ID: 383856
Cookbook: browseurl.jbs
Time: 11:19:37
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

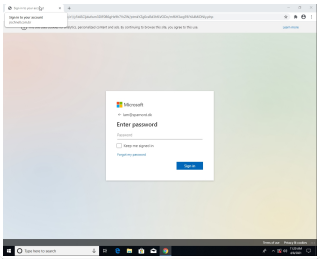
Analysis Report http://www.ztzusl.vibz.co.uk./#jrschnell....

Overview

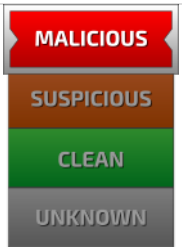
General Information

Sample URL:	http://www.ztzusl.vibz.co.uk./#jrschnell.com.br/site/z1/bGFtQHNwYXJub3JkLmRr
Analysis ID:	383856
Infos:	

Most interesting Screenshot:



Detection



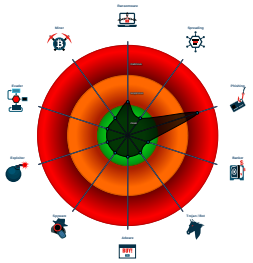
HTMLPhisher

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: 3880 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: 5856 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1540,11347640063778282216,12771895532885012560,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1688 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

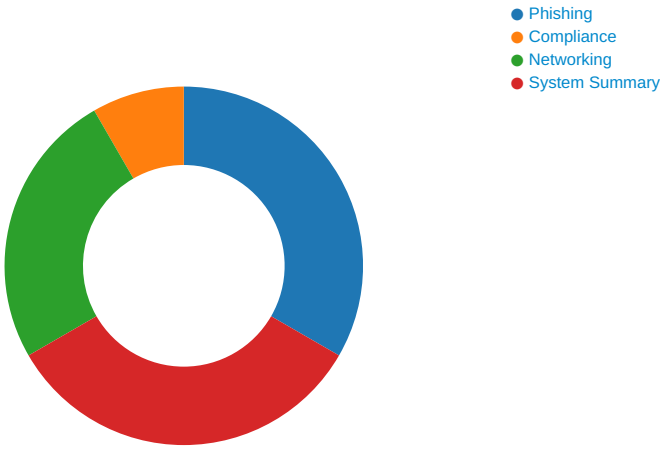
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

Phishing:

Yara detected HtmlPhish10

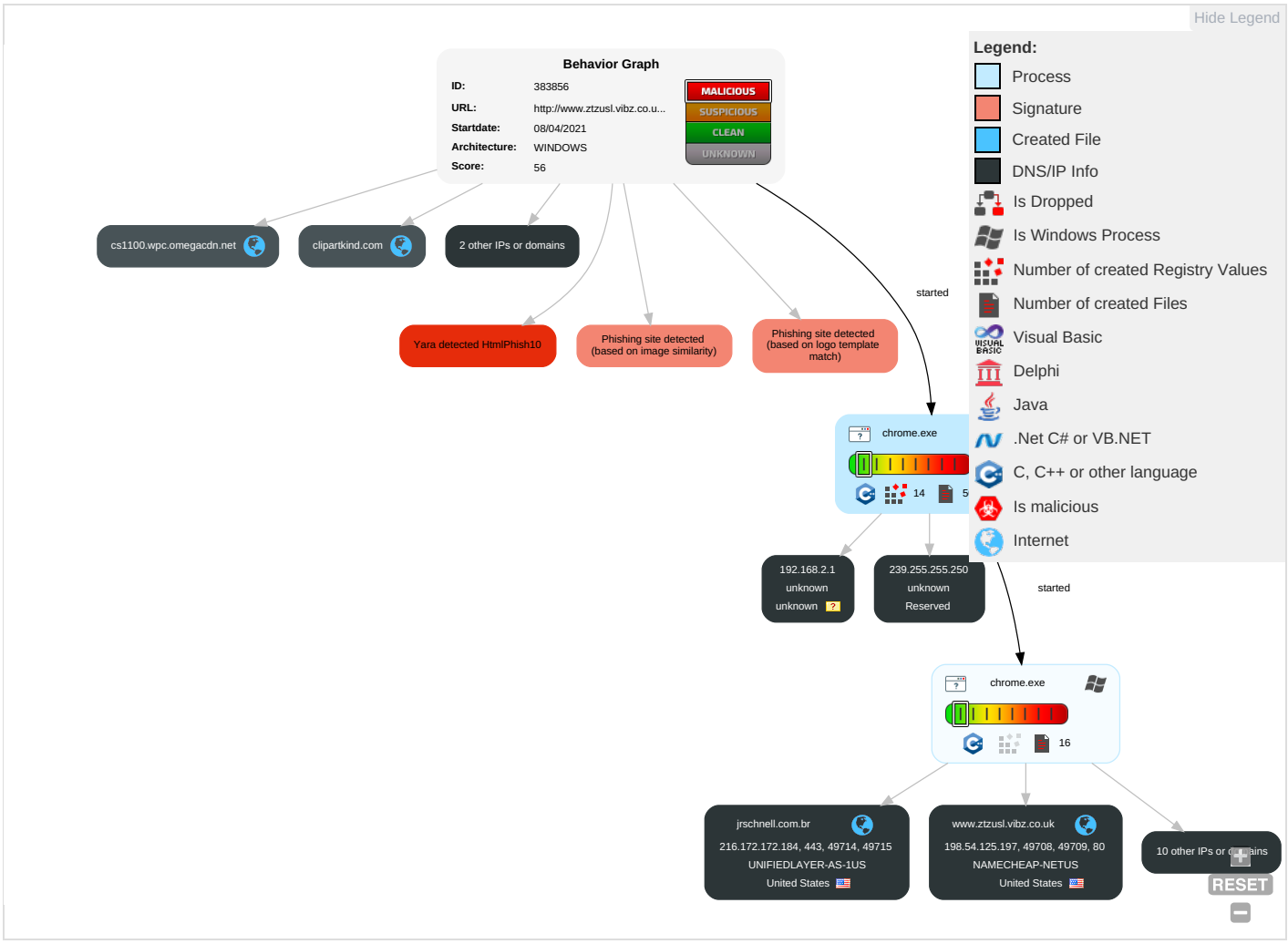
Phishing site detected (based on image similarity)

