

ID: 383614
Cookbook: browseurl.jbs
Time: 02:54:27
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2

Analysis Report https://firebasestorage.googleapis.com/v0/b/kcdvdjv037jcdi0e3767933.appspot.com/o/!}{%24%23%40^%26 jaf%40!__} .html?alt=media&token=08503d5e-c8e8-4a7c-b39c-8a3de4c0bf78#jason.maddern@navitas.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 8
- Domains and IPs 8
  - Contacted Domains 8
  - URLs from Memory and Binaries 8
  - Contacted IPs 8
  - Public 9
  - Private 9
- General Information 9
- Simulations 10
  - 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 42
  - UDP Packets 43
  - DNS Queries 45
  - DNS Answers 45
  - HTTPS Packets 45
- Code Manipulations 46
- Statistics 46
  - Behavior 46
- System Behavior 46
  - Analysis Process: chrome.exe PID: 5636 Parent PID: 3396 46
    - General 46
    - File Activities 47
    - Registry Activities 47
  - Analysis Process: chrome.exe PID: 3952 Parent PID: 5636 47

Copyright Joe Security LLC 2021

General 47
File Activities 47
Registry Activities 47
Disassembly 47

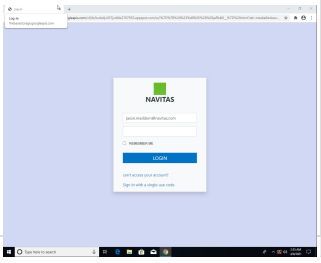
Analysis Report https://firebasestorage.googleapis.com…

Overview

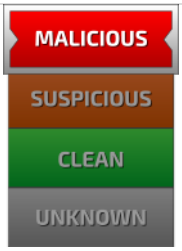
General Information

Sample URL:	https://firebasestorage.googleapis.com/v0/b/kcdvdjv037jcdi0e3767933.appspot...=media&token=08503d5e-c8e8-4a7c-b39c-8a3de4c0bf78#jason.maddern@navitas.com
Analysis ID:	383614
Infos:	

Most interesting Screenshot:



Detection



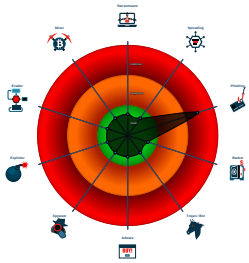
HTMLPhisher

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Phishing URL detected (based on va…
- Yara detected HtmlPhish10
- HTML body contains low number of …
- HTML title does not match URL
- URL contains potential PII (phishing…

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 5636 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://firebasestorage.googleapis.com/v0/b/kcdvdjv037jcdi0e3767933.appspot.com/o/!%7D%7B%24%23%40%5E%26%20jaf%40!__%7D%20.html?alt=media&token=08503d5e-c8e8-4a7c-b39c-8a3de4c0bf78#jason.maddern@navitas.com' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 3952 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1616,10129630995323838965,6101514469676002512,131072 --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

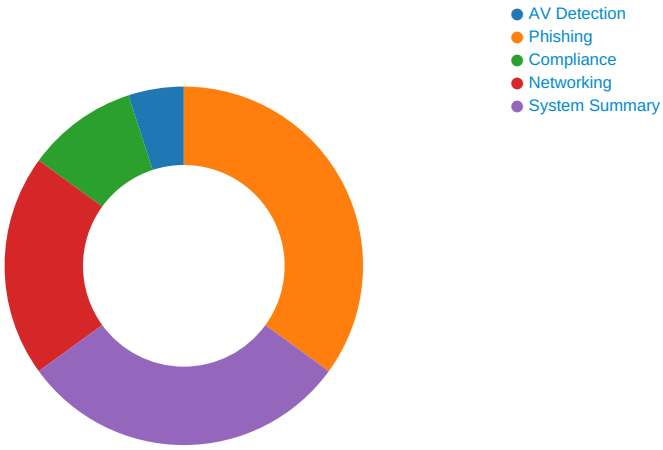
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Copyright Joe Security LLC 2021



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Phishing:

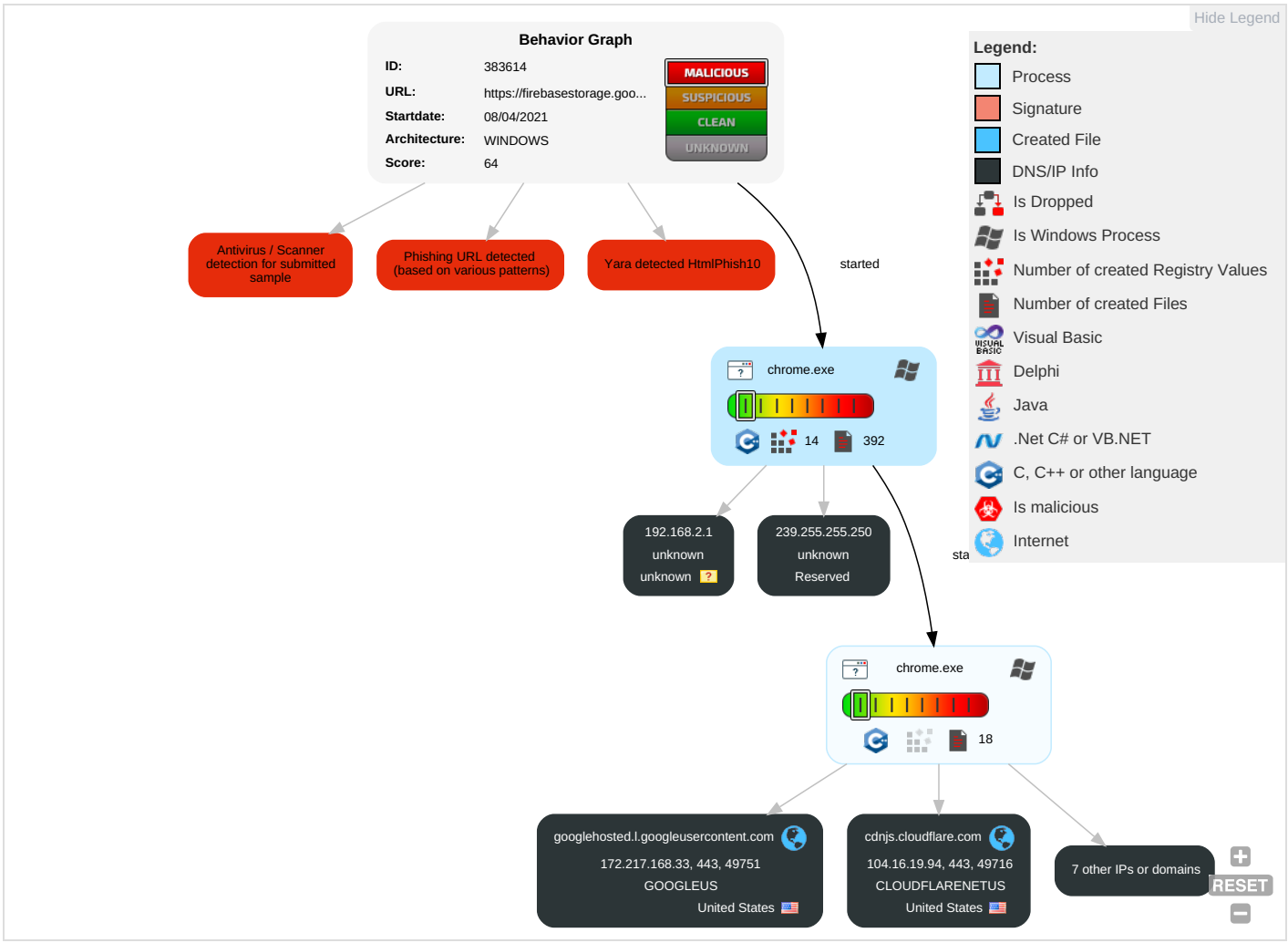
Phishing URL detected (based on various patterns)

Yara detected HtmlPhish10

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

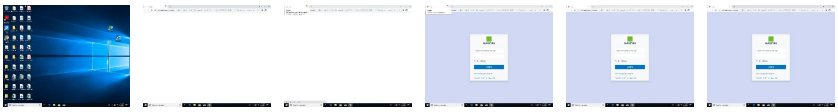
Behavior Graph

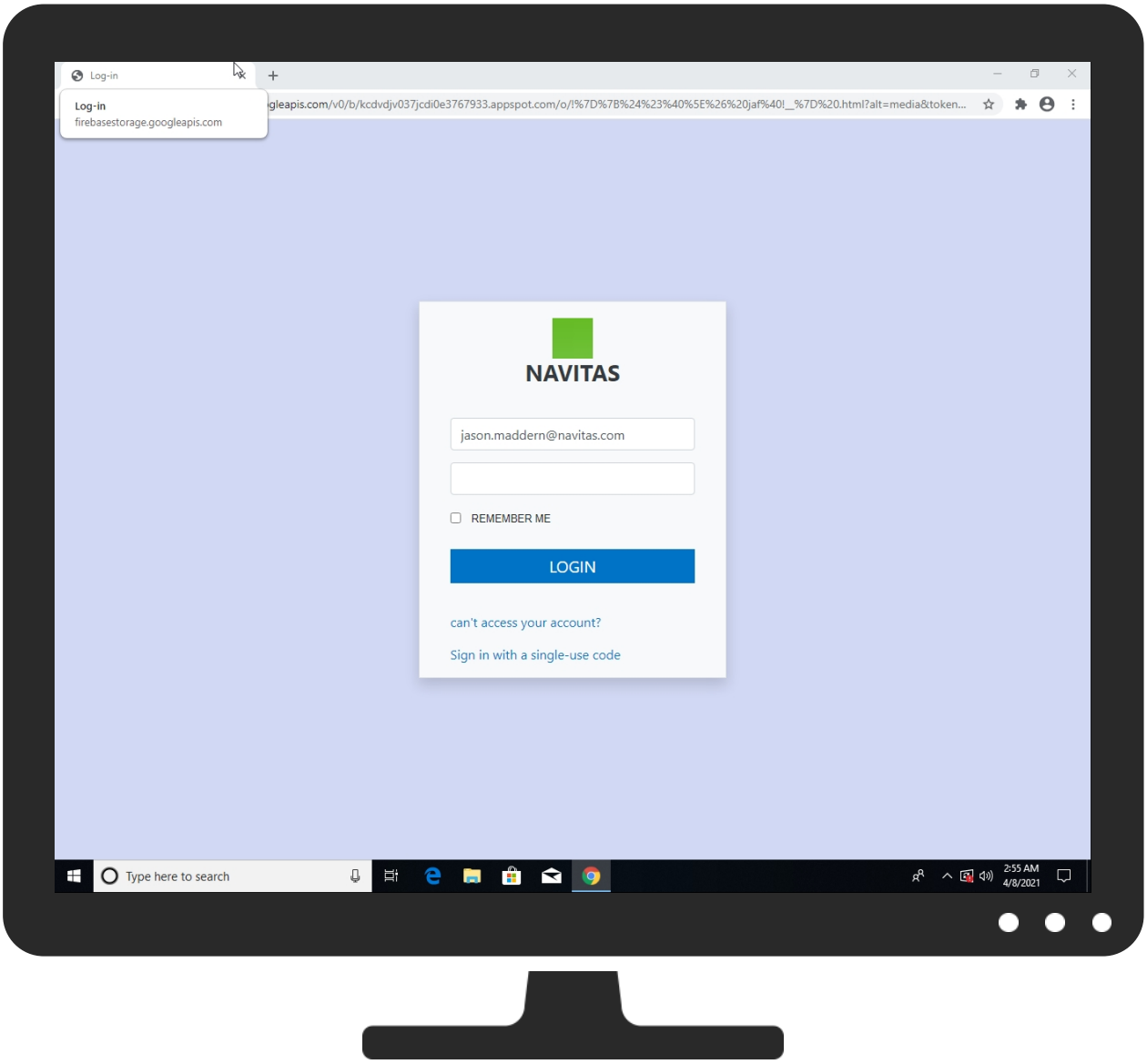


Screenshots

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://firebasestorage.googleapis.com/v0/b/kcdvdjv037jcdi0e3767933.appspot.com/o/!%7D%7B%24%23%40%5E%26%20jaf%40!__%7D%20.html?alt=media&token=08503d5e-c8e8-4a7c-b39c-8a3de4c0bf78#jason.maddern@navitas.com	2%	Virustotal		Browse
http://https://firebasestorage.googleapis.com/v0/b/kcdvdjv037jcdi0e3767933.appspot.com/o/!%7D%7B%24%23%40%5E%26%20jaf%40!__%7D%20.html?alt=media&token=08503d5e-c8e8-4a7c-b39c-8a3de4c0bf78#jason.maddern@navitas.com	0%	Avira URL Cloud	safe	
http://https://firebasestorage.googleapis.com/v0/b/kcdvdjv037jcdi0e3767933.appspot.com/o/!%7D%7B%24%23%40%5E%26%20jaf%40!__%7D%20.html?alt=media&token=08503d5e-c8e8-4a7c-b39c-8a3de4c0bf78#jason.maddern@navitas.com	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	

Domains and IPs

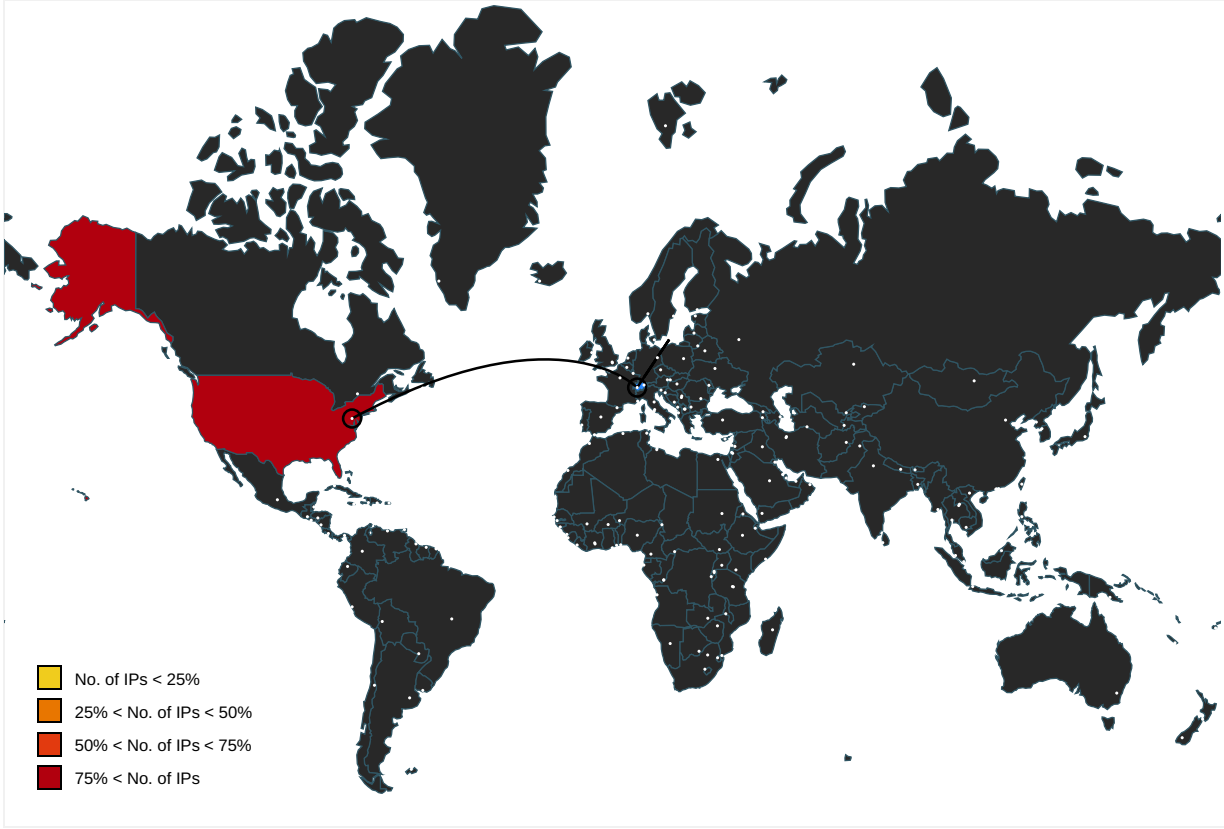
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
stackpath.bootstrapcdn.com	104.18.10.207	true	false		high
s3.amazonaws.com	52.217.76.78	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high
googlehosted.l.googleusercontent.com	172.217.168.33	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
cdn.jsdelivr.net	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	300c7021-d8b9-48a6-a74b-12782d b4358e.tmp.1.dr, 191ba0ee-a227-4778-aa0f-376ebe1a9c61.tmp.1.dr, 268198b6-5f46-4002-a89a-35bece8dc8ab.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js	e47a33ac8e679b3a_0.0.dr	false		high
http://https://clients2.googleusercontent.com	300c7021-d8b9-48a6-a74b-12782d b4358e.tmp.1.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js	f8d798d069065fcb_0.0.dr	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js	3e29eaa8f606a452_0.0.dr	false		high
http://https://code.jquery.com/jquery-3.2.1.slim.min.js	bc5a8aa50bf25355_0.0.dr	false		high
http://https://a.nel.cloudflare.com/report?s=xkpt82MHHMv3muDjCOwvAAgdJpt8uB5ERV7nx2Iz%2BKCgOGTBJFWZlxkLW2eh	Reporting and NEL.1.dr	false		high
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://cdn.jsdelivr.net/npm/jquery.session	75ea7cb2dc185fee_0.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.10.207	stackpath.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.217.168.33	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
52.217.76.78	s3.amazonaws.com	United States		16509	AMAZON-02US	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:	383614
Start date:	08.04.2021
Start time:	02:54:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://firebasestorage.googleapis.com/v0/b/kcdvdjv037jcdi0e3767933.appspot.com/o/!}{%24%23%40^%26 jaf%40!__} .html?alt=media&token=08503d5e-c8e8-4a7c-b39c-8a3de4c0bf78#jason.maddern@navitas.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

Copyright Joe Security LLC 2021

Number of analysed new started processes analysed:	13
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.phis.win@28/171@7/7
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): 204.79.197.200, 13.107.21.200, 104.42.151.234, 52.255.188.83, 23.54.113.53, 172.217.168.13, 216.58.215.238, 216.58.215.234, 173.194.160.74, 142.250.34.2, 172.217.168.10, 69.16.175.10, 69.16.175.42, 104.16.87.20, 104.16.86.20, 104.16.89.20, 104.16.85.20, 104.16.88.20, 13.88.21.125, 216.58.215.227, 23.0.174.185, 23.0.174.200, 172.217.168.4, 172.217.168.35, 52.147.198.201, 172.217.168.42, 172.217.168.74, 23.54.113.104, 20.50.102.62, 23.10.249.26, 23.10.249.43 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, au.download.windowsupdate.com.edgesuite.net, cds.s5x3j6q5.hwcdn.net, cdn.jsdelivr.net.cdn.cloudflare.net, arc.msn.com.nsatc.net, r5.sn-1gi7znes.gvt1.com, store-images.s-microsoft.com-c.edgekey.net, clientservices.googleapis.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, clients2.google.com, redirector.gvt1.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, www.google.com, 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, firebasestorage.googleapis.com, www.bing.com, fonts.googleapis.com, fs.microsoft.com, accounts.google.com, content-autofill.googleapis.com, dual-a-0001.a-msedge.net, ajax.googleapis.com, fonts.gstatic.com, r5---sn-1gi7znes.gvt1.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, www.googleapis.com, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, clients.l.google.com, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.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
02:55:14	API Interceptor	1x 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
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
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):	326
Entropy (8bit):	3.11466556781601
Encrypted:	false
SSDEEP:	6:kKmLkwTJ0N+SkQlPlEGYRMY9z+4KlDA3RUe0ht:bwTJrkPlE99SNxAhUe0ht
MD5:	1E27546CDC2820977DB5CE237D8BD07C
SHA1:	07D4981183DEC08CF22C831B0B70194CBD54ED4F
SHA-256:	44EC9D41FD288B2EE9F6F04FE63A753EF0CF90EDFD9E288403F6739E99588E2B
SHA-512:	FDF151FE78846B39A1E6DF3AAF94401657C13B55B6FA027ADB9311EB23BFCE8236B5BD55B608969CFC284741447763F02CD6C32FEC25257EAC797AD61F27443
Malicious:	false
Reputation:	low
Preview:	p..... .....6.E],..(..... ....$.....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."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\0869d031-5cb1-4aa4-82f8-d9dea2ef6fa2.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7465896143586006
Encrypted:	false
SSDEEP:	384:OujN/mSszt8sLyVNurLvCK3BawZH0NG18rnUCUxpoo87rj2mfEnEWmalOgk2N71K:OMSlpCw1BNOe7YCUQvDO2KAaS5s
MD5:	8D656DF669EEC3D51BFB73316CE3F688
SHA1:	0EE6FD7B84811B5349C5E9817867007779AD276B
SHA-256:	DE4635FB463C1107CDE53D787C2CA88960B3B52AC80A59BF13EAC94284F4644F
SHA-512:	F10B487603FD85D814ABD5012F97534BCBB238DC37FA29A5C5AD8198E13708B15D430A804D95C5670670B61EC4E64EA21E6AB900F16493D3561508B23EA07178
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....68.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\3131b0ff-c790-4d91-b772-b2d4467228f9.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):	355036
Entropy (8bit):	6.015591409292401
Encrypted:	false
SSDEEP:	6144:T6Q1sJQHD8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBn:2TowxzurRDn9nfNxF4ijZVtilBn
MD5:	CB73CFE403298C4FE225C46574A3EC94
SHA1:	490177EBDD408808C205075F3B5197A350F6FED0
SHA-256:	8F7E1F42EFDCE0FF76E892A2BEAF8CA2362AF71D1B4F3C8D783FBF29D1EF976F
SHA-512:	5A35A38E0C7D89CCA47DF3E0FAB1ADFAE7F1FEBFEB938D20511FC764B57AA122718A7F05AA4ABAAD8006878B5D3ACAECCA88FD952D3BE3CFAE52F688A52E 0F64

C:\Users\user\AppData\Local\Google\Chrome\User Data\3131b0ff-c790-4d91-b772-b2d4467228f9.tmp	
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":1.617875714203851e+12,"network":1.617843316e+12,"ticks":103176853.0,"uncertainty":4282600.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13262349311230

C:\Users\user\AppData\Local\Google\Chrome\User Data\6380d18b-7640-4e6a-9d86-f1cc0c30b22e.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):	355036
Entropy (8bit):	6.015591286334234
Encrypted:	false
SSDEEP:	6144:56Q1sJQHD8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBn:UTowxzurRDn9nfNxF4ijZVtilBn
MD5:	D8411B26BFD7E702BAEA4E5F55BE1546
SHA1:	1B7CC9445A4382BBE3DEE37B4D8D585C124BE7F8
SHA-256:	F43388AE4691724B2DB1116FA95A2560BF587D9594062CE59011094DA2C53CCB
SHA-512:	C9B55182BD3400E02761882AC1F11ED0185B9B3482E39BF6A24E80CE166850C9FC6701A92A02CD94291AB8FBEC7FAAC7287599618859A4D9421EEA4F1DF829B
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":1.617875714203851e+12,"network":1.617843316e+12,"ticks":103176853.0,"uncertainty":4282600.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075278957"},"policy":{"last_statistics_update":"13262349311230

C:\Users\user\AppData\Local\Google\Chrome\User Data\68ece7bf-824a-44e5-a2cc-99f6b611d946.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):	355036
Entropy (8bit):	6.015591056736498
Encrypted:	false
SSDEEP:	6144:N6Q1sJQHD8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBn:4TowxzurRDn9nfNxF4ijZVtilBn
MD5:	03A3052F64E99C0B4ABD3D13774A079E
SHA1:	5EE38C6CCA0A1516646CF73BAB48F30BCDB9EA2F
SHA-256:	F37BB357E1B33D29BD251207084C700C0A2BB56918F2356DF8A16F2981D94A5D
SHA-512:	160F05871EB6AEED27F07A2D7C186FE294951D16F76064E7BD9CA10062FFCA2DC7159776CB8FFE5AFBC4AD0C5DABE14C3C8685DE06B13E0E9BC45182D213E95
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":1.617875714203851e+12,"network":1.617843316e+12,"ticks":103176853.0,"uncertainty":4282600.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13262349311230

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXYDu6cR9iTXYDu6cR9iTXYDu6cR9n:+Y66cR4TXY66cR4TXY66cR9
MD5:	569FA64ACAA310B1DE1A6250CC7356B0
SHA1:	14251450C245F8612958BF94779E8B72AE6D6213
SHA-256:	AEE20ADEBF2D35EB8A39BE2DC391B0E5966EFCB4AFDC971BB3A18115C929F563
SHA-512:	850914A053EF541046B29260266C17FEFF2466A87784394F9AB3B565D2EA1E656F61F02BDB78F9F9676E90365F837F3709BCC0856B3B844256848F477250E0C7
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Reputation:	low
Preview:	sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1574577d-1303-4360-b2d2-7a001c227c51.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):	4996
Entropy (8bit):	4.960640809221
Encrypted:	false
SSDEEP:	96:nOF3GG4pSVFZlk0JCKL8UgkQS11PbOTQVuwn:nO34pS9C4Kukv7
MD5:	3CC71172C5C5D0EC6C6D5C60F8B2C4E8
SHA1:	6C6FE2BF0E84C7B42BDE5182225A677731D7159C
SHA-256:	0075FA52956E2D43128B83375019EAAD84453A7B99A6F43E50413189B20A97D2
SHA-512:	F086831D3EF33FF4900A4F5916EC4EE1E02B86AC6B0D13F56146321CC492673443DAC8B498F5D7CC5E86FE7A8F36BB067C62FB3C6500B33EA42EBF57E304392
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13262349311577523","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","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","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\300c7021-d8b9-48a6-a74b-12782db4358e.tmp	
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\39ca5eea-0084-47b0-a549-5f4c8acb9dde.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):	5.577758059078742
Encrypted:	false
SSDEEP:	48:Y7mcRUPfVwUK6UUhUKU7UoUeCwDbwUisYU3Ueh:ARUPuUfUUuKU7UoUHwQU/YU3Uc
MD5:	651CCA9D296F766AF29E71C34B169610
SHA1:	5E69722E68629492AF863220A7129F290F65009E
SHA-256:	41A68444EAB19EFE1FDDD9C79661B045272BC611F4C2750963B71C27745565CA
SHA-512:	3241F019BFA0204513C5380947EEACA7855BDC086C0352DFB7A21F2F1CC18ACE4B18808005D694D3C8228D20ADB7C9D427DBCE64C6D7F016D633271253E6DBD
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1649411714.44578,"host":"AKBA0EXj1W1QmJumkxUOTpibibkAwoUEp1CDrh5UFWY=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1617875714.445786},{"expiry":1633655714.437222,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617875714.437226},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1649411714.288309,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617875714.288313},{"expiry":1649411714.439959,"host":"qaDeFdT1UTirY0OQe+c5LKw+zjx6vF/+3vFh7CgrAOY=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1617875714.439963},{"expiry":1633013040.850112,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\43d3f142-9db5-407e-9615-b4eab73bf2c0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	22596
Entropy (8bit):	5.5353569386038615
Encrypted:	false
SSDEEP:	384:YoBtJlIS1Xr1kXqKf/pUZNCgVLH2HfDRrUBHGmnT8laW4I:hLlir1kXqKf/pUZNCgVLH2HfFrU1Gmn4
MD5:	3B2EE60C7325F31D728202707B39E69C
SHA1:	7EA2E31179CDBA2C75620B0AEC3C8AD20F918539
SHA-256:	A51778BD72C169E63C09E16516D9D46C427894101BD7DA00DCB6AA3357E8A047
SHA-512:	A616998E14DFFE69B49B6F31DC67B90E07C5E657F8E15654AB4FA4D7B96EBC818CF8158F7DC4FEDE2B7E1F56AEBA1AC4F187B38A175BDE2E080696D38C8D13AA
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":"13262349311303497","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\9ff5ae1b-f9b3-4e3f-a917-fd60ed51fb99.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9ff5ae1b-f9b3-4e3f-a917-fd60ed51fb99.tmp	
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):	336
Entropy (8bit):	5.194137533123134
Encrypted:	false
SSDEEP:	6:m1oXfFwa84q2P923iKKdK9RXXTZIFUtpkoXfFw1NJZmwPkoXfFwRMLDkwO923iK1:zPP84v45Kk7XT2FUtpjP8NJ/PjP2iD5D
MD5:	55E3410F2E962A526E3810C3B2BF9185
SHA1:	3ED6EFB468F0F69A203A7F9A99D19DA63874AE6A
SHA-256:	CE83FFDF4C2D66335F93733CF17CB2FAF21A6C1DD1D2A0C272EF5BE5FF61586F
SHA-512:	17B9F59BCDB543D83135BFCC7EFF98903DFD1AF0162BFAAB53A07F36E0209F4E3C2D658D427AFC0359AE0ACFE7C9687822FAB9060740D223B9B8D59BA94048 4
Malicious:	false
Reputation:	low
Preview:	2021/04/08-02:55:30.003 1464 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/ 04/08-02:55:30.056 1464 Recovering log #3.2021/04/08-02:55:30.277 1464 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrik eDatabase/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):	320
Entropy (8bit):	5.214993309630812
Encrypted:	false
SSDEEP:	6:m1oXfFSeX4q2P923iKKdKyDZIFUtpkoXfFlc8JZmwPkoXfFlc8DkwO923iKKdKyX:zPYeX4v45Kk02FUtpjPKJ/PjPKD5L5K1
MD5:	664813A33160AF849875B3E5E13AC801
SHA1:	DD0FF8476B1D9E220D0BBFE1AB2D046E3156029D
SHA-256:	BF68360E03DCC447B2EC2BFCE01D3A07FF8F11E7A3CDB5EBE8191368ABC9D8C4
SHA-512:	2C0C333E4E7604547A06A621CC02EEC0E4643AEAD2E366919E0539757CB9900892D3B730184630F89A4D2A292596A55735924A38F06A1E63931F993508AE7042
Malicious:	false
Reputation:	low
Preview:	2021/04/08-02:55:29.949 1464 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/04/08-02 :55:29.951 1464 Recovering log #3.2021/04/08-02:55:29.951 1464 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatab ase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3e29eaa8f606a452_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	244
Entropy (8bit):	5.3843324456341835
Encrypted:	false
SSDEEP:	6:mko/lXY68E9xEEUgLErtElLZH3u6oM+DzaEYZJhK6t:O/DYg5JZXuZHzaEc
MD5:	5BCA015B853276AB306878D5241705B4
SHA1:	8147F326B0F750F0E26ABB90027DC50212C42D23
SHA-256:	DF1637A8D84EEDA4DC9B21A89A79B79D74B7324E4706FE572E26C06760A18F11
SHA-512:	68CDC16426D015DE5818EE946B016745294AD3F967828052ADDACBB156CE0F02E47BD2EFCFF4A5DEF731228D54C580470E9B538F4AE3891804B0D61417A9E98
Malicious:	false
Reputation:	low
Preview:	0\r..m.....p...\5.h...._keyhttps://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js .https://firebasestorage.googleapis.com/...S../.....=u.U.uL..l...8.t..&..- E.z.c....A..Eo.....C.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\56aefa09742044bf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	241
Entropy (8bit):	5.581649125841777
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\56aefa09742044bf_0	
SSDEEP:	6:m0l/VYSHT8NWQAlKPUQykElLZHjS6EnnDx6Wt4ZG5RK6t:Dz8NWQCUUPJZe3nDnNr
MD5:	661876A98B625656C815F0DAFA6DEC71
SHA1:	57144512BCA5EB753111EAD813BBAB2837D31678
SHA-256:	8FA7BC3AE827CFC4044AB127529411AD9C0246CBF18EF10B2F96038F85C13757
SHA-512:	65BA2758223CDCAF97874E7AF74FE5D8390862318532583E8CF1FF08AEE4E79785068CBAE52B52A78D802C90901CD0B5A5AA3EBEAA7DF2F17465918686C60B3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m...0.;...._keyhttps://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js .https://firebasestorage.googleapis.com/~..S../.....!.....P..[..IQ_...U+'..L..TH. .A..Eo.....H.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\75ea7cb2dc185fee_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	248
Entropy (8bit):	5.5286513702298254
Encrypted:	false
SSDEEP:	6:mRyEYEmtANXL3XMHFElLZHDK6cX2ctQq7FTbK6t:z0yAhLMH+JZ2vZ7f
MD5:	3018F1E4B23CBD1B92857BD9DE441FF3
SHA1:	CF1CBBC2316C360A700ABB23F119882A6B6846CE
SHA-256:	E10AD3E234468BFE7BE8CB0CC82CCB0A1A1F48A07C0C44CAD618BD9AFCB34916
SHA-512:	2566ADAC275C5D723DF1BF51B716E9F349C5496F1B45898DEDF666298C6EEBD6D9B9FAC455779BB63F4531A750DCDD5AAEF993F0F4A5EA03FE49C92E5255E9 B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....t.....P...._keyhttps://cdn.jsdelivr.net/npm/jquery.session@1.0.0/jquery.session.min.js .https://firebasestorage.googleapis.com/...S../.....W...y+..@..(. .....KQQ'd..t.#..A..Eo.....%.W.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bc5a8aa50bf25355_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	225
Entropy (8bit):	5.580386289481337
Encrypted:	false
SSDEEP:	3:m+lFKs8RzYP2FycyGYWCULLuFvDCHElMKKhmHWlHCwkMOAPu2iV7XdGoMmtgztpD:mVYerCUlElLZHtwkMOAoVZ/ntgnK6t
MD5:	20E25BD20E41AD1B22793566748B713A
SHA1:	5B8FDD8FD9A59E2C7CA1158D1D996CDE2F7F640F
SHA-256:	8B33D6DE7B11669D5A220F0B28B8D605717A61D35DAA1E0E68ABF898DECA85C4
SHA-512:	45C3883170AC45C08BC86CE6C63B2A7AFB5CE0AEEE07D90C4EF9B35CFF097DFE64BF3EE24587793140CCA1F05A0B798E1C964ABB24898FEAB82956930F4661 4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]....%....._keyhttps://code.jquery.com/jquery-3.2.1.slim.min.js .https://firebasestorage.googleapis.com/#M.S../.....k..V...CLa;8...-...v.7K...<L{..A..Eo.....T. p.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e47a33ac8e679b3a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.349652914115175
Encrypted:	false
SSDEEP:	6:mDgEVYkb8E9xEvAErtElLZH9zgL7K6Sklt/qpe4iPiaoAXLK6t:Uggv4oJZxgPKUciOi9
MD5:	E74C863DD650A0CB7F7A189F468DE0F4
SHA1:	9CDCF2A80C67DA68658DDD6BB7E98C675CA477FB
SHA-256:	D2A4B817326BE5C3B775F5A30F7F53028287429E2728E2EE356DFA52884E3FB2
SHA-512:	E421EE90DC2EBA1A2FEA216634F3DFC7F7336A436CD3BD5BC35DF85B6C722756742B572288F8AA6E87995DD2E247EA9D892699E9F18E6AB5AA5A7B0ED26604 E1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...'....._keyhttps://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js .https://firebasestorage.googleapis.com/...S../.....E..5A..._$@..]m./.xgG.k.....].A..Eo.....b0l.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f8d798d069065fcb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	250
Entropy (8bit):	5.437496733563891
Encrypted:	false
SSDEEP:	6:mN/PYET08NaYWbVOqZtElLZHnv6um6pSHs+lDK6t:Mbg8NaY8Z2JZPNm6Cr1
MD5:	4559914FC30C794E467418EAE92E8AE6
SHA1:	E28CB2CC3EEEDA2966EF0537E659726C3AAD1868
SHA-256:	8B36F7CD6D05C65B969DD10FC312C27FFEADCCC3C1A218C9308EE2CBE3A9B193
SHA-512:	BB95E877E6D2CDBEA94FBD893D824C538D0BA1ED585E9DE7CDA41735760FCAC484212D8A8F15BB7C0618A23ED74507572D6A30FE83FBB3F6E614DC079D507 BB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....v....._keyhttps://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js .https://firebasestorage.googleapis.com/...S../.....b.5.e..Z....v....u-.. I.o4.8m....A..Eo.....s.....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):	240
Entropy (8bit):	4.58892362894176
Encrypted:	false
SSDEEP:	6:QqziD0PJ20AMF69TFJ3T0pFpFXrqBQ6YM:VeDCJ2pMqTXSpBrI
MD5:	D1828F01AF833C214252B1B0594DCC89
SHA1:	D9D39CDCED439687864F29FCEF1B83B3C00542B5
SHA-256:	72861E9DE20317AF3CFF07067AEE7654C5C0F8677234B5509A453A2A643CCDEF
SHA-512:	B0AF03C3E48848C827AABDE9CFBA506B925AE0DFFC4545852278E75048B3E939FC5A6F98F1D4C25DA6AE20DCEF6A6C46C86A6E4343821FDDFFC22854BC440 F4
Malicious:	false
Reputation:	low
Preview:	......?qoy retne....._..|.u...S../.....:.g..3z..S../.....D t...V...S../.....R.....)>...S../....._i.....S../.....US...Z....S../...../...3...5../.....^}.Np.....5../..... .S../.

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):	1.1558433725913997
Encrypted:	false
SSDEEP:	24:TLyqJLbXaFpEO5bNmISHn06UwaqpZdElVpnjFWVLqyQfxQh1:TekLLOpEO5J/Kn7U1qpZdGHWVO9fSX
MD5:	155A44426A830A0C4D342CD23F70AF11
SHA1:	3850217529371A188D90EF0D5B30F4E6A9406F2C
SHA-256:	52EE98A010B0D9548FC7626F4FF711C6757811B735657ACD343AE5127AAD203F
SHA-512:	D3CF977AABCF389EB4429A764DCBD0AAE691C4D8059759E1A04DD6BE3D56B4BD06AD525D77BF95FFD865D7EC3BF2ECBAA4DFEC2D1076A29BB84AEF797F2D C5E1
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):	0.9697958303633524
Encrypted:	false
SSDEEP:	24:DIL4rtEy8nrqLbJLbXaFpEO5bNmISHn06Uw8z8:DI++q5LLOpEO5J/Kn7U5z8
MD5:	140B506CC4886820F8743F600706977A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
SHA1:	C61CC447FCD5BBB4507182D598F0A5020006ED8C
SHA-256:	907544BF8BBA337D48C9F8DE412D42991D2642B505F59F30723427B8CBEA12AB
SHA-512:	DAA2DE94008FF9C0D397DE15E9D03761C2BF9297301EAE21A09CBB20E65914B3FD638F0DC2DF9FB7A154C709AF08161638E9C39D47E337155AA11D1D7A4828D 6
Malicious:	false
Reputation:	low
Preview:	.....!..7..... ....

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):	2518
Entropy (8bit):	3.802678717447306
Encrypted:	false
SSDEEP:	48:34Sxec002IAZRPEYHT732zvZTGolELPEYHT732zHIiF:34V08ZqQ3mfdQ3m7I0
MD5:	9C16E0FAD34DCE59D812B50534EAF32A
SHA1:	5CE460ACE37FED9E8995BA6A247292FFF8358FB7
SHA-256:	B626170E9C9ECF00CC6CC487E16970E209CD9DAA08954C75810BDFA0DA38269A
SHA-512:	6EBFA5CCAEE1B1A37674C8AF685E261B88CD9813272221EDBE2B5C79AEB358BF442731C3EB4A10C26AE3C250125B0A9CE91758246247C7071C53B1A4494CFC 7
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...c68a8fc1_977d_4258_b549_be2c898510c5.....:..... .....5..0.....&...{2F4F8386-A58B-4B0C-A17B-2FAAF764E551}.....m..h.....https://firebasestorage.googleapis.com/v0/b/kcdvd jv037jcdi0e3767933.appspot.com/o/!%7D%7B%24%23%40%5E%26%20jaf%40!__%7D%20.html?alt=media&token=08503d5e-c8e8-4a7c-b39c-8a3de4c0bf78#jason.ma ddern@navitas.com.....L.o.g.-.i.n.\...X.....P.....h.....`.....x.....m?:.s...n?:.s.....h.t.t.p.s.:././.f.i .r.e.b.a.s.e.s.t.o.r.a.g.e...g.o.o.g.l.e.a.p.i.s...c.o.m./.v.0./.b./.k.c.d.v.d.j.v.0.3.7.j.c.d.i.0.e.3.7.6.7.9.3.3...a.p.p.s.p.o.t...c.o.m./.o./.!.%.7.D.%.7.B.%.2.4.%.2.3.%.4.0.%.5 .E.%.2.6.%.2.0.j.a.f.%.4.0.!._

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491 A
Malicious:	false
Reputation:	low
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	322
Entropy (8bit):	5.158119314240767
Encrypted:	false
SSDEEP:	6:m1oXfFFdMM+q2P923iKKdK8aPrqIFUtpkoXfFFcd/ZmwPkoXfFFVrMVkwO923iKG:zP7dN+v45KkL3FUtpjP7cd//PjP7qV5M
MD5:	2DC4A7DC29F486054F09EF309D7870E2
SHA1:	9573547B176F426DA1B75681C0044D9805669BE6
SHA-256:	999263D50838B9F6623D470B802B357A7BF497C234C842844B29D60A606A58F4
SHA-512:	7F675FA4880F2369D7F0410C5BDB5E32A10600694BD5F53314AA1DAD35148234DAAC65FF9F6F38C63BD0B24D48F19FDB346C52B9C5DF5433861F82C7F9918CC
Malicious:	false
Reputation:	low
Preview:	2021/04/08-02:55:11.588 181c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/04/08-02:55:11.589 181c Recovering log #3.2021/04/08-02:55:11.590 181c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Reputation:	low
Preview:	.f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f. 5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.. .....f.5.....f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	319
Entropy (8bit):	5.210718721209915
Encrypted:	false
SSDEEP:	6:m1oXfFHq9+q2P923iKKdK8NIFUtpkoXfFHKEHZZmwPkoXfFHE9VkwO923iKKdK8n:zP04v45KkpFUtpjPRHZ/PjPaD5L5KkqJ
MD5:	0D62069284C5092AB4D3961B45866E05
SHA1:	E16C12B5FCB7E60345FC480FD0C7D36A4072A56D
SHA-256:	FB7B3D13742E8982EF9C65D3A573EA868F6E5C03C33193EE87BD182192B98DFF
SHA-512:	126D27C6E11B3BC4D39C9736ADE2E14976C92DF73717E17B8AF6A21675F000680094B4CE0C6CB2AC90E31C7798FE30DB0882CED678086B1405C3745608F8E7E
Malicious:	false
Reputation:	low
Preview:	2021/04/08-02:55:13.774 de8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/04/08-02:55:13.775 de8 Recovering log #3.2021/04/08-02:55:13.776 de8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkIjEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
Reputation:	low
Preview:	.f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	374
Entropy (8bit):	5.268554125318795
Encrypted:	false
SSDEEP:	6:m1oXfFumh4q2P923iKKdK25+Xqx8chI+IFUtpkoXfFuMdNJZmwPkoXfFuMdNDkwY:zPUmh4v45KkTXfchI3FUtpjPUMdNJ/P4
MD5:	F84407D586C31B5EB05FD83415700747
SHA1:	1BA1BEE77266C72D2D5E0AF02E8E9CAB97E503A0
SHA-256:	6D676A82CF176A3C4AAFEAEA7DC5AB40E3481B0C82F07529FACD526D61C4B932
SHA-512:	6356C21190A037D4FAEA3B975E7B1658EEF3119B28EE04CD6118488FC7BD808961BAE784BB5663496C814D2BE8151E08B2B02AB2B5D5E3165E0587644B3D7118

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Malicious:	false
Reputation:	low
Preview:	2021/04/08-02:55:29.866 1464 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/04/08-02:55:29.868 1464 Recovering log #3.2021/04/08-02:55:29.868 1464 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):	360
Entropy (8bit):	5.231069982957949
Encrypted:	false
SSDEEP:	6:m1oXfFgw4q2P923iKKdK25+XuoIFUtpkoXfFgERXJZmwPkoXfFiDkwO923iKKdKl:zPn4v45KkTXYFUtpjPdhJ/PjPMD5L5Ky
MD5:	B7D0FE281FB128E576FA61B326AF601A
SHA1:	AD3882AECE20F8569559E3F2E4EEB4E68D413066
SHA-256:	66E348FD57DC1D97A577EFCEE1539DFA54958CFAAE80CB51A56B4092512C870A
SHA-512:	8C7A14DD6D53279D13C73AA3993574A293E18921234B63AE4F35A17C1F83FED58BB5869A4D4D9C9CF9874671C46D1896D19366462C35D777334D22A94E79E656
Malicious:	false
Reputation:	low
Preview:	2021/04/08-02:55:29.624 1464 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/04/08-02:55:29.628 1464 Recovering log #3.2021/04/08-02:55:29.786 1464 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):	332
Entropy (8bit):	5.241678147474471
Encrypted:	false
SSDEEP:	6:m1oXfFM+h4q2P923iKKdKWT5g1IdqIFUtpkoXfFGuJZmwPkoXfFGuDkwO923iKKg:zPr4v45Kkg5gSRFUtpjPouJ/PjPouD53
MD5:	41A26B250FD9AE0C17DE3F41ADDFEC41
SHA1:	5F0CA60F9D225264DD1A18ADA14F39B324BE0261
SHA-256:	115BDDB09DD51EDFE38C7A42BF14051E30CF359A25438C40CABD7AE42E1555B8
SHA-512:	77FEDD66980ACE4618169923B60F727E81D04D620CEF6E411687E3011B086BE6D58D79473939BCCD38282F190AE26E3992526814C8FA8A0D48D36BCD4B8B5EF
Malicious:	false
Reputation:	low
Preview:	2021/04/08-02:55:28.922 1464 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/04/08-02:55:28.986 1464 Recovering log #3.2021/04/08-02:55:28.986 1464 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):	0.22831012964954714
Encrypted:	false
SSDEEP:	12:TLBj/bf2JZCFGtoycxEnVyRoNuQiGI/DZQJZCFGtoycxEnVV:TLB05cxE2suQ5cxEj
MD5:	C3C4C6F7B1312783FC51311259D3F514
SHA1:	7145F2161FA2EDE4C90CF396C152284E791D05A4
SHA-256:	1ED476A61BCA96D0CEDE7B4D6CFC132A5E25BC323B7CDA5400B661F387DAD4F8
SHA-512:	EC838B117EBA384364AC0CDA7778996470D4C82FBE5003CCC98300453185FCC02330413ED9354583A84E4C7CC0B62D5EC13D01F3DCAF3159E645EF4E1382087
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Category:	dropped
Size (bytes):	1399
Entropy (8bit):	5.655143995710712
Encrypted:	false
SSDEEP:	24:4Bo4a10ppT67so43W7DAD+UbU9D+tY78BJgskfa9yBDOxo7nQBrxzkr25wNiyPKA:O9p2sfBLowdU8JFEwhIdB
MD5:	7749598DC9FB26AC8C9F42DCECC17467
SHA1:	A2633A30F96BF5FD96043372820B4D6876E61BA1
SHA-256:	B849EF9F75DE7CFABD48520D945DE56CEEB2AA69A187C81CCF975AEA3D99519E
SHA-512:	C10259FD1283BCAEB0E530898A2B376E0E96408D6ED2C033968708949E2CD56457C099068E5170A1A42DBEDDED0579EA80DA9897DF78A876AE0E0BA40FB06BE 8
Malicious:	false
Reputation:	low
Preview:	.....".....08503d5e..4a7c..8a3de4c0bf78.._..alt..appspot..b..b39c..c8e8..com..firebasestorage..googleapis..html..https..in..jaf..jason..kcdvdjv037jcdi0e3767933.. log..maddern..media..navitas..o..token..v0*.....08503d5e.....4a7c.....8a3de4c0bf78....._.....alt.....appspot.....b.....b39c.....c8e8.....com.....firebasestorage.....g oogleapis.....html.....https.....in.....jaf.....jason.....kcdvdjv037jcdi0e3767933.....log.....maddern.....media.....navitas.....o.....token.....v0..2.....0.....3.....4.... .....5.....6.....7.....8.....9.....a.....b.....c.....d.....e.....f.....g.....h.....i.....j.....k.....l.....m.....n.....o..... .....p.....r.....s.....t.....v.....:

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):	0.0475180263318464
Encrypted:	false
SSDEEP:	6:7xlQ9AxlGljxlHLxlFxlmX9xlrxl8NxlfG9bNFlEwtCS/ledKl3n:7jQ9AjyjjrjFjG9jrj8NjfqLipS/sk3n
MD5:	D4599525684CF419A78DE44177123FC8
SHA1:	245D1DC8448554B1162411A9B3A3E71461839153
SHA-256:	85DE46BB477BF6E3B1C651054A3AFE4652B805F1DB7013A63D5CDEDC94816568
SHA-512:	80D7D824916695821D680813D14A976E3475F2A98DDBAC948DA38E299B5A9B265BD0EB5D5A5770E2EFB15A3F517AA78C517236BA4E07D98712D0B85A2408EE7
Malicious:	false
Reputation:	low
Preview:	.....p..... ....

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):	5.477694478397136
Encrypted:	false
SSDEEP:	48:WZG0ota7LMq8dbRiyUbQSefgGSNrS0U9RdiN9Nz:IEa7LMpdbRiyUbQ5fgG+rS03z
MD5:	CB65E32F36DF1D8E69705F98CF2FA749
SHA1:	901E60A667F5494D93B2580AA72D59863B81A6DC
SHA-256:	5587B13ECF8145A5731112512733CB6EE521BCD7ED540B117CBD574DA61FBAB4
SHA-512:	16AC9CB7CE4E80BF08E3E90C816D46D786E128A48D6425F8E5BB9D9D9688764EAF0B35E2D1BBF0D4AC03E5BBBB5D1B786E8D03265801C2B34137E5FD445DC5 F0
Malicious:	false
Reputation:	low
Preview:	.....*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSi nkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.R equestIdGenerator..320039000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["2021-04-08 02:55:31.70][INFO][mr.Init] MR instance ID: be916eaa-10f7-401f-b907-67a1c6281ae3\n","[2021-04-08 02:55:31.70][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-04-08 02:55:31.70][INFO][mr .Init] Native Mirroring Service is enabled.\n","[2021-04-08 02:55:31.70][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-04-08 02:55: 31.70][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-04-08 02:55:31.70][INFO][mr.CastProvider] Query enabled: true\n","[2021-04- 08 02:55:31.70][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):	334
Entropy (8bit):	5.168921588791707

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Encrypted:	false
SSDEEP:	6:m1oXfFF6iq2P923iKKdK8a2jMGIFUtpkoXfFFzS9ZmwPkoXfFFV/kwO923iKKdKw:zP7bv45Kk8EFUtpjP7zS9/PjP7V/5L5i
MD5:	CB5A5FA6220BEA61434A365F022401D4
SHA1:	FA5FB3840CFEB38A76487AE012E4237BCFC6E072
SHA-256:	3E87A711A70E935A75FD61B31F0623E30CFB8431C9FD335BE87D96899802019E
SHA-512:	0ABAD50E3A9C1B84EE71D25B67D882CE2B81DCDCB048E43E53A3BAD142A2197201B4DE57DE8982B7B8FF93C0ACD69DFC879F93E68D35E9D2E6153C8100FEE D7F
Malicious:	false
Reputation:	low
Preview:	2021/04/08-02:55:11.349 1804 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/0 4/08-02:55:11.356 1804 Recovering log #3.2021/04/08-02:55:11.364 1804 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):	333
Entropy (8bit):	5.191886757360134
Encrypted:	false
SSDEEP:	6:m1oXfFFL7U+q2P923iKKdKgXz4rRIFUtpkoXfFFnXZmwPkoXfFFpNVkwO923iKK2:zP7L7pv45KkgXiuFUtpjP7X/PjP7p5LR
MD5:	BA49139563D468CCD202BE667A3F9FAC
SHA1:	50DC45DD4B2B645B5982891B5357075A2F1289F7
SHA-256:	831DAC9A1833596800B9228F6C90BE3B15A6B76EB561AA75CCBE33D46A5947E2
SHA-512:	9539A7EDD42912D12C2556BC85216174A4E2E417527C56389FECC719D0F8BA7D6C6C9B6E80646380EB4E1DFC038541838EA7F5DAF616EFC402B27C5AFDC71E
Malicious:	false
Reputation:	low
Preview:	2021/04/08-02:55:11.617 de8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/04/08- 02:55:11.621 de8 Recovering log #3.2021/04/08-02:55:11.625 de8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notific ations/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):	0.963196864728139
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUYzto9SthS5wav:wIElwQF8mpcSW+J/X
MD5:	91866782B36DACB33552B20A81BB02F8
SHA1:	C0E54274388EF288E3249CEE7C36D2DD73078792
SHA-256:	A2B642726475EFB11BB4B6FCEF9A690E13C1C00BE61026159E7C27C457FF25A6
SHA-512:	82EBD591E53D3F8CBFA683A3C8D8124A3DA8B90E7468636F720A3BC6DBC964F7CB2C1A0036041525515DCA1D577846AA4F84A5656B1F9C59D1AEB37F1E7F557 F
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):	0.6276168433636444
Encrypted:	false
SSDEEP:	48:P4QqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUx4:P4QhIElwQF8mpcS6
MD5:	E87D7FFA7737486735858E947964D7F4
SHA1:	958CDD07D98D80DE13D9AAAA2EF4FF8ABA0A0501
SHA-256:	60D48219F11BB7EE2D6DB5BC4EA006E98B141E11677197BDF3D3D073816ECB70
SHA-512:	9DFEEB99734328BDE104CBFAFD30BDE6CA8752384DE6252C2F1771B47E72024EAA8072097504823A63701731972E43FAB4656948EA7439AB1B76A269EECB52A1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Preview:	.....s..... ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	322
Entropy (8bit):	5.109070298006692
Encrypted:	false
SSDEEP:	6:m1oXfFFKkq2P923iKKdKrQMxIFUtpkoXfFFpZmwPkoXfFFWkwO923iKKdKrQMFLJ:zP7pv45KkCFUtpjP7p/PjP7W5L5KktJ
MD5:	9CA742E255F4C0FD2D36D9013E808A3C
SHA1:	B6BAF1538827C8C2510FE9D2BD72B3AD55A00C6B
SHA-256:	8C7B3D1271DE242BEE8D86947E6794CFDED7398845446F354853C3958137716B
SHA-512:	81FDF2498647971F768BAD37668AB530B00C5F4D961DEC6B315D45F867BEBDA00D32D917BEEBCC33753C127DBD261BE4A5DF0B27B0C9EDA68BC9639BE14C8E8
Malicious:	false
Reputation:	low
Preview:	2021/04/08-02:55:11.507 14f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/04/08-02:55:11.508 14f0 Recovering log #3.2021/04/08-02:55:11.509 14f0 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):	347
Entropy (8bit):	5.1447015126504905
Encrypted:	false
SSDEEP:	6:m1oXfFFB4q2P923iKKdK7Uh2ghZIFUtpkoXfFFeG9ZmwPkoXfFFpWkwO923iKKdb:zP7iv45KklhHh2FUtpjP7eG9/PjP7pWi
MD5:	A8ABD9CE38BA6F1C91F8633C2207BB31
SHA1:	7A812F71E061CA0A5E4226746AD8D3EDDFA1FC57
SHA-256:	88644A9E972C9BE3B931C37EC2BE5DC8B551C9DAB42766C94E787753657FA1F8
SHA-512:	1043D7308DD6CEFCEFF0D3B605E55E318D98C3E596537D72D24D6159ACD5E6D892D97620F66EF7153D4E9FBE0C053D06D4E8CCC8C2815A3611A700CBD1BF0A
Malicious:	false
Reputation:	low
Preview:	2021/04/08-02:55:11.294 fc4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/04/08-02:55:11.298 fc4 Recovering log #3.2021/04/08-02:55:11.301 fc4 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\268198b6-5f46-4002-a89a-35bece8dc8ab.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\268198b6-5f46-4002-a89a-35bece8dc8ab.tmp	
Size (bytes):	325
Entropy (8bit):	4.956993026220225
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5rAcJksDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdVAsBdLJlyH7E4f3K33y
MD5:	0C03D530AC97788D62D27B2802C34D83
SHA1:	20F78B6B32D98FA52846C70DF78E4E5CEF663E2D
SHA-256:	7941FADA9867DAAE08EBC196BAFC6952DD506842C3E7D8FB14DF9D4E402D894B
SHA-512:	D5905C124060997A14322D12DECE5C00C63F7174743C740C974D00E88B03F203909CC2AC972B2759E8087B0B10F6306C6E66BF853319B5AC96907F34C8456C80
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542588505091","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):	432
Entropy (8bit):	5.249314616007073
Encrypted:	false
SSDEEP:	12:zP7NUR+v45KkFFUtpjP7s/PjP7sV5L5KkOJ:bJUm45KkfghqyL5KkK
MD5:	B4B83925DFC824F568E5F4616E036CE2
SHA1:	0E74EFBFE7B904013C5A1B18303AB7F083242C49
SHA-256:	F67D674531BD9F87E1C42ACDB0F3F13E731F56EFAF2ACB1954B1731A205E3D86
SHA-512:	A77BD78F85D20F2D946D9526989C4A32E9C0F512977083465E465CBFD8284E59CCC5576BE4BEEC665551085013A2CBF10538F41A641F006ACB4596733923C4DF
Malicious:	false
Reputation:	low
Preview:	2021/04/08-02:55:11.547 181c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/04/08-02:55:11.549 181c Recovering log #3.2021/04/08-02:55:11.549 181c 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):	434
Entropy (8bit):	5.266238913550607
Encrypted:	false
SSDEEP:	12:zP7tv45KkmiuFUtpjP7E/PjP7yh5L5Kkm2J:bV45KkSghyuzL5Kkr
MD5:	B00CFB2B8D88F9125F9342DF2C2626CD
SHA1:	1C6E5C5118C6F24C204CCDD199D517E83E200144
SHA-256:	DA40F7E7B77ABF0542601B59DF5E9D8CC4111766F285BA78FA0FA0318A089EA1
SHA-512:	B7585F6F7598D5A18E30C5EBE75331A55B6ACA962A79C6F4C8C89E60F9650059F096870373FDA85D51C7AC12F252F5CDF664906C9A1989908B26BBE4551C9F5C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Preview:	2021/04/08-02:55:11.615 1804 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/04/08-02:55:11.619 1804 Recovering log #3.2021/04/08-02:55:11.622 1804 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):	420
Entropy (8bit):	5.258101361637516
Encrypted:	false
SSDEEP:	6:m1oXfFkN+q2P923iKKdKusNpZQMxIFUtpkoXfFqXWZmwPkoXfFqiVkwO923iKKd0:zPGN+v45KkMFUtpjPf/PjPfV5L5KkTJ
MD5:	358D1C216C6D31EC3BA0B811CFF04832
SHA1:	919FDA57DAC82E218A43F7B0F4F9B6EA28B0392A
SHA-256:	9C8F6257714C48CC48E354941C176651B945E30DB3AEB954F43F70809C32DD13
SHA-512:	25AE259E9CCA068F02ADA74E2FC69EF617A8892C719431EBF5C1DE097DCCF7325EB2593BEE2282B6356F081AD838D2CE27168EBB204AE75B558DB6E94A737DC8
Malicious:	false
Reputation:	low
Preview:	2021/04/08-02:55:27.897 180c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/04/08-02:55:27.898 180c Recovering log #3.2021/04/08-02:55:27.898 180c 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\191ba0ee-a227-4778-aa0f-376ebe1a9c61.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.976576189225149
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5OV/sDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdysBdLJlyH7E4f3K33y
MD5:	5886A009EB58EE06A16EFD6D1BA9A046
SHA1:	A867B5052F3FBB811693DF8CE3FDAA794F2F2E40
SHA-256:	9E3392126DE2D81D019E0AB3E17F20BADD0EC9FBD944BCB7C4DAF449D937D496
SHA-512:	D24F30A2E35F903AC10AACC4425C58BECB1C6BE2BA30A3C2B9D9D46CE04914AA71F55B3B16ED89081AD65A7090C77F5DC4A258B7B98D71E6A994D176536FB27
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542597817103","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Reputation:	low
Preview:	.'..(..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.184609614935385
Encrypted:	false
SSDEEP:	12:zPl4v45KkkGHArBFUtpjPU/PjPKY5L5KkkGHAryJ:blK45KkkGgPghONL5KkkGga
MD5:	A217686DAF529555FD14B23BB9605A45
SHA1:	CD32F2DD0F22E58A10CD034A57803F8907344C23
SHA-256:	BA6C4B3E3D5E9DD2EF30F5B3DE60D4B8493116ED4A6072EE80B1A2050E3F46C5
SHA-512:	864D6018763F71BEB0B6AD38C6DC4E3A4A8616B7E08350912458B3FFA7E6766958AFC570241D784A53F3961098F4AAAB675EE77F325CC3DF18FA65DD8242E533
Malicious:	false
Reputation:	low
Preview:	2021/04/08-02:55:29.336 de8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/04/08-02:55:29.340 de8 Recovering log #3.2021/04/08-02:55:29.341 de8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	431
Entropy (8bit):	5.1968749238762
Encrypted:	false
SSDEEP:	12:zPY+v45KkkGHArqiuFUtpjP//PjPOcV5L5KkkGHArq2J:bx45KkkGgCghDOGL5KkkGg7
MD5:	5F0846A0FAA905B6686B79E0CD7BD8C3
SHA1:	A8BE576FD1E4714C86E94C3DAE30474063FCA164
SHA-256:	FBEBDE34E8B32DB72D99C4019B005626D6B0A0B6C6189E098CB5DF990765D08A
SHA-512:	61DC96C422CB372BA2EEA353EEC2AC5024EE424DC95B348F3A0235AFDBF3A000DBCEFCDCAD49B23BAF25DCFE12C2262C907D8639F4AF658BC3BC22CB7DC 8B31
Malicious:	false
Reputation:	low
Preview:	2021/04/08-02:55:29.340 8dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/04/08-02:55:29.343 8dc Recovering log #3.2021/04/08-02:55:29.345 8dc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	417
Entropy (8bit):	5.170185960159723
Encrypted:	false
SSDEEP:	12:zPRGc+v45KkkGHArAFUtpjPRE/PjPRAV5L5KkkGHArfJ:bg45KkkGgkghkIL5KkkGgV
MD5:	5AC55BCE6CEABA7403AE54DA489133B9
SHA1:	BA5954FF08F41B4663193A3A1A6264B67FECC392
SHA-256:	45633A207B9FA9F4BEDBEBF84B6A4CAAD14DEDDB549BEB1A78FEA929D727E1E3
SHA-512:	23B43C9E37CE4994535DDB6934A93AAE1F81B71FBF5E20AF98E65C9AE678F5D0D69DA6CDE2D4CC8ECAD469C8C8DC1312B4258A79F00C36D42C53B5D9A69E6 02
Malicious:	false
Reputation:	low
Preview:	2021/04/08-02:55:44.858 8dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Session Storage/MANIFEST-000001.2021/04/08-02:55:44.859 8dc Recovering log #3.2021/04/08-02:55:44.860 8dc Reusing old log C:\Users\user\AppData\Lo cal\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	323
Entropy (8bit):	5.192874082824348
Encrypted:	false
SSDEEP:	6:m1oXfFF99+q2P923iKKdKpIFUtpkoXfFF315ZmwPkoXfFF3CINVkwO923iKKdKaQ:zP794v45KkmFUtpjP7315/PjP73C05LX
MD5:	E5E6B489F3423DF072B055EFEE3176E1
SHA1:	D7BE04B45B98BB879E2732BBF1A89E50BA523549
SHA-256:	7778A95F6F563F6EE32459DD4EEE12232D211D10E0A4E7FE7F51BFFDA08FED2D
SHA-512:	04C8DB904E5E7F9E1FCFCA21469E80974CF4CE27EE81A6A5A9AC80553596FC9955F63578B3A7BD6DD7FA2AE182AF54B8D658278397A34D8A8E7E4323C297ABE 9
Malicious:	false
Reputation:	low
Preview:	2021/04/08-02:55:11.306 de8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/04/08- 02:55:11.311 de8 Recovering log #3.2021/04/08-02:55:11.313 de8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\L evelDB/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):	404
Entropy (8bit):	5.299249245985955
Encrypted:	false
SSDEEP:	12:zPBfv45KkkOrsFUtpjP1/PjPn5L5KkkOrzJ:bN45Kk+ghh5L5Kkn
MD5:	AC2831BDA5D7F7FC92E696723690C88B
SHA1:	451B79B408EE933CAF996C2D8F58A4EFA5CFAD04

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
SHA-256:	B40CD0BC9372767A0D4370E7B749B7464835C27CE2F77B5995365330407FB7C1
SHA-512:	8728DEE45C11EA59538373645754E99CA48418CBF3B81AD3CF012823FE80D073BC113D94110E432BD959E0598551323F8A810231AC1F05DD3AF59F3EA9EFE129
Malicious:	false
Reputation:	low
Preview:	2021/04/08-02:55:31.685 1810 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/04/08-02:55:31.686 1810 Recovering log #3.2021/04/08-02:55:31.686 1810 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12
Entropy (8bit):	3.188721875540867
Encrypted:	false
SSDEEP:	3:tdl:tD
MD5:	4FE59E73F2E3A484BFA7065E07BC7468
SHA1:	9CFF73013BD3A69C291F39BC6E46A7571887A00F
SHA-256:	67A3C5E5E428A05E2EB709DC16CAAE8D7BF67B3C535F4A9333A49B50F7DFDC58
SHA-512:	2A29031572DB2C1C01A3450514B7F021D2BCB112CF2967FE50B059C6E6CE2D09EE7EB9AD914E637D7069CDA0191AD8187DB50C5301CDC4FD13D1F661BF5728D
Malicious:	false
Reputation:	low
Preview:	.....YXt-O

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a71e61e4-40a1-4c22-b65a-23f6de49f0b7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.576807314177996
Encrypted:	false
SSDEEP:	384:YoBtULlS1Xr1kXqKf/pUZNCgVLH2HfDRrUklFW4r:MLlir1kXqKf/pUZNCgVLH2HfFrUkDW0
MD5:	89FF3991E4A4BEE08886F7CBE8CCF9A1
SHA1:	367E6A9A09B846DFA61C622E66AFD58126123881
SHA-256:	9EB540B793BDEA2AEEB3EA070A987D97F94FD784D72678AE5673B2563CE0B763
SHA-512:	82A4BDE95BDEBB809E9BE53B1C6020148B603E16ED6810451C42CC4577A3A98694A396414B58535ED1EEB80F41BE80C367466B37C1E60770F73A67A78FBE3A2
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":"13262349311303497","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\b1db336d-b13d-4990-9faf-16fb50bd979b.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):	5592
Entropy (8bit):	5.188255505562366
Encrypted:	false
SSDEEP:	96:nOF3/W4UK8fpSVFZIk0JCKL8UgkQS11PbOTQVuwn:nOI4KxS9C4Kukv7
MD5:	5AD45634D51330298226F0205171D1CF
SHA1:	6B76566EE15E0199AF356E1E1B1652E959D578F8
SHA-256:	C12C15F7635E407853478C604F1E7D8898D4D1A73ACA1269F3D0DFE051906D07
SHA-512:	559CE5ACBA97CE0F5A87334509C4386322DED8DF95FE5102EF4A47B12295D1ED243A5460F5E70101CA155DCFD58052F0512ADAC46C12E252D68B848B0978F25
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b1db336d-b13d-4990-9faf-16fb50bd979b.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13262349311577523","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","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","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
SSDEEP:	6:m1oXfFrQEfVq2P923iKKdKfrzAdIFUtpkoXfFrCigZmwPkoXfFrCilkwO923iKKF:zPiE9v45Kk9FUtpjP8/PjP85L5Kk2J
MD5:	0FCCB4C6BC025B32F8817B6C52D228ED
SHA1:	54A59364D76DE92031AEEE3646DADDB3AE36EE82
SHA-256:	6CB18B03ED2CA13D39CB62559AE4FE66F2A4FE2EE2DEF6D4DEA249EDD6152C1C
SHA-512:	A288BF59AADE636E90DA8DBD8701A22A41134817E9205A297160A6B2DEE0F5ADF2BA4569F37F86FD4897DBDE1BC78170366F8BC8AD7639983D93E58ED5B8DAC1
Malicious:	false
Reputation:	low
Preview:	2021/04/08-02:55:31.632 1810 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/04/08-02:55:31.634 1810 Recovering log #3.2021/04/08-02:55:31.634 1810 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

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

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

C:\Users\user\AppData\Local\Temp\00ba8e9f-836b-45f0-b357-7605248f5c36.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

C:\Users\user\AppData\Local\Temp\00ba8e9f-836b-45f0-b357-7605248f5c36.tmp	
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...I5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..I.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\5fa42d40-5425-4bd5-913c-900563c92636.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\a6e301e5-1c0a-4f9d-a5f8-af8c8687511c.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.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\ee97ac8e-f3b7-4694-ad38-27cac3985026.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\am\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\am\messages.json	
Size (bytes):	17307
Entropy (8bit):	5.461848619761356
Encrypted:	false
SSDEEP:	384:arfbEVrFvMP4rMhuDopC3vUuFBYZV6uml:aHEVrFvMP4KuFvr6D6uml
MD5:	26330929DF0ED4E86F06C00C03F07CE3
SHA1:	478F3B7E7A7E007BEE182B89C2EF6FFE6045E92C
SHA-256:	621B5139ED199022BB6529AF18ED4DC312AE9F3E90ECAF3B2C9E1D12114F5B22
SHA-512:	0BE6183A1BF12575C0F99960705D4249E79CDB8528C55FF132BE99A111F09494231AD6A36CD61B090A3B34C6971D68A29373BA346888E852C52E05DC14380682
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "1282768764603190 75": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": ".... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "... ...".. },.. "1802762746589457177": {.. "message": "...".. },.. "1850397500312020388": {.. "message": ".$START_LINK$Google Home .....END_LINK ... . Chromecast ....? $START_SPAN$*END_SPAN",.. "placeholde

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\ar\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16809
Entropy (8bit):	5.458147730761559
Encrypted:	false
SSDEEP:	192:0IprKC78JmUjk8RkeryFOYPATxLZ8fsbE3/IFV6c8TEKdl:Jrp8JjA8RkerK0lc3wFV6uml
MD5:	44325A88063573A4C77F6EF943B0FC3E
SHA1:	78908D766F3E7A0E4545E7BD823C8ED47C7164EB
SHA-256:	67A439A08804EF4BEF261BDBADD8F0FEFD51729167D01EDCA99DD4AF57D6108B
SHA-512:	889C02BC986794C58C76022E78F57F867DD1D5217687F12D679A33A2DB9E5A18F3A37CF94D8FE4585E747C78E4662EAB93361FF7D945990774C7CFCACCFB79D
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": ".. .. ..".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": "..... .....".. },.. "1850397500312020388": {.. "message": "... .... Chromecast .. $START_LINK$..... Google HomeEND_LINK. $START_SPAN$*END_SPAN",.. "pl aceholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {..

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	18086
Entropy (8bit):	5.408731329060678
Encrypted:	false
SSDEEP:	192:4jjpr342SIwPIasR9VhMkACVmrv8evj+3eXivOMbb2vVzCkwRV6V6c8TEKdl:4ZrYo+rxT+qOV6V6uml
MD5:	6911CE87E8C47223F33BEF9488272E40
SHA1:	980398F076BB7D451B18D7FDE2DE09041B1F55AD
SHA-256:	273DEF0F67F0FA080802B85EF6F334DE50A19408F46BDF41F0F099B1F5501EEA
SHA-512:	CDB69405BB553E46DCF02F71B1A394307D0051E7FA662DFFEBA7888F30DD933F13C7FD6E32F1D7AEAEE8746316873B6E1D92029724ABDC75E49DCC092172EA 2
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "......".. },.. "1213957982723875920": {.. "message": "... .. ..-..... ....?".. },.. "12827687 6460319075": {.. "message": "..... .. ..".. },.. "1428448869078126731": {.. "message": "..... .. ..".. },.. "1522140683318860351": {.. "message": "..... .. .., ...".. },.. "155090406471082895 8": {.. "message": "......".. },.. "1636686747687494376": {.. "message": ".....".. },.. "18027627 46589457177": {.. "message": ".... .. ..".. },.. "1850397500312020388": {.. "message": "..... .. .. Chromecast . $START_LINK$..... Google Hom eEND_LINK? $START_SPAN$*END_SPAN",.. "p

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\bn\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19695
Entropy (8bit):	5.315564774032776
Encrypted:	false
SSDEEP:	384:PrUCrcTIOeswIW/Vre/sZn8TFfzheV6uml:IPswIWtoK8xfG6uml
MD5:	F9DDF525C07251282A3BFFCEE9A09ABB

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\bn\messages.json	
SHA1:	A343A078E804AF400A8F3E1891E3390DA754A5CD
SHA-256:	C69C6C90F7EB8F10685CD815AF1F6F1B87CF30C4E8D95DF1D577DE1105AAD227
SHA-512:	EBD339C37162984672513019D470B92DF8B743DD69D4430361EF12D42FD1C208DBDE818A7BFE20BE8A7D63CD6E02B3F4344DEA1C4AEDB8719D789981A49DA4C
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".... ...".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... ....".. },.. "1522140683318860351": {.. "message": "..... ... .".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "$START_LINK$ Google

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15518
Entropy (8bit):	5.242542310885
Encrypted:	false
SSDEEP:	384:drGUBKxMF2ayv8FrIccUVFmwf+7d9VKS3V6uml:dCUBKxMFBy0FE3UzmQ+zkSl6uml
MD5:	A90CF7930E7C3BEC61EE252DEFAD574A
SHA1:	F630CA01114A7BDD39607CB84B8280CCE218A5C6
SHA-256:	A533740E17559E2ADF40B4555C60F21EEC84E92C09CDBC19EED033A0B4DD2474
SHA-512:	598F991B344FA6724617D6CE57BB0D6D64EF86B4F5317BF6AD5EDF43E6B0A385094E7885F7A8FA2B107405B31C3D9F76E92315BC1D9BB52ACD4ECAD342917DE1
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Es congela".. },.. "1213957982723875920": {.. "message": "Quina de les opcions.seg.ents descriu millor la vostra xarxa?".. },.. "128276876460319075": {.. "message": "Detecci. de dispositius".. },.. "1428448869078126731": {.. "message": "Flu.desa del v.deo".. },.. "1522140683318860351": {.. "message": "S'ha produ.t un error en la connexi.. Torneu-ho a provar.".. },.. "1550904064710828958": {.. "message": "Correcta".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volum".. },.. "1850397500312020388": {.. "message": "Pots veure el Chromecast a l'$START_LINK$aplicaci. Google.HomeEND_LINK?$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15552
Entropy (8bit):	5.406413558584244
Encrypted:	false
SSDEEP:	192:eVdprJrG5efiTk93ebrxZR1fdc8VDCwT9fTV6c8TEKdl:2rMqiQerxQ88W7V6uml
MD5:	17E753EE877FDED25886D5F7925CA652
SHA1:	8E4EC969777CC0CEB7C12D0C1B9D87EBBB9C4678
SHA-256:	C562FCCFCE374D446BFAC30AC9B18FF17E7A3EF101C919FF857104917F300382
SHA-512:	33D61F6327FC81D7A45AA2CC97922DC527F5F43E54AA1A1638DA6EE407024A2F10CFD82CC5C3C581C2E7B216276987CB26C3FA95198572E139ACF29CC5B7ADB
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Video zamrz.".. },.. "1213957982723875920": {.. "message": "Kter. popis nejl.pe vystihuje va.i s..?".. },.. "128276876460319075": {.. "message": "Zji..ov.n. za..zen.".. },.. "1428448869078126731": {.. "message": "Plynulost videa".. },.. "1522140683318860351": {.. "message": "P.ipojen. se nezda.ilo. Zkuste to pros.m znovu.".. },.. "1550904064710828958": {.. "message": "Plynul.".. },.. "1636686747687494376": {.. "message": "Perfektn.".. },.. "1802762746589457177": {.. "message": "Hlasitost".. },.. "1850397500312020388": {.. "message": "Vid.te sv.j Chromecast v.$START_LINK$aplikaci Google Home END_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15340
Entropy (8bit):	5.2479291792849105
Encrypted:	false
SSDEEP:	192:+Upr8XnI1MY2kPuir8j7Rd3kbTWc4QtV6c8TEKdl:FrJ1H9br8h6eZCV6uml
MD5:	F08A313C78454109B629B37521959B33
SHA1:	3D585D52EC8B4399F66D4BE88CED10F4A034FCCC
SHA-256:	23BF7E5EDF70291CA6D8F4A64788C5B86379EECB628E3DFA7DD83344612F7564
SHA-512:	9F2868AEBBF7F6167A7EA120FE65E752F9A65D1DC51072AA2413B2FDE374DA2D169D455A4788E341717F694179E6F1FA80413C080D9CD8CB397C3E84668CBFE

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\da\messages.json	
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Fryser".. },.. "1213957982723875920": {.. "message": "Hvilket af f.lgende udsagn beskriver bedst dit netv.rk?".. },.. "128276876460319075": {.. "message": "Enhedsregistrering".. },.. "1428448869078126731": {.. "message": "Videostabilitet".. },.. "152214068331 8860351": {.. "message": "Forbindelsen blev afbrudt. Pr.v igen.".. },.. "1550904064710828958": {.. "message": "Problemfri".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "180276274658945717 7": {.. "message": "Lydstyrke".. },.. "1850397500312020388": {.. "message": "Kan du se din Chromecast i $ START_LINK$ Google Home-appenEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "STAR

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15555
Entropy (8bit):	5.258022363187752
Encrypted:	false
SSDEEP:	192:AJprM71A4qyJSwlk5KR5rtXsmvL0xhVw921YV6c8TEKdl:2re3jJS5A5rt8msA2KV6uml
MD5:	980FB419ED6ED94AD75686AFFB4E4C2E
SHA1:	871BFBCA6BCBA9197811883A93C50C0716562D57
SHA-256:	585C7814AFD2453232BC940252D4AE821D6E6CBCFD74A793F78E5DB8BA5342F1
SHA-512:	1681FA9C3BA882250A5005FB807D759EB8A634F1AA011725B1C865C0028BE7AB7BC16DC821A7F5BBFBA84C91E7D663ADE715284798E7E84E8FFF2D254488882
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "H.ngenbleiben".. },.. "1213957982723875920": {.. "message": "Welche dieser Aussagen beschreibt dein Netzwerk am besten?".. },.. "128276876460319075": {.. "message": "Ger.teerkennung".. },.. "1428448869078126731": {.. "message": "Videowiedergabequalit.t".. },.. "1522140683318860351": {.. "message": "Fehler beim Herstellen der Verbindung. Bitte versuche es noch einmal.".. },.. "1550904064710828958": {.. "message": "St.rungsfrei".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lautst.rke".. },.. "18503975003 12020388": {.. "message": "Siehst du deinen Chromecast in der $START_LINK$Google Home AppEND_LINK? $START_SPAN$*END_SPAN",.. "placeholde rs": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17941
Entropy (8bit):	5.465343004010711
Encrypted:	false
SSDEEP:	384:S0rDuhLh41cZrP3TzDBknbpgo6djIV6uml:S0fuBh46ZD3TzDinbpgoUK6uml
MD5:	40EB778339005A24FF9DA775D56E02B7
SHA1:	B00561CC7020F7FE717B5F692884253C689A7C61
SHA-256:	F56BF7C171AA20038EE30B754478B69A98F3014C89362779B0A8788C7B9BEEE1
SHA-512:	8BED281A33EC1E4E88A9F9D62BB13FE0266C0FAF8856D1DC2A843D26DD3CE5E7D1400FD3325ABD783B0364EC4FB1188AD941D56AEB9073BC365BE0D12DE6C 013
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "......".. },.. "1213957982723875920": {.. "message": ".... ... .;".. },.. "1282768 76460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": "......".. },.. "1802762746589457177": {.. "message": "..... ....".. },.. "1850397500312020388": {.. "message": "..... .. .. Chromecast .... $START_LINK$..... Google HomeEND_LINK; $START_SPAN $*$END_SPAN$",.. "placeholders": {.. "END_LINK": {.. "content

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	14897
Entropy (8bit):	5.197356586852831
Encrypted:	false
SSDEEP:	96:2MKUOp5N7GTNMRuv6M0blt3FXGkW6/5NkkQ9NJKJhnH3t9F410sUA+ISN6cGDSyR:VKzprogudTGkWqrKcJhdIR+V6c8TEKdl
MD5:	8351AF4EA9BDD9C09019BC85D25B0016
SHA1:	F6EC1FFD291C8632758E01C9EE837B1AD18D4DCF
SHA-256:	F41C82D8A4F0E9B645656D630C882BE94A0FB7F8CEC0FE864B57298F0312B212
SHA-512:	75672B57F21F38F97341AD76A199AD764E9FBAB2384D701BF6EB06CEFDE6C4F20F047F9051A4E30D99621E5C1FBBDB9E38E8D2B47470806704B38DA130A146C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\en\messages.json	
Preview:	{.. "10189845614885205 17": {.. "message": "Freezes".. },.. "12139579827238759 20": {.. "message": "Which of the following best describes your network?".. },.. "12827687646031907 5": {.. "message": "Device Discovery".. },.. "14284488690781267 31": {.. "message": "Video Smoothness".. },.. "1522140683318860 351": {.. "message": "Connection failed. Please try again.".. },.. "15509040647108289 58": {.. "message": "Smooth".. },.. "16366867476874943 76": {.. "message": "Perfect".. },.. "18027627465894571 77": {.. "message": "Volume".. },.. "18503975003120203 88": {.. "message": "Are you able to see your Chrom ecast in the $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "START

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15560
Entropy (8bit):	5.236752363299121
Encrypted:	false
SSDEEP:	192:NAgprfy1pTCukFr+1DIyDRoanvV6c8TEKdl:KMrq6FrmvV6uml
MD5:	8A70C18BB1090AA4D500DE9E8E4A00EF
SHA1:	8AFC097FA956C1317DB0835348B2DA19F0789669
SHA-256:	FF173D1CEF665B1234E02F11070ABD2B65230318150734579A03C7F31B4AE3F4
SHA-512:	140BAF40A4ABE9B8AF0855B0EBB7DFDF17869EDFC4EE1037C5EA7FDD8EDEBD4850E055B6A4D7B8782657618BCE1517813779BA01BA993CC838BB43E0BE71E EEE
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": "Congelaci.n de im.genes".. },.. "12139579827238759 20": {.. "message": ".Cu.l de las siguientes respuestas descr ibe mejor tu red?".. },.. "12827687646031907 5": {.. "message": "Detecci.n de dispositivo".. },.. "14284488690781267 31": {.. "message": "Fluidez del v.deo".. },.. "15221406833188603 51": {.. "message": "Error en la conexi.n. Vuelve a intentarlo.".. },.. "15509040647108289 58": {.. "message": "V.deo fluido".. },.. "16366867476874943 76": {.. "message": "Perfecta".. },.. "18027627465894571 77": {.. "message": "Volumen".. },.. "18503975003120203 88": {.. "message": ".Puedes ver tu Chromecast en la $START_LINK$aplicaci.n Google.HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\et\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15139
Entropy (8bit):	5.228213017029721
Encrypted:	false
SSDEEP:	96:Z48bxhWYp5Ny5M63niwAKD4rrJSJ2RkPXh9P5NFP2+NBMU01jewUEVez3QOiSevy:ikxprot3lYkf/rHBc0KsUV6c8TEKdl
MD5:	A62F12BCBA6D2C579212CA2FF90F8266
SHA1:	F7E964A2D9BBDA364252BCE5CFBA3FD34FDD825E
SHA-256:	3EB3EB0B3B4A8E5A477D1B3C3A3891CCC7DC6B8879ECE243A7BD7C478068273D
SHA-512:	E300201245C00ADEC8F39D586875F8FA4607AB203572BF3CE353C1CA7CDCA05B8786810CA0CEE27E4EA54A5EFD53690F1EA7AA4148CFF472A66BB1120272356 6
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": "Hangub".. },.. "12139579827238759 20": {.. "message": "Milline j.rgmistest v.idetest kirjeldab k.ige paremini teie v.rku?".. },.. "12827687646031907 5": {.. "message": "Seadme tuvastamine".. },.. "14284488690781267 31": {.. "message": "Video sujuvus".. },.. "152 2140683318860351": {.. "message": ".hendamine eba.nnestus. Proovige uuesti.".. },.. "15509040647108289 58": {.. "message": ".htlane".. },.. "163668674768 7494376": {.. "message": "T.iuslik".. },.. "18027627465894571 77": {.. "message": "Helitugevus".. },.. "18503975003120203 88": {.. "message": "Kas n.ete oma Chromecasti $START_LINK$rakenduses Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "conte nt": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\fa\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17004
Entropy (8bit):	5.485874780010479
Encrypted:	false
SSDEEP:	192:rngaIprIX/t9wkjTJrs3hqaXxRQdiIMDnD+LhfHdoltV6c8TEKdl:4rin5rU1X7Qd0M9CtV6uml
MD5:	852BD3CFF960F1BC3A2AAB3CB3874EF9
SHA1:	C9F6F3C776542889FE3B67971D65ACFE048A3A0A
SHA-256:	D87597B6C10364501B98AA42524843F109009CCEF022D8E0170440D7F144F4C6
SHA-512:	2A7AE4D70E33E53EE31831CE2E61DD8DF103C4170EC483BDA14B8788E5DD536EEE84DBA340CACBDF16889C7E6465B48D82C4714E746E8A7B372D12CBDF371 95
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\fa\messages.json	
Preview:	{.. "1018984561488520517": {.. "message": ".... ... .".. },.. "1213957982723875920": {.. "message": ".... .. ..".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "....".. },.. "1802762746589457177": {.. "message": "..... ....".. },.. "1850397500312020388": {.. "message": ".... .... Chromecast ... . $START_LINK$ ..... Google HomeEND_LINK ..... $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\fi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15268
Entropy (8bit):	5.268402902466895
Encrypted:	false
SSDEEP:	192:efMprYXiYUNpj5Coik1tXxrUhvUzSPWV6c8TEKdl:eIrjbjosdrU5WV6uml
MD5:	3902581B6170D0CEA9B1ECF6CC82D669
SHA1:	C8208AC2B1DD6D4F8BDAAE01C8BD71FFFA5A732B
SHA-256:	D2A8180225A83A423BB6E17343DFA8F636D517154944002ED9240411B8C0C5E1
SHA-512:	612FDD8A3C5051F0A4F1E11E50B5D124B337C77D62D987D35C2AF9E08AFC6AFCEBAEE8D40FDFBCD1E1889F39758B96FAECBF6C6D1CF146C741A5261952050321
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Pys.htyy".. },.. "1213957982723875920": {.. "message": "Mik. seuraavista kuvaa parhaiten verkkoasi?".. },.. "128276876460319075": {.. "message": "Laitteiden tunnistaminen".. },.. "1428448869078126731": {.. "message": "Videon tasaisuus".. },.. "1522140683318860351": {.. "message": "Yhteys ep.onnistui. Yrit. uudelleen.".. },.. "1550904064710828958": {.. "message": "Tasainen".. },.. "1636686747687494376": {.. "message": "T.ydellinen".. },.. "1802762746589457177": {.. "message": "..nenvoimakkuus".. },.. "1850397500312020388": {.. "message": "N.etk. Chromecastisi $START_LINK$Google Home .sovelluksessaEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },..

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\fil\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15570
Entropy (8bit):	5.1924418176212646
Encrypted:	false
SSDEEP:	192:+esprzAsQp68wIJYkMyr2k0jR1/7Rr1uV6c8TEKdl:Gr78JDMyrR0tJuV6uml
MD5:	59483AD798347B291363327D446FA107
SHA1:	C069F29BB68FA7BA2631B0BF5BBF313346AC6736
SHA-256:	DD47530EAE96346CD4DC3267A0BB1091BB17B704803A93CDA2E3E81551B94F12
SHA-512:	091595CA135E965ED3DE376873541117F0E7A8EBDEB4714833EFDD6C820234373891BE5DEC437BA85CCB79CCCA053D407E6ADA17EBDAE7D313324A48775C000
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Hindi gumagalaw".. },.. "1213957982723875920": {.. "message": "Alin sa sumusunod ang pinakamahusay na naglalarawan sa iyong network?".. },.. "128276876460319075": {.. "message": "Pagtuklas ng Device".. },.. "1428448869078126731": {.. "message": "Pagka-smooth ng Video".. },.. "1522140683318860351": {.. "message": "Hindi nakakonekta. Pakisubukang muli.".. },.. "1550904064710828958": {.. "message": "Smooth".. },.. "1636686747687494376": {.. "message": "Perpekto".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Nakikita mo ba ang iyong Chromecast sa $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\fr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15826
Entropy (8bit):	5.277877116547859
Encrypted:	false
SSDEEP:	192:nLZprAZg3EkV3sjrICe8L/1Va7lt1rlxLAkoYHHavV6c8TEKdl:vrW+2jrI7TdLAk3MV6uml
MD5:	9B416146FE4F1403C2AACAC4DCF1A5C3
SHA1:	616F055C9FAD4CE972DF82EC8A9B2F4EDA3E7FAD
SHA-256:	7C7F5758F54008190ACCDDBD1761CBD980FB5FE0847E992874498228D2571DBC
SHA-512:	6E8E70380A8C6E2C0587ADFF6AE36963EC76694904841CE1DFE4EEE215B917AD3E8AF727555627FBDF6B8BA6A4A0674D2B90AC4E9331B6628A32F4C4348FB51B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\fr\messages.json	
Preview:	{.. "1018984561488520517": {.. "message": "Se fige".. },.. "1213957982723875920": {.. "message": "Parmi les propositions suivantes, laquelle d.crit le mieux votre r.seau.?".. },.. "128276876460319075": {.. "message": "D.tection d'appareils".. },.. "1428448869078126731": {.. "message": "Fluidit. de la vid.o".. },.. "1522140683318860351": {.. "message": ".chec de la connexion. Veuillez r.essayer.".. },.. "1550904064710828958": {.. "message": "Fluide".. },.. "1636866747687494376": {.. "message": "Parfaite".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Votre Chromecast est-il visible dans l'$START_LINK$application Google.HomeEND_LINK.? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\gu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19255
Entropy (8bit):	5.32628732852814
Encrypted:	false
SSDEEP:	384:Hq2Mr+qPlJKYMdzKgXr3dGsGF+yAK37Wf7Cy/V6uml:KxzTVgX7ykj6uml
MD5:	68B03519786F71A426BAC24DECA2DD52
SHA1:	B8E6608932EC5CEC4BC3C5475BFC3E312D2E2E7D
SHA-256:	C77A4D27E9E6CA25B9290056D93A656E3EBE975957E4C2EE9F0FB11B133D5CD4
SHA-512:	5FFE06A10774877AF25E05BA07F3032CC52F874896D67E320F4EF9D524A22E40B462CC6206700E9557EB354FA2730172DC6912EBCA49C671FB0EF155B17F9EFF
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "....".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636866747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "... ... $START_LINK$ Google Home ..END_LINK... Chromecast..

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\hi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19381
Entropy (8bit):	5.328912995891658
Encrypted:	false
SSDEEP:	384:zrGrSmhKy7KyY+bNEDqlQdrMEPxtShJV6uml:zBqG6QdwEPrW6uml
MD5:	20C86E04B1833EA7F21C07361061420A
SHA1:	617C0D70E162CF380005E9780B61F650B7A39F9B
SHA-256:	C2C27CA242DBDE600BA3AA7782156BC2B190A64D8A1B51EDC8007BDECA139553
SHA-512:	9FB91AA8E0226519E298B1136E8A1A3C1879DB7F0E6052AF1BFD55921CD698346278D04602510680A9695A76DD5C96D9665380580044C50D81392BB2CB3E8E95
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "128276876460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636866747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": ".... .. $START_LINK$ Google Home .....END_LINK ... . Ch

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\hr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15507
Entropy (8bit):	5.290847699527565
Encrypted:	false
SSDEEP:	192:Pdapr6h85tRwVQgkvJryLkla5Kfndg/V6c8TEKdl:Arwot2Q7BryVce/V6uml
MD5:	3ED90E66789927D80B42346BB431431E
SHA1:	2B061E3271DF4255B1FFC47BDB207CDEC0D9724F
SHA-256:	0B41E3C42414F72C9A12C05F8772597F9685115366A774C66018467AD4B71A74
SHA-512:	92BE43F1FFC8EFBF5BBC50573AC4C65F6104416A5B6CD04404C3A9854CA3DCF2A43A4044C168590CDF83887D234495843572331ADCD5B020D2E48A3956F3C16
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Zamrzavanje".. },.. "1213957982723875920": {.. "message": "Koje od sljede.eg najbolje opisuje va.u mre.u?".. },.. "128276876460319075": {.. "message": "Otkrivanje ure.aja".. },.. "1428448869078126731": {.. "message": "Ujedna.enost videoreprodukcije".. },.. "1522140683318860351": {.. "message": "Povezivanje nije uspjelo. Poku.ajte ponovo.".. },.. "1550904064710828958": {.. "message": "Glatko".. },.. "1636866747687494376": {.. "message": "Savr.ena".. },.. "1802762746589457177": {.. "message": "Glasno.a".. },.. "1850397500312020388": {.. "message": "Vidite li svoj Chromecast u $START_LINK$aplikaciji Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\hu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15682
Entropy (8bit):	5.354505633120392
Encrypted:	false
SSDEEP:	192:CCEAproS9fZv+JwkDMrC2NSxoSgbV6c8TEKdl:5r5VZv+RDMrazoV6uml
MD5:	8E9FF7E49473C5734A2F6F0812E12EB3
SHA1:	A4F10DDD1580582533D5EB59EDF6D8048F887C81
SHA-256:	6CDD2FB39ADECE00E88B989E464B05ED1414092D0492F6D0AE58D549BFD1A46A
SHA-512:	E9A4AF31B1A276F395599BB620A3164CABF3459F3C102DD3F57DFEA734510BD985DE65CB409E1975559ACCC615075439A08E1DEBE22C90A0ABCAA3CAFEE79AC7
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Lefagy".. },.. "1213957982723875920": {.. "message": "Az al.bbiak k.z.l melyik jellemzi legjobban h.l.zat.t?".. },.. "128276876460319075": {.. "message": "Eszk.zfelfedez.s".. },.. "1428448869078126731": {.. "message": "Vide. folyamatoss.ga".. },.. "1522140683318860351": {.. "message": "Sikertelen kapcsol.d.s. K.rj.k, pr.b.lja .jra.".. },.. "1550904064710828958": {.. "message": "Folyamatos".. },.. "1636686747687494376": {.. "message": "T.k.letes".. },.. "1802762746589457177": {.. "message": "Hanger.".. },.. "1850397500312020388": {.. "message": "L.tja a Chromecastot a $START_LINK$Google Home alkalmaz.sbanEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content":

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\id\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15070
Entropy (8bit):	5.190057470347349
Encrypted:	false
SSDEEP:	192:GsprMtChjkWfrEWL0KRCnEOWV6c8TEKdl:9rtAEr3LTRuWV6uml
MD5:	7ADF9F2048944821F93879336EB61A78
SHA1:	C3DA74FB544684D5B250767BB0CB66FFB7C58963
SHA-256:	3630947E1075E3663AD3E4824D0BE42CB47C0D615D8053E83B9595047C8BA9BE
SHA-512:	1F28BB80E1839C5581106BEA3AE2501C7618249D7E3115819F5A9A87771D59F5DE346C1B9C87F7FFC390604D5B9888CE738E25F2F04A094002A0FB3B22CBEC95
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Membeku".. },.. "1213957982723875920": {.. "message": "Dari berikut ini, manakah yang paling mendeskripsikan jaringan Anda?".. },.. "128276876460319075": {.. "message": "Penemuan Perangkat".. },.. "1428448869078126731": {.. "message": "Kelancaran Video".. },.. "1522140683318860351": {.. "message": "Sambungan gagal. Coba lagi.".. },.. "1550904064710828958": {.. "message": "Lancar".. },.. "1636686747687494376": {.. "message": "Sempurna".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Bisakah Anda melihat Chromecast di $START_LINK$aplikasi Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },..

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\it\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15256
Entropy (8bit):	5.210663765771143
Encrypted:	false
SSDEEP:	192:lYprk52dAaykVza8rE0QWBKD9+vq0hKEV6c8TEKdl:qrlA8r6DalV6uml
MD5:	BB3041A2B485B900F623E57459AE698A
SHA1:	502F5EA89F9FB0287E864B240EA39889D72053A4
SHA-256:	025737EF8FA06706B3F26D0F52B4844244A6D33DAE1D82FEF2931A14C003D57E
SHA-512:	BA51784073BEF82F3A116B33DA406FDB10EC823B9EE74375C46036DAD8BDCB4141F60845DE141ABE42CEEF9251572F6AB287CA5FC7669C60E4F68071D5AB8CD
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Si blocca".. },.. "1213957982723875920": {.. "message": "Quale delle seguenti definizioni descrive meglio la tua rete?".. },.. "128276876460319075": {.. "message": "Rilevamento dispositivi".. },.. "1428448869078126731": {.. "message": "Uniformit. video".. },.. "1522140683318860351": {.. "message": "Connessione non riuscita. Riprova.".. },.. "1550904064710828958": {.. "message": "Fluido".. },.. "1636686747687494376": {.. "message": "Perfetta".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Riesci a vedere il tuo dispositivo Chromecast nell'$START_LINK$app Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\ja\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\ja\messages.json	
Category:	dropped
Size (bytes):	16519
Entropy (8bit):	5.675556017051063
Encrypted:	false
SSDEEP:	192:nkprPhQdxkRWrZe1wYpMR5wnAV6c8TEKdl:YrLRWri65wAV6uml
MD5:	6F2CC1A6B258DF45F519BA24149FABDC
SHA1:	8A58C7880C6D22765DCBB6BCE22A192C1B109AE1
SHA-256:	42ECFEE727CFC4F2845FEFDACE5EDC2E0A40AFAD69973A3B950CE653A7633342
SHA-512:	F7454F0E14301C59CC54361ACC0A1C6D072EF9BDF5DEA60646FB90B1CE47612785938C784A4CF1DE3E62648A14420374933B5F5DA43907BC00D3799FF163A3D
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "..".. },.. "1213957982723875920": {.. "message": "..".. },.. "128276876460319075": {.. "message": "..".. },.. "1428448869078126731": {.. "message": "..".. },.. "1522140683318860351": {.. "message": "..".. },.. "15509040 64710828958": {.. "message": "..".. },.. "1636686747687494376": {.. "message": "..".. },.. "1802762746589457177": {.. "message": "..".. },.. "18503975 00312020388": {.. "message": "$START_LINK$Google Home ...END_LINK. Chromecast .....$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_ LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".

C:\Users\user\AppData\Local\Temp\scoped_dir5636_1324291470\CRX_INSTALL_locales\kn\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	20406
Entropy (8bit):	5.312117131662377
Encrypted:	false
SSDEEP:	384:a6C5rBSzvrZreGnla9ZBHRUDYr9yRwEcAa4rSeD5BSz0hJz8qbbM3gbr//Hkr44c:a6C5rBSzvFreGnla9ZBHRUDYr9yRwEcC
MD5:	2E3239FC277287810BC88D93A6691B09
SHA1:	FC5D585DA00ADC90BF79109C7377BD55E6653569
SHA-256:	5FC705AD19761204D8604EA069936A23731B055D51E7836CAAF16AC7719FBEEA
SHA-512:	DF8BC9E577D3ECB0E6C303E1D2C9E9A4A8317CAE810A9DFC88D91B373A4B665722C5A9AB5A589BB947FDA4C7CD9A6DF39DDD13EA47FE9EFF7E0AC43E49FF 3479
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "..... .....".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "1 28276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "180276274658 9457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": ".... $

Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 86

- 53 (DNS)
- 443 (HTTPS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 02:55:14.734889984 CEST	49711	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.739703894 CEST	49714	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.739905119 CEST	49715	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.746876955 CEST	443	49711	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.747003078 CEST	49711	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.747241020 CEST	49711	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.748748064 CEST	49716	443	192.168.2.5	104.16.19.94
Apr 8, 2021 02:55:14.751601934 CEST	443	49714	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.751687050 CEST	49714	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.751823902 CEST	443	49715	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.751883030 CEST	49715	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.752103090 CEST	49714	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.752273083 CEST	49715	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.752861023 CEST	49717	443	192.168.2.5	52.217.76.78
Apr 8, 2021 02:55:14.759068012 CEST	443	49711	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.760550022 CEST	443	49711	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.760602951 CEST	443	49711	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.760658979 CEST	49711	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.760663033 CEST	443	49716	104.16.19.94	192.168.2.5
Apr 8, 2021 02:55:14.760785103 CEST	49716	443	192.168.2.5	104.16.19.94
Apr 8, 2021 02:55:14.761256933 CEST	49716	443	192.168.2.5	104.16.19.94
Apr 8, 2021 02:55:14.763921022 CEST	443	49714	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.764122009 CEST	443	49715	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.765429020 CEST	443	49715	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.765487909 CEST	443	49715	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.765547991 CEST	443	49714	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.765559912 CEST	49715	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.765602112 CEST	443	49714	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.765657902 CEST	49714	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.773190022 CEST	443	49716	104.16.19.94	192.168.2.5
Apr 8, 2021 02:55:14.775613070 CEST	443	49716	104.16.19.94	192.168.2.5
Apr 8, 2021 02:55:14.775659084 CEST	443	49716	104.16.19.94	192.168.2.5
Apr 8, 2021 02:55:14.775731087 CEST	49716	443	192.168.2.5	104.16.19.94
Apr 8, 2021 02:55:14.853142977 CEST	443	49717	52.217.76.78	192.168.2.5
Apr 8, 2021 02:55:14.853295088 CEST	49717	443	192.168.2.5	52.217.76.78
Apr 8, 2021 02:55:14.853575945 CEST	49717	443	192.168.2.5	52.217.76.78
Apr 8, 2021 02:55:14.933538914 CEST	49711	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.934333086 CEST	49714	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.935086012 CEST	49715	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.935271025 CEST	49711	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.935403109 CEST	49714	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.935483932 CEST	49715	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.935590029 CEST	49711	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.935646057 CEST	49714	443	192.168.2.5	104.18.10.207

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 02:55:14.935704947 CEST	49715	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.944030046 CEST	49716	443	192.168.2.5	104.16.19.94
Apr 8, 2021 02:55:14.944343090 CEST	49716	443	192.168.2.5	104.16.19.94
Apr 8, 2021 02:55:14.944534063 CEST	49716	443	192.168.2.5	104.16.19.94
Apr 8, 2021 02:55:14.945482969 CEST	443	49711	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.945663929 CEST	443	49711	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.945873976 CEST	49711	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.946094036 CEST	443	49714	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.946424007 CEST	443	49714	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.946621895 CEST	49714	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.946902990 CEST	443	49715	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.947133064 CEST	443	49715	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.947243929 CEST	443	49711	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.947268963 CEST	443	49711	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.947304010 CEST	443	49715	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.947333097 CEST	443	49715	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.947357893 CEST	443	49714	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.947386980 CEST	443	49711	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.947406054 CEST	49715	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.947412014 CEST	443	49715	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.947436094 CEST	443	49714	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.947469950 CEST	49715	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.948272943 CEST	443	49714	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.953521967 CEST	443	49717	52.217.76.78	192.168.2.5
Apr 8, 2021 02:55:14.953551054 CEST	443	49717	52.217.76.78	192.168.2.5
Apr 8, 2021 02:55:14.953784943 CEST	443	49717	52.217.76.78	192.168.2.5
Apr 8, 2021 02:55:14.953824997 CEST	443	49717	52.217.76.78	192.168.2.5
Apr 8, 2021 02:55:14.953857899 CEST	443	49717	52.217.76.78	192.168.2.5
Apr 8, 2021 02:55:14.953866959 CEST	49717	443	192.168.2.5	52.217.76.78
Apr 8, 2021 02:55:14.953911066 CEST	49717	443	192.168.2.5	52.217.76.78
Apr 8, 2021 02:55:14.954415083 CEST	443	49715	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.954446077 CEST	443	49715	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.954484940 CEST	443	49715	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.954498053 CEST	49715	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.954520941 CEST	49715	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.954525948 CEST	49715	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.954550982 CEST	443	49715	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.954598904 CEST	49715	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.954626083 CEST	443	49715	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.954670906 CEST	443	49715	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.954674959 CEST	49715	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.954698086 CEST	443	49715	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.954715967 CEST	49715	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.954859018 CEST	443	49715	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.954909086 CEST	443	49715	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.954910040 CEST	49715	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.954952002 CEST	443	49715	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.954957962 CEST	49715	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.954989910 CEST	443	49715	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.955002069 CEST	49715	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.955018997 CEST	443	49715	104.18.10.207	192.168.2.5
Apr 8, 2021 02:55:14.955048084 CEST	49715	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.955048084 CEST	443	49717	52.217.76.78	192.168.2.5
Apr 8, 2021 02:55:14.955073118 CEST	443	49717	52.217.76.78	192.168.2.5
Apr 8, 2021 02:55:14.955074072 CEST	49715	443	192.168.2.5	104.18.10.207
Apr 8, 2021 02:55:14.955117941 CEST	49717	443	192.168.2.5	52.217.76.78

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 02:55:06.746754885 CEST	64344	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:06.759272099 CEST	53	64344	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:07.355843067 CEST	62060	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:07.369052887 CEST	53	62060	8.8.8.8	192.168.2.5

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 02:55:08.596153975 CEST	61805	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:08.608968019 CEST	53	61805	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:09.532036066 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:09.692270994 CEST	49557	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:09.704868078 CEST	53	49557	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:10.550772905 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:10.563549995 CEST	53	54795	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:12.582815886 CEST	61733	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:12.598344088 CEST	53	61733	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:14.208633900 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:14.211343050 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:14.214883089 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:14.218964100 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:14.236977100 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:14.237617016 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:14.241703033 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:14.244415998 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:14.497967005 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:14.523462057 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:14.584026098 CEST	56969	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:14.597071886 CEST	53	56969	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:14.709458113 CEST	55161	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:14.710800886 CEST	54757	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:14.711385012 CEST	49992	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:14.711997032 CEST	60075	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:14.712976933 CEST	55016	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:14.723875046 CEST	53	49992	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:14.724342108 CEST	53	60075	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:14.728458881 CEST	53	55161	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:14.733233929 CEST	53	55016	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:14.733834982 CEST	64345	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:14.737328053 CEST	57128	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:14.738456011 CEST	54791	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:14.747535944 CEST	53	54757	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:14.751034975 CEST	53	54791	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:14.756942987 CEST	53	57128	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:14.760946035 CEST	53	64345	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:14.857032061 CEST	50463	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:14.870223045 CEST	53	50463	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:14.943497896 CEST	50394	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:14.956250906 CEST	53	50394	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:14.995826006 CEST	58530	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:15.009123087 CEST	53	58530	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:15.502801895 CEST	63732	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:15.506268978 CEST	57344	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:15.516197920 CEST	53	63732	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:15.532426119 CEST	53	57344	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:15.989837885 CEST	54450	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:16.002412081 CEST	53	54450	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:16.193108082 CEST	59261	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:16.219088078 CEST	53	59261	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:16.979583025 CEST	57151	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:16.992902040 CEST	53	57151	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:17.721013069 CEST	59413	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:17.733843088 CEST	53	59413	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:18.614020109 CEST	60516	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:18.626672029 CEST	53	60516	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:19.573059082 CEST	52929	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:19.585902929 CEST	53	52929	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:28.789949894 CEST	62372	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:28.815901041 CEST	53	62372	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:32.067985058 CEST	61515	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:32.107057095 CEST	53	61515	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:36.635610104 CEST	56675	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 02:55:36.820663929 CEST	53	56675	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:49.928280115 CEST	57172	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:49.941167116 CEST	53	57172	8.8.8.8	192.168.2.5
Apr 8, 2021 02:55:59.921509027 CEST	55267	53	192.168.2.5	8.8.8.8
Apr 8, 2021 02:55:59.939084053 CEST	53	55267	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 02:55:14.709458113 CEST	192.168.2.5	8.8.8.8	0x440a	Standard query (0)	stackpath.bootstrapcdn.com	A (IP address)	IN (0x0001)
Apr 8, 2021 02:55:14.710800886 CEST	192.168.2.5	8.8.8.8	0x7540	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Apr 8, 2021 02:55:14.711997032 CEST	192.168.2.5	8.8.8.8	0xa836	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Apr 8, 2021 02:55:14.712976933 CEST	192.168.2.5	8.8.8.8	0x54da	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Apr 8, 2021 02:55:14.737328053 CEST	192.168.2.5	8.8.8.8	0xbbbb	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)
Apr 8, 2021 02:55:14.738456011 CEST	192.168.2.5	8.8.8.8	0x6456	Standard query (0)	s3.amazonaws.com	A (IP address)	IN (0x0001)
Apr 8, 2021 02:55:28.789949894 CEST	192.168.2.5	8.8.8.8	0xb59	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 02:55:14.724342108 CEST	8.8.8.8	192.168.2.5	0xa836	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 02:55:14.728458881 CEST	8.8.8.8	192.168.2.5	0x440a	No error (0)	stackpath.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Apr 8, 2021 02:55:14.728458881 CEST	8.8.8.8	192.168.2.5	0x440a	No error (0)	stackpath.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Apr 8, 2021 02:55:14.733233929 CEST	8.8.8.8	192.168.2.5	0x54da	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Apr 8, 2021 02:55:14.733233929 CEST	8.8.8.8	192.168.2.5	0x54da	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Apr 8, 2021 02:55:14.747535944 CEST	8.8.8.8	192.168.2.5	0x7540	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Apr 8, 2021 02:55:14.747535944 CEST	8.8.8.8	192.168.2.5	0x7540	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Apr 8, 2021 02:55:14.751034975 CEST	8.8.8.8	192.168.2.5	0x6456	No error (0)	s3.amazonaws.com		52.217.76.78	A (IP address)	IN (0x0001)
Apr 8, 2021 02:55:14.756942987 CEST	8.8.8.8	192.168.2.5	0xbbbb	No error (0)	cdn.jsdelivr.net	cdn.jsdelivr.net.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 02:55:28.815901041 CEST	8.8.8.8	192.168.2.5	0xb59	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 02:55:28.815901041 CEST	8.8.8.8	192.168.2.5	0xb59	No error (0)	googlehosted.l.googleusercontent.com		172.217.168.33	A (IP address)	IN (0x0001)

HTTPS Packets

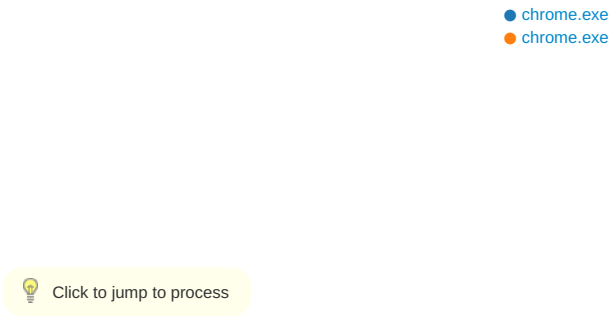
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 8, 2021 02:55:14.953857899 CEST	52.217.76.78	443	192.168.2.5	49717	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	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 Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5636 Parent PID: 3396

General

Start time:	02:55:10
Start date:	08/04/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://firebasestorage.googleapis.com/v0/b/kcdvdjv037jcdi0e3767933.appspot.com/o/!%7D%7B%24%23%40%5E%26%20jaf%40!__%7D%20.html?alt=media&token=08503d5e-c8e8-4a7c-b39c-8a3de4c0bf78#jason.maddern@navitas.com'
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true

Copyright Joe Security LLC 2021

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: 3952 Parent PID: 5636

General

Start time:	02:55:11
Start date:	08/04/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1616,10129630995323838965,6101514469676002512,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1680 /prefetch:8
Imagebase:	0x7ff677c70000
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

Copyright Joe Security LLC 2021