C5175FC3E4E3AA22418B5CDB6B77CE57E2
SHA-512:	69ADB80791755309AFCAD89B60EA5A375C562F7F101FD675C5E2E20A8982416AF0CC0989AB093D92DAB6C9B5648D4FFC31BB7CCEA708323ABC6E9B87530EE28
Malicious:	false
Reputation:	low
Preview:	2021/04/08-13:55:29.492 168 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/04/08-13:55:29.494 168 Recovering log #3.2021/04/08-13:55:29.494 168 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):	440
Entropy (8bit):	5.307756097777592
Encrypted:	false
SSDEEP:	6:m1NQi+q2PcNwi23iKKdKusNpqz4rRIFUtpkbZmwPkE1NVkwOcNwi23iKKdKusNpH:0D+vLZ5KkmiuFUtpo/Pr1NV54Z5Kkm2J
MD5:	F1534EDC0DE17B48B8D7007E520ECB47
SHA1:	4C24474E70B977BA6A7C2A8F21CC004A2B43682E
SHA-256:	392A076D5D18F6E6FEEEB66D30982354F863B7C8E27A8F3EDB8EA1E094E95F9E
SHA-512:	EC4FAB0DE938AC816119F575427E3912663ED1A01A6A7D17EF546C38B691D2254D5EB3159503C2F82CA41CE8DF87C4A7159863DAFB1990B9F9D7A67E38C971E
Malicious:	false
Reputation:	low
Preview:	2021/04/08-13:55:29.520 169c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/04/08-13:55:29.522 169c Recovering log #3.2021/04/08-13:55:29.523 169c 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):	426

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Entropy (8bit):	5.264774239170685
Encrypted:	false
SSDEEP:	6:m1w9E9+q2PcNwi23iKKdKusNpZQMxIFUtpkS2WZmwPkS9VkwOcNwi23iKKdKusNP:R29+vLZ5KkMFUtplJ/Pl9V54Z5KkTJ
MD5:	7D44606D8F433D7E084DCF9200CA6F6F
SHA1:	2B2D75E6F361C3BF4161BC6F4CBFBE1131DB292D
SHA-256:	EA9C9AD50C05560B07CE2571ACDC168A35ADF8836F3F0D996AB16C6A2A2C0E7E
SHA-512:	2803C5EDD2C89F055681916302799053C2E81E25CD33A3DBA0D50C5B7AEE778DD345D33B2E987AC4927AF4AAC457CF1839347769334F2B5029A4B290EB129D3
Malicious:	false
Reputation:	low
Preview:	2021/04/08-13:55:45.845 150c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2021/04/08-13:55:45.846 150c Recovering log #3.2021/04/08-13:55:45.846 150c 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\8f522560-96a5-408f-8ea6-b71e615dc657.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):	4.96345415074364
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5Z0WlyhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sd/0WCsBdLJlyH7E4f3K33y
MD5:	1FE877DDE8B96DED122AC08BB07A83C5
SHA1:	5BEA5FFAF686474CE8ACA1D95500C29D65007745
SHA-256:	3AD373EB6FF8EA394964EDA2A9E53ADD8DBA11DC9716ED3CA672F10DF369BA4D
SHA-512:	1854F005CD691674FCF27376150ABD6F036A79C42BB4FFECDCCA14A74CB21D8ADF2552CACE631E6E9C92C58E7EF27279CA30CE5648C8EB90B06F2247A462003
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544342473569","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):	592
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E8E:8N
MD5:	B505641E5E90B7CF4BC869DD1B4BE451
SHA1:	0EC7B13DC043E054AB48B8F45FE49EF1209C01AA
SHA-256:	2755F85F14CF33404CEEBF053D0CB79DC3B98D643A51075737E6A5BE154FE1D9
SHA-512:	610AF095630C93B0586F4D9CA84FA75454C472C557D4FDBC0D5C1851F9AABF8653079A7ADE4659ABADDEDC2E02E58AD13C7244CD004B0AA5A462307F293F833
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):	438
Entropy (8bit):	5.205665215679428
Encrypted:	false
SSDEEP:	12:SIvLZ5KkkGHArBFUtpy/Pt54Z5KkkGHAryJ:Tl5KkkGgPgAo5KkkGga
MD5:	5D738656FC3BE853DD9955A7D66937E1
SHA1:	F2261391B680BD11F83DBF09017001BBFD95491F
SHA-256:	B7DB102DDA352C8CA51B07CDC20397E273793C2639097392104440974 8CA2772
SHA-512:	B8663D9135EA6B12B5EE3155486905E8D3FF0B8E7BFF1A7652B99CE32D036918F4E5E81DDFF84AB80A3E703B12693A78FD7DCE8237AF767DE25F4F961884A20E
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Reputation:	low
Preview:	2021/04/08-13:55:38.091 1520 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/04/08-13:55:38.095 1520 Recovering log #3.2021/04/08-13:55:38.096 1520 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):	440
Entropy (8bit):	5.210557453397196
Encrypted:	false
SSDEEP:	12:Z9+vLZ5KkkGHArqiuFUtplJ/PU9V54Z5KkkGHArq2J:Al5KkkGgCgSo5KkkGg7
MD5:	9A6768576D687BA57C203A1CBDD31E33
SHA1:	07C21354878416B37A7955AD9476CD7130619BA7
SHA-256:	C2598EDF1A0A543EEAFE46D993C42AD2906C178F54EF030DC49DFF7797468F0E
SHA-512:	E58B6FD7E0CE94A36E083EE700C990E3236201F49B9E53BAC7CC3423C620C18CE6760341652B7FF58D68A8266D5D8A5B3B7490E672AA0CC980EAB12CF04A900A
Malicious:	false
Reputation:	low
Preview:	2021/04/08-13:55:38.091 150c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/04/08-13:55:38.095 150c Recovering log #3.2021/04/08-13:55:38.096 150c 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):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljl:5ljl
MD5:	E9C694B34731BF91073CF432768A9C44
SHA1:	861F5A99AD9EF017106CA6826EFE42413CDA1A0E
SHA-256:	01C766E2C0228436212045FA98D970A0AD1F1F73ABAA6A26E97C6639A4950D85
SHA-512:	2A359571C4326559459C881CBA4FF4FA9F312F6A7C2955B120B907430B700EA6FD42A48FBB3CC9F0CA2950D114DF036D1BB3B0618D137A36EBAAA17092FE5F0
Malicious:	false
Reputation:	low
Preview:	..&f.....&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):	426
Entropy (8bit):	5.181533371141247
Encrypted:	false
SSDEEP:	12:6IvLZ5KkkGHArAFUtpx/P754Z5KkkGHArfJ:Ll5KkkGgkgpo5KkkGgV
MD5:	50B20124AF0B31BFF9DF75E0188C60DE
SHA1:	9878A21E4BA34BC47B0B6DDB948557B030B91A2E
SHA-256:	5AFE74DE227FB4F5CE03015B2FB93D597DBAA339DDF06A6629FFD477CC33480C
SHA-512:	855B79F75F1D26497C435C11F38B700ACFE629F9CD402A92C9BB8FFD25B8EC708BD8920BDF47A4CEFCBEB3C42DDED4A68C0CF40ED6C2CB19BF4112E275CDB83
Malicious:	false
Reputation:	low
Preview:	2021/04/08-13:55:53.318 1518 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/04/08-13:55:53.319 1518 Recovering log #3.2021/04/08-13:55:53.320 1518 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
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):	329
Entropy (8bit):	5.27030364325569
Encrypted:	false
SSDEEP:	6:m11KHN+q2PcNwi23iKKdKpIFUtpk17ZmwPk1LVkwOcNwi23iKKdKa/WLJ:XIvLZ5KkmFUtp0/P054Z5KkaUJ
MD5:	1C8E863515C64E615CF49D89FC033C15
SHA1:	0D3AC7F6C1C7EE289694B50F18ABCB2FE7350F84
SHA-256:	091DAA6C0F77401007B39AE84F0553892338547F8994A55DFA2D447A766A0017
SHA-512:	31AE81AFAE592993E038F5FD573602E906EE1D9467ED35219C3F56FBFC3B04F985289023BF1ECDC38684D859C6006EE3DFD9556EDA0E2F5704D315E439514C0
Malicious:	false
Reputation:	low
Preview:	2021/04/08-13:55:29.202 168 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/04/08-13:55:29.203 168 Recovering log #3.2021/04/08-13:55:29.203 168 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):	410
Entropy (8bit):	5.303957318742044
Encrypted:	false
SSDEEP:	12:TT9+vLZ5KkkOrsFUtpjn2J/PjJ9V54Z5KkkOrzJ:T+l5Kk+gB+ro5Kkn
MD5:	E45A6789F509DF4829B80BA098822657
SHA1:	8C6550E22E805F911F4F5098CABDBD11C7BCEE06
SHA-256:	9DA51EEA7026CE340096A1840191CF1BDA289D312D532E830CBE65AB2A5D78B4
SHA-512:	668FCBEF434B77C437967CA5AE6C8E236C16ADB0EB5B604D9165C01A14219236CCEC2AC316BC7CBD69B2663D9EF80EED748F63691B7B5361C136ACA2EA7DC 14
Malicious:	false
Reputation:	low
Preview:	2021/04/08-13:55:40.175 150c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/04/08-13:55:40.176 150c Recovering log #3.2021/04/08-13:55:40.177 150c 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):	36
Entropy (8bit):	4.321888195526177
Encrypted:	false
SSDEEP:	3:vymV5tpX1hciAqRr/:vyiKiBN
MD5:	2C06ED64D748695B81766174CA9D5610
SHA1:	6E8BF371A8CE9F162982D01BF60ADBF2D712EFCE
SHA-256:	5D17CC120B99B5592A41582EC3AED86A56825A664DDA8764C17C36841A1E4FA1
SHA-512:	824EEDDCE17D1ED4E008FF0E19591FCD7930C073221F1C989C6AB0AAA4E6FBCA7C0BEE40629D9F4FBA0C23B8F2708F5A28C4F1FFC9C6DA39E5B164C204E89 AB
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Preview:	......l.t..\....Lr.L..?........,Z

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\Chrome Web Store Payments.ico.md5	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16
Entropy (8bit):	4.0
Encrypted:	false
SSDEEP:	3:SeFcn:Sec
MD5:	61B979ECA159ECAC9C7F8F1D6FD43E9D
SHA1:	0373696351FC2172E811DA8393DEC84036FA34A0
SHA-256:	AB05E0A6FF7E8FFF89F924B279D93AFC72ACCE817C4D250C60BB8059CC534303
SHA-512:	C95825DA33CBDDFA627D9FF9A5B8371BC5F4E643A09573B6E1E839A83B619F53D878C344030B9701DCBC24D4CECCC016CF4D298D10EE8C37D1B5FEC1A5168B6
Malicious:	false
Reputation:	low
Preview:	F......r...(R..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\ecf51cec-8cff-4906-8ef9-59ae0a4ab825.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 13 icons, 8x8, 32 bits/pixel, 10x10, 32 bits/pixel
Category:	dropped
Size (bytes):	175509
Entropy (8bit):	5.489440694064333
Encrypted:	false
SSDEEP:	1536:rKbsLAR2A4VBQV1111111111111Nr366R6faFR+up0y0y2im1OsFcgYzQNL9X:rKbsLAR2fe/FZntrslfX
MD5:	33EABC19FDF40F3D36B6870EF5861957
SHA1:	CF3EF59C3940B58C314E9F6A1616751553F2D9A2
SHA-256:	647D07F37554672865902B2CEE80864B5A5283C372C7263BB1497D5582054E57
SHA-512:	47CFEDB1FDBC9BC09905C70F69A5114C64A8FC791BCA480D24972275276F00CEB230C579B4217337F9C69ECB2AB3221A3B549F06E8074D76BCE2F31773FB69F
Malicious:	false
Reputation:	low
Preview:	.... .H............ .... .p............. .h...n......... ....n...((.... .h.......00.... ..%..~H..@@.... .(B..&n..``.... .....N......... .(....D........ .w`...M..(............. ....+.O-8&]P>/^Q?-^&:?I.1;<....qye.f.%.......X...E.....I...k}....{.m.t.CP..........E...\..............=H..,A..,J..;P...nn p}nnp}........~~~........!...!---2---2... ....(............. ....!...7.#.:3,";3,!<.&'/............NPLYt.F.K.%.....L..C.....1...`...KOPVutz}..A.BxX.......P.. .Q.....1...x...tqpyxuux...0D..DP..........G...........uojuppnw....t|..9F..-=..+:..5:..rr......llkrkkmw................................ggitllkv................................hhgssss~............YY\eYY[e........ ....nnnzXXXa............................RRR\..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b73ebcb9-306b-45b8-8b46-fce919e3aa81.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):	6104
Entropy (8bit):	5.205110173671036
Encrypted:	false
SSDEEP:	96:nR15aGzWfTNFIyYVeKik0JCkRWL81k/1mOkDW8XdEbOTQVuwn:n/xWfTXIyYIKk4kYUk/fkq8w
MD5:	F76B235E9A31C8BCB540DEFE2308DB77
SHA1:	1DE13664B0E65A91876E1890371C228CD0A823D3
SHA-256:	D9672FD31BB54146D72A7FFAA31791A4EEC24E6CCBB38B138A03B6D84447FB46
SHA-512:	EA5FC70DDA373145E05A9CD03860B987340555F2E39C70B8900231F1463F1B82BE99557EB93086EEB5B749F1C620E034992C3EECA2C2DC1D003E1306FDB8A1C
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13262388929457555","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ba93d5cd-37d3-4144-94b2-a68fc2f813a7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ba93d5cd-37d3-4144-94b2-a68fc2f813a7.tmp

Category:	dropped
Size (bytes):	19007
Entropy (8bit):	5.566945514045143
Encrypted:	false
SSDEEP:	384:TjRtsLl+4XQ1kXqKf/pUZNCgVLH2HfD5rUeHGnMzng4a:oLltQ1kXqKf/pUZNCgVLH2HfNrUOG4g9
MD5:	FDB36789A3B2FC4A67405420268A0305
SHA1:	88803885BC08F61C06D80BA3AF3671FA97FB2697
SHA-256:	F3E8065F8FCCC1AD69BFB4CAAD85317B08C880F82C8C5D27F252A5093589D6F4
SHA-512:	ACB576187C84AEE55C6704A908D4948A6E07E34FAA42DBCDDCFA30CD02870F76AB19DF56029805EA03D15522456D283A8C24E7764860213F7D857CF707BA839
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":"13262388929229385","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\bf9c0326-77d1-4881-b428-dfac92b2e452.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):	6134
Entropy (8bit):	5.2019390999174915
Encrypted:	false
SSDEEP:	96:nR15aGzWfTNFIyYVeKik0JCkRWL81k/1QkYdFbOTQVuwn:n/xWfTXIyYIKk4kYUk/KkYP
MD5:	21B4701BC3A7C0AF110FB9F615D505D6
SHA1:	7039F63C9BD3C5C89D401CF8CCEEC4E5515F8C07
SHA-256:	D63A27C61B46E9D811C42E240BEC78E5BE6F31B038B688827A7B60DC46C61744
SHA-512:	0883D61187A3ED78C53AAAD51E3A63A03A783E13FDE7EBB8927B167339E4C7407AE82BA2A313C05E7CABC540BF054B7E029F9D0D65916612FEBDD0D4B14AB3A8
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13262388929457555","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cd1a21d1-cdf0-43d4-ada8-753f589b87f8.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):	5286
Entropy (8bit):	5.003422474794767
Encrypted:	false
SSDEEP:	96:nR15azzWfpYVeKik0JCkRWL81k/1BbOTQVuwn:n/gWfpYIKk4kYUk/j
MD5:	080F288DA8EA8F922DF6DAF4396BB197
SHA1:	2EDCAA777D3977963638F547404E31F389B8F1B4
SHA-256:	CB4601309D32FB47AA54C1F5E05FA83E221C5348EFD1919CCFD306384842CA33
SHA-512:	FD4B9C3E5396388B3379F182C3CD81E1763157C25D2E61980917C549A99B722D17CC957293047D078B9E34E16B3582898613EDE34BC63B06DF9296E44C8EC3C6
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13262388929457555","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0",