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

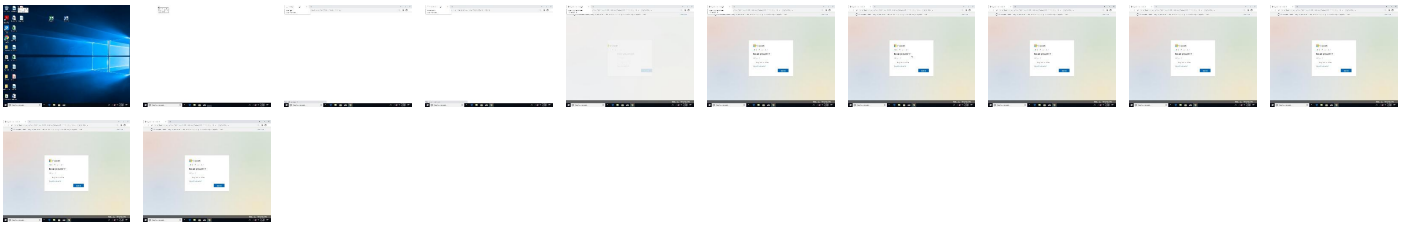
Behavior Graph

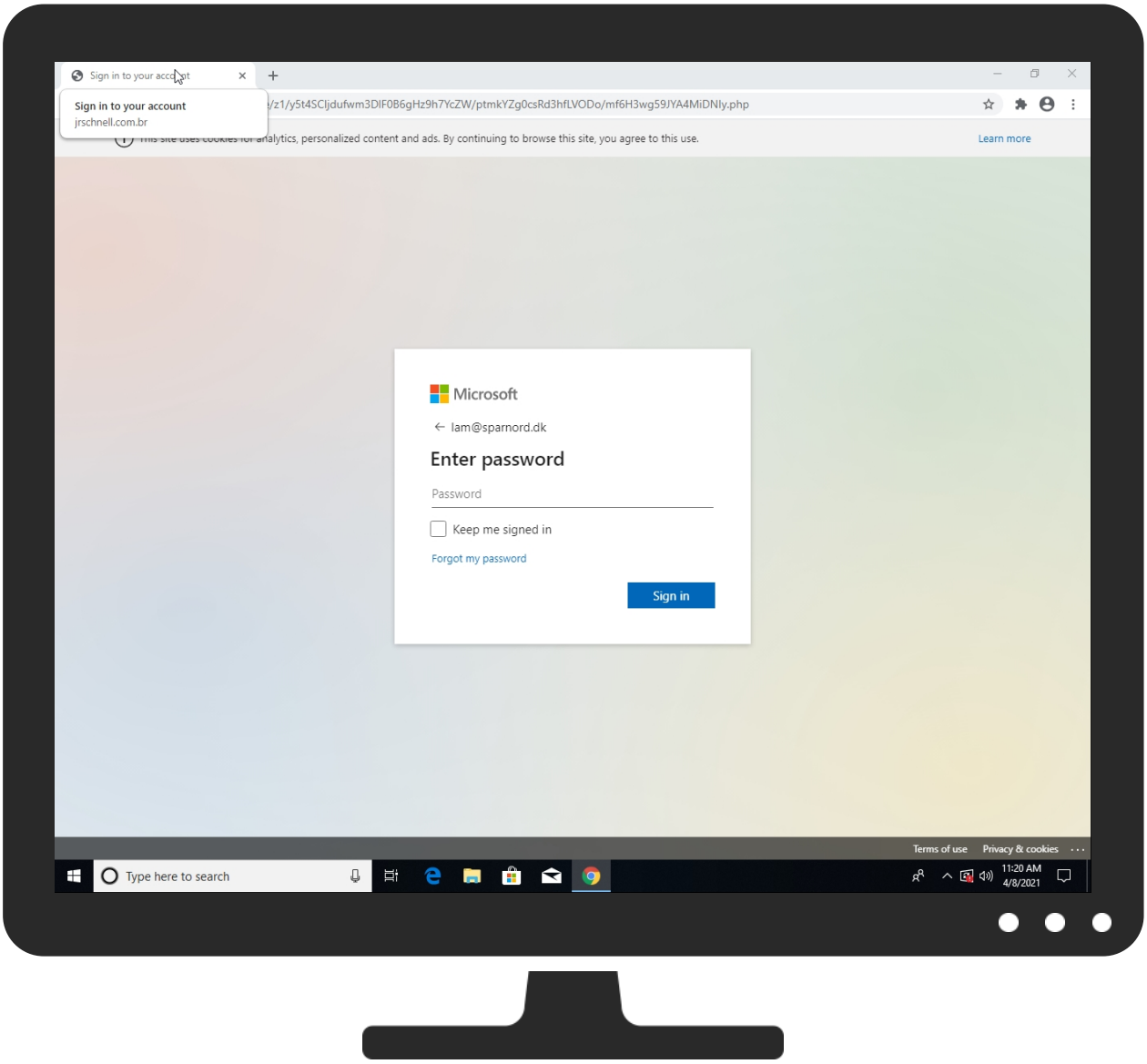


Screenshots

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/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/y5t4SCIjdufwm3DlF0B6gHz9h7YcZW/ptmkYZg0csRd3hfLVODo/mf6H3wg59JYA4Mi	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	172.67.192.199	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://https://jrschnell.com.br/site/z1/y5t4SCIjdufwm3DlF0B6gHz9h7YcZW/ptmkYZg0csRd3hfLVODo/mf6H3wg59JYA4MiDNIy.php	true		unknown
http://www.ztzusl.vibz.co.uk./	false	• Avira URL Cloud: safe	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	85f45a16-0382-45af-b147-50395de217b0.tmp.1.dr, 468071a4-6c7d-4327-9229-b9c7ff9f8d37.tmp.1.dr, 6c452b1a-6acf-4bcf-809d-623812ae33de.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/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://https://jrschnell.com.br/site/z1/y5t4SCIjdufwm3DlF0B6gHz9h7YcZW/ptmkYZg0csRd3hfLVODo/mf6H3wg59JYA4Mi	History.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
http://www.ztzusl.vibz.co.uk./#jrschnell.com.br/site/z1/bGFtQHNwYXJub3JkLmRrPlease	History.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://a.nel.cloudflare.com/report?s=%2Brkvlk2spclXqK6yTmx2usbGOs8A629aLK1Dqd3p0H0JYWQO71VtF1WOEgDU	Reporting and NEL.1.dr	false		high
http://https://clients2.googleusercontent.com	6c452b1a-6acf-4bcf-809d-623812ae33de.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
http://https://a.nel.cloudflare.com/report?s=x%2Fk503X%2FQhaDDfvDnSBp0jVUjYJ98bFOUyn9O3pstJJ87ASzqPO11BiOuN	Reporting and NEL.1.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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
172.67.192.199	cdn.clipart.email	United States		13335	CLOUDFLARENETUS	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
192.168.2.6
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383856
Start date:	08.04.2021
Start time:	11:19:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 20s
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:	16
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@34/214@11/11
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): 104.42.151.234, 52.255.188.83, 23.54.113.53, 104.43.139.144, 172.217.168.13, 216.58.215.238, 173.194.160.74, 74.125.173.166, 172.217.168.67, 172.217.168.74, 13.107.246.19, 13.107.213.19, 168.61.161.212, 142.250.34.2, 172.217.168.10, 172.217.168.42, 216.58.215.234, 95.100.54.203, 20.82.209.183, 23.10.249.43, 23.10.249.26, 23.0.174.200, 23.0.174.185, 172.217.168.35 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, standard.t-0009.t-msedge.net, arc.msn.com.nsatc.net, r5.sn-1gi7znes.gvt1.com, store-images.s-microsoft.com-c.edgekey.net, clientservices.googleapis.com, fs-wildcard.microsoft.com.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, clients2.google.com, redirector.gvt1.com, dual.t-0009.t-msedge.net, Edge-Prod-ZRH.ctrl.t-0009.t-msedge.net, audownload.windowsupdate.nsatc.net, update.googleapis.com, arc.trafficmanager.net, edgedl.gvt1.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, www.gstatic.com, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, accounts.google.com, content-autofill.googleapis.com, aadcdnoriginwus2.azureedge.net, aadcdnoriginneu.azureedge.net, r5---sn-1gi7znes.gvt1.com, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, www.googleapis.com, star-azureedge-prod.trafficmanager.net, r1---sn-1gieen7e.gvt1.com, aadcdnoriginneu.ec.azureedge.net, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, t-0009.t-msedge.net, blobcollector.events.data.trafficmanager.net, aadcdnoriginwus2.afd.azureedge.net, clients.l.google.com, 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\27117dd9-7858-4d4c-8374-ef16839ad30c.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):	164083
Entropy (8bit):	6.081899989270215
Encrypted:	false
SSDEEP:	3072:BwQzmnDWVhPFlyU7sCXgcbjH1FcbXafIB0u1GOJmA3iuR9:Gi6Q1sJQHDaqfIlUOoSiuR9
MD5:	398937F766836A2366CFC530D0759D36
SHA1:	0CCD21036D34B732CBE3D97434190EA644C8EB8E
SHA-256:	385CD968078D0B6A95CE4D80DE4213833DEF5EBB6E6E8CD2FBEC4A489BB68303
SHA-512:	B693948C74BFFBFE824F96318CBE1772680A261236232A2F71DAC8276D2771495D1923CA0628D27AAE41C3F747F4B2E037C9C66A15B5C29AF50B702AC4C23CF
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":1.617906032849408e+12,"network":1.617873635e+12,"ticks":102873649.0,"uncertainty":4388577.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\28dcbefa-31e9-44c9-98bc-b9e314d9ca01.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):	164083
Entropy (8bit):	6.081901824200476
Encrypted:	false
SSDEEP:	3072:26xzmnDWVhPFlyU7sCXgcbjH1FcbXafIB0u1GOJmA3iuR9:Px6Q1sJQHDaqfIlUOoSiuR9
MD5:	3C2CDFDB5EFC0927CE5720AEFD1D483C
SHA1:	1E6522FB32CBD5025A89A7C82EFE11C31CC2135B
SHA-256:	22224F7A547B7AF107669D7A25CEB29F43453961BD35CB5E669F21EF2FFDA0CC
SHA-512:	6DB181068095CD698A92C6F2C8CF3E3EE00D709C0F729D8DFEAE190AC45569BDA64738A7003D36E56FE7E21B1767A3A9DACBB7759BC78FB36828A472CE34F1E
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":1.617906032849408e+12,"network":1.617873635e+12,"ticks":102873649.0,"uncertainty":4388577.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016684776"},"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:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftIE1G1mkftIE1G1mkftIE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D021294256372C916B8155AC
Malicious:	false
Reputation:	low
Preview:	sdPC....................s}.....M..2.!..%sdPC....................s}.....M..2.!..%sdPC....................s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\12e68644-61a2-49ea-ac3b-c655cca306ab.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):	5.203673802006508
Encrypted:	false
SSDEEP:	96:nv9aGqf8aUHcVZok0JCMRWL8wkG1ekQhUbOTQVuwn:nvof5+c+4MYZkGUkQg
MD5:	71FA5559D02E9D945AEA2A545ED64961
SHA1:	85714D5C0B45984A2DBB6048211F0D14256DCFAB
SHA-256:	EB77825DA3966F88CFF46F849A53F297544A52BCD6CFD9ED177F36DC6E8FC402
SHA-512:	883DD86CF1C2800652ED8871389F0E346C50ED51753B38A57056C8DB6E583F09810CDC9ED27047CA3A171052C1220D3347C15DA36A4070B9D5E80D96B81FABB
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13262379630062876","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\27985dbb-12ee-42eb-805c-16dc3b9e2656.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.577073061195475
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\27985dbb-12ee-42eb-805c-16dc3b9e2656.tmp	
SSDEEP:	384:yoRVteLlxeXG1kXqKf/pUZNCgVLH2HfDOrU96c4t2:dYLl+G1kXqKf/pUZNCgVLH2HfqrUwcH
MD5:	DBAFEC06F964FC65987A346F47ABBB84
SHA1:	40E9368BB0A3F285426033D3ED7CACC72EB70E73
SHA-256:	371446762B615B42AC333240D7047DB07805DB71C32D1D4EA9FDF0BCB7608E8E
SHA-512:	D902CF299268FA8DFF9534C17303E7269079A3A117BED48CF0D612F8047F74D51C3DDBFB3C7935E8C81FCA71B90AB1B289BAA285B0CA293722E390D14B9DE3E A
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":"13262379629691889","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\50152995-54ba-4d0f-9cf9-590ee46c0e55.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):	5883
Entropy (8bit):	5.196014902836429
Encrypted:	false
SSDEEP:	96:nv9aGqf8aUHcVZok0JCMRWL8wkG1lbOTQVuwn:nvof5+c+4MYZkGH
MD5:	2A008607FDF24F540A601288ACBCFB2B
SHA1:	0C4F14C40D90F0ABEB9268906C4BC3D4F1C63A2B
SHA-256:	486A3C5393027A4B1C2F229FA71F2AD4347BF6F6259F842326A7C210089E34B6
SHA-512:	E1A69D0C8B38E8F220770D014E9F75C4CDF770BE9264F2AB0D906FF7ABBEA9017C4EB8E5A7C51D104CC2E971453A5F7AF56C7831A313DAE6B7BF0A70E87346 D
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13262379630062876","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6c452b1a-6acf-4bcf-809d-623812ae33de.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\868740ef-3c96-408f-a507-d8764ad40bd0.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):	24055
Entropy (8bit):	5.533619345904314
Encrypted:	false
SSDEEP:	384:yoRVtDLlxeXG1kXqKf/pUZNCgVLH2HfDOrUeHGgHG7nTYdc4I:dlLl+G1kXqKf/pUZNCgVLH2HfqrUOGkE

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\868740ef-3c96-408f-a507-d8764ad40bd0.tmp	
MD5:	165B364B2042CB408F86DB3A6A15A377
SHA1:	A52F82599E69F0283B8D1718601E24FFD06538F4
SHA-256:	789A56159EFECD309DD1F7EA5B4F3E85127DFEAB5A28B6204A466395C4AF5203
SHA-512:	BAADC8C69AFADD1C6B58C91BC163E26C169BCD94DF7E8B410CA9ECDF8A9A32F8650BBAE2E1AD1B9A2107A9B7F8980ABCE3CABD68A71217ED3FB9CEA154AD1F1C
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":"13262379629691889","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.179937533959465
Encrypted:	false
SSDEEP:	6:m1jUJq2PWXp+N23iKKdK9RXXTZIFUtpkjzZmwPkjpkwOWXp+N23iKKdK9RXX5LJ:tJva5Kk7XT2FUtpU/PU5f5Kk7XVJ
MD5:	EB9BF42F30569F1BF4997916A727A631
SHA1:	4ACBF8C7F222DD0E0561F2A221F3313C23222EAF
SHA-256:	EA761115290C69A5B19E268A5764B3E9EBD61CE6215A2F6E3FB240D437288A55
SHA-512:	2F1A1F8FC15E7EB4A35E3E55F03CEB87BD26692BA1BC8EB8EFF88643C0FC989DFF8C4C6E0A3E58499A96CC65AABE1EC83FC7DBA7F6C94FDB9BBF18E0867AC874
Malicious:	false
Reputation:	low
Preview:	2021/04/08-11:20:42.302 1ba4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/04/08-11:20:42.317 1ba4 Recovering log #3.2021/04/08-11:20:42.317 1ba4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.2027239787219255
Encrypted:	false
SSDEEP:	6:m1Xq2PWXp+N23iKKdKyDZIFUtpkDZmwPkwkwOWXp+N23iKKdKyJLJ:cva5Kk02FUtpY/Pp5f5KkWJ
MD5:	639B88A755392CFB8BC994D0BBE53BFD
SHA1:	6D45CD52F1B3B4E097D0461601A9732689E71D48
SHA-256:	630E3B2413A677E41EE9E19BBA78C450CCC849113772364AEEE85477D0CD7CB8
SHA-512:	57E27683E5F9166B56FADA64F6282461AC56CC9B6F736924943572632590D2DF370DF8B644858CB8734B8D21404E3EB31AF2BA742FCEF70EB3D421404E3E48F61
Malicious:	false
Reputation:	low
Preview:	2021/04/08-11:20:42.295 1ba4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/04/08-11:20:42.296 1ba4 Recovering log #3.2021/04/08-11:20:42.297 1ba4 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
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):	0.9684019185108185
Encrypted:	false
SSDEEP:	24:lcLgAZOZD/8qLbJLbXaFpEO5bNmISHn06Uwl8:l8NOZ8q5LLOpEO5J/Kn7Ur8
MD5:	435CF09067ED674C4833BCBBB2BF2BDC
SHA1:	CB0DA50BC004C6589ACF501249F5D7CD60906D0D
SHA-256:	8D0B7461ED7C9BC9B8084D6A42CB89BA1108F5BF5DC08614E4CF1BB52034234A
SHA-512:	D9C4685382D9914B3F0DDDA96188C05F33BC8F0E9B0B6CBB21BC5782AA915DD28E0EC4D03B7650347E5A26030F2C6F2E00720BB0EC1991040C87655082E481F
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3860
Entropy (8bit):	3.889520490120191
Encrypted:	false
SSDEEP:	48:349XkmxiWQrKboPS7vGUuiWPjBRQrQQrFPS7vGUuiWnzPS7vGYXBXjBRQrERRRL:34jETOvGLiU/EQEFOvGLi8OvGYXBX/E+
MD5:	9E3A700552D0E083E4011984148B4F6C
SHA1:	2937F51585B69A40188CA2014336B97C1EE02E78
SHA-256:	B22237C04F52F1D4F1403726452C477FA2D7D1559F567193767F40F1E7273E7E
SHA-512:	B485D76CF306D3CD212BE2684563BB9460DC64AC55440A6C4A9DA1064A6FD02C6063F9C08DCC9A1C7DB67654140E62935BEEF658144E624D1374A8710F9E33E
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...54520caa_a790_4568_8a9c_d1e9a7058ef2.....&..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....l...https://jrschnell.com.br/site/z1/y5t4 SCIjdufwm3DlF0B6gHz9h7YcZW/ptmkYZg0csRd3hfLVODo/mf6H3wg59JYA4MiDNIy.php.....h.....`.....H.....(Vx .z...)Vx.z.....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./.y.5.t.4.S.C.I.j.d.u.f.w.m.3.D.l.F.0.B.6.g.H.z.9.h.7.Y.c.Z.W./.p.t.m.k.Y.Z.g.0.c.s.R .d.3.h.f.L.V.O.D.o./.m.f.6.H.3.w.g.5.9.J.Y.A.4.M.i.D.N.I.y...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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
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):	317
Entropy (8bit):	5.194116928011572
Encrypted:	false
SSDEEP:	6:m1JOq2PWXp+N23iKKdK8aPrqIFUtpk+ZmwPkykwOWXp+N23iKKdK8amLJ:sOva5KkL3FUtpL/PB5f5KkQJ
MD5:	AE6408ABAC00A67048B67F3C4D442494
SHA1:	50A7BE8C21D8208DD0C313A328752B125DB67E68
SHA-256:	EDFEAD6A90D4EB1E8F539A78F664A92204F5D1ACE1C7B2E632D4C04602438D32
SHA-512:	845AF6C24ACA7600FFF958359887CCE157020A6C1DA42F2E0A38A8EE6CD410DEADA849E68049E6DDBF5A77A5E92A490017ADC961120B158021DF8B4C906681
Malicious:	false
Reputation:	low
Preview:	2021/04/08-11:20:30.072 980 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/04/08-11 :20:30.075 980 Recovering log #3.2021/04/08-11:20:30.075 980 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
Encrypted:	false
SSDEEP:	12:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW:
MD5:	9D7435EA49A80FDD66E4915F513017F9
SHA1:	469F6C6E4B19B85CC1BE497812B2F20864F4FF2C
SHA-256:	409D4C47E940688527D730B996E8991E010988C7671565467ED69D640D0947F3
SHA-512:	0561CD632D4219AEF4686DE40EC092921384CA89755D354801E0EAEC8645A8630A180807AF518AC8FCF01F71EB3D10FAA9CE1E62C7A7226A274975BDCB7EEB4 C
Malicious:	false
Reputation:	low
Preview:	.f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f. 5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.. .....f.5.....f.5.....f.5.....f.5.....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):	320
Entropy (8bit):	5.228330540867193
Encrypted:	false
SSDEEP:	6:m10R+q2PWXp+N23iKKdK8NIFUtpk2NZmwPknLVkwOWXp+N23iKKdK8+eLJ:eva5KkpFUtpPN/P0R5f5KkqJ
MD5:	9E4CC7C9ED43A21143E32510F6355417
SHA1:	6C737E778D30128375B1B03C4742D52A2A7FEED9
SHA-256:	3E9D50E85774C05DA63BEEC01D16630459D2B6CFC08C64CF6488041A12206FB0
SHA-512:	9C9ADF326D65EB8A3FC5047B36B44B19199A8CEE454F40EDE5F6BF135D771B5994CD9FCAF45B68B0FCDE548AB52335B2A6C57A8AB4A5D90EF4F7F8B34FF96E C5
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Reputation:	low
Preview:	2021/04/08-11:20:32.355 17d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/04/08-11:20:32.357 17d8 Recovering log #3.2021/04/08-11:20:32.358 17d8 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+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","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
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=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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):	2.050201571609391
Encrypted:	false
SSDEEP:	96:0BCNRmU8TDqAAoqOHXN3pMQAtBvKiW47H+cDtje:m8RmUG2JoqO3BpMQIBvKiW4achq
MD5:	06B5E581EA67978C74C873095F185899
SHA1:	FCB38CC346E8C3B71FF44121F473C90169DD5762
SHA-256:	0927B314A10732E3705C27742DF7104AF5AE51B885C3CA3BCC085A843ABF015F
SHA-512:	52A186F12862D9E43770F2490DAA9081D6C75B277D8D2567075EB2BDA88FEE27D92C25D2658A46C4C18006F3CC08EDFE5A7502E9AFC2848A1244BB65FFD7DD
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):	0.7749024044511349
Encrypted:	false
SSDEEP:	24:J/dyLiXxh0GY/l1rWR1PmCx9fZjsBX+T6Uwlnt3n:jdBmw6fU8t3n
MD5:	B6F88C7693A4BF33A689D86504B26E4B
SHA1:	0B264689FC58298A746CC615EC3911E7A84220C2
SHA-256:	2CC953989DC7C59997E8EB8C0CA716B8E4DFB1CB499AC6EAA09671EE90553ED8
SHA-512:	EEBD85B27B54A0388ABB6B246A67BF0A8C1B7FD0315D9BA2BF81773C0E1AF26E842D801C602A730404D0141653FF8F9454E28F33AB92A92CE808A2B2D962EE95
Malicious:	false
Reputation:	low
Preview:	.....9a.x..... ....

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):	372
Entropy (8bit):	5.249792703854947
Encrypted:	false
SSDEEP:	6:m1AOq2PWXp+N23iKKdK25+Xqx8chI+IFUtpkyZmwPk+kwOWXp+N23iKKdK25+Xqp:HOva5KkTXfchI3FUtpF/PX5f5KkTXfcF
MD5:	79B0ED7829DF18FE57329F08E61007DD
SHA1:	AF42E00A415D5981BCB1B5B6AB95C006125DAEB1
SHA-256:	F9F35360036133194DCAF42BC55692FE8B452D1218AA7747CE665A94E2BD1FFA
SHA-512:	1DD8775BAE09A95038CCD1863CABDAA364701CB1BD2CED9314C9B806A82C724D759777CD3096D32EDC90CC93C56F68D874FB35ADB8BC9F80D7DDF195FB14 03
Malicious:	false
Reputation:	low
Preview:	2021/04/08-11:20:42.257 1ba4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MA NIFEST-000001.2021/04/08-11:20:42.259 1ba4 Recovering log #3.2021/04/08-11:20:42.259 1ba4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.18291574642889
Encrypted:	false
SSDEEP:	6:m1qOq2PWXp+N23iKKdK25+XuoIFUtpkjZmwPk5kwOWXp+N23iKKdK25+XuxWLJ:Mva5KkTXYFUtpI/PQ5f5KkTXHJ
MD5:	E6362722C61F6C7F3FAAA571046942F3
SHA1:	974CDF2852EE99E717E18C7957CA3B1510CB2C64
SHA-256:	772D63C0DCE95039CDD25B35C0104D234A35A4D289C0254230762137919BD885
SHA-512:	FC7B9BD215AB45375F81F259FA9CAC241498A661FC19EB1D519BAAD715533F68F270A8F5CFCC057280788EE05E19839F9DB4B7657A46FB8F003CE582AAA792A
Malicious:	false
Reputation:	low
Preview:	2021/04/08-11:20:42.251 1ba4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST- 000001.2021/04/08-11:20:42.252 1ba4 Recovering log #3.2021/04/08-11:20:42.252 1ba4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data \Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.2005692741210865
Encrypted:	false
SSDEEP:	6:m1Zq2PWXp+N23iKKdKWT5g1IdqIFUtpkW9ZmwPkWPkwOWXp+N23iKKdKWT5g1I3e:Sva5Kkg5gSRFUtp9/PP5f5Kkg5gS3SJ
MD5:	5A772BF1B409FE34D4631B52E171C6E8
SHA1:	AFE7D6B0C5FE15DB7B8200A58F81CCBBBBE36FD3
SHA-256:	73151332CA089440661FEB9638E559EE2388AA223DEAD79C3A4D21490B7F36E9
SHA-512:	590F61343B7D3CA0EBBAD15538954EF3C162AEBF996CBBBF9D643312A9A1F53D3CBB7B51EB0AC500049C373CB44F6AF2DDC30F0B76845E49EFB02C551BAC6 53
Malicious:	false
Reputation:	low
Preview:	2021/04/08-11:20:42.239 1ba4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/04 /08-11:20:42.242 1ba4 Recovering log #3.2021/04/08-11:20:42.242 1ba4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM S tore\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):	0.32539347403915625
Encrypted:	false
SSDEEP:	24:TLxQIwIiaQrBpIiCvqNIiC6Uwv1sFIiaQryIiCsNIiCM:T9QruyEZwvyYQrDsEM
MD5:	0C2E2C87E5956C02C6E9748A68BF2E00

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
SHA1:	E5CC6F955891D2890EA9E43AAC00A92B73731457
SHA-256:	6FFEB5FE52179F7FAD133F7AC56293E77D9B657292A378DA828C0A20F9568393
SHA-512:	0162AE0CBEB888A5523AB4FAC520DFE8531B604720698D62066B4B0C58BED107817BBE4060055A75A5D7994A648B8FBDF4D5FB241C4D69300FB93FB7BDACE69 8
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):	1658
Entropy (8bit):	5.917053515127948
Encrypted:	false
SSDEEP:	48:1GS5498a7FCke913ADUFEwkQQr6D7txEUJQ:1GSua8kkeHADWuQE67Xm
MD5:	0133BFBD455A045E2314F0B85C39E5DA
SHA1:	3D0DB15D3099AA754992D5B66742CFF84E031212
SHA-256:	0976E4CA3DEE70E512678999706A49A84ABFEBC3F350A4F0827EB4FF88E2F626
SHA-512:	35042A0D18204E51BC0D38EAFA2D10057B30518DC24033E3662495824E30C9331A88E6A2608C07633A54F96B5D73D002E99151C48BFE66369146C7676A76D22E
Malicious:	false
Reputation:	low
Preview:	....."......account..br..com..https..in..jrschnell..mf6h3wg59jya4midniy..php..ptmkyzg0csrd3hflvodo..sign..site..to..y5t4scijdufwm3dlf0b6ghz9h7yczw..your..z1..bgftq hnwyxjub3jklmrr..co..http..please..uk..vibz..wait..www..ztzusl*.....account.....bgftqhnwyxjub3jklmrr.....br.....co.....com.....http.....https.....in.....jrschnell.....mf6h3wg59jy a4midniy.....php.....please.....ptmkyzg0csrd3hflvodo.....sign.....site.....to.....uk.....vibz.....wait.....www..."..y5t4scijdufwm3dlf0b6ghz9h7yczw.....your.....z1.....ztzusl..2. .."....0.....1.....3.....4.....5.....6.....7.....9.....a.....b.....c.....d.....e.....f.....g.....h.....i.....j.....k.....l.....m..... ....n.....o.....p.....q.....r.....s.....t.....u.....v.....w.....x.....y.....z.....:.....

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):	0.047324706358956754
Encrypted:	false
SSDEEP:	3:3Sq3llu/fllXSuNllXSvfllXSPNllXSKtFllXS/fllXS8tFllXS4MRgSWbNFl/l2:iqxFvyEuE686ng9bNFlWCj/lhIl3n
MD5:	1D40053FF5F23F7D8334C4B914AC8A2E
SHA1:	4EA9D5A7D82A9F3CCCDD8224FF0638A9B301CB48
SHA-256:	A3C9A244D4CCE317C1545B6860EE6BA76335ED072E4980E11446D4BC02D24A2C
SHA-512:	40B5AD54DFD8E5A62FABAFAB15D77AEDEBE7139D301EFD182C48BBBF3FA94313E71F7A529DFCB08E879D7EA97C724475C8189C19B7F4DD92868F5427A96B29 BE
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):	5.475543558861962
Encrypted:	false
SSDEEP:	48:mUZpfG+3orTa7zTMP28dbn9/3v3nBbQSefgG8NrS0U9RdiN9rH:maB4rTa7zTMPNdbn9/3v3nBbQ5fgGcrp
MD5:	ABC2E7E86928E6F82350A5EB5F0D3A8F
SHA1:	D354ECCF5DFBA3727CA8856FCC8BB561A20EFFB0
SHA-256:	7F0C62484BEFBFF869F0F98376D30EFAA98CA0E5A03E8F867E72BC4C31C4E698
SHA-512:	06B8B47B9B2A10AFE047A535052C68CF9E79FC9C3BE9CBED88B9E779BDAA5F5D38A16579C6F6D1E2BC2F140996665747EB8AD455A0B894203B8C05EE7E0F16 0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Preview:	dI.....*.....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..735122000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-04-08 11:20:46.40][INFO][mr.Init] MR instance ID: 5b9d69c3-8471-467c-a433-6a7be3da57c9\n","[2021-04-08 11:20:46.40][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-04-08 11:20:46.40][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-04-08 11:20:46.54][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-04-08 11:20:46.54][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-04-08 11:20:46.54][INFO][mr.CastProvider] Query enabled: true\n","[2021-04-08 11:20:46.54][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):	329
Entropy (8bit):	5.232871601175602
Encrypted:	false
SSDEEP:	6:m1zmMN+q2PWXp+N23iKKdK8a2jMGIFUtpkzmSQyZmwPkzmS2OVkwOWXp+N23iKKV:WN+va5Kk8EFUtpGlQy/PGl5V5f5Kk8bJ
MD5:	81051169D4CEE68A563BA0624C71D281
SHA1:	7E63A646E6093A071BAA89F08F5DB415C8C77191
SHA-256:	6339B3659E9EB0871AF654E0B5B39DE799EB29FC40861FE62B4A9A7AF1E16BA1
SHA-512:	B3BB65C9F5100462417AB57450695233D7B9D0B6C11AE6F3B57F943B1984B9DAFED3B3550911E6043DF6D689ECF10FBD73E8B5C5C74CD6363616FB3A731AEDF
Malicious:	false
Reputation:	low
Preview:	2021/04/08-11:20:29.762 6bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/04/08-11:20:29.775 6bc Recovering log #3.2021/04/08-11:20:29.777 6bc 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):	334
Entropy (8bit):	5.21325129976729
Encrypted:	false
SSDEEP:	6:m1xt+q2PWXp+N23iKKdKgXz4rRIFUtpkpZmwPksNVkwOWXp+N23iKKdKgXz4q8LJ:Yova5KkgXiuFUtpi/Pdz5f5KkgX2J
MD5:	575574A22386FB612633D2230783D258
SHA1:	8D2B8F6C6EE68C2F38BDC5C2C0B775AFEE8A7144
SHA-256:	42680AB2F2AAA9DC14E3C165DDFE5D862285D551902CA74BA61C35EBFCFB7E3C
SHA-512:	268F3DAACAF22384EFEDE6A258457571C7B73A05DDCAF17C2316B9F8529C0FBBBBCF5BED0F72FB645FD539E606787EBDFBEC29433408C47466D811FEEF003A3E
Malicious:	false
Reputation:	low
Preview:	2021/04/08-11:20:30.161 17d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/04/08-11:20:30.163 17d8 Recovering log #3.2021/04/08-11:20:30.164 17d8 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):	1.0555608592510275
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUcdarInh+Eh00N:wIElwQF8mpcSgdPgEhdNplkm0w/
MD5:	B202BF2697B55BE33C45883CD9E319CB
SHA1:	11A5F387430DF89C02C63E643A9CBA673DF2FF5F
SHA-256:	41A5171146662EC65E89D5143ABCCC28540953CC444CAC9D500A70BBE399E710
SHA-512:	2CBF7FDFC414FF4AD5DBC11826AE145AEA4102EC55A70D64F1AC85C1EAA7A1DD9773B2049AA87C1237B3D82DCEF10F2FCEB16B516D5B139951B5571684391A65
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):	0.627424384060703
Encrypted:	false
SSDEEP:	48:VdTWKPUueRqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUTz4:VdiKPUueRhIElwQF8mpcSM
MD5:	E065CC0978BD3815BEB66CD511B0AE71
SHA1:	4605884E3323C5882B592EA93A85D9A76634269F
SHA-256:	BB0483FB2C72C9CAE3B0E7009669994E7265FA5C9E8327145D2097F1A7F0658C
SHA-512:	FD832902DA779664642C0A9AA6B4DBC905E8C0163E9388544CF990EC834F8B4E9521DDCD6B60DD1E7E3ABDBCEBDA33342946D1A54FD828C39AD6C887E4BA659
Malicious:	false
Reputation:	low
Preview:	.....Yw[c..... ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.174531347961571
Encrypted:	false
SSDEEP:	6:m1zoWIIq2PWXp+N23iKKdKrQMxIFUtpkzoWqZmwPkzoWZ7kwOWXp+N23iKKdKrQq:WotIva5KkCFUtpGoJ/PGog5f5KktJ
MD5:	A20EF152313910202690CD1AF320694A
SHA1:	B08FD611A2D7ACDD28708C1EC7BCEB83E4A08C5C
SHA-256:	B65D52B76177A34E51E717583E2D83298F434227C2708137826EB379E7435386
SHA-512:	5FE28E5C0590139BB7AC603185CDAC13AFB09B121F39774C5A7D51DB93E2A645111AC547781A71C5C3936BB4D050754D0886902D9F07C09A0AEC4256BE98401
Malicious:	false
Reputation:	low
Preview:	2021/04/08-11:20:29.934 980 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/04/08-11:20:29.936 980 Recovering log #3.2021/04/08-11:20:29.937 980 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.202485734259925
Encrypted:	false
SSDEEP:	6:m1zZ3+q2PWXp+N23iKKdK7Uh2ghZIFUtpkzMMZmwPkzZQd3VkwOWXp+N23iKKdKs:WUva5KkIhHh2FUtpGMM/PGZQT5f5KkIT
MD5:	DF42C9C97FD36E073FA8BF78EF9069A2
SHA1:	8CA86682F4EED7DBF54BD2903706A6515117E3F0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
SHA-256:	99A31509FAF889BE2E62778003ADD65BCF5B6FDBD5761AC1ACB7786408B93890
SHA-512:	981A5D99DBBBAA5D6C8F587DAA6A62C80E703CE41F4D0B6B8927DE828FB3B3846CDE46123D575D6109758D849D0AFE1B0060A9ACD0B8FE8B5592E664A4C5FE C8
Malicious:	false
Reputation:	low
Preview:	2021/04/08-11:20:29.685 1358 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/04/08-11:20:29.690 1358 Recovering log #3.2021/04/08-11:20:29.693 1358 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site C haracteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\468071a4-6c7d-4327-9229-b9c7ff9 f8d37.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.223204790356719
Encrypted:	false
SSDEEP:	6:m1TAq2PWXp+N23iKKdKusNpV/2jMGIFUtpk4ZmwPk17kwOWXp+N23iKKdKusNpV0:4Ava5KkFFUtp5/PS5f5KkOJ
MD5:	874E73553A1CA8193704DC1B9937BEF7
SHA1:	2CEED42D05DD13932389073AD2DA305227AC526E
SHA-256:	8BA010753ABB5BEB6F59C9E2974B3DC543C0F41072AA0D46FA35353530F168F5
SHA-512:	9AD2F1A915BDB9207A63CA435432875B73DAC8196E490C9A3A821DC16605EC0635C0420F277BFB7B0ECD62E1F5BF214D3E053A214E1B50855B5906B2C32FEF0
Malicious:	false
Reputation:	low
Preview:	2021/04/08-11:20:30.010 980 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Local Storage\leveldb/MANIFEST-000001.2021/04/08-11:20:30.015 980 Recovering log #3.2021/04/08-11:20:30.016 980 Reusing old log C:\Users\user\AppD ata\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):	432
Entropy (8bit):	5.259215583469287
Encrypted:	false
SSDEEP:	6:m12k+q2PWXp+N23iKKdKusNpqz4rRIFUtpkH5ZmwPknwd3VkwOWXp+N23iKKdKua:Fva5KkmiuFUtpC5/PKwT5f5Kkm2J
MD5:	23DE682A439F8BF8F5CFD823FAC46BA9
SHA1:	337FF044B6EA7B79797ECCA1EECC97DC29F16B0A
SHA-256:	A24A94C487ECC9DAB2F32E5A17BA5764094B8F1DC2DA06384351FB868D1C86CC
SHA-512:	74498BFA3EAA4195BB55D968B54412B8EDEFF142E3339430B924C902B61C84A2B02EFD3C726F26B6E540E94C17446019305D2B1C51023CF020904C686BF41742
Malicious:	false
Reputation:	low
Preview:	2021/04/08-11:20:30.141 17f8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/04/08-11:20:30.143 17f8 Recovering log #3.2021/04/08-11:20:30.148 17f8 Reusing old log C:\Users\user\AppData\Lo cal\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):	418
Entropy (8bit):	5.30019108913512
Encrypted:	false
SSDEEP:	6:m1bLRN+q2PWXp+N23iKKdKusNpZQMxIFUtpkmRZZmwPk9VkwOWXp+N23iKKdKusx:sVIva5KkMFUtp/Z/Pe5f5KkTJ
MD5:	C6F45AF3756CA8BD9F09AD6BB7FF6E87
SHA1:	C4AF8BC5C78C1CAAD736023DB79C9C89ED979270
SHA-256:	D29684C9AA5BE1C9F2266DF1BCDDB24B8380993D37D4F20096B06B974F5561FE
SHA-512:	3DC29918B52B60FAAF7044F2509483FF88B250AF1A8B960AAB8B91043AA12022955028A9635B61E6C8067A4BDE90FD91F89FB7A8D07547BEA4DBF707285C4DE2
Malicious:	false
Reputation:	low
Preview:	2021/04/08-11:20:46.386 17d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2021/04/08-11:20:46.396 17d8 Recovering log #3.2021/04/08-11:20:46.397 17d8 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\85f45a16-0382-45af-b147-50395de217b0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\85f45a16-0382-45af-b147-50395de217b0.tmp

Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Reputation:	low
Preview:	.'..(.....

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.178815118332448
Encrypted:	false
SSDEEP:	12:4Iva5KkkGHArBFUtpG/PH5f5KkkGHAryJ:la5KkkGgPgcf5KkkGga
MD5:	42332A960E81EB423BEE639B036E22A9
SHA1:	2BA073249E28AFD6AB1A985EEFDAF04CAE4451FE
SHA-256:	5CB1AA49D7D7C41851B3249427AEBA9BAB447505358D3528F3685E4C691B5281
SHA-512:	87D663696D4262C3638F1B94239DD248C7DA98A10A2D0C688F3507116618514691041956 2C974541205FD75CE4BAFDFFFA7CA158AB909D1623E3A8E75E9B6536
Malicious:	false
Reputation:	low
Preview:	2021/04/08-11:20:42.826 980 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/04/08-11:20:42.828 980 Recovering log #3.2021/04/08-11:20:42.841 980 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):	429
Entropy (8bit):	5.2095478429062
Encrypted:	false
SSDEEP:	12:3M+va5KkkGHArqiuFUtpQ/PdMV5f5KkkGHArq2J:ta5KkkGgCgbf5KkkGg7
MD5:	EC31F819CF7F1B3E0D0ACCB8C181756F
SHA1:	289E29FF7FE4D57CABF9DB0C504F4E8D026ECB63
SHA-256:	FEA23EAA2AD6F430AA444B7D8F7C7454D9CEE039C36AA4FA013B84347E80F012
SHA-512:	1BF3963FA4EA9793361D767B674CD19381DF2D3801BEF3D6828D0FEA9ABB27E2FF83C68CF4E6DA00CCAA3F61F9FC8D82DD0FA6E6C1E99D97ED80C22EED25061
Malicious:	false
Reputation:	low
Preview:	2021/04/08-11:20:42.849 5fc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/04/08-11:20:42.852 5fc Recovering log #3.2021/04/08-11:20:42.854 5fc 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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.18742980432146
Encrypted:	false
SSDEEP:	12:YUM+va5KkkGHArAFUtpojm/PoKMV5f5KkkGHArfJ:ra5KkkGgkgshf5KkkGgV
MD5:	69A1699FF5687438E93EC993912B64F7
SHA1:	7580E44BD3F4EAEBE70DE3432BAC95DCBEACCDA5
SHA-256:	9E535B74725AC7C05F40042B2D960DC1A1C2B2D40D0F08FE751C4C4BECA04E3E
SHA-512:	9A6DC1813AEB685C70A704D002A8EA4B8EBB89766D3CC20D5073428162B3BEEAD616460514E6A91B48794BF53C646B5E2CB1CFB19811F203F2AF61526E57160
Malicious:	false
Reputation:	low
Preview:	2021/04/08-11:20:58.451 5fc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Session Storage/MANIFEST-000001.2021/04/08-11:20:58.452 5fc Recovering log #3.2021/04/08-11:20:58.453 5fc Reusing old log C:\Users\user\AppData\Lo cal\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	321
Entropy (8bit):	5.274781075348819
Encrypted:	false
SSDEEP:	6:m1zMO+q2PWXp+N23iKKdKpIFUtpkzOZmwPkzmOVkwOWXp+N23iKKdKa/WLJ:WMO+va5KkmFUtpGO/PGJV5f5KkaUJ
MD5:	33316B963400FE4D71FF23599D11DF3D
SHA1:	1B2E1F28AC8D56F6C11B800321475A0D9D00D32B
SHA-256:	8CF9AE1360AF4A3F3A5004B14D26D21ACEBC074B4AD070313166C9F3BBAA23D1
SHA-512:	4073D7EA3DC3E527CB07E3DF4C65DD21D61E8DEBD4B21AC2619FED334FE25E65DC48E6C8344ED7AF7ADB97D7D52AB4F1E4AC5733CD92CD0BA462D589C87 C1DF
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Reputation:	low
Preview:	2021/04/08-11:20:29.690 6bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/04/08-11:20:29.695 6bc Recovering log #3.2021/04/08-11:20:29.696 6bc 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):	399
Entropy (8bit):	5.35215784306748
Encrypted:	false
SSDEEP:	12:wM+va5KkkOrsFUtpiX/PPqMV5f5KkkOrzJ:+a5Kk+gcXf5Kkn
MD5:	0095B96E1F4F1777FE6FE350B415CD43
SHA1:	146BF07DE0B1DA988C9BBDE6ACD0008AE4CB9017
SHA-256:	5F715A72183BE1CB0A329F6A8E4CD330F37DF05651152B879FA696FA92A06C6F
SHA-512:	33BA40DEDF7DCB4C374C9C7BD572B267CCCE242C6768FE184EA3659CEC5A06B0DBE1E7830AE19BBA3581501ADCD651FF4987FAEACC2772B1FCD52B7B628499A
Malicious:	false
Reputation:	low
Preview:	2021/04/08-11:20:46.527 5fc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/04/08-11:20:46.528 5fc Recovering log #3.2021/04/08-11:20:46.529 5fc 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):	4.1916116417513765
Encrypted:	false
SSDEEP:	3:WyZ9FfE17nB/yWn:T3cb/F
MD5:	A33F2291FA3003BD0D68CE97EEBF1C65
SHA1:	8594D398DB6A223455FC7EF1312462E746766F44
SHA-256:	76AD4152752ED3110A9BF91AE6FA6C3F3CE9E2F54FAAF6D71BC6D45BACECA7C9
SHA-512:	4498F77B97C382EE7F6FD32A0BDF1CA7A1F89740AD71E79D84839D2C367B0341E1F93E6CDE2DD2CBE245FE25C4EDDCC68B6530BBAFF4A00B5742CADD84F8F4D
Malicious:	false
Reputation:	low
Preview:	.....X<.D*.....=..... .G2...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\58d2f1e6-f91a-4b6b-9041-6bebaadf3f4a.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.....nnp}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\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\Chrome Web Store Payments.ico.md5	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\Chrome Web Store Payments.ico.md5	
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\a8c9cf94-5609-4a4e-84ad-1bc3f5cd5906.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):	5.003572220720071
Encrypted:	false
SSDEEP:	96:nv9aGXfpcVZok0JCMRWL8wkG1lbOTQVuwn:nvlfpc+4MYZkGH
MD5:	05D8E26C9EAFABDE87181FF96C34AC46
SHA1:	CC218443ADD7EC6D4505D4DD39501376A1E6F009
SHA-256:	564C5B45DE0CA29368773B4ED37AF6C0830FEFFF33550388A5E021CBF3B499E5
SHA-512:	65C49E439767829DB5C9080800840D9C50119D9390C16CB248D920F45178C987DAC2A6AD6974995667D33DFF899E288087616176239BE707DBC05CFA2A3A87EB
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13262379630062876","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ad127bc6-da92-4f19-a79a-8271871a884a.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\bcda333a-3634-4e53-9325-446d3825989c.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):	5.5358428426172654
Encrypted:	false
SSDEEP:	384:yoRVtDLlxeXG1kXqKf/pUZNCgVLH2HfDOrU+HGInTYYRc4H:dlLl+G1kXqKf/pUZNCgVLH2HfqrUuGIr
MD5:	4588954CFD7A6574AAC2F6F2FD3CB586
SHA1:	AC82BD334E82C38B2F28507BDACFD123542A97AC

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bcda333a-3634-4e53-9325-446d3825989c.tmp	
SHA-256:	A09C3B02B139A0447AA47B56B756EE3DAB83FA71D7D047CF72C9F637C4F38005
SHA-512:	B2D2C99894E3DB13E69D45674854FB0B33D2D5CC8AD6416E4F8728C232F5FBA233D26C057A46F8B166E18DD04542C4E504A0A9EBF29A381E912A12EAA9FCB7 B
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.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":"13262379629691889","location":5,"manifest":{"a pp":{"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":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c4bb5421-f840-49fd-bc08-9acb16fb6a5d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1039
Entropy (8bit):	5.56287653825673
Encrypted:	false
SSDEEP:	24:YI6H0UhVsTG1KUerkq/HeUeXby2qUeXvb7wUehURUenHQ:YI6UUhVseKUewqPeUer2Uef3wUEYUenw
MD5:	5ACD8A10C29DC19D8C8A9687E249D04B
SHA1:	92907FE323A23A2970D8FFEB60804A9FB20E7F7A
SHA-256:	D9512B06B10902F9529FEF187EE1FDCE8A3ED987007B4F679281A59A1329A592
SHA-512:	FBA886B57F1435D70841BAC6A2D1810EE80CDD06996E22D1D1BC24C70B26DC967B33BDD4743D462A66F8607C5E93C6EB44CE00ED696B76759447453EB53047E
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains" :true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_inc lude_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mo de":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+ 6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1649442032.786137,"host":"8/RrMmQlCD2Gsp 14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617906032.786141},{"expiry":1633014077.462534,"hos t":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.475177892103404
Encrypted:	false
SSDEEP:	3:tUKO3IUshajkyZmwv3s3IUshOkRA0V8ss3IUshOkRA0WGv:m1fZmwPkqhVvkqhtv
MD5:	2123D1A5CFBE0631FD4E9ECC2FC96B6F
SHA1:	36D401ACD0FFCD9B076EACCF96B1FA49364339BD
SHA-256:	12A8D6E6BEDAA69EA6C88629FB072A69FA871DF2BDF29E5E8DE79E1C10CD0CBE
SHA-512:	690073C0997FCE7203F21DC6D6A012D7975C7208A7D8006E865FF929F49D02D2D9B49C0E5BC5F26B83FF196C0E6C7829E82854E9DE14C7EFB0DE09C42C9C26C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Preview:	2021/04/08-11:20:42.014 1ba4 Recovering log #3.2021/04/08-11:20:42.057 1ba4 Delete type=0 #3.2021/04/08-11:20:42.057 1ba4 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/vxQRDKlVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF04
Malicious:	false
Reputation:	low
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.181522775782021
Encrypted:	false
SSDEEP:	6:m1lELL+q2PWXp+N23iKKdKfrzAdIFUtpklXZmwPklqHVkwOWXp+N23iKKdKfrzId:oVva5Kk9FUtp4X/P4q15f5Kk2J
MD5:	5F75813C4DEC10F4AF7CF03F7CB06B56
SHA1:	3582BF62DE32FD9E5A989401C3BBB4E4B360262E
SHA-256:	1022EAFC572AB3134C58CEAEF00C2C29AF435CA886D4D6D0FDD9248254DD99E4
SHA-512:	5EFBEA5F24BB54F898F38535CDF4C7EE5B946C678A68A420D526E5B080387209ED0E3E11A11802B84460FF8846C21BC854ECB0A299D36C262777C5C63E16DD8
Malicious:	false
Reputation:	low
Preview:	2021/04/08-11:20:42.510 17d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/04/08-11:20:42.511 17d8 Recovering log #3.2021/04/08-11:20:42.512 17d8 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:tblolIrJ5ldQxl7aXVdJiG6R0RlAl: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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
SHA1:	AAD27C14B27F56B6E7C744A8EC5B1A7D767D7632
SHA-256:	02E71EB4C587FEB7EE00CE8600F97411C2774C2FC34CB95B92D5538E7F30DA59
SHA-512:	86010ED2B2EEBDCC5A8A076B37703669C294C6D1BFAAEA963E26A9C94B81B4C53EC765D9425E5B616159C43923F800A891F9B903659575DF02F8845521F8DC4(
Malicious:	false
Reputation:	low
Preview:	85.0.4183.121

C:\Users\user\AppData\Local\Google\Chrome\User Data\a661ec3e-2e2b-4b14-a3a9-33ed435d4b70.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7455091809483614
Encrypted:	false
SSDEEP:	384:TzAvDhS81xGTiNLrgvnd3Af14HhoGsrrmxvTxgVtlMrWXmWhy9jPDAONNPNi17aO:sKVlWpMshOe/7R50nrCZKfxDdM
MD5:	7A92C340E94CAF9C89DEA6E266175471
SHA1:	4D72B045D02EC5AA00C3836C321FE663D792B08F
SHA-256:	F32EE026305C66C7AF60BBA3C8AE9A233091BB297476E5755DB5377B7A735612
SHA-512:	2F2506388923675D3126CDFBAABAE82473C849288774C8819D7A87592582A309334FFBFE9523C06234C294147F87ED56CF5C1A59A611E01D6E4DB3111B1BC1D0
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\bcec266e-9864-43a9-92cf-1caed5c6f418.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):	164083
Entropy (8bit):	6.08190088150875
Encrypted:	false
SSDEEP:	3072:BNjzmnDWVhPFlyU7sCXgcbjH1FcbXafIB0u1GOJmA3iuR9:Xv6Q1sJQHDaqfIlUOoSiuR9
MD5:	EFC1D243D6C77091E007259D3BC97435
SHA1:	64CEA94028C443DBC1ADD2D0D828D0FE2774D39B
SHA-256:	E95EF9688E1EBFB15EB5E64AA2A4983BFFC496D8DAE0FA307E77DDE8A3F99E0B
SHA-512:	351CFD1F0C525C98A657060260BF19E25B91F93C51D8C45C61EBB31BB20A41E274A130F46C9A63FFC029A7DB738B70F7D1BCC3277B6EE66A87658A99467DC68
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":1.617906032849408e+12,"network":1.617873635e+12,"ticks":102873649.0,"uncertainty":4388577.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\058afb24-1d34-4f97-9ad2-ba45e66f9ad5.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:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326088
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\058afb24-1d34-4f97-9ad2-ba45e66f9ad5.tmp	
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...I5....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."I...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\5e148e82-d98e-440d-8e04-e9ca27f470a5.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\66f5417e-7261-43aa-a893-b0e0ec64211c.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\a98c1461-7371-4b8f-9438-8e4a0b6c4795.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...I5....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."I...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\c1df0f8a-ad9f-4ecd-afd2-6612a1ddbc41.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped

C:\Users\user\AppData\Local\Temp\c1df0f8a-ad9f-4ecd-afd2-6612a1ddbc41.tmp	
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\d04c78e9-9629-48f0-8ee5-3cf3c773e75c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;.._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&..._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U .KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....I-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F ....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\scoped_dir3880_153020419\058afb24-1d34-4f97-9ad2-ba45e66f9ad5.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\scoped_dir3880_153020419\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

C:\Users\user\AppData\Local\Temp\scoped_dir3880_153020419\CRX_INSTALL_locales\bg\messages.json	
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_dir3880_153020419\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": "Connecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3880_153020419\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D84885B
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_dir3880_153020419\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:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C53E0A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir3880_153020419\CRX_INSTALL_locales\da\messages.json	
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_dir3880_153020419\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB80552
Malicious:	false
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_dir3880_153020419\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
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": ". ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": ".. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3880_153020419\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_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3880_153020419\CRX_INSTALL_locales\en_GB\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\scoped_dir3880_153020419\CRX_INSTALL_locales\en_GB\messages.json	
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_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3880_153020419\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_dir3880_153020419\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_dir3880_153020419\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

C:\Users\user\AppData\Local\Temp\scoped_dir3880_153020419\CRX_INSTALL_locales\et\messages.json	
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_unavail able": {.. "message": "Rakendus pole praegu saadaval.".. },.. "craw_connect_to_network": {.. "message": "Looge .hendus v.rguga.".. },.. "iap_unavailable": {.. "message": "Rakendusesisesed maksed ei ole praegu saadaval.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logige Chrome'i sisse.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3880_153020419\CRX_INSTALL_locales\fi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.595421267152647
Encrypted:	false
SSDEEP:	12:1HEJRuzGGRuz+WYpU34ujSBu+dgYO8ZpU34J+Bu03OyZnLAOfTY5HN:1HEFcWYpPNa8ZpD+FOGAOfEHN
MD5:	3A01FEE829445C482D1721FF63153D16
SHA1:	F3EAAADDC03F943FC88B30B67F534AA13E3336DD
SHA-256:	0BDE54B20845124113383B6EB81E43A0F05E4EB0C44BEE3C1DFAC4CC5FEC2836
SHA-512:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BEA D8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Storen maksut".. },.. "app_name": {.. "message": "Chrome Web Storen maksut".. },.. "craw_app_unavail able": {.. "message": "Sovellus ei ole t.ll. hetkell. k.ytett.viss..".. },.. "craw_connect_to_network": {.. "message": "Muodosta verkkoyhteys.".. },.. "iap_unavai lable": {.. "message": "Sovelluksen sis.iset maksut eiv.t ole t.ll. hetkell. k.ytett.viss..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Kirjaudu sis..n Chromeen.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3880_153020419\CRX_INSTALL_locales\fil\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	658
Entropy (8bit):	4.5231229502550745
Encrypted:	false
SSDEEP:	12:1HEJADlbGGADlb+WYpU34hTUT+dgHfZAFFZO8ZpU34hTjzeT03OyZnLAOfTYHfvF:1HEYah6WYp7TUSoxOS8Zp7TOsOGAOfqV
MD5:	57AF5B654270A945BDA8053A83353A06
SHA1:	EEEF7A4F869F97CF471A05D345E74F982D15E167
SHA-256:	EC002ED92359F67818B49455DFC579E140368E6A004080AF022FD4F57F6B03F2
SHA-512:	5F0AE839FCF3F4EA48FF41A76655AE0F3821564AFD5D42FBB9FBB9A38E8D8F7BB5E9B6F71064588CD441261F644095A44A755C134CE546D506D9A21E488BAF52
Malicious:	false
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_dir3880_153020419\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

C:\Users\user\AppData\Local\Temp\scoped_dir3880_153020419\CRX_INSTALL_locales\fr\messages.json	
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_dir3880_153020419\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": {.. "messa ge": "..... .. ..".. },.. "craw_connect_to_network": {.. "message": "..... ....".. },.. "iap_unavailable": {.. "message": "..-.. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... Chrome ... .".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3880_153020419\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
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_dir3880_153020419\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_dir3880_153020419\CRX_INSTALL_locales\id\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators

C:\Users\user\AppData\Local\Temp\scoped_dir3880_153020419\CRX_INSTALL_locales\id\messages.json	
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:	970FEC9A9EF0BAF7F693C4C5977F3B47914579C5B5414FCE9DBB5E4574659A5BB9AD2DE0CC886B368F49C019785AF7D2D7FE82F71341F039EADC399ED776CA2
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pembayaran Chrome Webstore".. },.. "app_name": {.. "message": "Pembayaran Chrome Webstore".. },.. "craw_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 completed.".. },.. "please_sign_in": {.. "message": "Harap masuk ke Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3880_153020419\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_unavailable": {.. "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_dir3880_153020419\CRX_INSTALL_locales\ja\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	697
Entropy (8bit):	5.20469020877498
Encrypted:	false
SSDEEP:	12:1HEJ07uGG07u+WYpU34DB+dgnsVztO8ZpU34MwiB03OyZnLAOfTYmSH:1HEcnDNWYp1kxU8Zp2wiqOGAOfpSH
MD5:	9B3A5D473C3F2BBFAEECE94A07A940B8
SHA1:	61BACA342CF766BBA15C7B4D892A0E7DAC9405AA
SHA-256:	706312A4A2AEF3317223F141EB2B82685345B7EED444F16BB4DF3A272716DA1F
SHA-512:	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_dir3880_153020419\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

C:\Users\user\AppData\Local\Temp\scoped_dir3880_153020419\CRX_INSTALL_locales\ko\messages.json	
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_dir3880_153020419\CRX_INSTALL_locales\lt\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	665
Entropy (8bit):	4.66839186029557
Encrypted:	false
SSDEEP:	12:1HEJpqHnkGGpqHnk+WYpU346M+dgV6O8ZpU34WzSWz03OyZnLAOfTYx:1HELqHtKqHPWYpM3A8ZpwGzOGAOfg
MD5:	4CA644F875606986A9898D04BDAE3EA5
SHA1:	722A10569E93975129D67FBDB75B537D9D622AD1
SHA-256:	7C311AB751D840D750C11553C083785813E079C1D464FE568A98C9E3EF3DB96C
SHA-512:	E575E3D0622F5BD4B6C0EE79128A1B1F1882195670139D1983F4377D847141B8FB8EBB8BCED82AF3A220ED07D3577AFBE085BADC0E9C7678292B80E3EC5D344 4
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_dir3880_153020419\CRX_INSTALL_locales\lv\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	671
Entropy (8bit):	4.631774066483956
Encrypted:	false
SSDEEP:	12:1HEJFhVbGGFhVb+WYpU34wDoz+dgGedBO8ZpU34wF03OyZnLAOfTYGYID:1HENQkkWYp2Doy/em8Zp2WOGAOfRYID
MD5:	C5CE2C51391EAFD3DA9E4C71549A3C28
SHA1:	1F67FF6EF6E90C0CE3AAF56ED543A3EFD381574D
SHA-256:	1FA1DF2CA8516DEF490FB8484E9AA498ACFF80EEF5C9258FFE42D3678E6C7DED
SHA-512:	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.".. }..}..

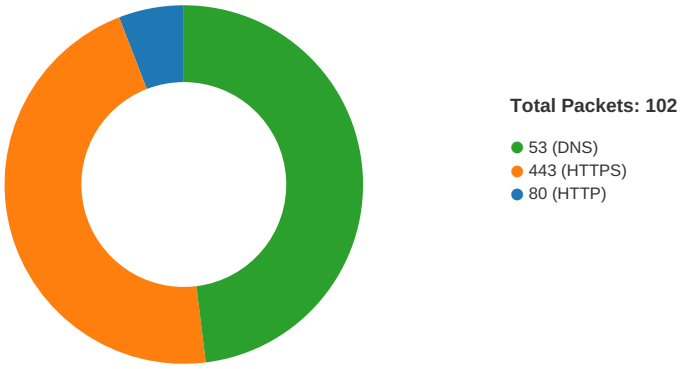
C:\Users\user\AppData\Local\Temp\scoped_dir3880_153020419\CRX_INSTALL_locales\nb\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.555032032637389
Encrypted:	false
SSDEEP:	12:1HEJhiOGGhiO+WYpU34OHSN+dgFjdGFZO8ZpU34JgdN03OyZnLAOfTYiD:1HEDiHIitWYpCYJ8ZpD1OGAOfRD
MD5:	93C459A23BC6953FF744C35920CD2AF9
SHA1:	162F884972103A08ADB616A7EB3598431A2924C5
SHA-256:	2CD700AEB57D89C2E73333D0702556EE3FF3863516170F85669BC680FCBDC4E0
SHA-512:	F76E6E8D8499306883C3EC1E774F7E8BB6B601096DA5A14D17D3E7D5732829542041E42B7350466589291ADCC83FB065FD591B4E20CFCF8EDC586E128ECBFCB
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Nettmarked-betalinger".. },.. "app_name": {.. "message": "Chrome Nettmarked-betalinger".. },.. "craw_app _unavailable": {.. "message": "Appen er utilgjengelig for .yeblikket.".. },.. "craw_connect_to_network": {.. "message": "Du m. koble til et nettverk.".. },.. "iap _unavailable": {.. "message": "Betaling i app er ikke tilgjengelig for .yeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Du m. logge p. 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 11:20:33.393758059 CEST	49708	80	192.168.2.3	198.54.125.197
Apr 8, 2021 11:20:33.394737959 CEST	49709	80	192.168.2.3	198.54.125.197
Apr 8, 2021 11:20:33.570023060 CEST	80	49708	198.54.125.197	192.168.2.3
Apr 8, 2021 11:20:33.570197105 CEST	49708	80	192.168.2.3	198.54.125.197
Apr 8, 2021 11:20:33.570883989 CEST	49708	80	192.168.2.3	198.54.125.197
Apr 8, 2021 11:20:33.573200941 CEST	80	49709	198.54.125.197	192.168.2.3
Apr 8, 2021 11:20:33.573311090 CEST	49709	80	192.168.2.3	198.54.125.197
Apr 8, 2021 11:20:33.758481979 CEST	80	49708	198.54.125.197	192.168.2.3
Apr 8, 2021 11:20:33.801014900 CEST	49708	80	192.168.2.3	198.54.125.197
Apr 8, 2021 11:20:34.272145987 CEST	49714	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.272888899 CEST	49715	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.384103060 CEST	49716	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.423773050 CEST	443	49714	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:34.423897028 CEST	49714	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.424190998 CEST	49714	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.426229954 CEST	443	49715	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:34.426342964 CEST	49715	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.426542044 CEST	49715	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.534548044 CEST	443	49716	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:34.534679890 CEST	49716	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.534895897 CEST	49716	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.575977087 CEST	443	49714	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:34.577807903 CEST	443	49714	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:34.577840090 CEST	443	49714	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:34.577858925 CEST	443	49714	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:34.577944040 CEST	49714	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.580189943 CEST	443	49715	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:34.581778049 CEST	443	49715	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:34.581835985 CEST	443	49715	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:34.581857920 CEST	443	49715	216.172.172.184	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:20:34.581890106 CEST	49715	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.588867903 CEST	49714	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.589483023 CEST	49715	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.589550018 CEST	49715	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.589688063 CEST	49714	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.590073109 CEST	49714	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.684942007 CEST	443	49716	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:34.688028097 CEST	443	49716	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:34.688066959 CEST	443	49716	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:34.688091040 CEST	443	49716	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:34.688157082 CEST	49716	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.690196037 CEST	49716	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.741275072 CEST	443	49714	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:34.741317034 CEST	443	49714	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:34.741333961 CEST	443	49714	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:34.741445065 CEST	49714	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.741686106 CEST	49714	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.743496895 CEST	443	49715	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:34.743532896 CEST	443	49715	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:34.743547916 CEST	443	49715	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:34.743565083 CEST	443	49715	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:34.743580103 CEST	443	49715	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:34.743594885 CEST	443	49715	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:34.743669033 CEST	49715	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.743695021 CEST	49715	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.743700027 CEST	49715	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.743704081 CEST	49715	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.743706942 CEST	49715	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.841516972 CEST	443	49716	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:34.841540098 CEST	443	49716	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:34.841630936 CEST	49716	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.841809988 CEST	443	49716	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:34.899703979 CEST	49716	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:34.933681965 CEST	443	49714	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:35.436806917 CEST	443	49714	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:35.499727011 CEST	49714	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:35.587634087 CEST	49714	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:35.587831974 CEST	49714	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:35.588397026 CEST	49714	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:35.739187956 CEST	443	49714	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:35.739224911 CEST	443	49714	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:35.739797115 CEST	443	49714	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:35.786106110 CEST	443	49714	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:35.788564920 CEST	49714	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:35.940294981 CEST	443	49714	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:35.980287075 CEST	443	49714	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:36.056832075 CEST	443	49714	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:36.056866884 CEST	443	49714	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:36.056885958 CEST	443	49714	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:36.056907892 CEST	443	49714	216.172.172.184	192.168.2.3
Apr 8, 2021 11:20:36.056950092 CEST	49714	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:36.057044983 CEST	49714	443	192.168.2.3	216.172.172.184
Apr 8, 2021 11:20:36.246154070 CEST	49723	443	192.168.2.3	152.199.23.37
Apr 8, 2021 11:20:36.246382952 CEST	49724	443	192.168.2.3	152.199.23.37
Apr 8, 2021 11:20:36.246577024 CEST	49725	443	192.168.2.3	152.199.23.37
Apr 8, 2021 11:20:36.246819019 CEST	49726	443	192.168.2.3	152.199.23.37
Apr 8, 2021 11:20:36.247015953 CEST	49727	443	192.168.2.3	152.199.23.37
Apr 8, 2021 11:20:36.262017965 CEST	443	49723	152.199.23.37	192.168.2.3
Apr 8, 2021 11:20:36.262037039 CEST	443	49724	152.199.23.37	192.168.2.3
Apr 8, 2021 11:20:36.262119055 CEST	49723	443	192.168.2.3	152.199.23.37
Apr 8, 2021 11:20:36.262181044 CEST	443	49725	152.199.23.37	192.168.2.3
Apr 8, 2021 11:20:36.262181044 CEST	49724	443	192.168.2.3	152.199.23.37
Apr 8, 2021 11:20:36.262237072 CEST	49725	443	192.168.2.3	152.199.23.37
Apr 8, 2021 11:20:36.262373924 CEST	443	49726	152.199.23.37	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:20:36.262432098 CEST	49726	443	192.168.2.3	152.199.23.37
Apr 8, 2021 11:20:36.262527943 CEST	49724	443	192.168.2.3	152.199.23.37
Apr 8, 2021 11:20:36.262675047 CEST	49723	443	192.168.2.3	152.199.23.37
Apr 8, 2021 11:20:36.262712002 CEST	443	49727	152.199.23.37	192.168.2.3
Apr 8, 2021 11:20:36.262795925 CEST	49727	443	192.168.2.3	152.199.23.37
Apr 8, 2021 11:20:36.271574974 CEST	49727	443	192.168.2.3	152.199.23.37

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:20:23.372920990 CEST	50200	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:23.386472940 CEST	53	50200	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:24.330821037 CEST	51281	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:24.342787981 CEST	53	51281	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:24.602919102 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:24.621597052 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:25.135086060 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:25.151684046 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:26.232714891 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:26.245177031 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:27.245193958 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:27.258599997 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:33.336036921 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:33.338639021 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:33.344980001 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:33.347255945 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:33.348942995 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:33.351443052 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:33.370915890 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:33.389619112 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:33.694089890 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:33.720360994 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:33.878108025 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:33.963407040 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:34.002963066 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:34.053175926 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:34.065917015 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:34.250344992 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:35.176168919 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:35.189506054 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:35.515640974 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:35.528085947 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:36.116722107 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:36.117250919 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:36.129431009 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:36.129769087 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:37.294926882 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:37.327389002 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:37.510026932 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:37.530810118 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:37.664526939 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:37.677284956 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:37.868446112 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:37.881135941 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:38.119339943 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:38.151180983 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:38.174393892 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:38.187623978 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:38.307770967 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:38.319472075 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:39.295207977 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:39.308463097 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:42.741408110 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:42.754106998 CEST	53	63619	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:20:43.144439936 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:43.172544003 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:43.382411003 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:43.409805059 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:43.690917969 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:43.704420090 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:44.707160950 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:44.719574928 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:45.107276917 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:45.134002924 CEST	53	56130	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:47.170170069 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:47.183201075 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:49.833765030 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:49.847006083 CEST	53	56338	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:53.993618965 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:54.005877972 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:54.870512009 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:54.884521961 CEST	53	58784	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:55.317934036 CEST	63978	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:55.336138964 CEST	53	63978	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:59.066013098 CEST	62938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:59.079195023 CEST	53	62938	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:59.771923065 CEST	55708	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:59.785036087 CEST	53	55708	8.8.8.8	192.168.2.3
Apr 8, 2021 11:20:59.834450960 CEST	56803	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:20:59.848030090 CEST	53	56803	8.8.8.8	192.168.2.3
Apr 8, 2021 11:21:00.504086971 CEST	57145	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:21:00.516870022 CEST	53	57145	8.8.8.8	192.168.2.3
Apr 8, 2021 11:21:01.585365057 CEST	55359	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:21:01.597893953 CEST	53	55359	8.8.8.8	192.168.2.3
Apr 8, 2021 11:21:02.397959948 CEST	58306	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:21:02.411312103 CEST	53	58306	8.8.8.8	192.168.2.3
Apr 8, 2021 11:21:05.829193115 CEST	64124	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:21:05.841218948 CEST	53	64124	8.8.8.8	192.168.2.3
Apr 8, 2021 11:21:16.058331013 CEST	49361	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:21:16.077107906 CEST	53	49361	8.8.8.8	192.168.2.3
Apr 8, 2021 11:21:16.097151995 CEST	63150	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:21:16.115044117 CEST	53	63150	8.8.8.8	192.168.2.3
Apr 8, 2021 11:21:31.072396994 CEST	53279	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:21:31.085889101 CEST	53	53279	8.8.8.8	192.168.2.3
Apr 8, 2021 11:21:31.599123001 CEST	53642	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:21:31.611998081 CEST	53	53642	8.8.8.8	192.168.2.3
Apr 8, 2021 11:21:32.165148020 CEST	55667	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:21:32.177798986 CEST	53	55667	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 11:20:33.347255945 CEST	192.168.2.3	8.8.8.8	0x575f	Standard query (0)	www.ztzusl.vibz.co.uk	A (IP address)	IN (0x0001)
Apr 8, 2021 11:20:33.878108025 CEST	192.168.2.3	8.8.8.8	0xba74	Standard query (0)	jrschnell.com.br	A (IP address)	IN (0x0001)
Apr 8, 2021 11:20:36.116722107 CEST	192.168.2.3	8.8.8.8	0xbf7e	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
Apr 8, 2021 11:20:36.117250919 CEST	192.168.2.3	8.8.8.8	0xb179	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Apr 8, 2021 11:20:37.294926882 CEST	192.168.2.3	8.8.8.8	0x8ca4	Standard query (0)	cdn.clipart.email	A (IP address)	IN (0x0001)
Apr 8, 2021 11:20:37.510026932 CEST	192.168.2.3	8.8.8.8	0x6e11	Standard query (0)	clipartkind.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:20:37.664526939 CEST	192.168.2.3	8.8.8.8	0x296e	Standard query (0)	a.nel.cloudflare.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:20:37.868446112 CEST	192.168.2.3	8.8.8.8	0x2b4	Standard query (0)	cdn.clipart.email	A (IP address)	IN (0x0001)
Apr 8, 2021 11:20:38.119339943 CEST	192.168.2.3	8.8.8.8	0x39b2	Standard query (0)	clipartkind.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 11:20:38.174393892 CEST	192.168.2.3	8.8.8.8	0xd575	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
Apr 8, 2021 11:20:43.144439936 CEST	192.168.2.3	8.8.8.8	0xcfd8	Standard query (0)	clients2.googleusercontent.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 11:20:33.389619112 CEST	8.8.8.8	192.168.2.3	0x575f	No error (0)	www.ztzusl.vibz.co.uk		198.54.125.197	A (IP address)	IN (0x0001)
Apr 8, 2021 11:20:34.250344992 CEST	8.8.8.8	192.168.2.3	0xba74	No error (0)	jrschnell.com.br		216.172.172.184	A (IP address)	IN (0x0001)
Apr 8, 2021 11:20:36.129431009 CEST	8.8.8.8	192.168.2.3	0xbf7e	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:20:36.129431009 CEST	8.8.8.8	192.168.2.3	0xbf7e	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Apr 8, 2021 11:20:36.129769087 CEST	8.8.8.8	192.168.2.3	0xb179	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:20:37.327389002 CEST	8.8.8.8	192.168.2.3	0x8ca4	No error (0)	cdn.clipart.email		172.67.192.199	A (IP address)	IN (0x0001)
Apr 8, 2021 11:20:37.327389002 CEST	8.8.8.8	192.168.2.3	0x8ca4	No error (0)	cdn.clipart.email		104.21.52.8	A (IP address)	IN (0x0001)
Apr 8, 2021 11:20:37.530810118 CEST	8.8.8.8	192.168.2.3	0x6e11	No error (0)	clipartkind.com		104.21.69.231	A (IP address)	IN (0x0001)
Apr 8, 2021 11:20:37.530810118 CEST	8.8.8.8	192.168.2.3	0x6e11	No error (0)	clipartkind.com		172.67.215.110	A (IP address)	IN (0x0001)
Apr 8, 2021 11:20:37.677284956 CEST	8.8.8.8	192.168.2.3	0x296e	No error (0)	a.nel.cloudflare.com		35.190.80.1	A (IP address)	IN (0x0001)
Apr 8, 2021 11:20:37.881135941 CEST	8.8.8.8	192.168.2.3	0x2b4	No error (0)	cdn.clipart.email		172.67.192.199	A (IP address)	IN (0x0001)
Apr 8, 2021 11:20:37.881135941 CEST	8.8.8.8	192.168.2.3	0x2b4	No error (0)	cdn.clipart.email		104.21.52.8	A (IP address)	IN (0x0001)
Apr 8, 2021 11:20:38.151180983 CEST	8.8.8.8	192.168.2.3	0x39b2	No error (0)	clipartkind.com		104.21.69.231	A (IP address)	IN (0x0001)
Apr 8, 2021 11:20:38.151180983 CEST	8.8.8.8	192.168.2.3	0x39b2	No error (0)	clipartkind.com		172.67.215.110	A (IP address)	IN (0x0001)
Apr 8, 2021 11:20:38.187623978 CEST	8.8.8.8	192.168.2.3	0xd575	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:20:38.187623978 CEST	8.8.8.8	192.168.2.3	0xd575	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Apr 8, 2021 11:20:43.172544003 CEST	8.8.8.8	192.168.2.3	0xcfd8	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:20:43.172544003 CEST	8.8.8.8	192.168.2.3	0xcfd8	No error (0)	googlehosted.l.googleusercontent.com		172.217.168.33	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	192.168.2.3	49708	198.54.125.197	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:20:33.570883989 CEST	716	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 11:20:33.758481979 CEST	845	IN	HTTP/1.1 200 OK date: Thu, 08 Apr 2021 09:20:33 GMT server: Apache x-powered-by: PHP/7.3.27 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 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/l[Ve$]!V.\|%T\6+Ui7J,ht$B\'(aQI|-j0J=c0==)" IvstAh?]UF0mTo]k}.l VB(#$)9c|tN(<fB

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	198.54.125.197	80	192.168.2.3	49709	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:20:44.926291943 CEST	3332	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
Apr 8, 2021 11:20:37.980906010 CEST	172.67.192.199	443	192.168.2.3	49738	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	Sun Jul 26 02:00:00 CEST 2020	Mon Jul 26 14:00:00 CEST 2021	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		
Apr 8, 2021 11:20:38.214977980 CEST	104.21.69.231	443	192.168.2.3	49739	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	Wed Oct 13 14:00:00 CEST 2021	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
							Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

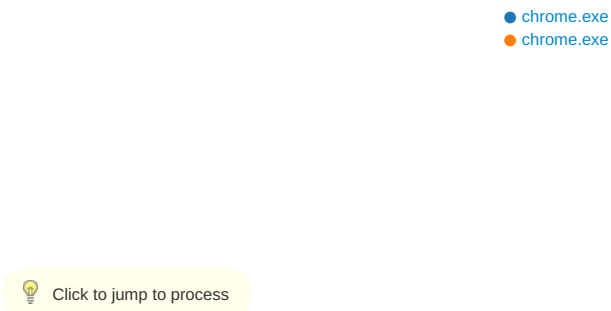
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 8, 2021 11:20:38.223577023 CEST	152.199.23.37	443	192.168.2.3	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		
Apr 8, 2021 11:20:38.250545025 CEST	152.199.23.37	443	192.168.2.3	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 11:20:38.318408966 CEST	152.199.23.37	443	192.168.2.3	49742	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 11:20:38.323632002 CEST	152.199.23.37	443	192.168.2.3	49743	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		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 3880 Parent PID: 3216

General

Start time:	11:20:28
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:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: chrome.exe PID: 5856 Parent PID: 3880

General

Start time:	11:20:30
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=1540,11347640063778282216,12771895532885012560,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1688 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly