ID: 384975
Cookbook: browseurl.jbs
Time: 18:30:46
Date: 10/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report https://main.d35pe6tu6wfnod.amplifyapp.com 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
AV Detection: 5
Phishing: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 9
Public 9
Private 9
General Information 9
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 41
No static file info 41
Network Behavior 41
Network Port Distribution 41
TCP Packets 41
UDP Packets 43
DNS Queries 44
DNS Answers 45
HTTPS Packets 46
Code Manipulations 47
Statistics 47
Behavior 47
System Behavior 47
Analysis Process: chrome.exe PID: 3560 Parent PID: 4420 47
General 47

File Activities 47
Registry Activities 47
Analysis Process: chrome.exe PID: 4404 Parent PID: 3560 48
General 48
File Activities 48
Registry Activities 48
Disassembly 48

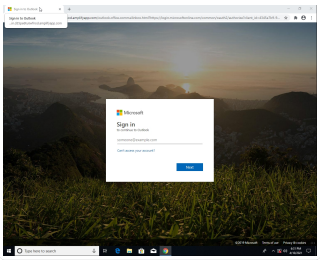
Analysis Report https://main.d35pe6tu6wfnod.amplifyap…

Overview

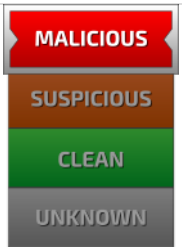
General Information

Sample URL:	http://https://main.d35pe6tu6wfnod.amplifyapp.com
Analysis ID:	384975
Infos:	

Most interesting Screenshot:



Detection



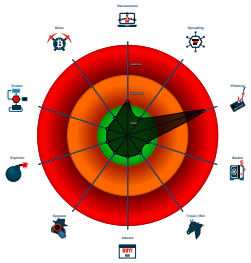
HTMLPhisher

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Phishing site detected (based on fav…
- 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
- Invalid T&C link found

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 3560 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://main.d35pe6tu6wfnod.amplifyapp.com' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 4404 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1544,7093597635801048285,11986457263259393063,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1680 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

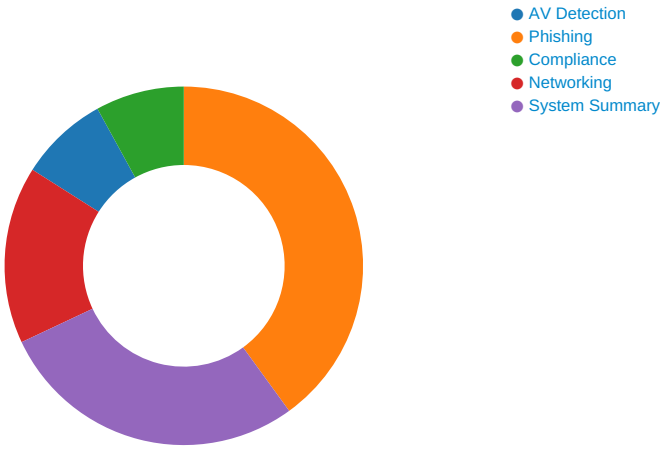
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

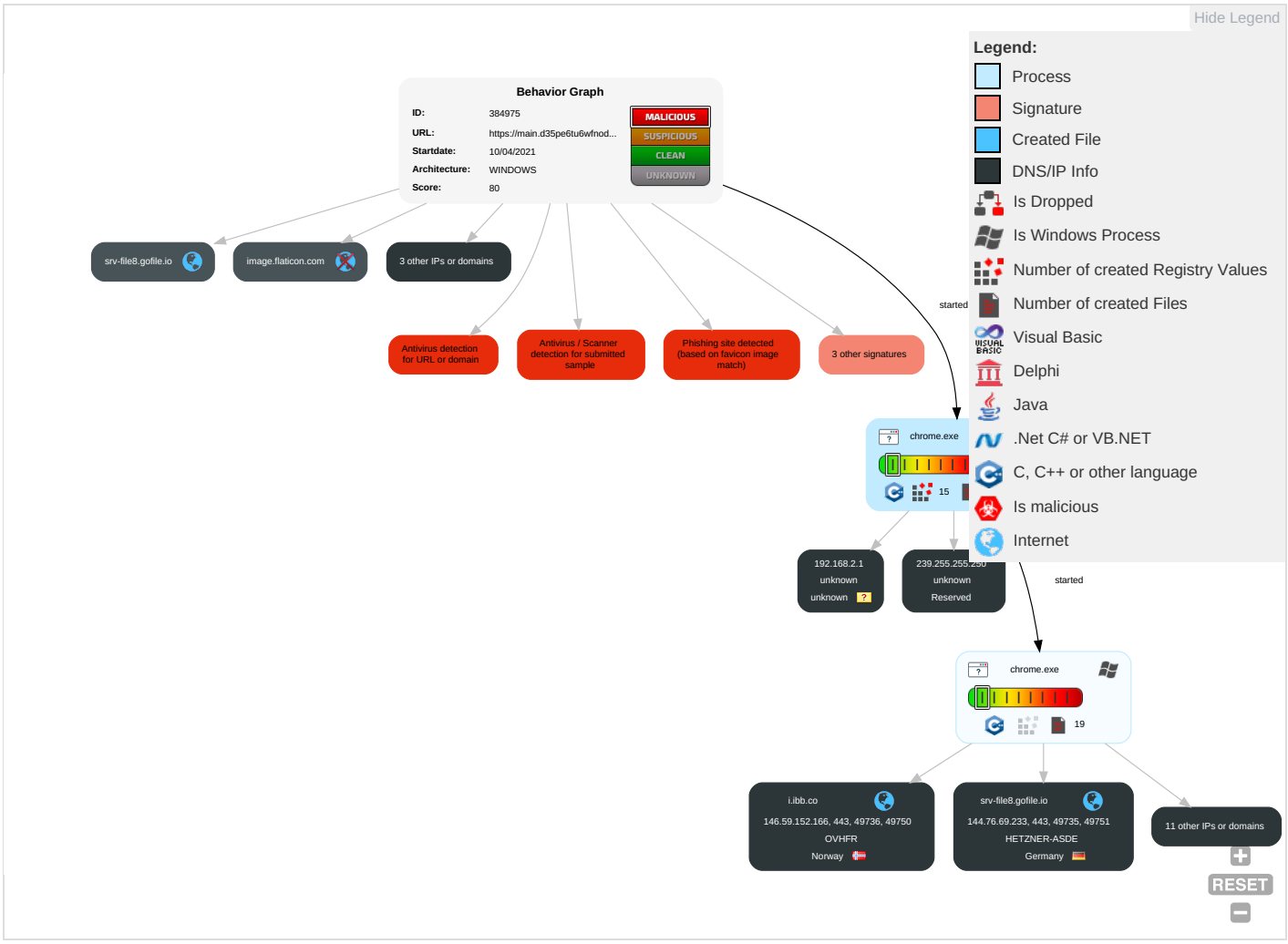
Phishing site detected (based on image similarity)

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	Impact
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	Modify System Partitior
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 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

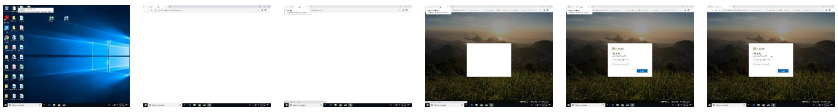
Behavior Graph

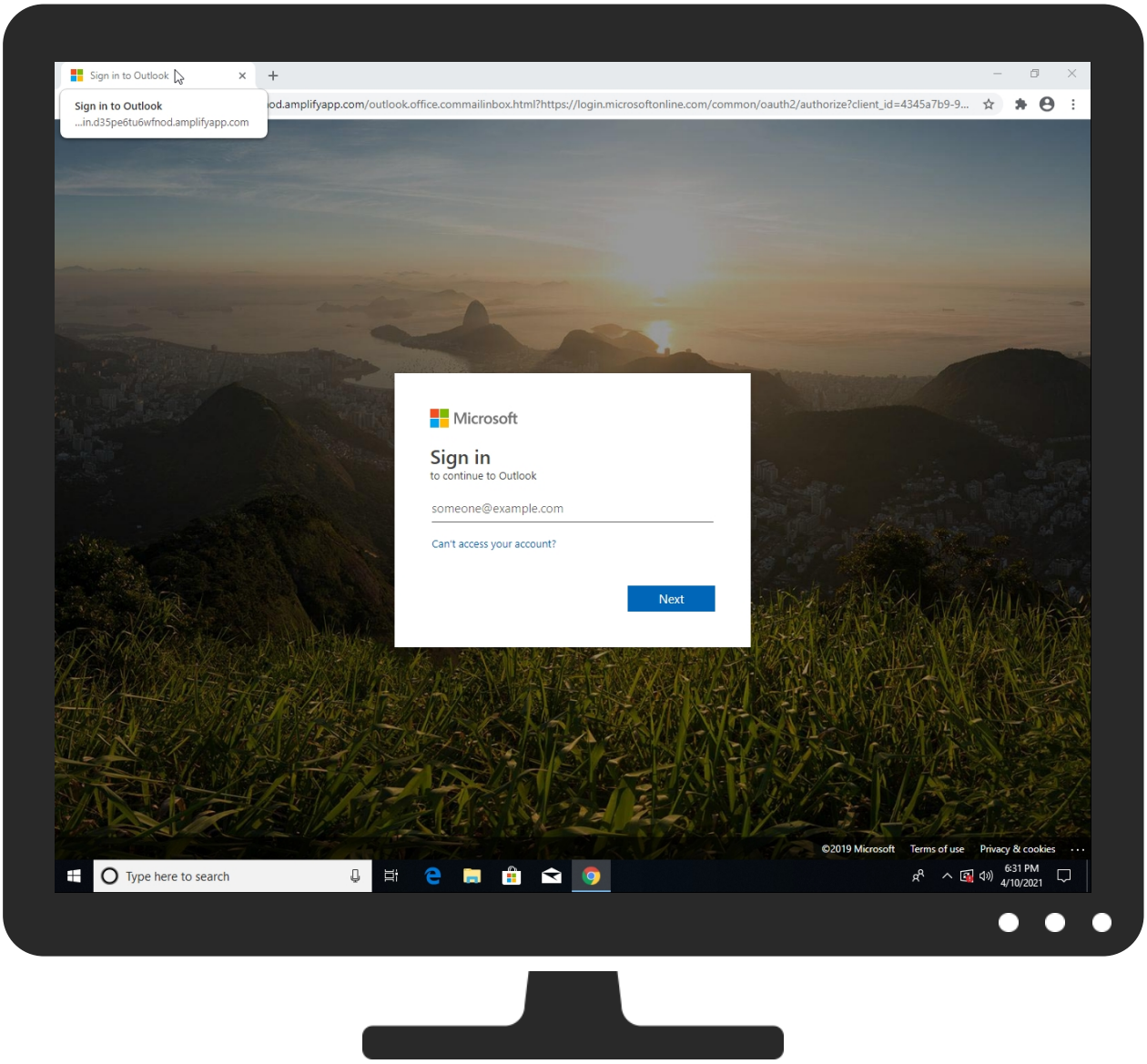


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://main.d35pe6tu6wfnod.amplifyapp.com	0%	Virustotal		Browse
http://https://main.d35pe6tu6wfnod.amplifyapp.com	0%	Avira URL Cloud	safe	
http://https://main.d35pe6tu6wfnod.amplifyapp.com	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cs1100.wpc.omegacdn.net	0%	Virustotal		Browse
ipv4.imgur.map.fastly.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://main.d35pe6tu6wfnod.amplifyapp.com/outlook.office.commailinbox.html?https://login.microsoftonline.com/common/oauth2/authorize?client_id=4345a7b9-9a63-4910-a426-35363201d503&redirect_uri=https%3A%2F%2Fwww.office.com%2Flanding&response_type=code%20id_token&scope=openid%20profile&response_mode=form_post&nonce=637478753968739283.ZGQwNWM4ZTgtMDRmOC00Zjc5LWFkODEtYjk3ZjdlMWUwODg0YTg0N2E3MDktMDhhMi00OTg5LTg1NWMtY2M3MmY4NTJiMjcy&ui_locales=en-US&mkt=en-US&client-request-id=07326398-218f-4df0-b177-e2fd0e4b58da&state=3_FqDfZM_S_DRpirdMLvzLCQ9DrHwvAzDqW46wIszpamzc2d0JIlKVUffM25_n3gFUghLWZlPtZDmCRbvUgv1UYf7v96uWY_2G-upJeGFfjHycsGLM1_JHUXj8cPtQOxfR4l8Vrk2rgpCe4eRV1TK14Y3LJgo5eEsldxYUCH-xx1e65TN5r_FDCP8SU8CL_T8wGPWVPzdUNz2zCX_fTbijDy9MLPUrqxkWxXDoBr-S3Rd2mNL3_QpbORVW7uEB5Hu-L9iXZm9Ux6W2PYn3jn0w&x-client-SKU=ID_NETSTANDARD2_0&x-client-ver=6.8.0.0	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://main.d35pe6tu6wfnod.amplifyapp.com/outlook.office.commailinbox.html?https://login.microsoftonline.com/common/oauth2/authorize?client_id=4345a7b9-9a63-4910-a426-35363201d503&redirect_uri=https%3A%2F%2Fwww.office.com%2Flanding&response_type=code%20id_token&scope=openid%20profile&response_mode=form_post&nonce=637478753968739283.ZGQwNWM4ZTgtMDRmOC00Zjc5LWFkODEtYjk3ZjdlMWUwODg0YTg0N2E3MDktMDhhMi00OTg5LTg1NWMtY2M3MmY4NTJiMjcy&ui_locales=en-US&mkt=en-US&client-request-id=07326398-218f-4df0-b177-e2fd0e4b58da&state=3_FqDfZM_S_DRpirdMLvzLCQ9DrHwvAzDqW46wIszpamzc2d0JIlKVUffM25_n3gFUghLWZlPtZDmCRbvUgv1UYf7v96uWY_2G-upJeGFfjHycsGLM1_JHUXj8cPtQOxfR4l8Vrk2rgpCe4eRV1TK14Y3LJgo5eEsldxYUCH-xx1e65TN5r_FDCP8SU8CL_T8wGPWVPzdUNz2zCX_fTbijDy9MLPUrqxkWxXDoBr-S3Rd2mNL3_QpbORVW7uEB5Hu-L9iXZm9Ux6W2PYn3jn0w&x-client-SKU=ID_NETSTANDARD2_0&x-client-ver=6.8.0.0	100%	UrlScan	phishing brand: microsoft	Browse
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://main.d35pe6tu6wfnod.amplifyapp.com/Sign	0%	Avira URL Cloud	safe	
http://https://main.d35pe6tu6wfnod.amplifyapp.com/outlook.office.commailinbox.html?https://login.microsofto	0%	Avira URL Cloud	safe	
http://https://main.d35pe6tu6wfnod.amplifyapp.com/2	0%	Avira URL Cloud	safe	
http://https://main.d35pe6tu6wfnod.amplifyapp.com/	0%	Avira URL Cloud	safe	
http://https://amplifyapp.com/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

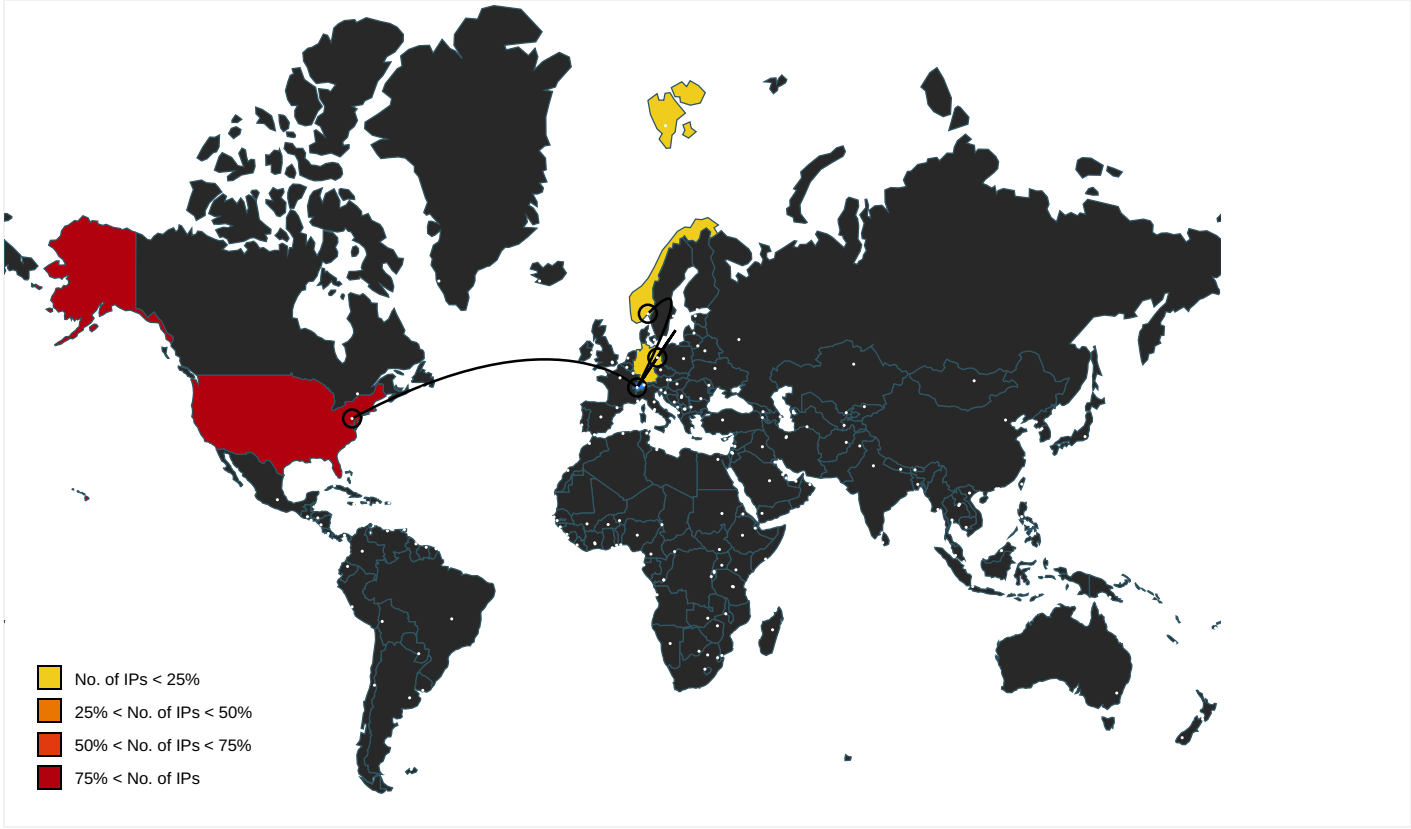
Name	IP	Active	Malicious	Antivirus Detection	Reputation
cs1100.wpc.omegacdn.net	152.199.23.37	true	false	• 0%, Virustotal, Browse	unknown
cdnjs.cloudflare.com	104.16.19.94	true	false		high
srv-file8.gofile.io	144.76.69.233	true	false		high
googlehosted.l.googleusercontent.com	172.217.168.33	true	false		high
main.d35pe6tu6wfnod.amplifyapp.com	13.32.25.32	true	false		unknown
ipv4.imgur.map.fastly.net	151.101.112.193	true	false	• 0%, Virustotal, Browse	unknown
i.ibb.co	146.59.152.166	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
i.stack.imgur.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
image.flaticon.com	unknown	unknown	false		high
aadcdn.msftauth.net	unknown	unknown	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	cca0649a-926d-4838-9626-dc0d5176767d.tmp.2.dr, 73a2365f-e731-4429-b42b-072c2d58e9ca.tmp.2.dr, 694805a0-2dd7-42ab-bab5-b4745b63901d.tmp.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://a.nel.cloudflare.com/report?s=C1fzOz90DL9bexwimRyB1uJnVPI%2FVuic%2FU1Qkk7KKrP6ipoj83kcQX03Dz	Reporting and NEL.2.dr	false		high
http://https://clients2.googleusercontent.com	73a2365f-e731-4429-b42b-072c2d58e9ca.tmp.2.dr	false		high
http://https://main.d35pe6tu6wfnod.amplifyapp.com	Current Session.0.dr	true		unknown
http://https://main.d35pe6tu6wfnod.amplifyapp.com/Sign	History.0.dr	true	• Avira URL Cloud: safe	unknown
http://https://main.d35pe6tu6wfnod.amplifyapp.com/outlook.office.commailinbox.html?https://login.microsofto	History.0.dr	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://main.d35pe6tu6wfnod.amplifyapp.com/2	History Provider Cache.0.dr	true	• Avira URL Cloud: safe	unknown
http://https://main.d35pe6tu6wfnod.amplifyapp.com/	Current Session.0.dr, Favicons.0.dr	true	• Avira URL Cloud: safe	unknown
http://https://amplifyapp.com/	03123a4ace810c09_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://code.jquery.com/jquery-3.1.1.min.js	03123a4ace810c09_0.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
146.59.152.166	i.ibb.co	Norway		16276	OVHFR	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.217.168.33	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
13.32.25.32	main.d35pe6tu6wfnod.amplifyapp.com	United States		7018	ATT-INTERNET4US	false
144.76.69.233	srv-file8.gofile.io	Germany		24940	HETZNER-ASDE	false
151.101.112.193	ipv4.imgur.map.fastly.net	United States		54113	FASTLYUS	false
152.199.23.37	cs1100.wpc.omegacdn.net	United States		15133	EDGECASTUS	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	384975
Start date:	10.04.2021

Start time:	18:30:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://main.d35pe6tu6wfnod.amplifyapp.com
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	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:	mal80.phis.win@33/216@13/10
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 52.255.188.83, 216.58.215.238, 172.217.168.13, 173.194.160.74, 74.125.173.166, 13.64.90.137, 172.217.168.35, 69.16.175.42, 69.16.175.10, 95.100.51.110, 23.0.174.185, 23.0.174.200, 172.217.168.10, 2.20.240.220, 142.250.34.2, 172.217.168.74, 216.58.215.234, 172.217.168.42, 104.43.139.144, 20.82.209.183, 95.100.54.203, 23.10.249.43, 23.10.249.26 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, cds.s5x3j6q5.hwcdn.net, e12524.dscg.akamaiedge.net, arc.msn.com.nsatc.net, cdn4.thumbrio.edgekey.net, r5.sn-1gi7znes.gvt1.com, 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, clients2.google.com, redirector.gvt1.com, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, edgedl.gvt1.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, accounts.google.com, content-autofill.googleapis.com, aadcdnoriginneu.azureedge.net, r5---sn-1gi7znes.gvt1.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, skypedataprdcolcus16.cloudapp.net, www.googleapis.com, r1---sn-1gieen7e.gvt1.com, aadcdnoriginneu.ec.azureedge.net, c-s.cms.ms.akadns.net, skypedataprdcoleus17.cloudapp.net, c.s-microsoft.com, blobcollector.events.data.trafficmanager.net, c.s-microsoft.com-c.edgekey.net, e13678.dscg.akamaiedge.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

Time	Type	Description
18:31:40	API Interceptor	5x Sleep call for process: chrome.exe modified

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\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	292980
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	6144:FJdwIm1m/QEOb1omJdwIm1m/QEOb1omJdwIm1m/QEOb1omJdwIm1m/QEOb1omJd4:pwksphwksphwksphwksphwkspP
MD5:	089C8D08B94A9C883E3AC39D04B18673
SHA1:	4BA3956D6D38EBC49835BB29BBB0B8026D289422
SHA-256:	19903B017E5F1A502B122EEE60483A4BDADEDBFE5D2126D1C2002E623F16B6E8
SHA-512:	6567769ABD5722971E40EC3E58ED182B0BD2FB5111BB5FEEADE5279FC758701B5D5979615579753FF3055DDCAA7E87705C141F8B342F4C8215D26CBFFA30A88
Malicious:	false
Reputation:	low
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-.J...."Y...$E.KB..D...D.....3.n..u.....\|..=H4..c&.....f.,..=..-....p2.:..`HX.....b..... Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..\|0.+?.`-../.xvy..e.....w.+^...w\|.Q.k.9&.Q.EzS.f.....>? w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k.._iK..xzW.w.M.>,5.}..}.tLX5Ls3_.. ).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s...,f `D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1630
Entropy (8bit):	3.127053792471246
Encrypted:	false
SSDEEP:	24:j5kPcUQUPh15kPcUQUPhpht5kPcUQUPhz5kPcUQUPhE5kPcUQUPht:U1ZhG1ZhphO1ZhE1ZhF1Zht
MD5:	573A4A582CD9246D37CCF31E008BD1F1
SHA1:	25366A65A45885FDF5C5FF9B0977788E7EC3BB3D
SHA-256:	426EB9F35D22198BDB0B02E7DFF5B471A32A6A9A2E5F33C1FE9953F4FD8E6DEB
SHA-512:	8F17BDA035824057683972A2F951E331589DEF5A8F77F0A10268677EB34E983AB58168370059003C633F4A05B379A15F6BAC43487715D793107F3389C3400F4C
Malicious:	false
Reputation:	low
Preview:	p..... .....9Blr...(..... .....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..."..0.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...p..... .....+{Qlr...(..... .....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..."..0.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...p..... ....r...(..... .....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r. u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..."..0.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...p..... .....;b..r.

C:\Users\user\AppData\Local\Google\Chrome\User Data\053d0f58-2397-4d38-95e7-114a26aba69f.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):	164170
Entropy (8bit):	6.0820782676726415
Encrypted:	false
SSDEEP:	3072:GPxIZM4iTMFp3l+7LSx8sogeFFcbXafIB0u1GOJmA3iuRM:kx4gMTo7Jsog0aqfIlUOoSiuRM
MD5:	F261EFDC4F50AE899FF1ECCEFA393347
SHA1:	9DE0EEB4211E9201B487448CD29ECE38930F0689
SHA-256:	2961B9B5AC6BD202F90B01447ECA92039E253D11BD27E642B2C9D9CDE8497ACE
SHA-512:	DC1263522541726AEC451D8471695D72B4D2164A0C09FA6AB124DFEA0228B4D49EAA7E3FAB1809891AE590B4D54ACA9F61D3437B7231D574BB047664BF81245
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":1.618104698837923e+12,"network":1.618072301e+12,"ticks":99831784.0,"uncertainty":4249483.0}},"os_crypt":{"encrypted_key":"RFB BUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr 2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1 vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\712e0d6f-a55d-4541-a0b9-5ee14bd84d28.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):	164170
Entropy (8bit):	6.082078450460204

C:\Users\user\AppData\Local\Google\Chrome\User Data\712e0d6f-a55d-4541-a0b9-5ee14bd84d28.tmp	
Encrypted:	false
SSDEEP:	3072:GP+iZM4iTMFp3l+7LSx8sogeFFcbXafIB0u1GOJmA3iuRM:k+egMTo7Jsog0aqfIlUOoSiuRM
MD5:	EA997F52DB28AAF6BD48AE12642BBA4B
SHA1:	D4EF5522F349D12ADB5EF91417B0533EB31C53BC
SHA-256:	92ADF689534441692D6767F28924AC306C596E04752FA094B3755500D80695DB
SHA-512:	6500A536DDF19C66F2391BF6FEAA0B9BF28206439753021181 2A76C6A7B4B9076718FA44658A323C8FE03C8AE05FA5253678EE18B867CAEC7537D46147F46777
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":1.618104698837923e+12,"network":1.618072301e+12,"ticks":99831784.0,"uncertainty":4249483.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+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\45949a70-282e-4729-85ab-a42fe07fa5bc.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):	1540
Entropy (8bit):	5.558120007049208
Encrypted:	false
SSDEEP:	48:YjVwUI6UUhAUcseKUewqPeUerPU+UeffwU5WUenw:PUBUUGUc3KUGPeUGU+UEoU8UD
MD5:	8B125BAA15708AC234BAFDC3CE476A8B
SHA1:	E01478A0E5053E2B4B7E17C96EC9EC14FAA646DA
SHA-256:	483B20449AC9782BED2E38ED85D3D66FE8E751DD54B7A3CA10E65D2D4FBBD633
SHA-512:	E18A2A357B2BEBA67BDEF8361B804DFC829BB3B2EC84DF8B346DFA3E548F6DDCC1FCDBD38D607C96CA7D1BF588B04062CE88E0395087B5A2DA99C49100C27637
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633884700.372906,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1618104700.37291},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1649640701.684602,"host":"dmttlOgMMo/ZEWP3MEx61fzb5SpdgCZkeSb7htj2Y10=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1618104701.684607},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1649640701.045784,"host":"3SRshiHi1ShOKmw5hb0KM/oKC3V5eksT0EdjjbDtOZQ=","mode":"force-https","sts_include_subdomains":true,"sts_obser

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\726188f3-b98a-45c9-ad6e-60525e21bb73.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):	24054
Entropy (8bit):	5.53384580413133
Encrypted:	false
SSDEEP:	384:JIlt1LlLQX41kXqKf/pUZNCgVLH2HfDE7rUQHGHZHGXnTK+HR4K:XLlG41kXqKf/pUZNCgVLH2HfA7rUUGHA
MD5:	328851F78624B00A636453A2491023D5
SHA1:	EAA3C66759DD357B137289C1160E80504DC2DC7A
SHA-256:	945D28944E4845ED25A114FE89BCE1D75E615713E3F1093B9875E6C4C1E9B30A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\726188f3-b98a-45c9-ad6e-60525e21bb73.tmp	
SHA-512:	A0F920EE5853B350829160929687551BC415567681A93AF15D8B9E4850A9BD8995D4908259DCF5B1168BFC104DDBBB9F915D689B425E961DD8A9E31CAF7290E0
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":"13262578296008083","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\73a2365f-e731-4429-b42b-072c2d58e9ca.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\83218606-9a66-4818-a026-adcc76313e26.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):	24056
Entropy (8bit):	5.533910248005408
Encrypted:	false
SSDEEP:	384:JIItALlLQX41kXqKf/pUZNCgVLH2HfDE7rUQHGHZHGgnTcUR4I:KLlG41kXqKf/pUZNCgVLH2HfA7rUUGHn
MD5:	442424B9BB14A0ED4E4A183E50FFA154
SHA1:	3C18E35A099E2A4330E81CA1607A074CC79E3C8B
SHA-256:	CB18125F90D5BC417A25E1A84A44A85C61DE8EB559A7E634E8BBD8748C82A7E0
SHA-512:	E8F80671D698181A94CEE949E7C3DC1E1E87531FB294075AA0693A5B0B2D56396AD219A64F72C28ECA8FF0F1B07527DF9005211C7FE6FB51E739A744BE850B28
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":"13262578296008083","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\84681e28-88fc-4246-8e43-5888a3ae91b4.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):	5.536072037813499
Encrypted:	false
SSDEEP:	384:JIItALlLQX41kXqKf/pUZNCgVLH2HfDE7rU0HGUnTcPGR4O:KLlG41kXqKf/pUZNCgVLH2HfA7rU4GU9
MD5:	6283E2AF85AE9D504AA2E9441134BF9B
SHA1:	92D8394594533569D1BEAB83B45411015514265C
SHA-256:	F75D6E37B812B8828FAF65FFEAE8D68E27369382F34A20FD6D20CFD771B2646B
SHA-512:	BCDAB573D8124CA9462C8A77528F8E0A8F47D7944B11073500744C72F8954183C79BB7C17C27446F495ADC58461CB8C741EF1A8572208B2CA4825326D8F28958
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\84681e28-88fc-4246-8e43-5888a3ae91b4.tmp	
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":"13262578296008083","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\98adc6fa-036f-40f9-b94c-a20dda050c35.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\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.2395138428532855
Encrypted:	false
SSDEEP:	6:mMppM+q2PWXp+N23iKKdK9RXXTZIFUtpZk6ZmwPZGMpMVkwOWXp+N23iKKdK9RX3:zpM+va5Kk7XT2FUtpP/P3MV5f5Kk7XVJ
MD5:	93D59AD4391CD8319A03FDADD45FA4D9
SHA1:	4D6AD560D240079BAB762DB12EF898E1E5927B5D
SHA-256:	D754D472002A6EA1C14CE19117718D0E9D8DCEAD8B1C7FB921A1B1D6ADD4C498
SHA-512:	88F9CF6ABF1DF3BACD8167FD41D6F51134EB388CA62B3B5EB8E5AD21952BC10F72DCF2975E50E9960EFCAE7629C25B4F0B38289820C9A7961C21E89A30975A5
Malicious:	false
Reputation:	low
Preview:	2021/04/10-18:31:43.456 1a6c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/04/10-18:31:43.459 1a6c Recovering log #3.2021/04/10-18:31:43.461 1a6c 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):	5.188813988506748
Encrypted:	false
SSDEEP:	6:mMEUTGqM+q2PWXp+N23iKKdKyDZIFUtpZEJsZmwPZEJHMVkwOWXp+N23iKKdKyJd:GUTpM+va5Kk02FUtpWJs/PWJHMV5f5K1
MD5:	C263C85A2AD8B2C0CFB0092FB29AA492
SHA1:	AC55AC98736EA33B4E040BB17997F9BF6D317F21
SHA-256:	82F8522E2F5CFEC9D5646A3007239372E72246AD56FBA7BCA1FE861E1871744A
SHA-512:	E5C0C099F17B5CDE45D19F64E0829095F5E9351F28B82EB0655FD152910E8DAD957E9012FD0091E97CEBBC1893A0863A678F7868DE33A4760F34618D40F9192F
Malicious:	false
Reputation:	low
Preview:	2021/04/10-18:31:43.443 1a6c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/04/10-18:31:43.446 1a6c Recovering log #3.2021/04/10-18:31:43.446 1a6c 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\Code Cache\js\03123a4ace810c09_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\03123a4ace810c09_0	
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.471013915867037
Encrypted:	false
SSDEEP:	3:m+loiIOA8RzYP2FycyG8ZFvD1fQK+HtlHCL0s//hiWyNPfLCGZmFn5/XpK5kt:mSIEYeMRfpL0s//CO/FnnK6t
MD5:	DBC02BDFDDA3E8E38032DB987BF054B5
SHA1:	6E94E6E025667B204A80099ABA8C5D53A8645EA5
SHA-256:	166C071950F68B5B4DEDFF08ACF80A1DF7BA390946C70AEE3240C0C08CC93C69
SHA-512:	3A006427616BE952BDE5E05DD984AF4305EC3284A5171055428F961C61E8F0DC91B34E2E11838E64D38E85D23BF15124679C0BFD0CCBE30DD0F809BD12C9460
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H....7.L...._keyhttps://code.jquery.com/jquery-3.1.1.min.js .https://amplifyapp.com/.5z.>./.....<~.pv.n..x(..d.yPc.PG.....7.A..Eo.....W.EG.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	264
Entropy (8bit):	4.699606982071429
Encrypted:	false
SSDEEP:	3:mRoT/LlHlZb3mlYlFRFWz/lll50FZz/lllK7u1Zlh/lllsu9KR8lhtOurlh/lllB:moxeaCzQ3zbn3pHkQ+IRwHzEl
MD5:	69B893A596D5076DDF97EB65E6322FAC
SHA1:	EB4569290F8022686F7D5059546E59F736C519D1
SHA-256:	CC3C9CD65ED11AC138E5D26D2A134419D01AFC8770361B895E48944F1AD8A4A0
SHA-512:	F5610DEC8A0C9DFC59D71AA4A0BF0734DAAFEA9CA69EF97FBAA73872067518F54E71CDB7F3F58B95451F913A5B5673C65FDF3DE49923B345F30D62AFF2332EI 7
Malicious:	false
Reputation:	low
Preview:	.....oy retne.....J:..@.o.>./.....^}.Np..@ikt../.....-..0..x@ikt../...../...3.KPu../.....KPu../.....&<..\.O$.KPu../.....p..(....KPu../.....q....._.KPu.. /.....+<P|...X.KPu../.....Y.{.>./.

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:	355D19828609971998B09B36E7C7D304B7FB88C7A726670BEBF5CF2E2710F8E71B0F9DEF6FE9712B484C1EB122AEEEFDECF31D13E02C4539C399DFB86EC7619 F
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9665486140937247
Encrypted:	false
SSDEEP:	24:WcLgAZOZD/1qLbJLbXaFpEO5bNmISHn06UwP8:W8NOZ1q5LLOpEO5J/Kn7Uc8
MD5:	E2B7EA97288597A4DE831DC7AB50D4CE
SHA1:	C3F1C75FDEB565D2681B56274378C66CEFB8FF45
SHA-256:	4C7197D36D1DD24B85FE12F1D2EFDDB793D4CAB0F50F705F0F8D4E59360E2C7A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
SHA-512:	9BE9BABE598327FA6B4414BB27A9EF6F6E3FB7E9D6B73FB10AE25188B2ADE60D17CAA91367D30BB946794CDE13CD3DAC8C1FEF1B2AEDD53E1475EA2DFE34AD45
Malicious:	false
Reputation:	low
Preview:	.....t.$.....

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):	3990
Entropy (8bit):	4.527812647736104
Encrypted:	false
SSDEEP:	48:340xifA+s+ysI2dyiKkivo2USBu0cMsA6IIwVMMBxPoK0GpqZMHOe9QwVTou01n:34lTsGlSEdRIIwC65o0kZMHOezU
MD5:	A7053849C8E57A99C38DCC44C97314AF
SHA1:	2D1356409BDCFC82CD1983B4A2E9BA1BCD4A01EC
SHA-256:	F047CD8CD9673EFC665309EA74A86260E986F5BE6C1B7966F35AA866C1045119
SHA-512:	ABAEC6C6FFB95986B606F65A9FCAFFBF941A85DA6C1DBDB74510707D00F0A9F3D885A3F31B541ACBA8272A225FD9B59FF554D108182298FD98557732925C0D1
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...cbf2d550_bb8d_47f3_97d7_bcbdd549ee2d.....{.....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....)..$.....R...https://main.d35pe6tu6wfnod.amplifyapp.com/outlook.office.commailinbox.html?https://login.microsoftonline.com/common/oauth2/authorize?client_id=4345a7b9-9a63-4910-a426-35363201d503&redirect_uri=https%3A%2F%2Fwww.office.com%2Flanding&response_type=code%20id_token&scope=openid%20profile&response_mode=form_post&nonce=637478753968739283.ZGQwNWM4ZTgtMDRmOC00Zjc5LWFkODEtYjk3ZjdlMWUwODg0YTg0N2E3MDktMDhhMi00OTg5LTg1NWMtY2M3MmY4NTJiMjcy&ui_locales=en-US&mkt=en-US&client-request-id=07326398-218f-4df0-b177-e2fd0e4b58da&state=3_FqDfZM_S_DRpirdMLvzLCQ9DrHwvAzDqW46wIszpamzc2d0JIlKVUffM25_n3gFUghLWZlPtZDmCRbvUgv1UYf7v96uWY_2G

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	183
Entropy (8bit):	4.267376444120917
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+GgGg:qT5z/t2qoEwhXeLKBt
MD5:	7FA0F874EABF1EED31988230680AD210
SHA1:	E71B360F1E8D5C278A051AD03DFB9027ACCF38C3
SHA-256:	09E15F8939364145E710C314EBD93FD19BF60C2B6B20BF8023315D617B6B141B
SHA-512:	AF4C2E595AA0B1FD96474A0E73530B38BE5F2906B10BE1DEFC0A9221129A3E5BB8D0816777550863AD426C5C836ECA1F0C384986C2A1108E2E4CA20EF10A782
Malicious:	false
Reputation:	low
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....F.....F.....

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

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):	320
Entropy (8bit):	5.152366987889689
Encrypted:	false
SSDEEP:	6:mLL+L+q2PWXp+N23iKKdK8aPrqIFUtpKkFaKWZmwPKkLVkwOWXp+N23iKKdK8amd:3L+va5KkL3FUtp3LW/P1LV5f5KkQJ
MD5:	C5A7A1E3F8DCE9DCE5196491A6B0B17A
SHA1:	F9A2ADB94D3833A72508BE5E5D5B711E40D9D7EE
SHA-256:	C74C36EF150DC03B38CA79AEF82F8C7ABCF75ACDAC2032C2FA033A1D4CDF21FA
SHA-512:	EAE17CD6E1BDA537D9B1EA4366A97DCA6ECA0F8D01EC5721227CCC5C62FF8C1A0A92BC7E1A88C137CEDCBB2E65D789B9BBC4C1225D5D7F71CDAFA501127 378D
Malicious:	false
Reputation:	low
Preview:	2021/04/10-18:31:36.301 10ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/04/10-18:31:36.302 10ec Recovering log #3.2021/04/10-18:31:36.303 10ec 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:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW:
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):	317
Entropy (8bit):	5.238487533525524
Encrypted:	false
SSDEEP:	6:mlWlM+q2PWXp+N23iKKdK8NIFUtpIWB1ZmwPIWPMVkwOWXp+N23iKKdK8+eLJ:4mM+va5KkpFUtpIO/PIwMV5f5KkqJ
MD5:	44505DDAF703EF4F6F639BBD33FEE3B5
SHA1:	5E9838D5B4642CC63043CC1BC258EAAE2D92C543
SHA-256:	BADFD36446478A7884F6D72C5031F61549FE092E7F35AEA3473C1D4291F10159
SHA-512:	685327F7AC8526A7AF1C976E9CBD7FEC4DFC735961C15111D659FA06256D1527EE49BFA06891F4A24EAC243B8F84888FF1ABCD2DD01379A35B82CDA62DC465 7
Malicious:	false
Reputation:	low
Preview:	2021/04/10-18:31:38.350 7fc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/04/10-18:31:38.351 7fc Recovering log #3.2021/04/10-18:31:38.352 7fc 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
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=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvuI11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRITANEQkqzU3TEi+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:GbylJnlTwGB7V9Hne4qasKxXltmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvuI11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRITANEQkqzU3TEi+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
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=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	18432

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Entropy (8bit):	1.8738389023476607
Encrypted:	false
SSDEEP:	48:zBmw6fU9G+s+ysI2dyiKkivo2UTQeBJtjI90R4vBdkGx+s++Gu16+sI2dyiKkivE:zBCIZsGlTPN090UosIu+I
MD5:	79D4CA7E0BFF8547A955EEAAA5A8E238
SHA1:	362A6A6A1B7C664CEBBEADA800EC996879029312
SHA-256:	E9538993B85C968980956BF79160A83698424B7506AE072D0554BDC3811F2E63
SHA-512:	4D5EC2D73D2E1B53F96845FF32B64CB45972401AC996417FF67CB695D8E97EE0E33C9E721BA382D37AC17A2BD81C0B6C096DD40CE45FD112B4B8AE230A1A065
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):	0.7768005805259339
Encrypted:	false
SSDEEP:	24:QeyLiXxh0GY/l1rWR1PmCx9fZjsBX+T6Uwy3n:QedBmw6fU13n
MD5:	568F21D8A419B4CAD8CE810CED049163
SHA1:	9E5A0E5D123B69A39D390CC3627C9FAAE12F896B
SHA-256:	4151828942740F273C1D7C1F731011A5068600E82CE3C455E560C708A251AE90
SHA-512:	129A2FD80026F894F0836A9132C300102D9172BB0A810F9B36D9E9CD930AC82A72767455BDA9622FDBAFC49D90C40ED99EC8DFAA65AC2540D4A48EE3E16E3409
Malicious:	false
Reputation:	low
Preview:	.....k.f..... ....

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):	5.247392784539381
Encrypted:	false
SSDEEP:	6:mMaM+q2PWXp+N23iKKdK25+Xqx8chI+IFUtpZAa6mZmwPZAOGqMVkwOWXp+N23ib:wM+va5KkTXfchI3FUtpSrm/PSOpMV5fk
MD5:	3B185560FE15DE5EE1D32C02998B4B4A
SHA1:	CBD8CA3E436288EA01073BD5B5972E0CBC262DC8
SHA-256:	B51EBC8BE839FCF40B06252B5F70F665C7BFDBB801AE0EB6AC0B9E84B0E40DB9
SHA-512:	6738BCCD7AFBD2EE406B4AE493A949CC7B8BFB48C6D690E40EA2C55E4CC72D3F130D3212F5A9F5A18FEC2111B5F0DFE0BB0D249370897C8B84E7E5910997EB24
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Reputation:	low
Preview:	2021/04/10-18:31:43.383 1a6c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/04/10-18:31:43.406 1a6c Recovering log #3.2021/04/10-18:31:43.407 1a6c 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):	5.21321185196476
Encrypted:	false
SSDEEP:	6:mMplM+q2PWXp+N23iKKdK25+XuoIFUtpZMsZmwPZMHMVkwOWXp+N23iKKdK25+Xp:7lM+va5KkTXYFUtp1/PQMV5f5KkTXHJ
MD5:	E7E3CF2C0808C210A5962621236760E6
SHA1:	0D55F58634637A7E9BE09A4E8C7BA02F34BE028F
SHA-256:	9248290EA825A43D02E341AECF111FA1E7D887C5D8F44244424783154691BD8F
SHA-512:	0F99D27E954AD3D9C05D88D7208DDF52CD44CB80F88AB581CEE90144DB0A40B5D8BBAB847269F49E2AE194DA12E203982FDAFC180298285AD80702980BD4768
Malicious:	false
Reputation:	low
Preview:	2021/04/10-18:31:43.342 1a6c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/04/10-18:31:43.347 1a6c Recovering log #3.2021/04/10-18:31:43.347 1a6c 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):	5.230585506303378
Encrypted:	false
SSDEEP:	6:mMU8M+q2PWXp+N23iKKdKWT5g1IdqIFUtpZ/ZmwPZCLlMVkwOWXp+N23iKKdKWTk:S8M+va5Kkg5gSRFUtpt/PuMV5f5Kkg5i
MD5:	D1B97EEEF5C2A67A6B9A373BFAC8511C
SHA1:	DEF3967E296EE8D60EC60859BA6051F0EDF24209
SHA-256:	2B994B7D7818AC538A48F1FE8CEBACFD72C1D6B66098806C3343382CA1AB5C50
SHA-512:	DEBB41E4B1008B5B1E56838BCF2EAA90889E5D8CE9DB086E331BE6D29413A132052DCB17EBB446755F20C546872FB38ADE08BA45C8798B3150F17567F013F0C5
Malicious:	false
Reputation:	low
Preview:	2021/04/10-18:31:43.328 1a6c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/04/10-18:31:43.329 1a6c Recovering log #3.2021/04/10-18:31:43.330 1a6c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.7287975411136633
Encrypted:	false
SSDEEP:	48:TQuw+s+ysI2dyiKkivo2UBu4RvAr+s+ysI2dyiKkivo2Ua4:LsGlhRDsGlv
MD5:	A0BDF3323DD4BB97AB82F4590D888EAF
SHA1:	65128BE9C6CBDA6FF2D1CAE2863807BDFCFBBB8C
SHA-256:	DDF7C8814E29E5EC71722BB6D58C01D005F5ED819A8276147A63142E6B3E8B4C
SHA-512:	59BD5E5AA831E41509A69359AE8E8F97F8509FAFAC051C610D9E9BFBD6B75032E6DBBFF705A41D46D8045E386483E0217DCEA68FC0F9BFC229079ABF7C95DCF
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
File Type:	data
Category:	dropped
Size (bytes):	4551
Entropy (8bit):	6.2611212184804685
Encrypted:	false
SSDEEP:	96:rqV56sYOfsO+FjrF25Bz+ciaB3TIsGl4E5H+e:rkGHvWscisDKaE5H+e
MD5:	B3E9DB2B0AF4FADAA5A0873BCCDBD9C2
SHA1:	2A60394F0610EDDE29F578043B3FAA95DC96CB2D
SHA-256:	9C87B591528E4B93831BED740F31B3E6FA5F243F12B8C5A89847BBD006E11C46
SHA-512:	6562A84462C124215817ED35C3847D03DF6BA179D7DFB30D5FBF7530B129D6566A11EAB51986CAB2C87B1F2995E621F0A5CD50225F974D3F2B30B677B01A8168
Malicious:	false
Reputation:	low
Preview:	....."...J..0..07326398..218f..2g..3..35363201d503..4345a7b9..4910..4df0..6.8.0.0..637478753968739283..9a63..a426..amplifyapp..authorize..b177..client..code..com..commailinbox..common..d35pe6tu6wfnod.1drpirdmlvzlcq9drhwvazdqw46wiszpamzc2d0jilkvuffm25..e2fd0e4b58da..en..fdcp8su8cl..form..fqdfzm..ftbijdy9mlpurqxkwxxdobr..html..https..id..in.4jhuxj8cptqoxfr4l8vrk2rgpce4erv1tk14y3ljgo5eesldxyuch..l9ixzm9ux6w2pyn3jn0w..landing..locales..login..main..microsoftonline..mkt..mode."n3gfughlwzlptzdmcrbvugv1uyf7v96uwy..netstandard2..nonce..oauth2..office..openid..outlook..post..profile..qpborvw7ueb5hu..redirect..request..response..s..s3rd2mnl3..scope..sign..sku..state..t8wgpwvpzdunz2zcx..to..token..type..ui..upjegffjhycsglm1..uri..us..ver..www..x..xx1e65tn5r.`zgqwnwm4ztgtmdrmoc00zjc5lwfkodetyjk3zjdlmwuwodg0ytg0n2e3mdktmdhhmi00otg5ltg1nwmty2m3mmy4ntjimjcy*...J....0.....07326398.....218f.....2g.....3.....35363201d503.....4345a7b9.....4910.....4df0.....6.8.0.0.....637478753968739283

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):	0.04761656801783402
Encrypted:	false
SSDEEP:	3:oS3llu/fllI2NlllHfllIHNlllStFlllHfllI0tFlIlgMRgSWbNFl/l/4ltNll/5:Vb42og9bNFlWCj/lUwKl3n
MD5:	56B1052041C83DA20E5DB4667161EAD9
SHA1:	17F43417EE1190B9B187FBCB3C92BFE8D9A91EE6
SHA-256:	1975B462B660E5C955200A2E8E72A6AA3C8DA77B0EC64E9D56BB43785D89C73F
SHA-512:	A6C3EC5746D68E908535C7E4B0822D0429DAD3749C789A3791989EA9850AE3E75795E41A3A9FA7B582079FDAB38CE7648FBAEE771DB58044A637992DF11EBA8
Malicious:	false
Reputation:	low
Preview:	.....%.zd..... ....

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):	5.4673870896401375
Encrypted:	false
SSDEEP:	48:zDVGjmRa7LMC8db5r7SbQSefgGk+mNrS0U9RdiN9a:gKa7LMBdb5r7SbQ5fgGrS0I
MD5:	A5305A9700518171393EA55F2646B6EE
SHA1:	133D268F9905ED98B806DA377BDBEFCD53C8F7CB
SHA-256:	F39361BA693A6B952F9751509A4B7EE6331478C9FF3EFCE3F33B41103ED40703
SHA-512:	6BE28908C0261C20D3220C2EAC5758ACCF8DA40093514794CE1F534B4E6FAD28D9462ECDE034F74F34A224C8E42490E6A2A3E856FE69AC968F2B489C06F8558
Malicious:	false
Reputation:	low
Preview:	..O...*.....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..872914000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-04-10 18:31:44.54][INFO][mr.Init] MR instance ID: bd980b8d-cf0f-4810-999c-e7cdf4ae1b8a\n","[2021-04-10 18:31:44.54][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-04-10 18:31:44.54][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-04-10 18:31:44.54][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-04-10 18:31:44.54][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-04-10 18:31:44.54][INFO][mr.CastProvider] Query enabled: true\n","[2021-04-10 18:31:44.54][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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Entropy (8bit):	5.163774215128504
Encrypted:	false
SSDEEP:	6:mLd4q2PWXp+N23iKKdK8a2jMGIFUtpKAZmwPKLDkwOWXp+N23iKKdK8a2jMmLJ:lva5Kk8EFUtpH/PW5f5Kk8bJ
MD5:	A732C3C91A802537CF3FE439ABA957C8
SHA1:	2134B8280DFA6F811CFCEA6A854CD50249DC3597
SHA-256:	6F89CC322D21C9FF72C464A39969843706C848D16F8CD01A7E3E43FD5A518E69
SHA-512:	D7D86E75880ACD7C0BC2C94724A3558CAEF31F763ED5DA47A787DE5321D3CBB2FFFB3D7F7914A3C518E6AF25A97A77E130FFE5F28F6085BD0A3DFA81DA4AD7F
Malicious:	false
Reputation:	low
Preview:	2021/04/10-18:31:36.081 d14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/04/10-18:31:36.082 d14 Recovering log #3.2021/04/10-18:31:36.083 d14 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.220647459833881
Encrypted:	false
SSDEEP:	6:mLYqM+q2PWXp+N23iKKdKgXz4rRIFUtpKDmZmwPKDpMVkwOWXp+N23iKKdKgXz4n:j3+va5KkgXiuFUtpV/P5V5f5KkgX2J
MD5:	59A64FA4D681A1A6B84969D30FE7FFB6
SHA1:	E56049D755F45C159682ED677829C4714FDC7945
SHA-256:	79072AF20E130F2DC01ADB9212ED71E4374ECF38FFEA773B1412EDC58B76CD88
SHA-512:	9CFA90EEFA9D7CC558953DCAEA39BCB723214EDCDC7C8DCE31D474AEFED9A8954B9142DBDBEF6B1AE7A12964CF2C68F039D926B2E75F7301D04C4983F816222
Malicious:	false
Reputation:	low
Preview:	2021/04/10-18:31:36.317 fac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/04/10-18:31:36.319 fac Recovering log #3.2021/04/10-18:31:36.319 fac 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):	0.9933645879197334
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUYzqg6ZDhoTRsv:wIElwQF8mpcSfKUqN41
MD5:	AF499321ED719B9EB6F4A0A9FF82C192
SHA1:	A4E5ED271FA6B873B62D7F77769788977AA38737
SHA-256:	F2941F9B6AB46A1777E511EBF99557F6E5B5A685152D59EFF041CA6CF1AC8462
SHA-512:	2830E2A0BE97C90DABE011A6AC3480FDC2C9367069151135F6AB737DB1D554C29AFA49D0437F0D9F735592C054C88CFAF15199D7E8F53F1D0E5CE847E39F9DAC
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):	0.6277771280127119
Encrypted:	false
SSDEEP:	48:3hYsB2IcnqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGU24:hUhIElwQF8mpcSd
MD5:	4C1DB3DB9B0422906EBE29D232663022
SHA1:	6EE22093F458AA8FBE5A1BD609052CC140DE6A72
SHA-256:	A79291D8271F36BE97711E575465A3F2BC8082C9D783B62B67DB188AA469B038

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
SHA-512:	BE2CB31639118126EE5CEC3BD0812F5F794569F50FA6B9B53F78783129CED0A616F330ABD3DADE8A517721B33E85BCADD9CD293B9E8012361C5058F2C3AE5A6
Malicious:	false
Reputation:	low
Preview:	.....a..... ....

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):	320
Entropy (8bit):	5.145407643783402
Encrypted:	false
SSDEEP:	6:mLTAQ+q2PWXp+N23iKKdKrQMxIFUtpKEIdNAgZmwPKEUaXAQVkwOWXp+N23iKKd0:Rva5KkCFUtpuX/P+q5f5KktJ
MD5:	55A512FFD1B98BC4AB38660FFC29B8AF
SHA1:	AC650804FCDE1C94A11852C6F6D7A7D2024F0CE9
SHA-256:	D422A8BC9F327045336AFAAF61E46310CA63242AE048A31B276F4DBBB2193DA9
SHA-512:	7C292337A81F089B83656439746FA51C930DCB0AC39734F6CBDC4192ECE4ECCD05C4C09A54DD145A9B949546B28050B6A66C0C20DAFCB1E5204088280607000
Malicious:	false
Reputation:	low
Preview:	2021/04/10-18:31:36.209 1048 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/04/10-18:31:36.210 1048 Recovering log #3.2021/04/10-18:31:36.211 1048 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):	345
Entropy (8bit):	5.156339555284139
Encrypted:	false
SSDEEP:	6:mLC+q2PWXp+N23iKKdK7Uh2ghZIFUtpKIZmwPKcGBVkwOWXp+N23iKKdK7Uh2gnd:kva5KklhHh2FUtpT/P1GP5f5KklhHLJ
MD5:	82AFD0393A90B4F24C8ADBE9D82836B4
SHA1:	5E5688176BDEBF27568D08D3CB2F40F03B46B537
SHA-256:	7F6638E3FB6B85CA9B5B99D716E5A98DAE78BBEDD016DF0FAA0691CDD9660802
SHA-512:	D253CD97C21102D72D49DA2F816C2BA96014AF05662F9ED308A2840249D982654568FA37AE1B41817DFFF9B01CBE867D5451F8962A26852D8883B6EFC2B3B193
Malicious:	false
Reputation:	low
Preview:	2021/04/10-18:31:36.002 c68 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/04/10-18:31:36.008 c68 Recovering log #3.2021/04/10-18:31:36.009 c68 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\694805a0-2dd7-42ab-bab5-b4745b63901d.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"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\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):	430
Entropy (8bit):	5.270973465511364
Encrypted:	false
SSDEEP:	6:mL+6AQ+q2PWXp+N23iKKdKusNpV/2jMGIFUtpKAU0AgZmwPKAU0AQVkwOWXp+N2u:1va5KkFFUtpyW/Pyq5f5KkOJ
MD5:	197970D788F8B6643F81DAE5DDD2B26B
SHA1:	E130A2F34AC63ED218F7A5EAB136C6E93951D258
SHA-256:	54A9676E41EB6BDFBF66A28302CC12AD1F19BC7D39FCB8956F329127A72CD945
SHA-512:	537F7A6EB7629D1166A9E8B3ECD1A254F14AA1550080FCFC88D726A35BD6C80E5062CE829333E3160BC7D21282EFFB7120C58548A1FD1A78822AAEFE1A39305
Malicious:	false
Reputation:	low
Preview:	2021/04/10-18:31:36.249 1048 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/04/10-18:31:36.251 1048 Recovering log #3.2021/04/10-18:31:36.251 1048 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.286018693862088
Encrypted:	false
SSDEEP:	6:mL3M+q2PWXp+N23iKKdKusNpqz4rRIFUtpK9ZmwPK9SMMVkwOWXp+N23iKKdKusX:qM+va5KkmiuFUtpO/PISMMV5f5Kkm2J
MD5:	4246AD3AF6B523E1CC7833912064574A
SHA1:	172AD4E252D144E6AD8D64B9DB5CF07E77B5A852
SHA-256:	C328EBBB74BF9F90781EF4B720D6CAC5420F6FBE5CB531ECDA67D10B74C38714

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
SHA-512:	5EE82E85B3C43562AE42B726A979F0D559676007BC1FE0EC667F5372E1C4901437CEA61DD555A7F4575ABED9CBA09F03BEADA3B1AB56CD7D188A78ACB19E66DC
Malicious:	false
Reputation:	low
Preview:	2021/04/10-18:31:36.313 7fc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/04/10-18:31:36.316 7fc Recovering log #3.2021/04/10-18:31:36.317 7fc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.258654690358742
Encrypted:	false
SSDEEP:	6:mAsXAQ+q2PWXp+N23iKKdKusNpZQMxIFUtpJtXAgZmwPJtXAQVkwOWXp+N23iKK+:5Nva5KkMFUtpJv/PJ95f5KkTJ
MD5:	76B9C99ED09ABC1568DB7703BDFD100B
SHA1:	CE3EBA4BD45E4C0DA118CEB2FDD459FB6C3DADC2
SHA-256:	39111DD00114B4D8B4F7EA16CB2291332167FD324F3AD7AA53994188EB0A4EAB
SHA-512:	1D960F04462CE871C74BD20015B7807E82C420EE2482E8376EEB69D5F73077F22B0ABFA3D70AC6F68A29A740132959E950879050D931C718E9FE030916513337
Malicious:	false
Reputation:	low
Preview:	2021/04/10-18:31:52.454 1048 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/04/10-18:31:52.455 1048 Recovering log #3.2021/04/10-18:31:52.455 1048 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\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	592
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E8E:8N
MD5:	B505641E5E90B7CF4BC869DD1B4BE451
SHA1:	0EC7B13DC043E054AB48B8F45FE49EF1209C01AA
SHA-256:	2755F85F14CF33404CEEBF053D0CB79DC3B98D643A51075737E6A5BE154FE1D9
SHA-512:	610AF095630C93B0586F4D9CA84FA75454C472C557D4FDBC0D5C1851F9AABF8653079A7ADE4659ABADDEDC2E02E58AD13C7244CD004B0AA5A462307F293F833
Malicious:	false
Reputation:	low
Preview:	.'..(.....'..(.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.204015744227386
Encrypted:	false
SSDEEP:	12:8va5KkkGHArBFUtpX5/P2T5f5KkkGHAryJ:Ga5KkkGgPgxif5KkkGga
MD5:	FC7C815AB991A63335D580108478C7E7
SHA1:	643DF66AD4DDEB7FE649281387C81004B0EF4D42
SHA-256:	56B7DE47080DAAAF94E3F8A540FF3B0F8F77B00FECCB27E98EEC6551236FD9A7
SHA-512:	3C582682EE39C3E085E18AE06A30FC0152234FDA73BFBCCEF15E6E8083870FA718CD619A6457836C9FEB80C85452C8E4FA210B19DE7AADB915C480682C46968
Malicious:	false
Reputation:	low
Preview:	2021/04/10-18:31:43.512 1048 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/04/10-18:31:43.516 1048 Recovering log #3.2021/04/10-18:31:43.517 1048 Reusing old log C:\Users\user\A ppData\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):	5.230639577689558
Encrypted:	false
SSDEEP:	12:ft+va5KkkGHArqiuFUtpxmW/PitV5f5KkkGHArq2J:faa5KkkGgCgfOf5KkkGg7
MD5:	10FA4694C2012CCB0F9F60CFA21CAA6B
SHA1:	F98186A80A5DD37B2AD5B869D24BD1F45CB4AB52
SHA-256:	574E78DA0DBBE1B1515710C58A86F8D0A43E22BF7C08A59097B659A3928AE7DF
SHA-512:	C2BB7B049E0F2590117A3E67CF870F4270869C507364637A8434DE2D4F0D961D1F9C4C6DA77AC41CC260B33ED7787F5EB6D25A4F7F7D6FAECE08C5C4DA3590
Malicious:	false
Reputation:	low
Preview:	2021/04/10-18:31:43.519 6cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Platform Notifications/MANIFEST-000001.2021/04/10-18:31:43.522 6cc Recovering log #3.2021/04/10-18:31:43.523 6cc Reusing old log C:\Users\user\AppData\Local \Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljl:5ljl
MD5:	E9C694B34731BF91073CF432768A9C44
SHA1:	861F5A99AD9EF017106CA6826EFE42413CDA1A0E
SHA-256:	01C766E2C0228436212045FA98D970A0AD1F1F73ABAA6A26E97C6639A4950D85
SHA-512:	2A359571C4326559459C881CBA4FF4FA9F312F6A7C2955B120B907430B700EA6FD42A48FBB3CC9F0CA2950D114DF036D1BB3B0618D137A36EBAAA17092FE5F0
Malicious:	false
Reputation:	low
Preview:	..&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.2077424305766895
Encrypted:	false
SSDEEP:	12:Fva5KkkGHArAFUtpNu1/Px5f5KkkGHArfJ:Ja5KkkGgkgC1f5KkkGgV
MD5:	FC026AF7517A2D724EE799C24EEC1D9F
SHA1:	9A11F7A436EB7EA71D75B517DC4E77E7AC32D941
SHA-256:	DBBE611676C20C95EB6E02D059B49A2DA7B650A28D3F222F1EFD7CF09D9A479D
SHA-512:	2BC004D0437F999F85AE171AEB36755546A9C26DE16E04330B0C3CDAF6F55E683D07AD14E0A8D80A3D99E8611CEFE7CD31DB38372772EC412C30119E30A0DC 7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Preview:	2021/04/10-18:31:58.779 1048 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/04/10-18:31:58.780 1048 Recovering log #3.2021/04/10-18:31:58.781 1048 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\cca0649a-926d-4838-9626-dc0d5176767d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF2124
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.207554197423216
Encrypted:	false
SSDEEP:	6:mLcUe+q2PWXp+N23iKKdKpIFUtpK+ZSZZmwPK+xVkwOWXp+N23iKKdKa/WLJ:FX+va5KkmFUtp70/P7xV5f5KkaUJ
MD5:	CC4F8E1B10AF744E3765499522311BD1
SHA1:	57AAEB13AB89C16556A0AF56AFA3F2BDE2461C82
SHA-256:	7E1FAE2728F423EF0DC187CF6FF26DFFA2EF251C810BA874172A0C9D91DC0FD3
SHA-512:	D5C49FA7B5967C730D3BD24F36488DEA1E0A037C4DB996242A327D1354FA6D58EEFD6EB0798EF21A4D0FB83FB387576FBC4E5D975DD02A9A77B7D4D3C51FA82B
Malicious:	false
Reputation:	low
Preview:	2021/04/10-18:31:36.009 162c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/04/10-18:31:36.011 162c Recovering log #3.2021/04/10-18:31:36.012 162c 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Entropy (8bit):	5.310437257691607
Encrypted:	false
SSDEEP:	12:/nDv+va5KkkOrsFUtpv/J/Pv/9V5f5KkkOrzJ:/Ya5Kk+g9f5Kkn
MD5:	77E47D58CA5CCD126C0181F53D4A6531
SHA1:	29EF530BDB1EF943F4727CC0737751D47ACDB3BF
SHA-256:	2CBF53BCBDA9ECBCF6195E7894F306945C949032EE406871273BA61DEEAB5684
SHA-512:	99FD56170B3F2E8D39B28F96913E763D3ABA6609E65B34E43710C436E91E59217E90B3854155E746DB38CF0B4FB202DAEAEE06A32591BECD80EFB6A167B3A44
Malicious:	false
Reputation:	low
Preview:	2021/04/10-18:31:44.530 fac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbm eomcjbeemfm/MANIFEST-000001.2021/04/10-18:31:44.532 fac Recovering log #3.2021/04/10-18:31:44.532 fac Reusing old log C:\Users\user\AppData\Local\Goog le\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):	24
Entropy (8bit):	3.9387218755408684
Encrypted:	false
SSDEEP:	3:20F38Ben:p8I
MD5:	4B6446EF89B18B89A943033D8F1D4038
SHA1:	538F9F9815E48FC9D55DF02C555FF970F7DBF509
SHA-256:	83BB08B324DEDCE61262B45124CC9BF456A69ACEDC347178F04CC10C30DD27ED
SHA-512:	7194E58A4E7FFB032DF4AA75246FC3E6C1E75EA4E4DE00282F16843BF820D89CB27FB330EA0BF7425C16752ACF4E3CEF482813431D1DC3B9F7DF14FE52E5B47 4
Malicious:	false
Reputation:	low
Preview:	.....[_.....k@.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\7ff924de-643d-42d2-a26e-4ddd3395252c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 13 icons, 8x8, 32 bits/pixel, 10x10, 32 bits/pixel
Category:	dropped
Size (bytes):	175509
Entropy (8bit):	5.489440694064333
Encrypted:	false
SSDEEP:	1536:rKbsLAR2A4VBQV1111111111111Nr366R6faFR+up0y0y2im1OsFcgYzQNL9X:rKbsLAR2fe/FZntrslfX
MD5:	33EABC19FDF40F3D36B6870EF5861957
SHA1:	CF3EF59C3940B58C314E9F6A1616751553F2D9A2
SHA-256:	647D07F37554672865902B2CEE80864B5A5283C372C7263BB1497D5582054E57
SHA-512:	47CFEDB1FDBC9BC09905C70F69A5114C64A8FC791BCA480D24972275276F00CEB230C579B4217337F9C69ECB2AB3221A3B549F06E8074D76BCE2F31773FB69F
Malicious:	false
Reputation:	low
Preview:	..... .H..... ..... .p..... .h...n..... ....n...((.... .h.....00.... ..%..~H..@@.... .(B..&n..``.... .....N..... .(....D..... .w`...M..(..... .....+.O-8&]P>/^Q?-^&:?I.1;<....qye.f.%.....X...E.....I...k}....{.m.t.CP.....E...\.....=H..,A..,J..;P.....nn p}nnp}.....~~~.....!...!---2---2... .....(..... .....!...7.#.:3,";3,!<.&'/.....NPLYt.F.K.%.....L..C.....1...`...KOPVutz}..A.BxX.....P.. .Q.....1...x...tqpyxuux...0D..DP.....G.....uojuppnw....t|..9F..-=..+:..5:..rr.....llkrkkmw.....ggitllkv.....hhgssss~.....YY\eYY[e..... ....nnnzXXXa.....RRR\.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\Chrome Web Store Payments.ico.md5	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16
Entropy (8bit):	4.0
Encrypted:	false
SSDEEP:	3:SeFcn:Sec
MD5:	61B979ECA159ECAC9C7F8F1D6FD43E9D
SHA1:	0373696351FC2172E811DA8393DEC84036FA34A0
SHA-256:	AB05E0A6FF7E8FFF89F924B279D93AFC72ACCE817C4D250C60BB8059CC534303
SHA-512:	C95825DA33CBDDFA627D9FF9A5B8371BC5F4E643A09573B6E1E839A83B619F53D878C344030B9701DCBC24D4CECCC016CF4D298D10EE8C37D1B5FEC1A5168 B6

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\Chrome Web Store Payments.ico.md5	
Malicious:	false
Reputation:	low
Preview:	F.....r...(R..

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):	4.425882596966453
Encrypted:	false
SSDEEP:	3:tUKOWLRXL9AWZmwv3sWLRXLVCPAA7V8ssWLRXLVCPAA7WGv:mMXLZZmwPZXLUPl7VvZXLUPl7tv
MD5:	B57C555C40399C995FFAEC68E959ED4F
SHA1:	AC4126895CC42F7854E05BE16BFBEE364C5BDE3D
SHA-256:	AB092B3F265E0B84924D1A96F723490E958EF7DF4E403B5C981DBB8152620897
SHA-512:	FE1C8E055A520ED5454572808C65B86A9AB21A7D638785B7B4BB2686EEB379E83A795AAEFDA809A5D29F089EB2ACD339AF64B306E80AA2F1A5E573E0BC6900F 9
Malicious:	false
Reputation:	low
Preview:	2021/04/10-18:31:42.774 1638 Recovering log #3.2021/04/10-18:31:42.823 1638 Delete type=0 #3.2021/04/10-18:31:42.823 1638 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKIVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF 04
Malicious:	false
Reputation:	low
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e26f1860-38b0-46b1-9521-0cb493f4dd9f.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):	5673
Entropy (8bit):	5.184882195373312
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e26f1860-38b0-46b1-9521-0cb493f4dd9f.tmp	
SSDEEP:	96:nxCV9nGBvfKGFjcVoook0JCKL8NGkP1jAbOTQVuwn:nxWGvf5Fjc04KwGkP9S
MD5:	111F46C8107044F9C3377593DC509516
SHA1:	10A7BF95ED8360C8A31AEEBC9CDDF526ACE40AD0
SHA-256:	4D2EC5E6EF13D92ACA9327E340EEE1551B2C85E7726708C09790A548FBA24BF4
SHA-512:	E07D2F369DFD2D827BAB0DAB85F02656C332C1E983DCFE292D31918657E24755E316F4ABB890511C6A7B75613BE9C13D6C950EF275B717FBEF546E8D1402824
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13262578296287581","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","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","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.191579401209878
Encrypted:	false
SSDEEP:	6:mMiSfSVq2PWXp+N23iKKdKfrzAdIFUtpZiQgZmwPZiQIkwOWXp+N23iKKdKfrzId:yVva5Kk9FUtptg/PtI5f5Kk2J
MD5:	3BA2B9BEC6088E6F189C3B81528D07CD
SHA1:	57BC74D5FF02732DF49C0975173B51E99D564EC9
SHA-256:	0004BF2616EF94C4D44A849683694CDD407BFCFD98712A7B18306B6C2DCBF398
SHA-512:	72C9569934DBFCBE066628190E6882E27166E0A0F9157182C0558D86CB853249AAED5B1579A44933D7CF7D7118A400B41CBF9230E1A9A1899D077223C22198B1
Malicious:	false
Reputation:	low
Preview:	2021/04/10-18:31:43.647 16a0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/04/10-18:31:43.648 16a0 Recovering log #3.2021/04/10-18:31:43.648 16a0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\b720e139-d126-48b9-b8da-d91fe153d714.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):	164170
Entropy (8bit):	6.0820782676726415
Encrypted:	false
SSDEEP:	3072:GPxlZM4iTMFp3l+7LSx8sogeFFcbXafIB0u1GOJmA3iuRM:kx4gMTo7Jsog0aqfIlUOoSiuRM
MD5:	F261EFDC4F50AE899FF1ECCEFA393347
SHA1:	9DE0EEB4211E9201B487448CD29ECE38930F0689
SHA-256:	2961B9B5AC6BD202F90B01447ECA92039E253D11BD27E642B2C9D9CDE8497ACE
SHA-512:	DC1263522541726AEC451D8471695D72B4D2164A0C09FA6AB124DFEA0228B4D49EAA7E3FAB1809891AE590B4D54ACA9F61D3437B7231D574BB047664BF81245
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":1.618104698837923e+12,"network":1.618072301e+12,"ticks":99831784.0,"uncertainty":4249483.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\fd952a64-a8b2-47e3-aaef-9027f236f4bd.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7463415414428103
Encrypted:	false
SSDEEP:	384:bjdmSszt8sLyVNurLvCK3BawZH0NG18rnUCUxpoo87rj2mfEnEWmalOgk2N71GfW:3SlpCw1BNOe7YCUQvDO2KAaS51
MD5:	D120E05FB455B67222C739843D7D2CED
SHA1:	FFB52C33C0FF7B979E4E68A3292A3A67CD79F242
SHA-256:	7CEC13E8B8779D66213FDE9C21D5A5441AB09C49383B3678BDD066BC848A7175
SHA-512:	337C36647E710EA951AE8B3F5326DE4F28C45B0C8F9895BF51F8A4B3FAA4B09B46C1D6205F9A8A60048D89D47840C77BD9E590F6C9EFB1BD17AFE38554BBAC52
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\Temp\052b5b32-1e9b-45a1-860c-db3c19cc6b7f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."I...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.I....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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\57b9baeb-b997-4dfe-98ba-d4e14c5da338.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3

C:\Users\user\AppData\Local\Temp\57b9baeb-b997-4dfe-98ba-d4e14c5da338.tmp	
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..''0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...'].....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\be4e925c-d05b-4f06-bf51-a693ba6aaec2.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\c9044496-1a15-4088-9094-fc1425747352.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\dca5c874-007b-4694-aa8a-a045c53f9a0f.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

C:\Users\user\AppData\Local\Temp\dca5c874-007b-4694-aa8a-a045c53f9a0f.tmp	
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\dfc40dfa-4014-4f9c-987f-19282c192d53.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_dir3560_1740971245\052b5b32-1e9b-45a1-860c-db3c19cc6b7f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L]....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.I....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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_dir3560_1740971245\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F770C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir3560_1740971245\CRX_INSTALL_locales\bg\messages.json	
Preview:	{.. "app_description": {.. "message": "..... . ... Chrome".. },.. "app_name": {.. "message": "..... . ... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "...., ...".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "...., ... Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3560_1740971245\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CE B4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "C onnecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3560_1740971245\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:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D84885 B
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed .".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3560_1740971245\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5 E0A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_u navailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be comp leted.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3560_1740971245\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB805 52
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_una vailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "The trans action could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3560_1740971245\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_unavail able": {.. "message": ". ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": ".. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3560_1740971245\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:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65 FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unava ilable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3560_1740971245\CRX_INSTALL_locales\en_GB\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false

C:\Users\user\AppData\Local\Temp\scoped_dir3560_1740971245\CRX_INSTALL_locales\en_GB\messages.json	
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_dir3560_1740971245\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_dir3560_1740971245\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_dir3560_1740971245\CRX_INSTALL_locales\et\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	595
Entropy (8bit):	4.467205425399467
Encrypted:	false
SSDEEP:	12:1HEJfPGGGfPG+WYpU34Ze7z+dgrW9O8ZpU34ZwZz03OyZnLAOfTYgoLIR:1HEdvqlWYpTeObk8ZpT/OGAOfuLIR
MD5:	CFF6CB76EC724B17C1BC920726CB35A7
SHA1:	14ED068251D65A840F00C05409D705259D329FFC
SHA-256:	C85800BF45942FCC7FD6B1DF929C25F9CC2A977A6678966BD03D4B6B69889AFD
SHA-512:	53D7D01BB30C0306DE65A79FD9551D2E8C1F71F4F45F71906B009071CB3E0F231E6A50FDD78773E9B4DE94085BC7B97F829842FA21A89A2080D33458B745C46F
Malicious:	false

C:\Users\user\AppData\Local\Temp\scoped_dir3560_1740971245\CRX_INSTALL_locales\et\messages.json	
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_dir3560_1740971245\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_dir3560_1740971245\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_dir3560_1740971245\CRX_INSTALL_locales\fr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	677
Entropy (8bit):	4.552569602149629
Encrypted:	false
SSDEEP:	12:1HEJALf/nbGGALf/nb+WYpU34Owdgbyb+dgdQjO8ZpU34ITQpGnbyb03OyZnLAO8:1HE4Hna1Hn6WYpNdgpY8ZpSTQwnBOGAh
MD5:	8D11C90F44A6585B57B933AB38D1FFF8
SHA1:	3F9D44EA8807069A32AACA2AAAD02FD892E6CC90
SHA-256:	599491F8C52B945C16C441ADF45BFD45AFAE046DA07757D97C56AF4DE75ED3B5
SHA-512:	D7EF7F5AD7EF1A1595825D79B69E2B1E988AD3CF1F3881496FCCD30F241E4E9C6E457F9F5D0F855DE3536DB7A40C3E1C55946B50D3F556F4A35285066A0CD6F
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "app_name": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "craw_app_unavailable": {.. "message": "Application indisponible pour le moment.".. },.. "craw_connect_to_network": {.. "message": "Veuillez vous connecter . un r.seau.".. },.. "iap_unavailable": {.. "message": "Les paiements via l'application ne sont pas disponibles pour le moment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Veuillez vous connecter . Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3560_1740971245\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_dir3560_1740971245\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_dir3560_1740971245\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_dir3560_1740971245\CRX_INSTALL_locales\id\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	604
Entropy (8bit):	4.465685261172395
Encrypted:	false
SSDEEP:	12:1HEJs25bGGs25b+WYpU34ORBHAeSJ+dgkmO8ZpU34s22C/SzFAs03OyZnLAOfTYR:1HEBaA6WYpaHFH8ZptOYOGAOf2D
MD5:	EAB2B946D1232AB98137E760954003AA

C:\Users\user\AppData\Local\Temp\scoped_dir3560_1740971245\CRX_INSTALL_locales\id\messages.json	
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_dir3560_1740971245\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_dir3560_1740971245\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_dir3560_1740971245\CRX_INSTALL_locales\ko\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	631
Entropy (8bit):	5.160315577642469
Encrypted:	false
SSDEEP:	12:1HEJ1GG1+WYpU34K3aT+dgh8d0HTO8ZpU34KaNkaT03OyZnLAOfTY/YeHx:1HEajWYpc3aSl0Hq8Zpc6kasOGAOfyYA
MD5:	9F6B4D82A70C74CA751E2EAE70FAB5CF
SHA1:	0534F125FFCE8222277CF2BE3401C59DAF9217F8
SHA-256:	D1467B8D037114403E8F4EFC52E88C4A7FEB96126BE4CFF883FEFF1084EF7E68
SHA-512:	ED9319830314385D09C06F62EE34186E8CA576C857981205E4468A28B3ACD2AB03384E77B866032C324ABDD97A56EFD08E2D6E0C79D563578B3EC52517819BD8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir3560_1740971245\CRX_INSTALL_locales\ko\messages.json	
Preview:	{.. "app_description": {.. "message": "Chrome . ... ..".. },.. "app_name": {.. "message": "Chrome . ... ..".. },.. "craw_app_unavailable": {.. "message": ".. .. ..".. },.. "craw_connect_to_network": {.. "message": "..... .....".. },.. "iap_unavailable": {.. "message": ".. .. ..".. },.. "jwt_retrieve_failed": {.. " message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Chrome. .....".. }..}..

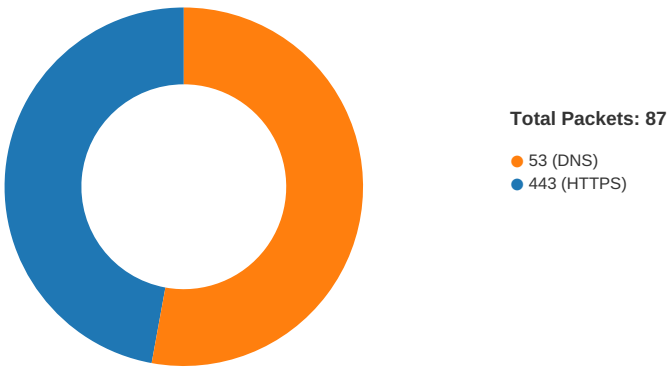
C:\Users\user\AppData\Local\Temp\scoped_dir3560_1740971245\CRX_INSTALL_locales\lt\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	665
Entropy (8bit):	4.66839186029557
Encrypted:	false
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..".. }..}..

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 10, 2021 18:31:39.620439053 CEST	49713	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:39.621692896 CEST	49715	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:39.639695883 CEST	443	49713	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:39.639821053 CEST	49713	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:39.640113115 CEST	49713	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:39.642219067 CEST	443	49715	13.32.25.32	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 10, 2021 18:31:39.642306089 CEST	49715	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:39.642564058 CEST	49715	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:39.659518003 CEST	443	49713	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:39.662132025 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:39.665505886 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:39.665544033 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:39.665584087 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:39.665637016 CEST	49715	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:39.665962934 CEST	443	49713	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:39.666002989 CEST	443	49713	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:39.666074038 CEST	49713	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:39.666135073 CEST	443	49713	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:39.669589996 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:39.669635057 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:39.669753075 CEST	49715	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:39.674254894 CEST	443	49713	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:39.674297094 CEST	443	49713	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:39.674366951 CEST	49713	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:39.727842093 CEST	49713	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:39.864106894 CEST	49715	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:39.864984989 CEST	49713	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:39.866626978 CEST	49713	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:39.866884947 CEST	49715	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:39.867521048 CEST	49715	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:39.884291887 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:39.884321928 CEST	443	49713	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:39.884392977 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:39.885502100 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:39.888353109 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:39.888524055 CEST	49715	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:39.892625093 CEST	443	49713	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:39.892683029 CEST	443	49713	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:39.892784119 CEST	49713	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:39.906188965 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:40.973056078 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:40.973093987 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:40.973233938 CEST	49715	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:41.059396029 CEST	49715	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:41.059608936 CEST	49715	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:41.077450037 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:41.077491045 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:41.529145002 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:41.533957958 CEST	49715	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:41.534497976 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:41.534539938 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:41.534570932 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:41.534625053 CEST	49715	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:41.534688950 CEST	49715	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:41.548674107 CEST	49715	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:41.552146912 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:41.566452026 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:41.620625973 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:41.620681047 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:41.620717049 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:41.620743036 CEST	49715	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:41.633099079 CEST	49729	443	192.168.2.3	104.16.19.94
Apr 10, 2021 18:31:41.645231962 CEST	443	49729	104.16.19.94	192.168.2.3
Apr 10, 2021 18:31:41.645355940 CEST	49729	443	192.168.2.3	104.16.19.94
Apr 10, 2021 18:31:41.645781040 CEST	49729	443	192.168.2.3	104.16.19.94
Apr 10, 2021 18:31:41.657840014 CEST	443	49729	104.16.19.94	192.168.2.3
Apr 10, 2021 18:31:41.660053015 CEST	443	49729	104.16.19.94	192.168.2.3
Apr 10, 2021 18:31:41.660101891 CEST	443	49729	104.16.19.94	192.168.2.3
Apr 10, 2021 18:31:41.660171986 CEST	49729	443	192.168.2.3	104.16.19.94
Apr 10, 2021 18:31:41.661227942 CEST	49715	443	192.168.2.3	13.32.25.32

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 10, 2021 18:31:41.670571089 CEST	49729	443	192.168.2.3	104.16.19.94
Apr 10, 2021 18:31:41.670638084 CEST	49729	443	192.168.2.3	104.16.19.94
Apr 10, 2021 18:31:41.670795918 CEST	49729	443	192.168.2.3	104.16.19.94
Apr 10, 2021 18:31:41.683047056 CEST	443	49729	104.16.19.94	192.168.2.3
Apr 10, 2021 18:31:41.683078051 CEST	443	49729	104.16.19.94	192.168.2.3
Apr 10, 2021 18:31:41.683104038 CEST	443	49729	104.16.19.94	192.168.2.3
Apr 10, 2021 18:31:41.684631109 CEST	443	49729	104.16.19.94	192.168.2.3
Apr 10, 2021 18:31:41.685018063 CEST	49729	443	192.168.2.3	104.16.19.94
Apr 10, 2021 18:31:41.696902037 CEST	443	49729	104.16.19.94	192.168.2.3
Apr 10, 2021 18:31:41.702744007 CEST	443	49729	104.16.19.94	192.168.2.3
Apr 10, 2021 18:31:41.702773094 CEST	443	49729	104.16.19.94	192.168.2.3
Apr 10, 2021 18:31:41.702835083 CEST	49729	443	192.168.2.3	104.16.19.94
Apr 10, 2021 18:31:41.702924013 CEST	443	49729	104.16.19.94	192.168.2.3
Apr 10, 2021 18:31:41.702950001 CEST	443	49729	104.16.19.94	192.168.2.3
Apr 10, 2021 18:31:41.702991962 CEST	443	49729	104.16.19.94	192.168.2.3
Apr 10, 2021 18:31:41.703003883 CEST	49729	443	192.168.2.3	104.16.19.94
Apr 10, 2021 18:31:41.703052998 CEST	443	49729	104.16.19.94	192.168.2.3
Apr 10, 2021 18:31:41.703083038 CEST	443	49729	104.16.19.94	192.168.2.3
Apr 10, 2021 18:31:41.703102112 CEST	49729	443	192.168.2.3	104.16.19.94
Apr 10, 2021 18:31:41.703140974 CEST	443	49729	104.16.19.94	192.168.2.3
Apr 10, 2021 18:31:41.703166008 CEST	443	49729	104.16.19.94	192.168.2.3
Apr 10, 2021 18:31:41.703186035 CEST	49729	443	192.168.2.3	104.16.19.94
Apr 10, 2021 18:31:41.719954967 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:41.720079899 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:41.720118999 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:41.720143080 CEST	49715	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:41.720915079 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:41.720942020 CEST	443	49715	13.32.25.32	192.168.2.3
Apr 10, 2021 18:31:41.720969915 CEST	49715	443	192.168.2.3	13.32.25.32
Apr 10, 2021 18:31:41.721098900 CEST	443	49715	13.32.25.32	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 10, 2021 18:31:34.465342045 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:34.478307009 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:35.778855085 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:35.793303013 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:36.493275881 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:36.506320000 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:37.982393980 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:37.995805979 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:39.589828968 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:39.590039015 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:39.593956947 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:39.595026016 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:39.605302095 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:39.618388891 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:39.618586063 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:39.635016918 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:39.651434898 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:39.666167974 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:39.913104057 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:39.925903082 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:40.010066986 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:40.036801100 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:40.602442026 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:40.616022110 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:41.584799051 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:41.610660076 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:41.612855911 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:41.631125927 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:41.815969944 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:41.830245018 CEST	53	54366	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 10, 2021 18:31:41.834912062 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:41.836055994 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:41.836683035 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:41.837358952 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:41.837943077 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:41.844810963 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:41.848454952 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:41.856635094 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:41.857285023 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:41.858272076 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:41.869654894 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:41.946146011 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:42.057667971 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:42.076186895 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:43.046200991 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:43.072274923 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:43.450035095 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:43.487526894 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:43.614146948 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:43.626813889 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:44.252995968 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:44.279469967 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:44.401398897 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:44.442807913 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:44.677030087 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:44.700192928 CEST	53	56338	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:44.703284979 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:44.716242075 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:44.721478939 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:44.748332977 CEST	63978	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:44.753220081 CEST	53	58784	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:44.770148993 CEST	53	63978	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:45.016000032 CEST	62938	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:45.042738914 CEST	53	62938	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:45.631997108 CEST	55708	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:45.658549070 CEST	53	55708	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:50.831976891 CEST	58306	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:31:50.844765902 CEST	53	58306	8.8.8.8	192.168.2.3
Apr 10, 2021 18:31:59.996721029 CEST	64124	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:32:00.008531094 CEST	53	64124	8.8.8.8	192.168.2.3
Apr 10, 2021 18:32:01.265034914 CEST	49361	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:32:01.277658939 CEST	53	49361	8.8.8.8	192.168.2.3
Apr 10, 2021 18:32:02.016628981 CEST	63150	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:32:02.029290915 CEST	53	63150	8.8.8.8	192.168.2.3
Apr 10, 2021 18:32:02.899852991 CEST	53279	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:32:02.913238049 CEST	53	53279	8.8.8.8	192.168.2.3
Apr 10, 2021 18:32:03.333820105 CEST	56881	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:32:03.347474098 CEST	53	56881	8.8.8.8	192.168.2.3
Apr 10, 2021 18:32:03.673780918 CEST	53642	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:32:03.746989012 CEST	53	53642	8.8.8.8	192.168.2.3
Apr 10, 2021 18:32:04.224579096 CEST	55667	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:32:04.237032890 CEST	53	55667	8.8.8.8	192.168.2.3
Apr 10, 2021 18:32:10.660020113 CEST	54833	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:32:10.672600985 CEST	53	54833	8.8.8.8	192.168.2.3
Apr 10, 2021 18:32:12.344064951 CEST	62476	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:32:12.357299089 CEST	53	62476	8.8.8.8	192.168.2.3
Apr 10, 2021 18:32:13.556206942 CEST	49705	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:32:13.569694042 CEST	53	49705	8.8.8.8	192.168.2.3
Apr 10, 2021 18:32:14.965076923 CEST	61477	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:32:14.977305889 CEST	53	61477	8.8.8.8	192.168.2.3
Apr 10, 2021 18:32:23.556159019 CEST	61633	53	192.168.2.3	8.8.8.8
Apr 10, 2021 18:32:23.574563026 CEST	53	61633	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 10, 2021 18:31:39.593956947 CEST	192.168.2.3	8.8.8.8	0xcfb9	Standard query (0)	main.d35pe6tu6wfnod.amplifyapp.com	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:41.612855911 CEST	192.168.2.3	8.8.8.8	0xa7f9	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:41.834912062 CEST	192.168.2.3	8.8.8.8	0x655e	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:41.836055994 CEST	192.168.2.3	8.8.8.8	0x8405	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:41.836683035 CEST	192.168.2.3	8.8.8.8	0x3d9b	Standard query (0)	srv-file8.gofile.io	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:41.837358952 CEST	192.168.2.3	8.8.8.8	0x2d71	Standard query (0)	i.ibb.co	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:41.837943077 CEST	192.168.2.3	8.8.8.8	0xd8ba	Standard query (0)	image.flaticon.com	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:41.844810963 CEST	192.168.2.3	8.8.8.8	0xa39f	Standard query (0)	i.stack.imgur.com	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:44.252995968 CEST	192.168.2.3	8.8.8.8	0x9a93	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:44.677030087 CEST	192.168.2.3	8.8.8.8	0xf55a	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:44.703284979 CEST	192.168.2.3	8.8.8.8	0xa20d	Standard query (0)	i.ibb.co	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:44.721478939 CEST	192.168.2.3	8.8.8.8	0xc795	Standard query (0)	srv-file8.gofile.io	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:44.748332977 CEST	192.168.2.3	8.8.8.8	0x1c01	Standard query (0)	image.flaticon.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 10, 2021 18:31:39.618388891 CEST	8.8.8.8	192.168.2.3	0xcfb9	No error (0)	main.d35pe6tu6wfnod.amplifyapp.com		13.32.25.32	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:39.618388891 CEST	8.8.8.8	192.168.2.3	0xcfb9	No error (0)	main.d35pe6tu6wfnod.amplifyapp.com		13.32.25.39	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:39.618388891 CEST	8.8.8.8	192.168.2.3	0xcfb9	No error (0)	main.d35pe6tu6wfnod.amplifyapp.com		13.32.25.58	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:39.618388891 CEST	8.8.8.8	192.168.2.3	0xcfb9	No error (0)	main.d35pe6tu6wfnod.amplifyapp.com		13.32.25.2	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:41.631125927 CEST	8.8.8.8	192.168.2.3	0xa7f9	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:41.631125927 CEST	8.8.8.8	192.168.2.3	0xa7f9	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:41.848454952 CEST	8.8.8.8	192.168.2.3	0x8405	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Apr 10, 2021 18:31:41.856635094 CEST	8.8.8.8	192.168.2.3	0xd8ba	No error (0)	image.flaticon.com	cdn4.thumbrio.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Apr 10, 2021 18:31:41.857285023 CEST	8.8.8.8	192.168.2.3	0xa39f	No error (0)	i.stack.imgur.com	ipv4.imgur.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Apr 10, 2021 18:31:41.857285023 CEST	8.8.8.8	192.168.2.3	0xa39f	No error (0)	ipv4.imgur.map.fastly.net		151.101.112.193	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:41.858272076 CEST	8.8.8.8	192.168.2.3	0x655e	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Apr 10, 2021 18:31:41.858272076 CEST	8.8.8.8	192.168.2.3	0x655e	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:41.869654894 CEST	8.8.8.8	192.168.2.3	0x3d9b	No error (0)	srv-file8.gofile.io		144.76.69.233	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:41.946146011 CEST	8.8.8.8	192.168.2.3	0x2d71	No error (0)	i.ibb.co		146.59.152.166	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:41.946146011 CEST	8.8.8.8	192.168.2.3	0x2d71	No error (0)	i.ibb.co		146.59.152.166	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 10, 2021 18:31:41.946146011 CEST	8.8.8.8	192.168.2.3	0x2d71	No error (0)	i.ibb.co		145.239.131.51	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:41.946146011 CEST	8.8.8.8	192.168.2.3	0x2d71	No error (0)	i.ibb.co		145.239.131.55	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:41.946146011 CEST	8.8.8.8	192.168.2.3	0x2d71	No error (0)	i.ibb.co		145.239.131.60	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:44.279469967 CEST	8.8.8.8	192.168.2.3	0x9a93	No error (0)	clients2.google.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Apr 10, 2021 18:31:44.279469967 CEST	8.8.8.8	192.168.2.3	0x9a93	No error (0)	googlehosted.l.google.com		172.217.168.33	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:44.700192928 CEST	8.8.8.8	192.168.2.3	0xf55a	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Apr 10, 2021 18:31:44.700192928 CEST	8.8.8.8	192.168.2.3	0xf55a	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:44.716242075 CEST	8.8.8.8	192.168.2.3	0xa20d	No error (0)	i.ibb.co		146.59.152.166	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:44.716242075 CEST	8.8.8.8	192.168.2.3	0xa20d	No error (0)	i.ibb.co		146.59.152.166	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:44.716242075 CEST	8.8.8.8	192.168.2.3	0xa20d	No error (0)	i.ibb.co		145.239.131.51	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:44.716242075 CEST	8.8.8.8	192.168.2.3	0xa20d	No error (0)	i.ibb.co		145.239.131.55	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:44.716242075 CEST	8.8.8.8	192.168.2.3	0xa20d	No error (0)	i.ibb.co		145.239.131.60	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:44.753220081 CEST	8.8.8.8	192.168.2.3	0xc795	No error (0)	srv-file8.gofile.io		144.76.69.233	A (IP address)	IN (0x0001)
Apr 10, 2021 18:31:44.770148993 CEST	8.8.8.8	192.168.2.3	0x1c01	No error (0)	image.flaticon.com	cdn4.thumbrio.edgekey.net		CNAME (Canonical name)	IN (0x0001)

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 10, 2021 18:31:41.900393009 CEST	151.101.112.193	443	192.168.2.3	49733	CN=i.stack.imgur.com, O="Imgur, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, 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	Mon Oct 19 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Sat Nov 20 00:59:59 CET 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					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		
Apr 10, 2021 18:31:44.873369932 CEST	144.76.69.233	443	192.168.2.3	49751	CN=srv-file8.gofile.io CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Feb 16 15:47:42 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Mon May 17 16:47:42 CEST 2021 Wed Sep 29 21:21:40 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=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior

System Behavior

Analysis Process: chrome.exe PID: 3560 Parent PID: 4420

General

Start time:	18:31:35
Start date:	10/04/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://main.d35pe6tu6wfnod.amplifyapp.com'
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: chrome.exe PID: 4404 Parent PID: 3560

General

Start time:	18:31:36
Start date:	10/04/2021
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=1544,7093597635801048285,11986457263259393063,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1680 /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