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
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):	4.671506405959806
Encrypted:	false
SSDEEP:	3:tUKO3IUyfGF3JZmwv3s3IUytI+AJ0V8ss3IUytI+AJ0WGv:m1lF3JZmwPkgVs0VvkgVs0tv
MD5:	4980B631597B8C53B363E6B3AE8C97E4
SHA1:	3D4B5A50FA9F02F03AF13F4B10B1F61A68068F13
SHA-256:	B019DE4A2B2E306111B870B3C300EE3D31D8F09EDE27E4990B75511637AEEB14
SHA-512:	D264A4C9B1EC0A3893610B430EF111AF8F774BFEE3D996AC3573351C86985D51A433902028A01A7589EBF23E0FAD767BB3B99B315118283FE6767418CF33AF31
Malicious:	false
Reputation:	low
Preview:	2021/04/08-13:55:37.221 1b6c Recovering log #3.2021/04/08-13:55:37.279 1b6c Delete type=0 #3.2021/04/08-13:55:37.279 1b6c 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
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF 04
Malicious:	false
Reputation:	low
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e092c941-846d-4ca0-92ae-0bad6a7a4a2a.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):	875
Entropy (8bit):	5.563497773513628
Encrypted:	false
SSDEEP:	24:YU6H0UhvrRlG1KUevEhUeT717wUlRUevxQ:YU6UUhveKUevGUetwU7Uev2
MD5:	74293D5B0FB4E7752009A0F007E16253
SHA1:	EDCCF7B4E9C605BEAEDA7844C2A7828F101DE322
SHA-256:	3290273ECA4EF1D0FCCD556EB1266FE6B9D5EA12AF7BF8BD9FCF8FE34AD633F1
SHA-512:	485D989A9E41813CA09D8D6191916DEE2F805D3BA0CAB8DE1AE70EFB16887DC6E8E98FCF90F37CA4B9BA32259AE3B86DE6235AA28A121B6E1BB2AE55750444 AB
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e092c941-846d-4ca0-92ae-0bad6a7a4a2a.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014895.618904,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478895.618908},{"expiry":1633014895.522238,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478895.522241},{"expiry":1633014902.981094,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478902.981097},{"expiry":1649451333.843601,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617915333.843604},{"expiry":1633014895.739906,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478895.739909}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f43117c8-c32d-45b2-9ca0-289f206cbafc.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):	5.535663029780903
Encrypted:	false
SSDEEP:	384:TjRtJLl+4XQ1kXqKf/pUZNCgVLH2HfD5rU2HGknTr1jg4La:dLltQ1kXqKf/pUZNCgVLH2HfNrUWGkng
MD5:	E057E39C6BB5FE63CE5BB5FFBCF60228
SHA1:	EE5F2C444A1BB9CDBE9894C0A1D6816B3D0E5DC8
SHA-256:	255AE20D384775954941051641B2ED39FB238C28BD28EC5DCAB4F3818F6B0E8D
SHA-512:	1E93FE37612D4CFBF98E919DE4731F1F653B7EDC5F420E28DBC8EBE3C6C9BEAD0DBC64FCDD00B945B424229F2A1BFE123DB6382035C76E61CEAC21144F522C7
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":"13262388929229385","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/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

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):	346
Entropy (8bit):	5.232603068619771
Encrypted:	false
SSDEEP:	6:m1hq2PcNwi23iKKdKfrzAdIFUtpkuZmwPkCkwOcNwi23iKKdKfrzILJ:2vLZ5Kk9FUtpB/Pb54Z5Kk2J
MD5:	3E0DC0CEC051FB8595073B8B11C7987D
SHA1:	257E4271AC691BCCF2097562E8B6E5C90385D3D3
SHA-256:	EE5197D0B9DED067353B22CCFE461F6058333476F603894524558D89C10DBD50
SHA-512:	2236D28F7139DFB82C36D37F6ED8FE21DCE3B89549992464E161207C57B09B4BF49D0F6204AC713195973D83A0370AAF3F16494D5BD27D9E294DE93D6B2E3E0A
Malicious:	false
Reputation:	low
Preview:	2021/04/08-13:55:39.237 1520 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/04/08-13:55:39.239 1520 Recovering log #3.2021/04/08-13:55:39.239 1520 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_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:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Temp\0c3f6955-ecb0-44f3-86e0-dd6fb8e44048.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\3bc3ff2e-5fcd-416e-9d4b-9bbdd5589dd3.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F332688
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..''0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.[1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.I....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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\7e8babb5-7628-4bb3-8797-c4b873789bbb.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

C:\Users\user\AppData\Local\Temp\7e8babb5-7628-4bb3-8797-c4b873789bbb.tmp	
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;..._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q...:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a.:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\add8fe13-175d-496e-abde-a7ccd4b6652f.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..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LlP/....](.A.....l...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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\b564911b-f54e-4259-9034-5451d99c9559.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\f326f68b-75ea-4103-a897-c68291f47aa3.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_dir5056_1542486938\3bc3ff2e-5fcd-416e-9d4b-9bbdd5589dd3.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..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F770C
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... . ... Chrome".. },.. "app_name": {.. "message": "..... . ... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "...., ...".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "...., ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CEB4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "C onnecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\cs\messages.json	
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D8488 B
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed .".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5 E0A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_unavailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB805 52
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_unavailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	787
Entropy (8bit):	4.973349962793468
Encrypted:	false
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWlOGAOf+XD:WguYpCZnpEZbGoD
MD5:	05C437A322C1148B5F78B2F341339147
SHA1:	AB53003A678E44A170E73711FBD9949833BBF3AA
SHA-256:	A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070
SHA-512:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B4

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\el\messages.json	
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavail able": {.. "message": ". ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": ".. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... ... Chrome..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unava ilable": {.. "message": "App currently unavailable..".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network..".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed..".. },.. "please_sign_in": {.. "message": "Please sign into Chrome..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\en_GB\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unava ilable": {.. "message": "App currently unavailable..".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network..".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed..".. },.. "please_sign_in": {.. "message": "Please sign into Chrome..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	661
Entropy (8bit):	4.450938335136508
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyZnLAOfTY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OGAOffD
MD5:	82719BD3999AD66193A9B0BB525F97CD
SHA1:	41194D511F1ACC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE018
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento..".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red..".. },.. "iap_unavailable": {.. "message": "Los pagos en la aplicaci.n no est.n disponibles en este momento..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed..".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\es_419\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	637
Entropy (8bit):	4.47253983486615
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34GLO03OyZnLAOfTYiJD:1HEvaC6WYpcDeEFxq8Zp4LlOGAOfvD
MD5:	6B2583D8D1C147E36A69A88009CBEBC7
SHA1:	4D4DEEB4BE6AA0181825F3371A761ABC5B4D5937
SHA-256:	6659BC3705311D7641A73995DCFEA80C7734F2F4EBBC3787B3892A240348324F
SHA-512:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA3
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "En este momento, Pagos En-Apps no est. disponible.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\et\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	595
Entropy (8bit):	4.467205425399467
Encrypted:	false
SSDEEP:	12:1HEJfPGGGfPG+WYpU34Ze7z+dgrW9O8ZpU34ZwZz03OyZnLAOfTYgoLIR:1HEdvqlWYpTeObk8ZpT/OGAOfuLIR
MD5:	CFF6CB76EC724B17C1BC920726CB35A7
SHA1:	14ED068251D65A840F00C05409D705259D329FFC
SHA-256:	C85800BF45942FCC7FD6B1DF929C25F9CC2A977A6678966BD03D4B6B69889AFD
SHA-512:	53D7D01BB30C0306DE65A79FD9551D2E8C1F71F4F45F71906B009071CB3E0F231E6A50FDD78773E9B4DE94085BC7B97F829842FA21A89A2080D33458B745C46F
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome'i veebipoe maksed".. },.. "app_name": {.. "message": "Chrome'i veebipoe maksed".. },.. "craw_app_unavailable": {.. "message": "Rakendus pole praegu saadaval.".. },.. "craw_connect_to_network": {.. "message": "Looge .hendus v.rguga.".. },.. "iap_unavailable": {.. "message": "Rakendusesisesed maksed ei ole praegu saadaval.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logige Chrome'i sisse.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\fi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.595421267152647
Encrypted:	false
SSDEEP:	12:1HEJRuzGGRuz+WYpU34ujSBu+dgYO8ZpU34J+Bu03OyZnLAOfTY5HN:1HEFcWYpPNa8ZpD+FOGAOfEHN
MD5:	3A01FEE829445C482D1721FF63153D16
SHA1:	F3EAAADDC03F943FC88B30B67F534AA13E3336DD
SHA-256:	0BDE54B20845124113383B6EB81E43A0F05E4EB0C44BEE3C1DFAC4CC5FEC2836
SHA-512:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BEAD8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Storen maksut".. },.. "app_name": {.. "message": "Chrome Web Storen maksut".. },.. "craw_app_unavailable": {.. "message": "Sovellus ei ole t.ll. hetkell. k.ytett.viss..".. },.. "craw_connect_to_network": {.. "message": "Muodosta verkkoyhteys.".. },.. "iap_unavailable": {.. "message": "Sovelluksen sis.iset maksut eiv.t ole t.ll. hetkell. k.ytett.viss..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Kirjaudu sis..n Chromeen.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\fil\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	658
Entropy (8bit):	4.5231229502550745
Encrypted:	false

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\fil\messages.json	
SSDEEP:	12:1HEJADlbGGADlb+WYpU34hTUT+dgHfZAFFZO8ZpU34hTjzeT03OyZnLAOfTYHfvF:1HEYah6WYp7TUSoxOS8Zp7TOsOGAOfqV
MD5:	57AF5B654270A945BDA8053A83353A06
SHA1:	EEEF7A4F869F97CF471A05D345E74F982D15E167
SHA-256:	EC002ED92359F67818B49455DFC579E140368E6A004080AF022FD4F57F6B03F2
SHA-512:	5F0AE839FCF3F4EA48FF41A76655AE0F3821564AFD5D42FBB9FBB9A38E8D8F7BB5E9B6F71064588CD441261F644095A44A755C134CE546D506D9A21E488BAF52
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "app_name": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Kasalukuyang hindi available ang app.".. },.. "craw_connect_to_network": {.. "message": "Mangyaring kumonekta sa isang network.".. },.. "iap_unavailable": {.. "message": "Kasalukuyang hindi available ang Mga Pagbabayad na In-App.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Mangyaring mag-sign in sa Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\fr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	677
Entropy (8bit):	4.552569602149629
Encrypted:	false
SSDEEP:	12:1HEJALf/nbGGALf/nb+WYpU34Owdgbyb+dgdQjO8ZpU34ITQpGnbyb03OyZnLAO8:1HE4Hna1Hn6WYpNdgpY8ZpSTQwnBOGAh
MD5:	8D11C90F44A6585B57B933AB38D1FFF8
SHA1:	3F9D44EA8807069A32AACA2AAAD02FD892E6CC90
SHA-256:	599491F8C52B945C16C441ADF45BFD45AFAE046DA07757D97C56AF4DE75ED3B5
SHA-512:	D7EF7F5AD7EF1A1595825D79B69E2B1E988AD3CF1F3881496FCCD30F241E4E9C6E457F9F5D0F855DE3536DB7A40C3E1C55946B50D3F556F4A35285066A0CD6F
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "app_name": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "craw_app_unavailable": {.. "message": "Application indisponible pour le moment.".. },.. "craw_connect_to_network": {.. "message": "Veuillez vous connecter . un r.seau.".. },.. "iap_unavailable": {.. "message": "Les paiements via l'application ne sont pas disponibles pour le moment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Veuillez vous connecter . Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\hi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.791154467711985
Encrypted:	false
SSDEEP:	24:1HEs07J0JWYp9vnCSVLP8Zp6CsOGAOf8SLm:Wh7qgYp1CMLUph1GiSLm
MD5:	E376D757C8FD66AC70A7D2D49760B94E
SHA1:	1525C5B1312D409604F097768503298EC440CC4D
SHA-256:	8106D98C4F8DA16DB698444409558E29CC96735E188BFA303C333A5D99231C1D
SHA-512:	673F3F259AF2946E4F49BBED14A2A70D44BF9FDA9D7A71DC9172BA9B7B3C7F7062B16D29682B638D485B0520ED6F99E7A735F28C7C719B539559005B69FA7555
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome ... .".. },.. "app_name": {.. "message": "Chrome ... .".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "..... ....".. },.. "iap_unavailable": {.. "message": "..-.. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... Chrome ... .".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\hr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	618
Entropy (8bit):	4.56999230891419
Encrypted:	false
SSDEEP:	12:1HEJGiimxmbZGGGiimxmbZ+WYpU34OBOEuhopIO+dgcapZO8ZpU34GiiZrMrQphK:1HE4H4TH8WYpNjTta28ZpQVLP0SOGAOK
MD5:	8185D0490C86363602A137F9A261CC50
SHA1:	5BD933B874441CEACB9201CCC941FF67BAED6DC0
SHA-256:	A2B2EC359A9DD9DCCCE02859CE1E738BD30FAA4A05F1DC522893FFDF722BBC15
SHA-512:	D7629978FC031EA5F716F9C1065FB2FEAB48C15F10CD68830DC966FA1002C03DDC7ACDE314C7D075F9F3A0A68552A6ACBCCDEE24CF20B6C3DD1BCE6562D03 6E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\hr\messages.json	
Preview:	{.. "app_description": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "app_name": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "craw _app_unavailable": {.. "message": "Aplikacija trenuta.no nije dostupna.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se s mre.om.".. },.. "iap_unavailable": {.. "message": "Pla.anje u aplikaciji trenuta.no nije dostupno.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be comple ted.".. },.. "please_sign_in": {.. "message": "Prijavite se na Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\hu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	683
Entropy (8bit):	4.675370843321512
Encrypted:	false
SSDEEP:	12:1HEJVJiGGVJi+WYpU34Hpo9O+dgMmfgijO8ZpU34Huo9O03OyZnLAOfTYBIAYm:1HEVrk5WYpQzTUg/8ZpwoXOGAOfYIAd
MD5:	85609CF8623582A8376C206556ED2131
SHA1:	1E16EB70DB5E59BB684866FF3E3925C2DEF25A12
SHA-256:	32A249749F12ADB6A220BF9ADC272C7E5D9AD5497A38B0086D961E3ABA17FBC6
SHA-512:	27883430865D3CFA6EDFE8C6CE1442BD96150B5CE520CCF7D556A330CAA6392C712B47BD86F7350E174876BC681F6DEC94D1312402655B0AF90883A2899EC78
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. },.. "app_name": {.. "message": "Chrome Internetes .ruh.z Fizet.si r endszere".. },.. "craw_app_unavailable": {.. "message": "Az alkalmaz.s jelenleg nem .rhet. el.".. },.. "craw_connect_to_network": {.. "message": "K.rj.k, csatlako zzon egy h.l.zathoz.".. },.. "iap_unavailable": {.. "message": "Az alkalmaz.son bel.li fizet.s jelenleg nem .rhet. el.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Jelentkezzen be a Chrome-ba.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\id\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	604
Entropy (8bit):	4.465685261172395
Encrypted:	false
SSDEEP:	12:1HEJs25bGGs25b+WYpU34ORBHAeSJ+dgkmO8ZpU34s22C/SzFAs03OyZnLAOfTYR:1HEBaA6WYpaHFH8ZptOYOGAOf2D
MD5:	EAB2B946D1232AB98137E760954003AA
SHA1:	60BDC2937905B311D2C9844DF2D639D7AC9F7F67
SHA-256:	C6E8800450602DE0F39FE9F6854472383813FB454B08ABAE7E25A9167CE004C3
SHA-512:	970FEC9A9EF0BAF7F693C4C5977F3B47914579C5B5414FCE9DBB5E4574659A5BB9AD2DE0CC886B368F49C019785AF7D2D7FE82F71341F039EADC399ED776CA 2
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pembayaran Chrome Webstore".. },.. "app_name": {.. "message": "Pembayaran Chrome Webstore".. },.. "cr aw_app_unavailable": {.. "message": "Aplikasi tidak tersedia saat ini.".. },.. "craw_connect_to_network": {.. "message": "Sambungkan ke jaringan.".. },.. "iap_unavailable": {.. "message": "Pembayaran Dalam Aplikasi saat ini tidak tersedia.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be co mpleted.".. },.. "please_sign_in": {.. "message": "Harap masuk ke Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\it\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	603
Entropy (8bit):	4.479418964635223
Encrypted:	false
SSDEEP:	12:1HEJsqd/bGGsqd/b+WYpU34OcX4+dgUvIO8ZpU34vq703OyZnLAOfTYsD:1HEXd/aKd/6WYpZrv58ZpskOGAOfzD
MD5:	A328EEF5E841E0C72D3CD7366899C5C8
SHA1:	2851ED658385804E87911643F5A4200B1FB26E13
SHA-256:	CD891C45F7586FB4A2514205A11F260E4A6D4482FA03D901909DD9F57BE0536D
SHA-512:	E47297896E981774EC3B59D41B89D6BA9333F6B4435EB9727D8645A46B10C7D408ADE06844871FA757382FBE7E645276449DB7B1B23BC59C9A71A5CB5A5ECC5
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamenti Chrome Web Store".. },.. "app_name": {.. "message": "Pagamenti Chrome Web Store".. },.. "craw_app_una vailable": {.. "message": "App al momento non disponibile.".. },.. "craw_connect_to_network": {.. "message": "Collegati a una rete.".. },.. "iap_unavailable": {.. "message": "La funzione Pagamenti In-App non . al momento disponibile.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accedi a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\ja\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\ja\messages.json	
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	697
Entropy (8bit):	5.20469020877498
Encrypted:	false
SSDEEP:	12:1HEJ07uGG07u+WYpU34DB+dgnsVztO8ZpU34MwiB03OyZnLAOfTYmSH:1HEcnDNWYp1kxU8Zp2wiqOGAOfpSH
MD5:	9B3A5D473C3F2BBFAEECE94A07A940B8
SHA1:	61BACA342CF766BBA15C7B4D892A0E7DAC9405AA
SHA-256:	706312A4A2AEF3317223F141EB2B82685345B7EED444F16BB4DF3A272716DA1F
SHA-512:	94F6FEE9A11BD890AB8211C98D1CC142348961EBCF756F66477A3E3A76519804B70BE0AE4E551739F8AFE32D7ADE6EDE04EF6B9B9EED03E3A857E6058EEDD4C6
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome .....".. },.. "app_name": {.. "message": "Chrome .....".. },.. "craw_app_unavailable": {.. "message": "..... .....".. },.. "craw_connect_to_network": {.. "message": ".....".. },.. "iap_unavailable": {.. "message": ".....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Chrome .....".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\ko\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	631
Entropy (8bit):	5.160315577642469
Encrypted:	false
SSDEEP:	12:1HEJ1GG1+WYpU34K3aT+dgh8d0HTO8ZpU34KaNkaT03OyZnLAOfTY/YeHx:1HEajWYpc3aSl0Hq8Zpc6kasOGAOfyYA
MD5:	9F6B4D82A70C74CA751E2EAE70FAB5CF
SHA1:	0534F125FFCE8222277CF2BE3401C59DAF9217F8
SHA-256:	D1467B8D037114403E8F4EFC52E88C4A7FEB96126BE4CFF883FEFF1084EF7E68
SHA-512:	ED9319830314385D09C06F62EE34186E8CA576C857981205E4468A28B3ACD2AB03384E77B866032C324ABDD97A56EFD08E2D6E0C79D563578B3EC52517819BD8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome . ... ..".. },.. "app_name": {.. "message": "Chrome . ... ..".. },.. "craw_app_unavailable": {.. "message": ".. .. ..".. },.. "craw_connect_to_network": {.. "message": "..... .....".. },.. "iap_unavailable": {.. "message": ".. .. ..".. },.. "jwt_retrieve_failed": {.. " message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Chrome. .....".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\lt\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	665
Entropy (8bit):	4.66839186029557
Encrypted:	false
SSDEEP:	12:1HEJpqHnkGGpqHnk+WYpU346M+dgV6O8ZpU34WzSWz03OyZnLAOfTYx:1HELqHtKqHPWYpM3A8ZpwGzOGAOfg
MD5:	4CA644F875606986A9898D04BDAE3EA5
SHA1:	722A10569E93975129D67FBDB75B537D9D622AD1
SHA-256:	7C311AB751D840D750C11553C083785813E079C1D464FE568A98C9E3EF3DB96C
SHA-512:	E575E3D0622F5BD4B6C0EE79128A1B1F1882195670139D1983F4377D847141B8FB8EBB8BCED82AF3A220ED07D3577AFBE085BADC0E9C7678292B80E3EC5D3444
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema".. },.. "app_name": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema".. },.. "craw_app_unavailable": {.. "message": "Programa .iuo metu negalima.".. },.. "craw_connect_to_network": {.. "message": "Prisijunkite prie tinklo.".. },.. "iap_unavailable": {.. "message": "Mok.jimai programoje .iuo metu negalimi.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prisijunkite prie .Chrome..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\lv\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	671
Entropy (8bit):	4.631774066483956
Encrypted:	false
SSDEEP:	12:1HEJFhVbGGFhVb+WYpU34wDoz+dgGedBO8ZpU34wF03OyZnLAOfTYGYID:1HENQKkWYp2Doy/em8Zp2WOGAOfRYID
MD5:	C5CE2C51391EAFD3DA9E4C71549A3C28
SHA1:	1F67FF6EF6E90C0CE3AAF56ED543A3EFD381574D

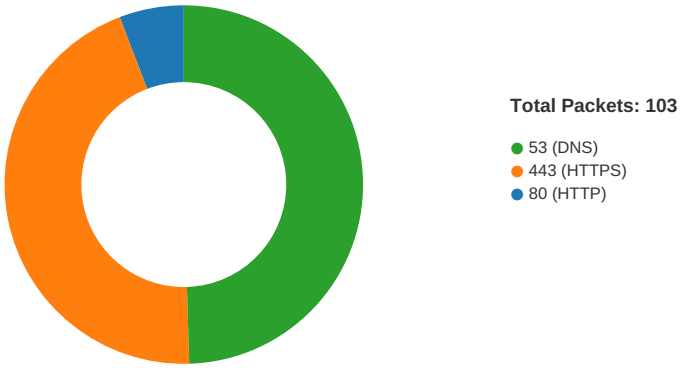
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1542486938\CRX_INSTALL_locales\lv\messages.json	
SHA-256:	1FA1DF2CA8516DEF490FB8484E9AA498ACFF80EEF5C9258FFE42D3678E6C7DED
SHA-512:	C85F6281E682F52BC2147DEA7E2F3BB4DC48D98BADA8687B05C6C7271C78EA7F5431CD51671A4184C9AE004FC53C016E3C594697F483195CCBA08A93821EEF
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome interneta veikala maks.jumu sist.ma".. },.. "app_name": {.. "message": "Chrome interneta veikala maks.jumu s ist.ma".. },.. "craw_app_unavailable": {.. "message": "Lietotne pagaid.m nav pieejama.".. },.. "craw_connect_to_network": {.. "message": "L.dzu, izveidojiet savienojumu ar t.klu.".. },.. "iap_unavailable": {.. "message": "Maks.jumi lietotn.s pa.laik nav pieejami.".. },.. "jwt_retrieve_failed": {.. "message": "The transacti on could not be completed.".. },.. "please_sign_in": {.. "message": "L.dzu, pierakstieties p.rl.k. Chrome.".. }..}..

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:55:33.667709112 CEST	49703	80	192.168.2.7	198.54.125.197
Apr 8, 2021 13:55:33.668335915 CEST	49704	80	192.168.2.7	198.54.125.197
Apr 8, 2021 13:55:33.841121912 CEST	80	49703	198.54.125.197	192.168.2.7
Apr 8, 2021 13:55:33.841322899 CEST	49703	80	192.168.2.7	198.54.125.197
Apr 8, 2021 13:55:33.842348099 CEST	49703	80	192.168.2.7	198.54.125.197
Apr 8, 2021 13:55:33.843230009 CEST	80	49704	198.54.125.197	192.168.2.7
Apr 8, 2021 13:55:33.843360901 CEST	49704	80	192.168.2.7	198.54.125.197
Apr 8, 2021 13:55:34.029381037 CEST	80	49703	198.54.125.197	192.168.2.7
Apr 8, 2021 13:55:34.166435003 CEST	49703	80	192.168.2.7	198.54.125.197
Apr 8, 2021 13:55:34.306375027 CEST	49712	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.306899071 CEST	49713	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.389801025 CEST	49714	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.450870991 CEST	443	49712	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.450894117 CEST	443	49713	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.451004982 CEST	49712	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.451044083 CEST	49713	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.451844931 CEST	49713	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.452012062 CEST	49712	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.537158012 CEST	443	49714	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.537259102 CEST	49714	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.537509918 CEST	49714	443	192.168.2.7	216.172.172.184

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:55:34.596775055 CEST	443	49712	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.601438046 CEST	443	49712	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.601634979 CEST	443	49712	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.601691961 CEST	443	49712	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.601732016 CEST	49712	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.603980064 CEST	443	49713	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.606105089 CEST	443	49713	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.606133938 CEST	443	49713	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.606153011 CEST	443	49713	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.606247902 CEST	49713	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.612202883 CEST	49712	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.612832069 CEST	49713	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.612917900 CEST	49713	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.613039970 CEST	49712	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.613176107 CEST	49712	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.684721947 CEST	443	49714	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.687558889 CEST	443	49714	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.687607050 CEST	443	49714	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.687628031 CEST	443	49714	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.687666893 CEST	49714	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.688718081 CEST	49714	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.757164955 CEST	443	49712	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.757188082 CEST	443	49712	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.757198095 CEST	443	49712	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.757222891 CEST	443	49713	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.757318020 CEST	443	49712	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.757329941 CEST	49712	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.757345915 CEST	443	49713	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.757354021 CEST	49713	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.757369995 CEST	443	49713	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.757426023 CEST	49712	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.757433891 CEST	49713	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.757442951 CEST	49713	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.757451057 CEST	443	49713	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.757514000 CEST	49713	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.757549047 CEST	443	49713	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.757638931 CEST	443	49713	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.757672071 CEST	49713	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.757694006 CEST	49713	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.757714033 CEST	49712	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.798579931 CEST	443	49712	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.840576887 CEST	443	49714	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.840600967 CEST	443	49714	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.840868950 CEST	49714	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:34.840894938 CEST	443	49714	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.902121067 CEST	443	49712	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:34.958412886 CEST	49714	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:35.417418003 CEST	443	49712	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:35.466517925 CEST	49712	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:35.510093927 CEST	49712	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:35.510371923 CEST	49712	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:35.510652065 CEST	49712	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:35.654532909 CEST	443	49712	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:35.654562950 CEST	443	49712	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:35.654891014 CEST	443	49712	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:35.689352036 CEST	443	49712	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:35.694165945 CEST	49712	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:35.884069920 CEST	443	49712	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:35.889867067 CEST	443	49712	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:35.961714029 CEST	443	49712	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:35.961795092 CEST	49712	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:35.961884022 CEST	443	49712	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:35.961911917 CEST	443	49712	216.172.172.184	192.168.2.7
Apr 8, 2021 13:55:35.961926937 CEST	443	49712	216.172.172.184	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:55:35.961988926 CEST	49712	443	192.168.2.7	216.172.172.184
Apr 8, 2021 13:55:36.068249941 CEST	49722	443	192.168.2.7	152.199.23.37
Apr 8, 2021 13:55:36.068484068 CEST	49723	443	192.168.2.7	152.199.23.37
Apr 8, 2021 13:55:36.068830967 CEST	49724	443	192.168.2.7	152.199.23.37
Apr 8, 2021 13:55:36.069133997 CEST	49725	443	192.168.2.7	152.199.23.37
Apr 8, 2021 13:55:36.069402933 CEST	49726	443	192.168.2.7	152.199.23.37
Apr 8, 2021 13:55:36.084150076 CEST	443	49722	152.199.23.37	192.168.2.7
Apr 8, 2021 13:55:36.084182024 CEST	443	49723	152.199.23.37	192.168.2.7
Apr 8, 2021 13:55:36.084245920 CEST	49722	443	192.168.2.7	152.199.23.37
Apr 8, 2021 13:55:36.084280014 CEST	49723	443	192.168.2.7	152.199.23.37
Apr 8, 2021 13:55:36.084557056 CEST	443	49724	152.199.23.37	192.168.2.7
Apr 8, 2021 13:55:36.084585905 CEST	49722	443	192.168.2.7	152.199.23.37
Apr 8, 2021 13:55:36.084640026 CEST	49724	443	192.168.2.7	152.199.23.37
Apr 8, 2021 13:55:36.084647894 CEST	443	49725	152.199.23.37	192.168.2.7
Apr 8, 2021 13:55:36.084708929 CEST	49725	443	192.168.2.7	152.199.23.37

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:55:20.859894037 CEST	50848	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:20.873317003 CEST	53	50848	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:21.847781897 CEST	61242	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:21.860630035 CEST	53	61242	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:23.136055946 CEST	58562	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:23.149669886 CEST	53	58562	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:23.883147955 CEST	56590	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:23.901854038 CEST	53	56590	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:24.333180904 CEST	60501	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:24.345887899 CEST	53	60501	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:25.167047024 CEST	53775	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:25.179599047 CEST	53	53775	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:26.248671055 CEST	51837	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:26.261548042 CEST	53	51837	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:27.727641106 CEST	55411	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:27.742078066 CEST	53	55411	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:30.017620087 CEST	63668	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:30.030695915 CEST	53	63668	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:33.635632038 CEST	58717	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:33.640604973 CEST	59762	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:33.641592979 CEST	54329	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:33.644934893 CEST	58052	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:33.645410061 CEST	54008	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:33.653520107 CEST	53	54329	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:33.658298016 CEST	53	58052	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:33.661972046 CEST	53	58717	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:33.665712118 CEST	53	54008	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:33.680267096 CEST	53	59762	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:33.918015003 CEST	59451	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:33.930546045 CEST	53	59451	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:34.092689991 CEST	52914	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:34.105787992 CEST	53	52914	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:34.140943050 CEST	64569	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:34.304543972 CEST	53	64569	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:35.118410110 CEST	52816	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:35.130779028 CEST	53	52816	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:35.468497038 CEST	50781	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:35.481193066 CEST	53	50781	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:36.037009001 CEST	54230	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:36.037611008 CEST	54911	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:36.049660921 CEST	53	54230	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:36.061300039 CEST	53	54911	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:36.696866035 CEST	59730	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:36.719778061 CEST	53	59730	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:36.812103033 CEST	59310	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:55:36.831758022 CEST	53	59310	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:36.956953049 CEST	51919	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:36.969922066 CEST	53	51919	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:37.449634075 CEST	64296	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:37.488771915 CEST	53	64296	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:37.751120090 CEST	56680	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:37.780193090 CEST	53	56680	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:37.863995075 CEST	58820	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:37.876713991 CEST	53	58820	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:37.981329918 CEST	60983	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:38.012643099 CEST	53	60983	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:39.280241013 CEST	49247	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:39.294047117 CEST	53	49247	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:39.302795887 CEST	52286	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:39.315438986 CEST	53	52286	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:40.013695002 CEST	56064	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:40.027017117 CEST	53	56064	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:46.729316950 CEST	60599	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:46.744477987 CEST	53	60599	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:47.767951965 CEST	59571	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:48.786084890 CEST	59571	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:48.799042940 CEST	53	59571	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:49.582330942 CEST	52689	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:49.627685070 CEST	53	52689	8.8.8.8	192.168.2.7
Apr 8, 2021 13:55:52.310306072 CEST	50290	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:53.326929092 CEST	50290	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:55:53.340204000 CEST	53	50290	8.8.8.8	192.168.2.7
Apr 8, 2021 13:56:01.051099062 CEST	60427	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:56:01.063908100 CEST	53	60427	8.8.8.8	192.168.2.7
Apr 8, 2021 13:56:03.007256031 CEST	56209	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:56:03.036463022 CEST	53	56209	8.8.8.8	192.168.2.7
Apr 8, 2021 13:56:07.212220907 CEST	59582	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:56:07.234566927 CEST	53	59582	8.8.8.8	192.168.2.7
Apr 8, 2021 13:56:09.926378965 CEST	60949	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:56:09.939152956 CEST	53	60949	8.8.8.8	192.168.2.7
Apr 8, 2021 13:56:11.337342978 CEST	58542	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:56:11.350179911 CEST	53	58542	8.8.8.8	192.168.2.7
Apr 8, 2021 13:56:12.033323050 CEST	59179	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:56:12.046148062 CEST	53	59179	8.8.8.8	192.168.2.7
Apr 8, 2021 13:56:12.790273905 CEST	60927	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:56:12.803142071 CEST	53	60927	8.8.8.8	192.168.2.7
Apr 8, 2021 13:56:13.583187103 CEST	57854	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:56:13.596477032 CEST	53	57854	8.8.8.8	192.168.2.7
Apr 8, 2021 13:56:14.077224016 CEST	62026	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:56:14.095443964 CEST	53	62026	8.8.8.8	192.168.2.7
Apr 8, 2021 13:56:14.398052931 CEST	59453	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:56:14.411230087 CEST	53	59453	8.8.8.8	192.168.2.7
Apr 8, 2021 13:56:14.924611092 CEST	62468	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:56:14.936517000 CEST	53	62468	8.8.8.8	192.168.2.7
Apr 8, 2021 13:56:29.605896950 CEST	52563	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:56:29.619157076 CEST	53	52563	8.8.8.8	192.168.2.7
Apr 8, 2021 13:56:30.179080963 CEST	62826	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:56:30.205573082 CEST	53	62826	8.8.8.8	192.168.2.7
Apr 8, 2021 13:56:30.645097017 CEST	62046	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:56:30.658792019 CEST	53	62046	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 13:55:33.645410061 CEST	192.168.2.7	8.8.8.8	0xfe7b	Standard query (0)	www.ztzusl.vibz.co.uk	A (IP address)	IN (0x0001)
Apr 8, 2021 13:55:34.140943050 CEST	192.168.2.7	8.8.8.8	0x711d	Standard query (0)	jrschnell.com.br	A (IP address)	IN (0x0001)
Apr 8, 2021 13:55:36.037009001 CEST	192.168.2.7	8.8.8.8	0x4abd	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 13:55:36.037611008 CEST	192.168.2.7	8.8.8.8	0xef3f	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
Apr 8, 2021 13:55:36.696866035 CEST	192.168.2.7	8.8.8.8	0x6915	Standard query (0)	cdn.clipart.email	A (IP address)	IN (0x0001)
Apr 8, 2021 13:55:36.812103033 CEST	192.168.2.7	8.8.8.8	0x2dc6	Standard query (0)	clipartkind.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:55:36.956953049 CEST	192.168.2.7	8.8.8.8	0x5f1	Standard query (0)	a.nel.cloudflare.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:55:37.449634075 CEST	192.168.2.7	8.8.8.8	0x4d39	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:55:37.751120090 CEST	192.168.2.7	8.8.8.8	0x964d	Standard query (0)	cdn.clipart.email	A (IP address)	IN (0x0001)
Apr 8, 2021 13:55:37.863995075 CEST	192.168.2.7	8.8.8.8	0xe31	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
Apr 8, 2021 13:55:37.981329918 CEST	192.168.2.7	8.8.8.8	0x3233	Standard query (0)	clipartkind.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 13:55:33.665712118 CEST	8.8.8.8	192.168.2.7	0xfe7b	No error (0)	www.ztzusl.vibz.co.uk		198.54.125.197	A (IP address)	IN (0x0001)
Apr 8, 2021 13:55:34.304543972 CEST	8.8.8.8	192.168.2.7	0x711d	No error (0)	jrschnell.com.br		216.172.172.184	A (IP address)	IN (0x0001)
Apr 8, 2021 13:55:36.049660921 CEST	8.8.8.8	192.168.2.7	0x4abd	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:55:36.061300039 CEST	8.8.8.8	192.168.2.7	0xef3f	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:55:36.061300039 CEST	8.8.8.8	192.168.2.7	0xef3f	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Apr 8, 2021 13:55:36.719778061 CEST	8.8.8.8	192.168.2.7	0x6915	No error (0)	cdn.clipart.email		104.21.52.8	A (IP address)	IN (0x0001)
Apr 8, 2021 13:55:36.719778061 CEST	8.8.8.8	192.168.2.7	0x6915	No error (0)	cdn.clipart.email		172.67.192.199	A (IP address)	IN (0x0001)
Apr 8, 2021 13:55:36.831758022 CEST	8.8.8.8	192.168.2.7	0x2dc6	No error (0)	clipartkind.com		104.21.69.231	A (IP address)	IN (0x0001)
Apr 8, 2021 13:55:36.831758022 CEST	8.8.8.8	192.168.2.7	0x2dc6	No error (0)	clipartkind.com		172.67.215.110	A (IP address)	IN (0x0001)
Apr 8, 2021 13:55:36.969922066 CEST	8.8.8.8	192.168.2.7	0x5f1	No error (0)	a.nel.cloudflare.com		35.190.80.1	A (IP address)	IN (0x0001)
Apr 8, 2021 13:55:37.488771915 CEST	8.8.8.8	192.168.2.7	0x4d39	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:55:37.488771915 CEST	8.8.8.8	192.168.2.7	0x4d39	No error (0)	googlehosted.l.googleusercontent.com		172.217.168.33	A (IP address)	IN (0x0001)
Apr 8, 2021 13:55:37.780193090 CEST	8.8.8.8	192.168.2.7	0x964d	No error (0)	cdn.clipart.email		172.67.192.199	A (IP address)	IN (0x0001)
Apr 8, 2021 13:55:37.780193090 CEST	8.8.8.8	192.168.2.7	0x964d	No error (0)	cdn.clipart.email		104.21.52.8	A (IP address)	IN (0x0001)
Apr 8, 2021 13:55:37.876713991 CEST	8.8.8.8	192.168.2.7	0xe31	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:55:37.876713991 CEST	8.8.8.8	192.168.2.7	0xe31	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Apr 8, 2021 13:55:38.012643099 CEST	8.8.8.8	192.168.2.7	0x3233	No error (0)	clipartkind.com		104.21.69.231	A (IP address)	IN (0x0001)
Apr 8, 2021 13:55:38.012643099 CEST	8.8.8.8	192.168.2.7	0x3233	No error (0)	clipartkind.com		172.67.215.110	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.ztzusl.vibz.co.uk.

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49703	198.54.125.197	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:55:33.842348099 CEST	1093	OUT	GET / HTTP/1.1 Host: www.ztzusl.vibz.co.uk. Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Apr 8, 2021 13:55:34.029381037 CEST	1193	IN	HTTP/1.1 200 OK date: Thu, 08 Apr 2021 11:55:33 GMT server: Apache x-powered-by: PHP/7.3.27 accept-ranges: none vary: Accept-Encoding content-encoding: gzip content-length: 364 content-type: text/html; charset=UTF-8 Data Raw: 1f 8b 08 00 00 00 00 00 03 4d 51 4d 6f c2 30 0c bd 4f e2 3f 74 ec 90 44 0d 69 61 1b fb 28 e1 b6 f3 a6 ed b0 03 30 29 a4 06 32 ba 12 b5 81 32 35 f9 ef 4b 60 20 a2 c8 7a 7e b6 9f 2d bb 73 d5 b9 1a ad cc 4f 31 8e 02 00 91 07 10 f9 37 32 ca 14 30 7e 2b 40 d4 10 7d 0a 65 18 63 a3 e4 c8 86 e4 5a 56 4a 9b c8 fc 6a e0 5d 03 7b 93 7c 8b 9d 38 b2 dd 71 c7 0b c3 4e 14 78 b1 2d a5 51 9b 12 6b 2a a8 a4 6b 0a 34 27 2d f0 33 2f 49 5b 81 d9 56 65 24 5d a6 16 f8 1a 21 56 81 2e 84 04 9c 7c 25 f4 c3 54 aa 5c 12 d2 36 2b 55 00 96 bd 1e 69 f3 89 9c f1 b5 37 d6 4a b7 e6 93 b3 18 9c c5 f2 09 cc dc 2c bb 68 74 0a a1 e9 b4 89 91 cb 24 ef bb ec 42 d4 f7 0e 92 a4 d5 5c 9f 27 28 a1 89 de 61 f9 b2 d7 d8 d7 cd 51 ec 93 49 7c 80 14 2d 11 a1 87 12 e7 fe bb 6a 87 d1 30 4a f9 3d bb 63 b7 d9 30 1a f0 94 3d e1 94 3d e2 29 ba 99 22 12 f7 49 76 88 f1 ee c3 73 92 74 e3 41 86 68 3f 0d 1f d5 a6 b2 d6 9b be 5d 55 b0 b0 c5 46 8a 30 b7 6d 54 99 6f 1a bb 13 95 5d 19 a3 6b eb 7d d8 bf 2e 6c bd 9d d7 87 e5 20 56 eb 42 19 8c ac 1f 28 a5 ad 23 24 ec df 1f 29 39 de 63 7c 74 4e f7 f5 28 9c 3c 90 7f d3 8a 66 42 01 02 00 00 Data Ascii: MQMo0O?tDia(0)225K` z~-sO1720~+@}ecZVJj{|8qNx-Qk*k4'-3/I[Ve$]!V.\|%T\6+Ui7J,ht$B\'(aQI|-j0J=c0==)" IvstAh?]UF0mTo]k}.I VB(#$)9c|tN(<fB

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	198.54.125.197	80	192.168.2.7	49704	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:55:45.295249939 CEST	3237	IN	HTTP/1.1 400 Bad request content-length: 90 cache-control: no-cache content-type: text/html connection: close Data Raw: 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 3c 68 31 3e 34 30 30 20 42 61 64 20 72 65 71 75 65 73 74 3c 2f 68 31 3e 0a 59 6f 75 72 20 62 72 6f 77 73 65 72 20 73 65 6e 74 20 61 6e 20 69 6e 76 61 6c 69 64 20 72 65 71 75 65 73 74 2e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <html><body> 400 Bad request Your browser sent an invalid request.</body></html>

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 8, 2021 13:55:37.910770893 CEST	152.199.23.37	443	192.168.2.7	49738	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Apr 8, 2021 13:55:37.911031008 CEST	152.199.23.37	443	192.168.2.7	49739	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Apr 8, 2021 13:55:37.992553949 CEST	152.199.23.37	443	192.168.2.7	49740	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 8, 2021 13:55:38.005889893 CEST	152.199.23.37	443	192.168.2.7	49741	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Apr 8, 2021 13:55:38.077769041 CEST	104.21.69.231	443	192.168.2.7	49742	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Oct 13 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Wed Oct 13 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior

System Behavior

Analysis Process: chrome.exe PID: 5056 Parent PID: 3600

General

Start time:	13:55:28
Start date:	08/04/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'http://www.ztzusl.vibz.co.uk./#jrschnell.com.br/site/z1/bGFtQHNwYXJub3JkLmRr'
Imagebase:	0x7ff76d1c0000
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: 4884 Parent PID: 5056

General

Start time:	13:55:29
Start date:	08/04/2021
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=1496,6792534671230322255,6132008020722060178,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1728 /prefetch:8
Imagebase:	0x7ff76d1c0000
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	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly