ID: 452174
Cookbook: browseurl.jbs
Time: 22:41:05
Date: 21/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report
http://qtcheiz.northcroft.co.th/#ZGFybGFhbmRyaWNAY29sZHdlbGxiYW5rZXIuY29t#aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbQ==#jngdheuy
Overview 33
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Overview 3
Sigma Overview 3
Jbx Signature Overview 3
AV Detection: 4
Phishing: 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted URLs 7
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
Private 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 40
No static file info 40
Network Behavior 40
Network Port Distribution 40
TCP Packets 40
UDP Packets 40
DNS Queries 40
DNS Answers 40
HTTP Request Dependency Graph 41
HTTP Packets 41
HTTPS Packets 42
Code Manipulations 43
Statistics 43
Behavior 43
System Behavior 43
Analysis Process: chrome.exe PID: 5336 Parent PID: 4364 43
General 43
File Activities 43
Registry Activities 43
Analysis Process: chrome.exe PID: 912 Parent PID: 5336 43
General 43
File Activities 44
Registry Activities 44
Disassembly 44

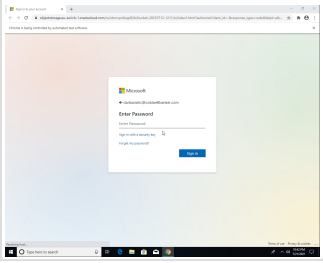
Windows Analysis Report http://qtcheiz.northcroft.co.th…

Overview

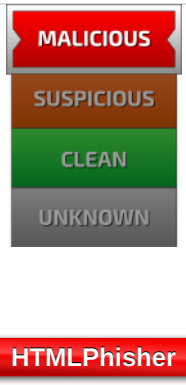
General Information

Sample URL:	http://qtcheiz.northcroft.co.th/#ZGFybGFhbmRyaWNAY29sZHdlbGxiYW5rZXIuY29t#aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbQ==#jngdheuy
Analysis ID:	452174
Infos:	

Most interesting Screenshot:



Detection



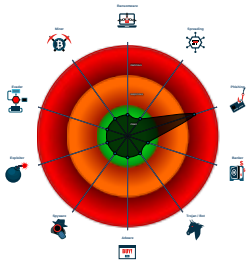
HTMLPhisher

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Yara detected HtmlPhish10
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5336 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'http://qtcheiz.northcroft.co.th/#ZGFybGFhbmRyaWNAY29sZHdlbGxiYW5rZXIuY29t#aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbQ==#jngdheuy' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 912 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1552,14705750287286471760,12854902564490349709,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1800 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Phishing:

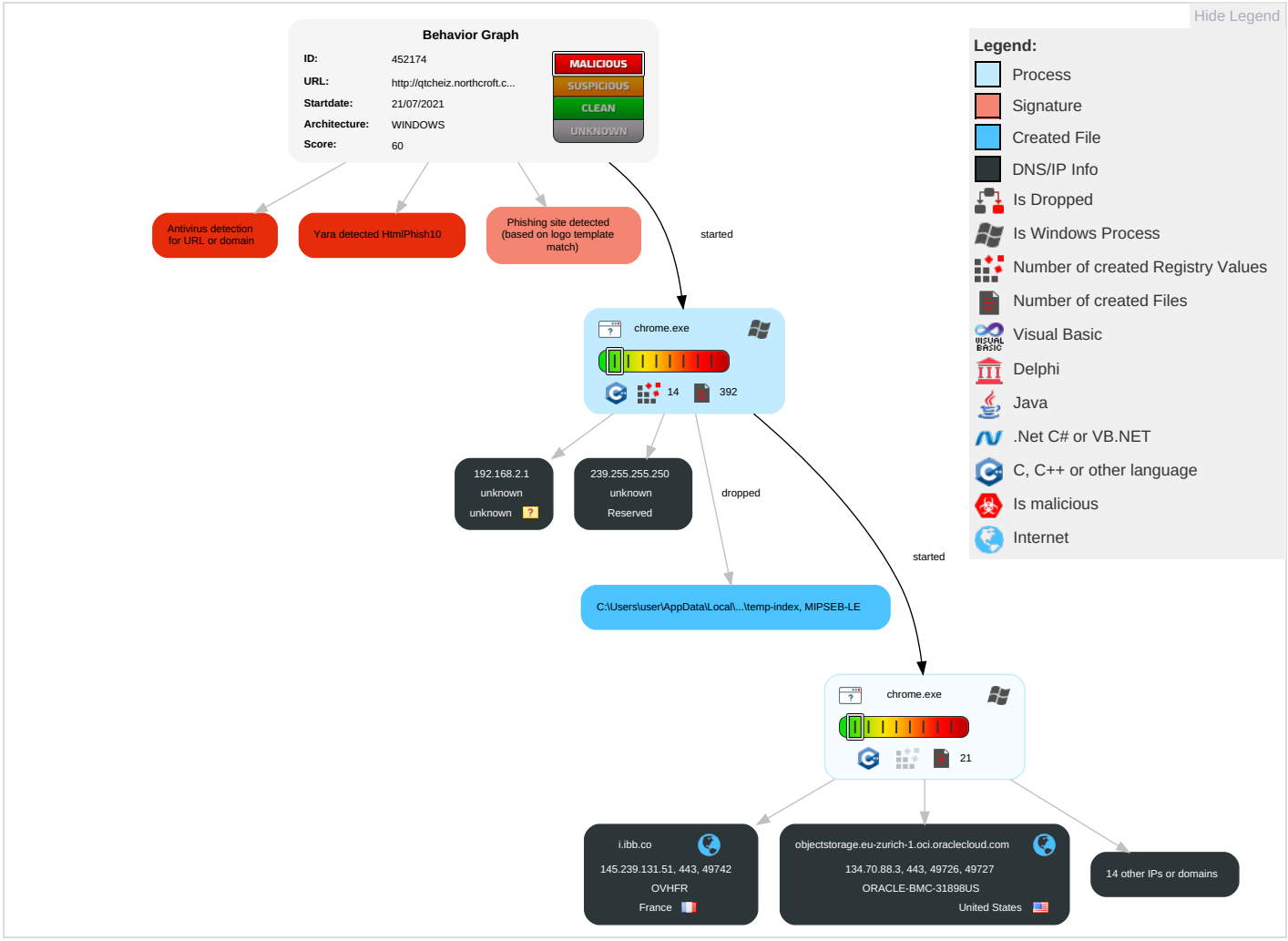
Yara detected HtmlPhish10

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

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

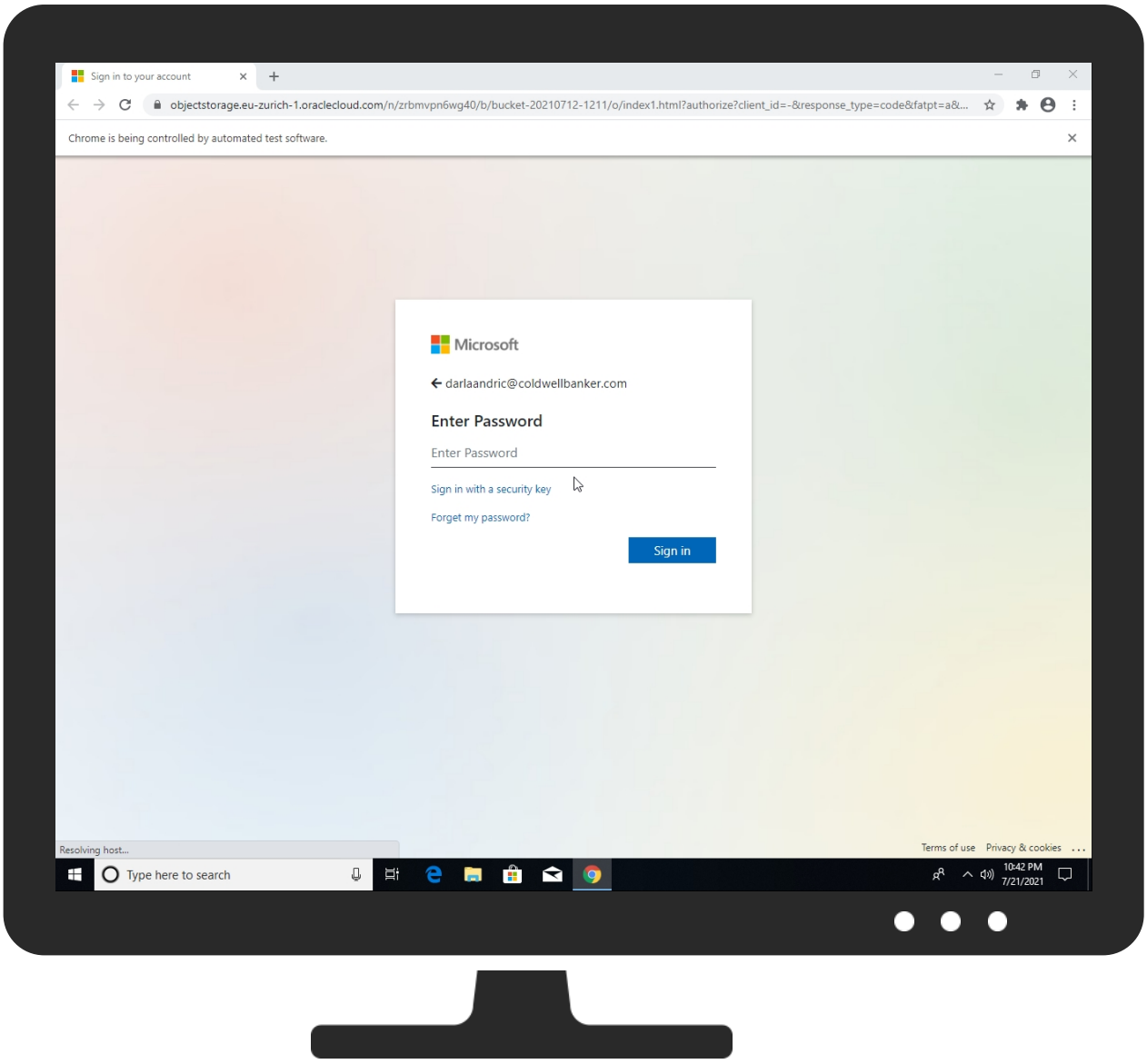
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://qtcheiz.northcroft.co.th/#ZGFybGFhbmRyaWNAY29sZHdlbGxiYW5rZXIuY29t#aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbQ==#jngdheuy	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://objectstorage.eu-zurich-1.oraclecloud.com/n/zrbmvpn6wg40/b/bucket-20210712-1211/o/index1.html?authorize?client_id=-&response_type=code&fatpt=a&client_id=51483342-085c-4d86-bf88-cf50c7252078&scope=openid+profile+email+offline_access&response_mode=form_post&redirect_uri=https%3a%2f%2flogin.microsoftonline.com%2fcommon%2ffederation%2foauth2&state=rQIIAXWSPW_TUBSGc5M0NFEFFUKCMQMsSE6urz9iR-qQkMR1SK7TfDRNlihx7Npx7Osmzpd_AUhIdM6ChISQKiYECPETKiHKWgl16YCYKibEhNud5bzDeYaj9zmPI3SKzj5kGZbrZwYiJfZ5hmJFGlJ9FvEUwzE8gyA95CAzuZvY_vBi653ysiw_v1z9ePSq3liDeG9szrWUSuwTcN_wPHeaTacXi0WK6Lqp3izSnwE4A-AnAOvwhuZQrcZJeMozvMAKPMeyIqQhzQhsqjoqLpV2Z4ntotfxsak0IKwWykalaXHdguV1C6URbrb8jl2yqvbeAo_yFm7mkFLlediWVze8Xx9V2qVRFckB3_KDhFiSYcevG-fhO0pu5hnoepCJ6Wu_w3GdTOyeS6beOvIWKK7myMMnxHE01UtdY5rjmWrfM4lTmxBXm3imNt0RW-6AyowPO8v-3N49WvGZXE9mMnSuKez2jD4tmBanaOVaiS9alcG0WyaC8BT7ECqNUeeAlkTUVmpIsor7_FKrMQuvW9GJinEmT0mzglxddsdUHtXn6l7JLRt4sH9QrxozvS4Tm-RbNf59JBbUahPnNHI7OMoxh0l3QnRzrJ1Fwa_oFoxkNzcT26EHoWToTxS83gjMXX28jH79-0168-lCvfiOQ6cbaavBtdHYkg8xHJSlMWfKMzNQPWNVPY9cC9mNll9aHUmyAnfoLH0cA8ex2FUMPLsV-hL_n-vzxL3gX0QKIgqySShkGZSlhe4_0&estsfed=1&uaid=ac0c8cb48f4f494a89e479dd259f5253&fci=4345a7b9-9a63-4910-a426-&mkt=en-US#darlaandric@coldwellbanker.com	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://qtcheiz.northcroft.co.th	0%	Avira URL Cloud	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	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://qtcheiz.northcroft.co.th/#ZGFybGFhbmRyaWNAY29sZHdlbGxiYW5rZXIuY29t#aHR0cHM6Ly93d3cuZ29vZ2xlLm	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external	0%	URL Reputation	safe	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external	0%	URL Reputation	safe	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external	0%	URL Reputation	safe	
http://https://csp.withgoogle.com/csp/report-to/downloads-lorry	0%	Avira URL Cloud	safe	
http://qtcheiz.northcroft.co.th/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	142.250.203.99	true	false		high
objectstorage.eu-zurich-1.oci.oraclecloud.com	134.70.88.3	true	false		high
accounts.google.com	172.217.168.45	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
qtcheiz.northcroft.co.th	203.151.56.123	true	false		unknown
clients.l.google.com	142.250.203.110	true	false		high
googlehosted.l.googleusercontent.com	172.217.168.65	true	false		high
i.ibb.co	145.239.131.51	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
ka-f.fontawesome.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high
objectstorage.eu-zurich-1.oraclecloud.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://objectstorage.eu-zurich-1.oraclecloud.com/n/zrbmvpn6wg40/b/bucket-20210712-1211/o/index1.html?authorize?client_id=-&response_type=code&fatpt=a&client_id=51483342-085c-4d86-bf88-cf50c7252078&scope=openid+profile+email+offline_access&response_mode=form_post&redirect_uri=https%3a%2f%2flogin.microsoftonline.com%2fcommon%2ffederation%2foauth2&state=rQIIAXWSPW_TUBSGc5M0NFEFFUKCMQMsSE6urz9iR-qQkMR1SK7TfDRNlihx7Npx7Osmzpd_AUhIdM6ChISQKiYECPETKiHKWgl16YCYKibEhNud5bzDeYaj9zmPI3SKzj5kGZbrZwYiJfZ5hmJFGlJ9FvEUwzE8gyA95CAzuZvY_vBi653ysiw_v1z9ePSq3liDeG9szrWUSuwTcN_wPHeaTacXi0WK6Lqp3izSnwE4A-AnAOvwhuZQrcZJeMozvMAKPMeyIqQhzQhsqjoqLpV2Z4ntotfxsak0IKwWykalaXHdguV1C6URbrb8jl2yqvbeAo_yFm7mkFLIediWVze8Xx9V2qVRFckB3_KDhFiSYcevG-fhO0pu5hnoepCJ6Wu_w3GdTOyeS6beOvIWKK7myMMnxHE01UtdY5rjmWrfM4lTmxBXm3imNt0RW-6AyowPO8v-3N49WvGZXE9mMnSuKez2jD4tmBanaOVaiS9alcG0WyaC8BT7ECqNUeeAlkTUVmpIsor7_FKrMQuvW9GJinEmT0mzglxddsdUHtXn6l7JLRt4sH9QrxozvS4Tm-RbNf59JBbUahPnNHI7OMoxh0l3QnRzrJ1Fwa_oFoxkNzcT26EHoWToTxS83gjMXX28jH79-0168-lCvfiOQ6cbaavBtdHYkg8xHJSlMWfKMzNQPWNVPY9cC9mNll9aHUmyAnfoLH0cA8ex2FUMPLsV-hL_n-vzxL3gX0QKIgqySShkGZSlhe4_0&estsfed=1&uaid=ac0c8cb48f4f494a89e479dd259f5253&fci=4345a7b9-9a63-4910-a426-&mkt=en-US#darlaandric@coldwellbanker.com	false	• SlashNext: Fake Login Page type: Phishing & Social Engineering	high
http://qtcheiz.northcroft.co.th/	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
145.239.131.51	i.ibb.co	France		16276	OVHFR	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
203.151.56.123	qtcheiz.northcroft.co.th	Thailand		4618	INET-TH-ASInternetThailandCompanyLimitedTH	false
104.18.11.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.217.168.65	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
134.70.88.3	objectstorage.eu-zurich-1.oci.oraclecloud.com	United States		31898	ORACLE-BMC-31898US	false
142.250.203.99	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	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:	33.0.0 White Diamond
Analysis ID:	452174
Start date:	21.07.2021
Start time:	22:41:05
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://qtcheiz.northcroft.co.th/#ZGFybGFhbmRyaWNAY29sZHdlbGxiYW5rZXIuY29t#aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbQ==#jngdheuy
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	11

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:	mal60.phis.win@29/174@12/12
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
22:41:59	API Interceptor	2x 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

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic

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, 61020 bytes, 1 file
Category:	dropped
Size (bytes):	122040
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	3072:0tdeYPiuWAVtlLBGbtdeYPiuWAVtlLBGm:0rec7VDBGbrec7VDBGm
MD5:	516136E560C1392A28EDFA1A957050D7
SHA1:	BBDF208E48EFC052D332255EF84184BFC946BF5F
SHA-256:	4F812F7C8163C50FE75F441AC6797E18D02B8B66895BC94D0E1153FE24FADEFE
SHA-512:	8F25750E9014F7576E5C81E1A3DE605BB29839A38F0E60D58AB79E034ED1847D9E88A427A834BCA95BF7C4627197AC1194D5A487E0D5E5F88B95E46C4574A425
Malicious:	false
Reputation:	low
Preview:	MSCF....\.....,.....I.....l.....R.q .authroot.stl.N....5..CK..8T....c_.d....A.K....=.D.eWI..r."Y...."i..,.=.l.D.....3...3WW.....y...9..w..D.yM10....`.0.e.._.'..a0xN....)F.C..t .z.,.O20.1``L.....m?H..C..X>Oc..q.....%.!^v%<...O...-..@/.....H.J.W..... T...Fp..2.|$....._Y..Y`&..s.1.....s.{..,."':o}9.....%._.xW*S.K..4"9.....q.G:.....a.H.y.. ..r...q./6.p.;.` =*.Dwj.....!.....s).B..y.....A.!W.....D!s0..!"X...l.....D0.....Ba...Z.0.o..l.3.v..W1F hSp.S)@.....'Z..QW...G...G.G.y+.x...aa`.3..X&4E..N...._O..<X.....K...xm..+M...O.H...)... .....*..o..~4.6.....p.`Bt.(..*V.N.!.p.C>..%.ySXY.>.`..f|.*...'^K`\..e.....j/..|..)..&i...wEj.w...o..r<.$.....C.....}.x...L..&..).r..\...>....v.....7...^..L!.$..'m...*,*.....7F$..~..S.6$S.-y....|.!.....x ...~k...Q/.w.e...h.[...9<x...Q.x.][}*_%Z..K.).3..'....M.6QkJ.N.....Y..Q.n.[.(.... ...Bg..33..[...S..[... .Z..<i.-.]...po.k.,...X6.....y3^.t[.Dw.]ts. R..L..`..ut_F....

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):	652
Entropy (8bit):	3.1503175808495025
Encrypted:	false
SSDEEP:	12:qY5kPlE99SNxAhUe0eV5kPlE99SNxAhUe0et:d5kPcUQUfeV5kPcUQUfet
MD5:	D8BA168382D9290297936FCD7A061FF5
SHA1:	93E25DEEAB9FC643696C9D7E4EF3672C64C1346E
SHA-256:	C324380947A95FC814C382335B05AD9A0D63E22BE362D92FD07ED3E48EE93393
SHA-512:	A2732E57B0351520D006D774304AD044D94B5513E105EC212BC677EE29EEC1D0102C9708E38940234872218D4B746EE9B95B4AFF01465FEAFD7D05A85550923C
Malicious:	false
Reputation:	low
Preview:	p..... .....XJ.~..(..... .....T'._.....$.....\...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.6.5.4.2.7.7.5.f.d.7.1.::0."...p..... .....L.vJ.~..(..... .....T'._.....$.....\...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.6.5.4.2.7.7.5.f.d.7.1.::0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\2ef16e51-7228-406e-bcce-71431087411e.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):	173828
Entropy (8bit):	6.079791963165406
Encrypted:	false
SSDEEP:	3072:2uv1gVSNH8838AAZ20/IV8l4fpi4UJRFcbXafIB0u1GOJmA3iuRH:nvsSGAV8l4fAzJ/aqfIlUOoSiuRH
MD5:	77A7E875A7B11B0F76FABD11CBF6CED0
SHA1:	474870ACE846A219AD5607F90A7964CA8A78A69C
SHA-256:	DEBE1E8D6D66083DE69360CFF262C064530BBD6F5F3D5E602607DF14A3F21499

C:\Users\user\AppData\Local\Google\Chrome\User Data\2ef16e51-7228-406e-bcce-71431087411e.tmp	
SHA-512:	0E0D5428FBDCD5410A27CFE0C5F722E852BA7A8DDF6B265574CDB5C1F40DD66F0C0451D0A273051373558A06B8DA8E4CDF9491F84C1C6DD0FD8102A874CB4E 0
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":1.626932516133504e+12,"network":1.626900119e+12,"ticks":6888068441.0,"uncertainty":5197788.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\54b03d5d-ee80-4ee3-af08-6691f12b9736.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):	173828
Entropy (8bit):	6.079791156039502
Encrypted:	false
SSDEEP:	3072:2fg1gVSNH8838AAZ20/IV8l4fpi4UJRFcbXafIB0u1GOJmA3iuRH:WgsSGAV8l4fAzJ/aqfIlUOoSiuRH
MD5:	DC9790542202F9E1D98669A3002E45D7
SHA1:	9903CFE7421B9BB5442B2C046DAD74BD882CD20F
SHA-256:	0509575AE9CD7A5E8A299BE1F9DE2A34C182D17E00C279A8291259763569CA04
SHA-512:	8C7A00F06795FD9FEEB542CEB2CA3FB1157AB11EC7CE63313BAF8534B5B5E5E76AA362BE421C97E3CFAAD173D1785797750AA37584F9037D46F8A58EB1B36DF7
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":1.626932516133504e+12,"network":1.626900119e+12,"ticks":6888068441.0,"uncertainty":5197788.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\5c6621a2-41f4-4417-85ef-c4c6472aab06.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.743288742493418
Encrypted:	false
SSDEEP:	384:7HvIQa9ru2RcTNgrJvcI3Tw67HGPGnarF6s6xDOiWFrxEmFSJqgIcDOCGQNt1AZR:B+x52KTn8eneIaAn3aEKmwwVQ
MD5:	0AE3AB8DB7A922E17D89607503E7557C
SHA1:	FDF0E35A5F04D869015647AE4333877CB2D627B9
SHA-256:	80FE8ED674EB3C565242DEB25A586692A9D56A9D5F7508D7458D79EA407A96AA
SHA-512:	58B86D57B1BB278C59A68EFCF226E3E8D3426590741667BC144A786EFE7B5FBF72C78509D3E84FA3FF8639B90C6A423864BE86F1F13F47E06BD54E7014EC63C4
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...e@8.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\9a7ef721-87e8-43b9-80a2-bb30c044f2fd.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):	173828
Entropy (8bit):	6.079792180502234
Encrypted:	false
SSDEEP:	3072:Rfg1gVSNH8838AAZ20/IV8l4fpi4UJRFcbXafIB0u1GOJmA3iuRH:pgsSGAV8l4fAzJ/aqfIlUOoSiuRH
MD5:	CCF5E318D27D968DA85CE32FB25EF385
SHA1:	E085188FF754BA14AACE6A398123321FA7123D92
SHA-256:	ACFD098D8344F2EAA335F1AD1392CB76B2E47C3272DAC7FE16BA0DF8D6253CF4
SHA-512:	170FA830895932538B4BAEE60F6B7DF76F184DD32AADA6FBAC713950AD721373AA75D3918D07AE441F66229B258A120B7B12415F3EF7025E1C804A449A3A4DE0

C:\Users\user\AppData\Local\Google\Chrome\User Data\9a7ef721-87e8-43b9-80a2-bb30c044f2fd.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":1.626932516133504e+12,"network":1.626900119e+12,"ticks":6888068441.0,"uncertainty":5197788.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016659284"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftlE1G1mkftlE1G1mkftlE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D0212942563 72C916B8155AC
Malicious:	false
Reputation:	low
Preview:	sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1fd7db45-e92e-48b6-8f0f-11a515ddfe77.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):	2433
Entropy (8bit):	4.875259230445592
Encrypted:	false
SSDEEP:	48:Y2TntwXGDH3qyvz5saDsiRLsuTs13SE6Ne8AsRz6zsX8qoYhbD:JTnOXGDHa+z17Be36NjZzHrJhH
MD5:	181A570E65F1889CB005DC56EA208417
SHA1:	748D9DD0CFEBF72356DF9EC472C1D8F15F293646
SHA-256:	E683CF361948D7747BFA9AD4B1C4D0A25E5BFEA74FCFCC6DD380B9671F0F6C00
SHA-512:	8E318A23732AE9345028223C200DEE7AFD79A1F1476E6B0598D553FDFD8E48A6B172EDC41DB003695A3F0B5992A0433DFF6EEBF5535A9B0B8DB740A6E2D3139
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13273998118161180","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13273998118162840","port"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\335f0e7a-050c-4df7-aca2-3e72d5a73f9e.tmp

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\533add13-01d5-470e-a44c-be849bef5c4c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22595
Entropy (8bit):	5.535729702270241
Encrypted:	false
SSDEEP:	384:VcqJtILlCNXV1kXqKf/pUZNCgVLH2HfDNrUDHGwnTlkcMP+f4A:ViLlyV1kXqKf/pUZNCgVLH2HfJrUjGwd
MD5:	7F480DBE659463456DD0906ED9474639
SHA1:	B0FE2F07E46D7FDC15D3737DF6976EFE8C53959F
SHA-256:	57258F380091A751725FB628CABEF794C824039F847F216D4CF6ED4A7B1B75E0
SHA-512:	DD835499B3F7D70FC4A231E06AD91161597B642DE4FE4D60C4822EE41817AB4D9D80AA822DDB03FAA3B9F5EB87EB6E1D8964F60E4F7E7635F1CA7CF6A775DC8D
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":"13271406112642599","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\542fda5e-f98f-4653-865d-b5d0543a2ae2.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):	5.535572632129791
Encrypted:	false
SSDEEP:	384:VcqJtILlCNXV1kXqKf/pUZNCgVLH2HfDNrUDHGDnTlkc7+f4V:ViLlyV1kXqKf/pUZNCgVLH2HfJrUjGDz
MD5:	DD5F243D0E52D8E014E004FC58C3E664
SHA1:	49AABFE8B0A2CDD51F683A284C098BCC5A7B79FF
SHA-256:	5ECED400F806C23486C1338BC4F96991EBB15C39D1D20B8C391D12F827EE5284
SHA-512:	FB115A9FCE12C0D352E3715417D85F16F4AB7CF0241E65C37E03BB68083927E1146879AEDC1B5F79848E099EC4406E005CCDFCDF5C0B1FA6920516B46CF64C9
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":"13271406112642599","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\707748d8-06ef-431d-8cd1-5c81acb8cbfe.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7de7aac2-8e75-44ca-894f-8f4680534f25.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7de7aac2-8e75-44ca-894f-8f4680534f25.tmp	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5317
Entropy (8bit):	4.99583482867056
Encrypted:	false
SSDEEP:	96:nGCzGXMpcKI15ok0JC/VRWL83xkI1IbOTQVuwn:nGCAMpc84/VY6xkIE
MD5:	218960A798B212811D740B59D116B7CD
SHA1:	F826796B7B0AD969C8F7D16ECDDAEEDC8AE0BD96
SHA-256:	16700C6B1C8EB597BD7BF70F6EB51A3DD862EB559A4F33C0F70B158D58B6E6A6
SHA-512:	D6D95A097C8069791BE8475733DCCB7357A5FF938372D8423E9CBF24CA85FF2B50D578D3BCE2291D66FD64B54F0F8D8A56987786BDA105EA6A41E92774AC6ED
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271406112979399","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8984dc36-6988-4ca8-b60d-fbea851885df.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):	1543
Entropy (8bit):	5.580837444102126
Encrypted:	false
SSDEEP:	48:YxVwUS6UUheeUoZ0KUgcqPeUer2Uef3wU0sYUdUenw:lU3UUpUoOKUwPeU9UEgUtYUdUD
MD5:	26B215F3E30EA0510E8C71194E18FB72
SHA1:	F205664DE2BF13AD7C195EE8E80E558BD43CA8D6
SHA-256:	FE0194C37B983F74058886BED5AF0426AAD8F64E61BD036E81C0E4E30F6EDB3A
SHA-512:	A28E68684AF5709B8C0343989C5ED8868457A85E15662F37056F767552B59C39A73FFDB81D7622E670E356E195CB47703842A0C68FA9E1DA43C3737081306133
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1642712519.440933,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626932519.440936},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1658468519.559082,"host":"PmHKo9+NfFu9AjQSxw3MoTtfuXIu9G3fM8KGQt4xie4=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626932519.559086},{"expiry":1658468519.442816,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626932519.442819},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_ob

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):	331
Entropy (8bit):	5.185994256771064
Encrypted:	false
SSDEEP:	6:m8UL4q2PWXp+N23iKKdK9RXXTZIFUtp/XIZZmwP2F43DkwOWXp+N23iKKdK9RXXH:SMva5Kk7XT2FUtp/X0/P2FE5f5Kk7XVJ
MD5:	9C907EAF192D2ED9591645F6EE73C978
SHA1:	DC035064405B686A5F224A68CAE1E28C9A1EF4FF
SHA-256:	4F52402499AAFF53B33D7788022A6AACA2FF6E14434AAE3484E4A0580CF3165F
SHA-512:	74D99ABB2119F89F9FC2745EBA0D33DBA6BA0A7F1351418C483959DC47E9C47DD2D097C4EBB8182018A68721B80FB68CE55BA82E874D921063C4E8172D337CEB
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:42:09.777 2a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/07/21-22:42:09.779 2a4 Recovering log #3.2021/07/21-22:42:09.787 2a4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	315
Entropy (8bit):	5.170466330050089

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Encrypted:	false
SSDEEP:	6:mJDq2PWXp+N23iKKdKyDZIFUtpXU9ZmwPXUPkwOWXp+N23iKKdKyJLJ:mDva5Kk02FUtpXk/PXE5f5KkWJ
MD5:	C64B928B8F8812C92CF3D38014106C9C
SHA1:	A75222F68B010D94B2394714772B78BA7EB023B3
SHA-256:	4E66C124A6915EB905B540761352C1957EEEFB7AAFC788EE3B5B7739BD6DD350
SHA-512:	DF978133EFF4493C20D545F4F5039DEB4262A76EBE96261671EB4DAAF03F440AC7C4CFF2A98AB8D3F7CE71246F22D1F5168DA4313D6BBB9161F1F9BC415B91D9
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:42:09.769 2a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/07/21-22:42:09.771 2a4 Recovering log #3.2021/07/21-22:42:09.771 2a4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\29acef4d73e591ec_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97728
Entropy (8bit):	5.784122912783479
Encrypted:	false
SSDEEP:	1536:EoqyOcUK7qe1KIeUzujeVeqM9+F5MOz7Wqjc4av265DgRX/NoA6jQpTQt9G1qvF5:A5Kf/eRMS9+5MO64E2wD0oA6YB1qD
MD5:	64403B2908B4DB350D8B293264E0DAD5
SHA1:	243B747F9F29FC28A7BBC8059DA113992E96A1BE
SHA-256:	54DD40DC86705A96F0396AC4F0106D943FB1EF8B033BD0BF80250831C46F7161
SHA-512:	ACECFB84A6FF6962B38CB21E026C5CAA2D4D9755AA26612629EDBC71D9FF6B9AEFEDBA9D162E12630E49100CC87B1C47EBD2306FE969587CDD9355142CBA49E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...r&.....FB083AC4F49D38F84ACBB1E36D541095AB8EFA19CEA1FF5C49A265DC4724CEAE.....'.JN....O!...h|...p.....!.....L.....(.....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....O.`....I`....Da....*.....Q.@..1.....module....Q.@rdUs....exports...Qc.. E..document.(S.....5.a.....a.....a.....a.....a.....Pc.....exportsa.....I.....@.-....LP.!.....@...https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.jsa.....D`....D`&...D`.....`z...&...&..!.&....&.(S....!..`.C.....q.L`.....Rc@.....M.....QbN..7....d.....Qb.|.....e.....Qb.`.....f.....Qb.D.i....h.....S...Qb^..$....j....Qb.....k.....Qb.....l.....Qb.Q.....n.....Qb.%.....o.....QbR.....p.....Qb...V....q.....Qb6..7....r.....Qb:tu.....s.....R....QbrY.s....v.....Qbr.....w.....Qb.%.....x.....Qb...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4ad9234e445d4284_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.929549731137413
Encrypted:	false
SSDEEP:	6:mKIXYSHT8NWQAlKPUQyVyQDIUyVkklTxU5HEkYFhK6tTrZ5e5wYugzGIvxU5HEkY:diz8NWQCUU3akkl9U5kkW7ZrZAuAGIpW
MD5:	541F4146AD637DD196BB3B4C682068DD
SHA1:	2DCF67390B9D90B7EB3760F1DA3212A12EE7C426
SHA-256:	518B338FD333FE733605E43286DF4CE5E5B05DDB735BF05F9B92E4523CD8B4BA
SHA-512:	8A469C8915EF3589AA6ABE616F5F2571B2E435524591E28E5ACD2BB740CEC0CE04B8E2BFF4A51E42050146A13B021BDDD3CE18D6A650325AB975790D229A736
Malicious:	false
Reputation:	low
Preview:	0\r..m.....^....._keyhttps://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js .https://oraclecloud.com/].k.F&/.....g#-N..N.rF.....N.tsK.Y.+...A..Eo.....vCRu.....A..Eo.....].k.F&/..}..FB083AC4F49D38F84ACBB1E36D541095AB8EFA19CEA1FF5C49A265DC4724CEAE..g#-N..N.rF.....N.tsK.Y.+...A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\86d2d4c4aefd5c8f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.461561003988308
Encrypted:	false
SSDEEP:	6:mValPYET08NaYWbVOqZ2yQDlWVqU8efDeePj5RK6t:9g8NaY8Z+0V8ADeerp
MD5:	D185650B40A1BF9AA6D53575D8E074C5
SHA1:	1175D6212C3C402D8B312CD19C60DAEC11F265FD
SHA-256:	1C58CCD387191783B8C4519B064A482E3B588E1398313483667A0D30EB53ADF6
SHA-512:	F4519A860CC00D9FA9B842719FA1F411E3100684D2F9E50A89E30E013907FB9108C5B9F6ED929F3D11D5DD5EF78A368890B7D70E14F49164930A4EDEBEC0E0D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\86d2d4c4aefd5c8f_0	
Preview:	0\r..m.....g...e.@3...._keyhttps://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js .https://oraclecloud.com/.,k.F&/.....K.....Ql....W....jL.;zfT :@%.q ...K.Y..A..Eo.....K.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\92a59e12c6439cb6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	229
Entropy (8bit):	5.394347459158857
Encrypted:	false
SSDEEP:	6:mi4eVY68E9xEEUgLEr2yQDE/uVs/o7oKSbK6t:T4eDYghrMo0K0
MD5:	1D4AEC27B6A2D7F06236FB860725DF78
SHA1:	3E072049668A09D77E304CC48E7CCEFA29F13EBB
SHA-256:	1BF1B0FDA9A29D74C3B677F271B7FD9B92871E443EF40A6F9C82AED41EAB8E89
SHA-512:	31B5BFE228DD174A788024DB7E67885112BE679A7EE91E9F239BB38C3EDE81CF8F088B33EABCD3B39867005D04904BEF42357CE018BF8577F4D40B837A030C0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a.....]....._keyhttps://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js .https://oraclecloud.com/..m.F&/.....e.....]...k..H(A.#!...8..=..%.E0... A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f5013d11a0f41b5a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	203
Entropy (8bit):	5.49477661926104
Encrypted:	false
SSDEEP:	6:mwm/XYlNYpSVkvyQDSxjWFVOm3ZtN3nG4rxK6t:dSpSVuu0fxEg
MD5:	988C3BEDA91B6974582A6A33F29684E3
SHA1:	2B75F273D2379CA3A4E067161138262DE274A8A8
SHA-256:	B8F68BDDE15D16602E26D7EFAA5060E47D479D293F1EBE743557290155E392B5
SHA-512:	3D35BFDA22AE414532C410149540DFEED95B4BED4AD61E566B34A214919BF90BF780D6B5D04F51F27D594B0FD1307483087880519CEA3708542F960902458B87
Malicious:	false
Reputation:	low
Preview:	0\r..m.....G...N,.R...._keyhttps://kit.fontawesome.com/585b051251.js .https://oraclecloud.com/GOl.F&/.....VZ...AG=....Fa!+S~...Z.@+}....A..Eo.....jb.$.....A..E o.....

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:	MIPSEB-LE ECOFF executable not stripped - version 0.0
Category:	dropped
Size (bytes):	360
Entropy (8bit):	4.991543292690707
Encrypted:	false
SSDEEP:	6:+bhSkA80VWFS3lW6lazQ3zbn3pHkQ+IRwHxCl:+bssSIPzyz7V4hxCl
MD5:	0D4FDDDED48A527B81A7668840FA7C7B
SHA1:	85FCA0C1CBD2A68E1F4B1ADE5ACA649163F0BAD7
SHA-256:	A11049073AEA855998FAF921348A86B00E36435BAD983835D6CD95737BF3D88C
SHA-512:	73BFE9F53501D623237568EBF905FB7156DA63D193C107C92C13BEF5EAA4ED6068D014A8486CFDC9FDE5421DFE517BED04DE83934D79C35B2057F55B408B91D
Malicious:	false
Reputation:	low
Preview:	`...n.noy retne.....sM.)..s.F&/.....C.....s.F&/.....\.....s.F&/.....Z....=....d.F&/.....B]DN#.J..d.F&/.....^}.Np..@ikt../.....-..0..x@ikt../...../.. .3.KPu../.....KPu../.....&<..\.O$.KPu../.....p..(....KPu../.....q...._.KPu../.....+<P|...X.KPu../.....w.F&/.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	0.6863571317626186
Encrypted:	false
SSDEEP:	12:TLyen4ufFdbXGwcFOaOndOtJRbGMNmt2SH/+eVpUHFxOUwae6:TLyqJLbXaFpEO5bNmISHn06Uwd
MD5:	1C0EAEEE6463CAE33B7A7CD9D9DF4DA5

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
SHA1:	FBC6A28A1501E40154FDC0A9D0C2F34A5F88AA65
SHA-256:	ED8AE7C5E6885874A39F4E86258F552670352A18D29BE1FF4D372A2F4CD06C8A
SHA-512:	355D19828609971998B09B36E7C7D304B7FB88C7A726670BEBF5CF2E2710F8E71B0F9DEF6FE9712B484C1EB122AEEEFDECF31D13E02C4539C399DFB86EC7619F
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9673851368193657
Encrypted:	false
SSDEEP:	24:+cLgAZOZD/sWqLbJLbXaFpEO5bNmISHn06UwGt8:+8NOZsWq5LLOpEO5J/Kn7Uj8
MD5:	C474A316150FBFCDD5B5349122E99620
SHA1:	B74E8521A7E26BF0F0D90AD5EC49E14B36FD3901
SHA-256:	459CFF8D7AD9C7EE1AE128900A9588E1F1427B4D0E9544811AE1EB53934A578E
SHA-512:	AE1F80F8395E7EABA6920311D0DF6936856940ABA9521AECE853C312F3D633E193EF15A8FE884648D221CDBAF9FAC5EA0942465F416D2A864A150A2EB60F99A3
Malicious:	false
Reputation:	low
Preview:	.....w.@R..... ....

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):	5076
Entropy (8bit):	4.605001552422819
Encrypted:	false
SSDEEP:	96:34CWs3aDEAc8C1UV13GlWgMM2hs68trj0ozxVcIdw:3uDEAc8zPWgMhL60AVcIdw
MD5:	B6B33C5268C0CACCF78E4EF5FF5C8B59
SHA1:	4237B6BA9B7C9355F55258128E60E4E6D6113FD0
SHA-256:	B6DD031A20A447A414108CD857C977A4332F7BBBD72B48C703F8768824495EC2
SHA-512:	CAB0D4D63D337AC6ABAE39ECE25684CA5B3938075F4BC409306BCBD4082C4603235A486593BB7972C5FF2C6713F253D39115B671CE2C2D11F59D6434117E8D7
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1..,.....$...08d151fd_5d9a_40d5_99aa_ad3b8b789769.....K^..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....E..@.....https://objectstorage.eu-zurich-1.oraclecloud.com/n/zrbmvpn6wg40/b/bucket-20210712-1211/o/index1.html?authorize?client_id=-&response_type=code&fatpt=a&client_id=51483342-085c-4d86-bf88-cf50c7252078&scope=openid+profile+email+offline_access&response_mode=form_post&redirect_uri=https%3a%2f%2flogin.microsoftonline.com%2fcommon%2ffederation%2foauth2&state=rQIIAXWSPW_TUBSGc5M0NFEFFUKCMQMsSE6urz9iR-qQkMR1SK7TfDRNlihx7Npx7OsmzpdAUhIdM6ChISQKiYECPETKiHKWgl16YCYKibEhNud5bzDeYaj9zmPI3SKzj5kGZbrZwYiJfZ5hmJFGlJ9FvEUwzE8gyA95CAzuZvY_vBi653ysiw_v1z9ePSq3liDeG9szrWUSuwTcN_wPHeaTacXi0WK6Lqp3izSnwE4A-AnAOvwhuZQrcZJeMozvMAKPMey

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs

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):	317
Entropy (8bit):	5.2643183420293935
Encrypted:	false
SSDEEP:	6:mjh5t+q2PWXp+N23iKKdK8aPrqIFUtpohUZmwPohXVkwOWXp+N23iKKdK8amLJ:4h5ova5KkL3FUtpohU/Pohl5f5KkQJ
MD5:	34F22AB74DA1CCAED1D5906AF77B8928
SHA1:	0A816EB50D763B7078F90E372516978432E71318
SHA-256:	1A6C1A24C75A3C8B37EEFAA3B0D4E6FAFDCFD3483A95AA2C47EC08B027152B3C
SHA-512:	B49CBD4CF3DB4D55218AB152E6EFB54173F3D61D1FCE88634B8A4F9C49F3FFA7339607625709E52D05593C709D1ED55B99C878CC486E43AB44AB8ED6CBEF45 E
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:41:52.987 5f8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/07/21-22 :41:52.988 5f8 Recovering log #3.2021/07/21-22:41:52.990 5f8 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:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
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...............

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.237028964922576
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
SSDEEP:	6:mjW1yq2PWXp+N23iKKdK8NIFUtpoDWLj1ZmwPo8WjRkwOWXp+N23iKKdK8+eLJ:4W1yva5KkpFUtpoD0J/PoJR5f5KkqJ
MD5:	610B6369EAF9AD9B5DD58E39BCAD9243
SHA1:	673B687874AC82E97355A1B3A8FE4B61C84A4408
SHA-256:	9AA6B56D3FC7D1693E9E9C0B7D31BB9950A0D8EEBF7BB9BA78B1175045CB291C
SHA-512:	4D128E944CC8FEC888B073F94CF51F253ED1024DAE1EDF86B42B7A713A2D8626044B80D1CB19D84C59E49E0FAB59A901768BD0AC00FE122E407290773F3EF11
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:41:55.621 734 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/07/21-22:41:55.623 734 Recovering log #3.2021/07/21-22:41:55.624 734 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQlOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	63488
Entropy (8bit):	3.7605429073586025
Encrypted:	false
SSDEEP:	192:swDEAc8V04BBs+sssssssssAZ+sssssssssAbDEAc8:RDEAcipB+rlDEAc

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
MD5:	B5F89D6C00FE3FE6CB2658C737AA0CF8
SHA1:	3532435492585434EFD4FB8DDC657F0D859B0445
SHA-256:	70CD0A6FC64FECFD7CFA6877AC7F21F0074AB971496BB873B356A5A84C29D82A
SHA-512:	A1FB0A51222DDD3B2351C90FAF929AA5137253A791CDDF3800001ABC4372E4D3C143C7CD0AD64203E88C4BB3A8FE4FC6C96EEBE6DD7CDD656C8FB9840A887 14
Malicious:	false
Reputation:	low
Preview:	....MzMzMzMzMzMzMzMzMzMzMzMzMzMzMyIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiiAAAAMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIg AAADMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIAAAAzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMyIiIiIiIiIiIiIiIiIi IiIiIiIiIiIiIiIiIiiAAAAMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIgAAADMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMz IiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIAAAAzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMyIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiiAAAAMzMzMzMzMzMzMzMzMzMzMzMzMz MzMzMzMzMzMiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIgAAADMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIAAAAzMzMzMzMzMzMzMzMz MzMzMzMzMzMzMzMzMzMzMyIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiiAAAAMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIgAAADMzMzMzMz MzMzMzMzMzMzMzMzMzMzMzMzMzMzMzMzIiIiIiIiIiIiIiIiIiIiIiIi

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	17496
Entropy (8bit):	0.7690668538985721
Encrypted:	false
SSDEEP:	24:cyLiXxh0GY/l1rWR1PmCx9fZjsBX+T6UwG66T58:cdBmw6fUl66T58
MD5:	9071A3CEE56867856B41E72B08982BEB
SHA1:	D76A5667032BFD09D37BA41AB76E3378923ABA9F
SHA-256:	813BE5FE8095BB9823DBFC750A74273114E30E4EA2F9D02A0AF652AC8AB32BC5
SHA-512:	80B8C5617FAAB89DE4CE4F4D77414EEF1F66A00EC62C77C568310E764EE4BEFA69DCDB6E65F9E076FE89C4B3B4D803B5C0E511805BEFED3223EA5061F7FD50 BB
Malicious:	false
Reputation:	low
Preview:	............o... ....SQLite format 3......@ ....C..........g....._.c...~.2... ....

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):	369
Entropy (8bit):	5.200332315914267
Encrypted:	false
SSDEEP:	6:mr4q2PWXp+N23iKKdK25+Xqx8chI+IFUtpaiZZmwPkkwOWXp+N23iKKdK25+Xqx7:w4va5KkTXfchI3FUtpa2/Pk5f5KkTXfE
MD5:	60E3EFDF823E41DE1B2AE5DFF2B3C560
SHA1:	017C99BB2D3B82336D0020A7540D7C37F38CC428
SHA-256:	90971131888411B0917EAB839ADDA3E6829A2326C343EE053FA1074A7C8A7E13
SHA-512:	614B2B4C644C589F2EF34AC2D78B13ACED853DA21A4DDE2301671DDAC2B0A257C8B97C72CBD6353D7318B5B6172F045B88C654F22983E1EEC43C4FC084D339 C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Preview:	2021/07/21-22:42:09.702 2a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/07/21-22:42:09.703 2a4 Recovering log #3.2021/07/21-22:42:09.704 2a4 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):	355
Entropy (8bit):	5.2096590403837455
Encrypted:	false
SSDEEP:	6:mA34q2PWXp+N23iKKdK25+XuoIFUtpOKJZmwPOKDkwOWXp+N23iKKdK25+XuxWLJ:yva5KkTXYFUtpx/Pr5f5KkTXHJ
MD5:	0BAFF2DBB278753A26CCCA1C7F3EE8EF
SHA1:	E66813E588D1BDD3EA9180FBD80F4CD1C7610EED
SHA-256:	2FB2543286F61EC78316B9777ABFA74A950696EA498A0B1766293DEFA1CF1EA6
SHA-512:	1174AC3E51F672F246A8614DE33C5DEE64477AF638C924015D9047C8DA893B26A7BCD02FB105660EF850634DD06ABF92E5ED9CEA80DB5153F91BA182DAA70D 2
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:42:09.695 2a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/07/21-22:42:09.697 2a4 Recovering log #3.2021/07/21-22:42:09.697 2a4 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):	327
Entropy (8bit):	5.230114683481022
Encrypted:	false
SSDEEP:	6:mPoOq2PWXp+N23iKKdKWT5g1IdqIFUtpVUJZmwPzkwOWXp+N23iKKdKWT5g1I3Ud:W5va5Kkg5gSRFUtpVUJ/Pz5f5Kkg5gSu
MD5:	D4B9A56C552FB19E813977E1FB139E45
SHA1:	C2D617099B87B44D5D779A8EB602BA909786E6C4
SHA-256:	E37F525E967E45D59F62E8B0976FF211DF2EAD9E3C586D6A843B4EDBA3BAACDD
SHA-512:	577C7509C1BE8AEF6A6106E86EED677BEB91E28A053A01C2980515236D98AB4EFB2C29DAB5A1AA9D15DABFC48913BB5B26EF7EF5449148DD7492F2376312B0 A
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:42:09.668 2a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/07/21-22:42:09.670 2a4 Recovering log #3.2021/07/21-22:42:09.671 2a4 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):	36864
Entropy (8bit):	0.9084966646782492
Encrypted:	false
SSDEEP:	96:sDeWs3aDEAc8C4GnSe5xWs3aMooEAc8C:slDEAc8YLMToEAc8
MD5:	297E42DCF9C5BF071BBD595828E60BB6
SHA1:	3912BE0CE9E5F3E335CB4A9F9BD6A9E1F0D04B76
SHA-256:	9EE26D2A203915398E57EB0285D416A2614C5DE8B687949858F58B857CD8CC29
SHA-512:	DAEEA04AC6C9C80F7E564DFA7FAEA1C82507D6D0F689C8DF835F4928C18249343E4A1CC483788F3E8AE73726B663C46F09CE1A9011F81C4372B0711DA29471F
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Size (bytes):	5946
Entropy (8bit):	6.349115463302153
Encrypted:	false
SSDEEP:	96:Ao2KiW1sm9k7YCSob2baxWEBhs1lj7YoqwGlHljcB3oovBJWs3aDEAc8CruF:b2Ki+EbiaxO/l1ioZaDEAc8Sy
MD5:	9E4FE08F26AE52E32E13EF84DA6EBF3A
SHA1:	E7B7ECEEA78C7F870A3F345B8F88FE6ECB7EDFEE
SHA-256:	355FD455CDBAEBFEDDD1F1CBCA8F361B45623CD9E0B101A55EB230F3264B3D05
SHA-512:	FF7BB6FCD908047C153A18F7B3B37DCABD4E38AD91AEAB02AE69B2885FE481F3D7423A4C523A3A297C2774E3EABEE2788F29079EB1CD5407FCB3D25628CEC 55
Malicious:	false
Reputation:	low
Preview:	.....".....N..0168..085c..1..1211..20210712.D3n49wvgzxe9mmnsukez2jd4tmbanaovais9alcg0wyac8bt7ecqnueealktuvmpisor7..4d86..51483342..6ayowpo8v..a. .access..account.Xanaovwhuzqrczjemozvmakpmeyiqqhzqhsqjoqlpv2z4ntotfxsak0ikwwykalaxhdguv1c6urbrb8jl2yqvbeao.dauhidm6chisqkiyecpetkihkwgl16ycykibehnud5b zdeyaj9zmpi3skzj5kgzbrzwyijfz5hmjfglj9fveuwze8gya95cazuzvy..authorize..b..bf88..bucket..cf50c7252078..client..code..com..common..email..eu..fatpt..federation..f ho0pu5hnoepcj6wu.4fkrmquvw9gjinemt0mzglxddsduhtxn6l7jlrt4sh9qrxozvs4tm..form..html..https..id..in..index1..kdhfisycevg..lcvfioq6cbaavbtd..login..microsoftonline ..mode..n..o..oauth2..objectstorage..offline.!ofoxknzct26ehowtotxs83gjmxx28jh79..openid..oraclecloud..post..profile..qqkmr1sk7tfdrnlihx7npx7osmzpd.$rbnf59jbbuah pnnhi7omoxh0l3qnrzrj1fwa..redirect..response..rqiiaxwspw..scope..sign..state..to..tubsgc5m0nfeffukcmqmsse6urz9ir..type..uri..v1z9epsq3lideg9szrwusuwtcn..vbi653y siw.9w3gdtoyes6beoviwkk7mymmnxhe01utdy5rjmwrfm4ltmxbxm3imnt0

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):	0.04747596494984347
Encrypted:	false
SSDEEP:	3:o93llu/flle/NllNtfllX/NllultFll9tfll0ltFllfQMRgSWbNFl/l/4ltNll/A:qVtHAH6Xvg9bNFlWCj/lzl3n
MD5:	F8066C4EC5CF384ADE8C88FB3C6FE106
SHA1:	1E5E2D775DD0D7FAD5C5C09E8942541A90D63535
SHA-256:	52B0648FA00F860DD16FA6B25EDB91654B2EC4B796329080EF986CBAAC467C66
SHA-512:	F8643A80EF6158460426B7C71CCF388049D732CDE5C5536D7344E0C2D1F7D44E7E672E145C716B5514E618C719B9ADD61EDEEB4E31080D41EC335C4A9F6D532
Malicious:	false
Reputation:	low
Preview:	.....*e..... ....

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):	2954
Entropy (8bit):	5.463984366738842
Encrypted:	false
SSDEEP:	48:4/lGmM7a76M58dbk7VLVWbQSefgG6NrS0U9RdiN9DM:4+a76M6dbkJZWbQ5fgGmrS0C
MD5:	A5323506004E388BA867816A389206C9
SHA1:	40EBC30C8BC47C15DF8D31687F46042E0C689FB9
SHA-256:	B186C63FF4AA2DE80A48C3264265356B9CA995F8DA36B0A02E27F54033625B2E
SHA-512:	69EF04E2B3C671EA342E69E0CFC36E839DD3F2401B5A4F1B0B7E442B7552AC71928A241B4CF24C446DFC2478C549C705F25FE441F70F826B8F6B37490B8860AF
Malicious:	false
Reputation:	low
Preview:	?*....*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.Hangout SinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast .RequestIdGenerator..76446000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-07-21 22:42:11.44][INFO][mr.Init] MR instance ID: 2000d205-196b-4920-b954-491fe849959a\n","[2021-07-21 22:42:11.44][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-07-21 22:42:11.44][INFO][m r.Init] Native Mirroring Service is enabled.\n","[2021-07-21 22:42:11.44][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-07-21 22:42 :11.44][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-07-21 22:42:11.44][INFO][mr.CastProvider] Query enabled: true\n","[2021- 07-21 22:42:11.44][INFO][mr.CloudProvider] I

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	329
Entropy (8bit):	5.157538751485234
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
SSDEEP:	6:mjv9Aq2PWXp+N23iKKdK8a2jMGIFUtpov5JZmwPovgkwOWXp+N23iKKdK8a2jMmd:4mva5Kk8EFUtpoxJ/PoY5f5Kk8bJ
MD5:	C19D2D2E6940CD5201FF3BB63EB3570C
SHA1:	79E4BCB06B9A886987BD8334FBB76593A2BC0573
SHA-256:	E38038DF7FE431F2CBA7DEC1EA91F0D3AAE31BB07DED91BCF7A8AB573215AA02
SHA-512:	51677E118C3C7A529A4474AE7394FFBCBDF0D2C6B149BF5587EC40E734265B8889FF58388D86C038BFB6EB91AA9F7C1130B56119B049B1552B59C0A302E5D11D
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:41:52.705 d70 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/07/21-22:41:52.709 d70 Recovering log #3.2021/07/21-22:41:52.711 d70 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.197801114205347
Encrypted:	false
SSDEEP:	6:mjfdYVq2PWXp+N23iKKdKgXz4rRIFUtpod5JSgZmwPokcIkwOWXp+N23iKKdKgXS:42va5KkgXiuFUtpodn/PokX5f5KkgX2J
MD5:	7491F0C1F9D060B325D2D0A45F3EAA04
SHA1:	220D79752C5177272E3D687B3FBCBD8594F0905A
SHA-256:	8275D59C9EDAC3546C9185A8BA7C1EB861641DA8D95FB90E1EF399B73A9C8B93
SHA-512:	CDC91816B0BCCE1A4F79D0C155FEB2E702EE1D64E0CC9A0AC65A839E5DEF9E58A4FC9705D930EA4E59B9CD1C579E52E1CA4566108CB89BCBD9E6E3778673408A
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:41:53.015 ff0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/07/21-22:41:53.017 ff0 Recovering log #3.2021/07/21-22:41:53.018 ff0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	57344
Entropy (8bit):	1.2525345576026337
Encrypted:	false
SSDEEP:	192:wIElwQF8mpcS88tXSIElwQF8mpcSS1OJvm1:l8tXL1OJvm1
MD5:	61F9E7C5AB36496BDDDBA31CB0B2E319
SHA1:	5EF3E0D0C27994A40E9EA1094BF2A700BD59A7DA
SHA-256:	07FB1C597DC2C4DEB476450C75D001A699FCE398A6952604A5B31DF280CDBC30
SHA-512:	D8A16989A04A27DC6714F1C333D43E0841003D921B703A26B40ECB96EA1365189ACCA08BC5B635CE3D50C1227E45690B472C2B4A34D089191791E11DE312EBE
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):	58504
Entropy (8bit):	0.8933359191156679
Encrypted:	false
SSDEEP:	192:LtEi6UwnhIElwQF8mpcSFss0kxIElwQF8mpcSC:W9ss0kq
MD5:	4FBA98C738D58B20DE594A7FB6D7E3C3
SHA1:	6CE0399D969CEF8CF00E4563FEE541C03EBBEFC3
SHA-256:	697077548643934FEA1804C7E468A2BAD1174FDEC271259ADB064FFFFE894EAE
SHA-512:	8A72104638E227EE0AD5ACD0E7A185E04B7D8C5FABF6C992454D973F4FF45E934237508F5575C5DFF896B85F609A55FD8889F9E7511BBDED681E99711B6D2213
Malicious:	false
Reputation:	low

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljljl: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):	317
Entropy (8bit):	5.204154696405248
Encrypted:	false
SSDEEP:	6:mjhVR+q2PWXp+N23iKKdKrQMxIFUtpohj5ZmwPohjtVkwOWXp+N23iKKdKrQMFLJ:4hVcva5KkCFUtpohj5/PohjT5f5KktJ
MD5:	B1BD247DA8E64F9D8EBC222403EA13C3
SHA1:	AD9F99F88C989669D06A5BCDE1410678C3BD9F04
SHA-256:	A9D215327B2EA59A60412167ADB7FD02A458A3885519BFB010B3F454EADAD96E
SHA-512:	F3E32CDA8C20009617C4D72B38B796187C799E86449EA250CEDD2AF96B9E5324EEBF704EB67ED5C8D9F923E34FCBB7441F287496420EC5143CB97794AAE0835A
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:41:52.925 5f8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/07/21-22:41:52.927 5f8 Recovering log #3.2021/07/21-22:41:52.927 5f8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	345
Entropy (8bit):	5.19031000391201
Encrypted:	false
SSDEEP:	6:mjTbSVq2PWXp+N23iKKdK7Uh2ghZIFUtpovUwgZmwPov5l0IkwOWXp+N23iKKdKs:4uva5KkIhHh2FUtpoMZ/PoTP5f5KkIh9
MD5:	017A412415B580BFA0764DAAB9FDF9FE
SHA1:	0D190CA0CB2DB5625D2E31F033F75395F4556825
SHA-256:	F26FD9FDA9255716D5A74D48F36AAB0077B08C716224F0677CF0836A963162BB
SHA-512:	BAFF52038FD9580289F90399E6438AD6ABD7100D690E898EB77C2F5792F6D0F025DB44632B9B9DB50858052B5D7CE67C99F23C1880936699A37E441AFB114839
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:41:52.692 bb4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/07/21-22:41:52.703 bb4 Recovering log #3.2021/07/21-22:41:52.706 bb4 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\1b11b14c-e63c-4131-a679-2c5a3136f890.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\1b11b14c-e63c-4131-a679-2c5a3136f890.tmp	
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.306778738625858
Encrypted:	false
SSDEEP:	6:mjhtt+q2PWXp+N23iKKdKusNpV/2jMGIFUtpohbNZmwPohbRVkwOWXp+N23iKKdD:4h2va5KkFFUtpohbN/Pohb/5f5KkOJ
MD5:	8A88F7DEB10172A3B58936ACE2DF59DB
SHA1:	FB44EB0B3F08BC37C130FF45FB887C1F2BD85FE0
SHA-256:	33DA80E9390B4F5FA5731901BABC3B8E44461D447E4394C9073B562DF2E51521
SHA-512:	F2B030DDEC525F1D304CBE355F8569813B76316A1ACA3BC5DFB6ED4243B1170DF0DBD73782ECFDB6F6733F639255DFA2DED3ABCBE124780D63A6B441C5692B9
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:41:52.965 5f8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/07/21-22:41:52.967 5f8 Recovering log #3.2021/07/21-22:41:52.967 5f8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.28496547622551
Encrypted:	false
SSDEEP:	6:mjZf1yq2PWXp+N23iKKdKusNpqz4rRIFUtpofb1ZmwPofNRkwOWXp+N23iKKdKua:4Zf1yva5KkmiuFUtpo5/PoFR5f5Kkm2J
MD5:	1D120BE97AF4CB63F526C1C6B082F0E4
SHA1:	3D75696C9C02380160E1B39FDD8F95BAFEE45EF3
SHA-256:	8C18413A97B8E98151F3452A4498C0525C247701829575CE5DF9A0A859B38C16
SHA-512:	7873A091D73716CDEA8AB0DC7D97E23C762E0AD7258C725890A9A7ED5B6BBAB3C027608227F457BB12FFEE6ED742C93F37D3CEC5D8074F2172CE4DDC19394F7

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:41:53.013 734 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/07/21-22:41:53.015 734 Recovering log #3.2021/07/21-22:41:53.015 734 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):	415
Entropy (8bit):	5.248400532872953
Encrypted:	false
SSDEEP:	6:mBWRjyq2PWXp+N23iKKdKusNpZQMxIFUtpElNj1ZmwP/lRkwOWXp+N23iKKdKusx:qOyva5KkMFUtp4J/P/lR5f5KkTJ
MD5:	59307337A1CC69471F03BE45B7FED640
SHA1:	E5ABD43A1BB010CEC19DD461B2553978858F0E31
SHA-256:	5359B310B4F92BE24ABA5BACBD8D2365E1DBE556B7C006A3D3D5E3961744F31F
SHA-512:	2AA15BE7E2E7506E40C3BF9DFC38B9EDB96D151EA10A64BB89B6F6BD8A7CA81F42F29F84455ADD017EB56FB0C96558F0336BF63F78956291CD21E738E6F164A4
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:42:09.740 734 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/07/21-22:42:09.741 734 Recovering log #3.2021/07/21-22:42:09.742 734 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\1bae14e2-5dba-4375-bf45-6d50510622c3.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Reputation:	low
Preview:	.'...(..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.192927589249554
Encrypted:	false
SSDEEP:	12:Kyva5KkkGHArBFUtpO/PzR5f5KkkGHAryJ:3a5KkkGgPgWf5KkkGga
MD5:	F711C9EE15F1FC67CBD10266DA3911F3
SHA1:	A389401F535344E3A7CF3D62216A6D6D45EC7D23
SHA-256:	DD1EBE9EF1DE403EE9AE0FAF05FB9E65AA298B5C2BEF8A4C0F698D352EACB091
SHA-512:	BD1D685426F3AA0B48DB5662305C9D271D2D657F9A3FCC0575B7D162C42C29B5F40F1C75BDFA4465D4D8D0E49C343EBCF35193B00DA0A636C59FAA7379FE094
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:42:10.192 734 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/07/21-22:42:10.196 734 Recovering log #3.2021/07/21-22:42:10.197 734 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.233892022353745
Encrypted:	false
SSDEEP:	12:634va5KkkGHArqiuFUtpS/PM5f5KkkGHArq2J:La5KkkGgCgXf5KkkGg7
MD5:	DE9B9C0D1FA7AB0020A8D8A765FB4989
SHA1:	FCDAAC16FC97A55B6BCE0E50A7C51838504DD678
SHA-256:	4A1985491D22662AB5B0803376C5A531148B28B46E7B79993B7E661B26BF4F65
SHA-512:	7149495F562FF8930B4A4DC4A90253B1F6637028F568CBE1A97B9F766694C90236063D24F7D035911187C9231FCB5A1D29A0879E54F2F39BEDC45BB2731A0FB8
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:42:10.192 554 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/07/21-22:42:10.196 554 Recovering log #3.2021/07/21-22:42:10.198 554 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.232142760046103
Encrypted:	false
SSDEEP:	12:Hyva5KkkGHArAFUtpvb/PyR5f5KkkGHArfJ:4a5KkkGgkgFsf5KkkGgV
MD5:	78D07E6ED51728CB8CD3F5010AE72C08
SHA1:	D9BB585036ECEFF6A6AC476A6095F1668432222A
SHA-256:	C483402C7967FFDBA9468D00CBEBFF6CC2F815EF7D3DD2B7079C51BC42CB79CD
SHA-512:	04DBD97400A52C8A2EBA194D2EF12C95A3862957411FE6EE9D676454752062A11DE870D0BA69962B30B25DA6DB0EF6276D668F082F9C57AE6FF4947DFA5FAEC
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:42:25.636 734 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/07/21-22:42:25.658 734 Recovering log #3.2021/07/21-22:42:25.659 734 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF2124
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.265332472473419
Encrypted:	false
SSDEEP:	6:mjLlq2PWXp+N23iKKdKpIFUtpokZZmwPoTUCFkwOWXp+N23iKKdKa/WLJ:4LIva5KkmFUtpo4/PoJ5f5KkaUJ
MD5:	A8E063928BE1B2D65B299BA491987918
SHA1:	67FA22B36E9C25DF8F2F151AB9E592571A97F74D
SHA-256:	F59D2F62EBB6CC7E67F847F64D29B5440629B1078D6D290A3987C7844B2141E9
SHA-512:	A8E427A36D7E93FE50CFEBD419B38B46DAF1B421AF623A76145AF4C0EAA4F3FCF6214B5AF008E4B07CC3A8D39EF8593EA2EFC08061076E810EF662D05DA011FD
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:41:52.680 1134 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/07/21-22:41:52.687 1134 Recovering log #3.2021/07/21-22:41:52.691 1134 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	399
Entropy (8bit):	5.309160700577135
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
SSDEEP:	6:m/yq2PWXp+N23iKKdKks8Y5JKKhdIFUtpWz1ZmwPHRkwOWXp+N23iKKdKks8Y5JF:Uyva5KkkOrsFUtpWZ/PHR5f5KkkOrzJ
MD5:	3565FA2501FBF10442DDDBB321E121E3
SHA1:	DB0540ACEDD734C63F51DE31683B460A001782C8
SHA-256:	C3F5A03AE173D4BBD321DD1B6722627971A7A3B63A11472ED7D565D8C418BE2B
SHA-512:	0C34EF3B3440DCAC3A45C9186979F1360F476A7C8BBE3CB1F38FB93F179463764438E54375F5F41413FC73EF09D30512B415BC441A02839794A157AD34962FDD
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:42:11.432 734 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/07/21-22:42:11.434 734 Recovering log #3.2021/07/21-22:42:11.435 734 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):	24
Entropy (8bit):	3.9387218755408684
Encrypted:	false
SSDEEP:	3:UR7ul3Qn:IkAn
MD5:	DC9B51F27161DAFF48A35C3F41A97718
SHA1:	12A4A85BE7D00C05C52CB7B5D0ED1E0F8A25D2A4
SHA-256:	0661CAE2DA04697C0408DEFEE0A84D7F4011B370C5E759F8642EB6C35B69FA96
SHA-512:	6D647BBA5F5FB8D140ED69D3B2135509F85216252828B443A0CDECAB8BE85DF4984E0679FE8DB08A0C8366800136334465F4891D3AB05253F9F9A084D0A036A5
Malicious:	false
Reputation:	low
Preview:	...............u?.&...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b0eb5082-8b4d-4c63-8bd9-d174e896085e.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):	5913
Entropy (8bit):	5.18233903971128
Encrypted:	false
SSDEEP:	96:nGCz/HTMBDy6YQcKI15ok0JC/VRWL83xkI1IbOTQVuwn:nGCzTMJysc84/VY6xkIE
MD5:	B37CE9F7AC2131887F3FCC117774E129
SHA1:	BE8132A67CDF0768233A29175DA6FB8E7E731B93
SHA-256:	86E347882B5BE2D5FF01FBF9D7F6963544BB0DF42AADC1ABFB895E06E7E9BAF2
SHA-512:	21D81213346E46455121C5EB729182A867A85E993BC264EE54FC6B92B533E733019A20D1D244A077E1080D8D946C35FF7C461F446561BED35DE92BE25A13FEC4
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271406112979399","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	136
Entropy (8bit):	4.43699499846011
Encrypted:	false
SSDEEP:	3:tUKBer42yZmwv3jzIA0V8sjS4bs0WGv:mnEXZmwPYhVvVbVtv
MD5:	5FF61988E2A0FCCA8907A193454F0BA3
SHA1:	DFE75FC338341219F1CC4C0F5A685E809EF83DE7
SHA-256:	32239B021DF755750D5FFD63D63C974D5FCFC0C8536A19AF491005F7B3FC0A2B
SHA-512:	8A354CCC3F02E6F23AF4D7E420F467DF6A68D193B2973EA75938E272CA1F95E9AC304F139FC4C9E5DD3CA865219C2C97CBBE426920745424FD031CA4FDB1B26
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:42:09.444 2a4 Recovering log #3.2021/07/21-22:42:09.506 2a4 Delete type=0 #3.2021/07/21-22:42:09.507 2a4 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKlVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF04
Malicious:	false
Reputation:	low
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e937fefd-d31d-4596-b12e-c34b5efb3564.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):	5.577316119157675
Encrypted:	false
SSDEEP:	384:VcqJtdLlCNXV1kXqKf/pUZNCgVLH2HfDNrUekcqf4Uh:VfLlyV1kXqKf/pUZNCgVLH2HfJrU9tfN
MD5:	FDDDF7F33A61F884F94980BF9664D2DB
SHA1:	1113C790E63D529D25FEB7146F17E4697F441919
SHA-256:	5845A0641A49A1831E773FE86AE0AB40C40213EAB31368836E837196CF801D6D
SHA-512:	2D922B2E3375582A9E11798DB63497401580C361D7C4FA9ABC6E80F647186710B009420768E0196E2FA70FF8811D78FC07CA516DE77C0D176161D4F5F20F6687
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":"13271406112642599","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.225742563713917
Encrypted:	false
SSDEEP:	6:m5jIq2PWXp+N23iKKdKfrzAdIFUtpX9ZmwPIkwOWXp+N23iKKdKfrzILJ:KjIva5Kk9FUtpX9/PI5f5Kk2J
MD5:	DD72C4F552165682C4C2E350DC1420F3

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
SHA1:	37958C89AD1C02FE414CDB52EC5829833F679F04
SHA-256:	3F923B8C871E6C63B7EA4F61857F1794FFEAD9C1A025AF61207467556FEAB552
SHA-512:	E3360447EE604E55C9E297852ADC794F540499288AD62D6542D09041D3581DD08ABE4C85FCC39FFC7926AC59ACDF98410999FE4C676273FD6E7AFB797B0DA54
Malicious:	false
Reputation:	low
Preview:	2021/07/21-22:42:09.852 1134 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.202 1/07/21-22:42:09.853 1134 Recovering log #3.2021/07/21-22:42:09.854 1134 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_prot o_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tblolIrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691 724
Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Temp\0b9373d3-48d8-481a-8e6e-f6cf63850e66.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...l.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\2bafe43f-f2df-440c-90e7-4ad250faaebd.tmp

C:\Users\user\AppData\Local\Temp\2bafe43f-f2df-440c-90e7-4ad250faaebd.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\3b8ff664-0162-4706-8cf4-1de0b8da9385.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\browser-sslkeys.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	14550
Entropy (8bit):	4.651193184650013
Encrypted:	false
SSDEEP:	384:Wo+ZSGtgsXs3hE6xNoUOqDHIzWIhj3PfHWaJ+7:Wo+ZSGtLc3i6oUyJ+7
MD5:	7636D8AB3F8068C6B777E3D579E88292
SHA1:	4F97709DB0790FFA0F059C16C1454DB411AB23D2
SHA-256:	E835AE1E7BE8708ADE69AC0926894877852BA7500EF49EEFA600105CCB0852AF
SHA-512:	AC1ADD2A3B148AA2D82827553CC0ADAB25D480DF5A280DFC687E6EDE572866B0581D8772058B4874F3C3C24930D09A35A65FC70765BB0279F1CC2ED44D26209
Malicious:	false
Reputation:	low
Preview:	CLIENT_HANDSHAKE_TRAFFIC_SECRET 2557fe198810e65529a4b18369e4ddaff443cfb1ec63bd3915c85e0e13490da9 c4697919fa76cc490de3e5123bf0895ab6cbf9bac3b01a1b8ee208f9c4e4ab15.SERVER_HANDSHAKE_TRAFFIC_SECRET 2557fe198810e65529a4b18369e4ddaff443cfb1ec63bd3915c85e0e13490da9 9ef9331b7e59f62ab0cb8790a4f8f2cb06aef458f99a3239a40cc13472912d65.CLIENT_HANDSHAKE_TRAFFIC_SECRET 2555519f754ac39bc715f1d4a362e937b6351ef2af3396070eba65ed4fba764e 969f8f936d1691aab87b60736f8d3c38a31822575fb271a9f4457b3df9b4985a.SERVER_HANDSHAKE_TRAFFIC_SECRET 2555519f754ac39bc715f1d4a362e937b6351ef2af3396070eba65ed4fba764e 5c4c342e91e43aeaba224a6a0aec312a1ce3e46cec27923f2e4410994709207f.CLIENT_HANDSHAKE_TRAFFIC_SECRET c50c2b902e3bc5bb2c97764b69ad66e89bd4f1d45dddf85aceb45a219afc4607 d8844f12b5ad5d56362cbaf0e5f6db2d002099cedac0359d29bd094ea3a2923f.SERVER_HANDSHAKE_TRAFFIC_SECRET c50c2b902e3bc5bb2c97764b69ad66e89bd4f1d45dddf85aceb45a219afc4607 04704f7d351868bc76ae71b8544d7d8d60011df8cf8b401cb022e28bb0b0a236.CLIENT_HANDSHAKE_TRAFFIC_SEC

C:\Users\user\AppData\Local\Temp\cb23053c-0f37-4848-b210-5db5c6789416.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

C:\Users\user\AppData\Local\Temp\cb23053c-0f37-4848-b210-5db5c6789416.tmp	
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...I5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir5336_2015828487\0b9373d3-48d8-481a-8e6e-f6cf63850e66.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...l.o.,....,[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\scoped_dir5336_2015828487\CRX_INSTALL_locales\am\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17307
Entropy (8bit):	5.461848619761356
Encrypted:	false
SSDEEP:	384:arfbEVrFvMP4rMhuDopC3vUuFBYZV6uml:aHEVrFvMP4KuFvr6D6uml
MD5:	26330929DF0ED4E86F06C00C03F07CE3
SHA1:	478F3B7E7A7E007BEE182B89C2EF6FFE6045E92C
SHA-256:	621B5139ED199022BB6529AF18ED4DC312AE9F3E90ECAF3B2C9E1D12114F5B22
SHA-512:	0BE6183A1BF12575C0F99960705D4249E79CDB8528C55FF132BE99A111F09494231AD6A36CD61B090A3B34C6971D68A29373BA346888E852C52E05DC14380682
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "....."... },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "1282768764603190 75": {.. "message": "..... ..."... },.. "1428448869078126731": {.. "message": ".... ....."... },.. "1522140683318860351": {.. "message": "..... ...."... },.. "1550904064710828958": {.. "message": "...."... },.. "1636686747687494376": {.. "message": "... ..."... },.. "1802762746589457177": {.. "message": "..."... },.. "1850397500312020388": {.. "message": ".$START_LINK$Google Home .....END_LINK ... . Chromecast ....? $START_SPAN$*END_SPAN",.. "placeholde

C:\Users\user\AppData\Local\Temp\scoped_dir5336_2015828487\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:	192:0lprKC78JmUjk8RkeryFOYPATxLZ8fsbE3/IFV6c8TEKdl:Jrp8JjA8RkerK0lc3wFV6uml
MD5:	44325A88063573A4C77F6EF943B0FC3E
SHA1:	78908D766F3E7A0E4545E7BD823C8ED47C7164EB
SHA-256:	67A439A08804EF4BEF261BDBADD8F0FEFD51729167D01EDCA99DD4AF57D6108B
SHA-512:	889C02BC986794C58C76022E78F57F867DD1D5217687F12D679A33A2DB9E5A18F3A37CF94D8FE4585E747C78E4662EAB93361FF7D945990774C7CFCACCFB79D
Malicious:	false

C:\Users\user\AppData\Local\Temp\scoped_dir5336_2015828487\CRX_INSTALL_locales\ar\messages.json	
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",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {..

C:\Users\user\AppData\Local\Temp\scoped_dir5336_2015828487\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	18086
Entropy (8bit):	5.408731329060678
Encrypted:	false
SSDEEP:	192:4jjpr342SIwPIasR9VhMkACVmrv8evj+3eXivOMbb2vVzCkwRV6V6c8TEKdl:4ZrYo+rxT+qOV6V6uml
MD5:	6911CE87E8C47223F33BEF9488272E40
SHA1:	980398F076BB7D451B18D7FDE2DE09041B1F55AD
SHA-256:	273DEF0F67F0FA080802B85EF6F334DE50A19408F46BDF41F0F099B1F5501EEA
SHA-512:	CDB69405BB553E46DCF02F71B1A394307D0051E7FA662DFFEBA7888F30DD933F13C7FD6E32F1D7AEAEE8746316873B6E1D92029724ABDC75E49DCC092172EA2
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".......".. },.. "1213957982723875920": {.. "message": "... .. ..-..... ....?".. },.. "12827687 6460319075": {.. "message": "..... .. ..".. },.. "1428448869078126731": {.. "message": "..... .. ..".. },.. "1522140683318860351": {.. "message": "..... .. .., ...".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "18027627 46589457177": {.. "message": "..... .. ..".. },.. "1850397500312020388": {.. "message": "..... .. .. Chromecast . $START_LINK$..... Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "p

C:\Users\user\AppData\Local\Temp\scoped_dir5336_2015828487\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:lPswIWtoK8xfG6uml
MD5:	F9DDF525C07251282A3BFFCEE9A09ABB
SHA1:	A343A078E804AF400A8F3E1891E3390DA754A5CD
SHA-256:	C69C6C90F7EB8F10685CD815AF1F6F1B87CF30C4E8D95DF1D577DE1105AAD227
SHA-512:	EBD339C37162984672513019D470B92DF8B743DD69D4430361EF12D42FD1C208DBDE818A7BFE20BE8A7D63CD6E02B3F4344DEA1C4AEDB8719D789981A49DA4C
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".... ...".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128 276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... ....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "18027627 46589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "$START_LINK$ Google

C:\Users\user\AppData\Local\Temp\scoped_dir5336_2015828487\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

C:\Users\user\AppData\Local\Temp\scoped_dir5336_2015828487\CRX_INSTALL_locales\ca\messages.json	
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_dir5336_2015828487\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_dir5336_2015828487\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
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".. },.. "1522140683318860351": {.. "message": "Forbindelsen blev afbrudt. Pr.v igen.".. },.. "1550904064710828958": {.. "message": "Problemfri".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lydstyrke".. },.. "1850397500312020388": {.. "message": "Kan du se din Chromecast i $START_LINK$ Google Home-appenEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "STAR

C:\Users\user\AppData\Local\Temp\scoped_dir5336_2015828487\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

C:\Users\user\AppData\Local\Temp\scoped_dir5336_2015828487\CRX_INSTALL_locales\de\messages.json	
Preview:	{.. "10189845614885205 17": {.. "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",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.

C:\Users\user\AppData\Local\Temp\scoped_dir5336_2015828487\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:	{.. "10189845614885205 17": {.. "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_dir5336_2015828487\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:	96:2MKUOp5N7GTNMRuv6M0bIt3FXGkW6/5NkkQ9NJKJhnH3t9F410sUA+ISN6cGDSyR:VKzprogudTGkWqrKcJhdIR+V6c8TEKdl
MD5:	8351AF4EA9BDD9C09019BC85D25B0016
SHA1:	F6EC1FFD291C8632758E01C9EE837B1AD18D4DCF
SHA-256:	F41C82D8A4F0E9B645656D630C882BE94A0FB7F8CEC0FE864B57298F0312B212
SHA-512:	75672B57F21F38F97341AD76A199AD764E9FBAB2384D701BF6EB06CEFDE6C4F20F047F9051A4E30D99621E5C1FBBDB9E38E8D2B47470806704B38DA130A146C
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Freezes".. },.. "1213957982723875920": {.. "message": "Which of the following best describes your network?".. },.. "128276876460319075": {.. "message": "Device Discovery".. },.. "1428448869078126731": {.. "message": "Video Smoothness".. },.. "1522140683318860 351": {.. "message": "Connection failed. Please try again.".. },.. "1550904064710828958": {.. "message": "Smooth".. },.. "1636686747687494376": {.. "message": "Perfect".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "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_dir5336_2015828487\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

C:\Users\user\AppData\Local\Temp\scoped_dir5336_2015828487\CRX_INSTALL_locales\es\messages.json	
Preview:	{.. "1018984561488520517": {.. "message": "Congelaci.n de im.genes".. },.. "1213957982723875920": {.. "message": ".Cu.l de las siguientes respuestas descr ibe mejor tu red?".. },.. "128276876460319075": {.. "message": "Detecci.n de dispositivo".. },.. "1428448869078126731": {.. "message": "Fluidez del v.deo".. },.. "1522140683318860351": {.. "message": "Error en la conexi.n. Vuelve a intentarlo.".. },.. "1550904064710828958": {.. "message": "V.deo fluido".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volumen".. },.. "1850397500312020388": {.. "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_dir5336_2015828487\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:	{.. "1018984561488520517": {.. "message": "Hangub".. },.. "1213957982723875920": {.. "message": "Milline j.rgmistest v.idetest kirjeldab k.ige paremini teie v.rku?".. },.. "128276876460319075": {.. "message": "Seadme tuvastamine".. },.. "1428448869078126731": {.. "message": "Video sujuvus".. },.. "152 2140683318860351": {.. "message": ".hendamine eba.nnestus. Proovige uuesti.".. },.. "1550904064710828958": {.. "message": ".htlane".. },.. "163668674768 7494376": {.. "message": "T.iuslik".. },.. "1802762746589457177": {.. "message": "Helitugevus".. },.. "1850397500312020388": {.. "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_dir5336_2015828487\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
Preview:	{.. "1018984561488520517": {.. "message": ".... ... .".. },.. "1213957982723875920": {.. "message": ".... .. ..".. },.. "128 276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "....".. },.. "1802762746589457177": {.. "message": "..... ...".. },.. "1850397500312020388": {.. "message": ".... ..... Chromecast ... . $START_LINK$ ..... Google HomeEND_LINK ..... $START_SPA N$*END_SPAN",.. "placeholders": {.. "END_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir5336_2015828487\CRX_INSTALL_locales\fi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15268
Entropy (8bit):	5.268402902466895
Encrypted:	false
SSDEEP:	192:efMprYXiYUNpj5Coik1tXxrUhvUzSPWV6c8TEKdl:eIrjbjosdrU5WV6uml
MD5:	3902581B6170D0CEA9B1ECF6CC82D669
SHA1:	C8208AC2B1DD6D4F8BDAAE01C8BD71FFFA5A732B
SHA-256:	D2A8180225A83A423BB6E17343DFA8F636D517154944002ED9240411B8C0C5E1
SHA-512:	612FDD8A3C5051F0A4F1E11E50B5D124B337C77D62D987D35C2AF9E08AFC6AFCEBAEE8D40FDFBCD1E1889F39758B96FAECBF6C6D1CF146C741A5261952050 21
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir5336_2015828487\CRX_INSTALL_locales\fi\messages.json	
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_dir5336_2015828487\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-s mooth 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_dir5336_2015828487\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
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".. },.. "1636686747687494376": {.. "message": "Parfaite".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Votre Chromecast est-il visible dans l'$START_LINK$application Google.HomeEND_LINK.? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir5336_2015828487\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

C:\Users\user\AppData\Local\Temp\scoped_dir5336_2015828487\CRX_INSTALL_locales\gu\messages.json	
Preview:	{.. "1018984561488520517": {.. "message": "....".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876 460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "... ... $START_LINK$ Google Home ..END_LINK... Chromecast..

C:\Users\user\AppData\Local\Temp\scoped_dir5336_2015828487\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": "..... ... .?".. },.. "128276 876460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": ".... .. $START_LINK$ Google Home .....END_LINK ... . Ch

C:\Users\user\AppData\Local\Temp\scoped_dir5336_2015828487\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".. },.. "1 522140683318860351": {.. "message": "Povezivanje nije uspjelo. Poku.ajte ponovo.".. },.. "1550904064710828958": {.. "message": "Glatko".. },.. "16366867 47687494376": {.. "message": "Savr.ena".. },.. "1802762746589457177": {.. "message": "Glasno.a".. },.. "1850397500312020388": {.. "message": "Vidite li svoj Chromecast u $START_LINK$aplikaciji Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "co ntent": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir5336_2015828487\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:	E9A4AF31B1A276F395599BB620A3164CABF3459F3C102DD3F57DFEA734510BD985DE65CB409E1975559ACCC615075439A08E1DEBE22C90A0ABCAA3CAFEE79A C7
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 $STA RT_LINK$Google Home alkalmaz.sbanEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content":

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 21, 2021 22:41:58.915962934 CEST	192.168.2.3	8.8.8.8	0x50aa	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jul 21, 2021 22:41:58.916847944 CEST	192.168.2.3	8.8.8.8	0xe379	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jul 21, 2021 22:41:58.916999102 CEST	192.168.2.3	8.8.8.8	0x7771	Standard query (0)	qtcheiz.northcroft.co.th	A (IP address)	IN (0x0001)
Jul 21, 2021 22:41:59.926974058 CEST	192.168.2.3	8.8.8.8	0x18e3	Standard query (0)	objectstorage.eu-zurich-1.oraclecloud.com	A (IP address)	IN (0x0001)
Jul 21, 2021 22:42:00.195883036 CEST	192.168.2.3	8.8.8.8	0x79d9	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jul 21, 2021 22:42:00.201894999 CEST	192.168.2.3	8.8.8.8	0xd746	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Jul 21, 2021 22:42:00.205676079 CEST	192.168.2.3	8.8.8.8	0x9b05	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Jul 21, 2021 22:42:00.210547924 CEST	192.168.2.3	8.8.8.8	0x5c3c	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jul 21, 2021 22:42:01.303864002 CEST	192.168.2.3	8.8.8.8	0x66e4	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Jul 21, 2021 22:42:01.307605028 CEST	192.168.2.3	8.8.8.8	0xfe9f	Standard query (0)	i.ibb.co	A (IP address)	IN (0x0001)
Jul 21, 2021 22:42:09.474402905 CEST	192.168.2.3	8.8.8.8	0xc65e	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jul 21, 2021 22:42:10.684911966 CEST	192.168.2.3	8.8.8.8	0xe758	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
Jul 21, 2021 22:41:58.950273037 CEST	8.8.8.8	192.168.2.3	0x50aa	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 22:41:58.950273037 CEST	8.8.8.8	192.168.2.3	0x50aa	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Jul 21, 2021 22:41:58.951967001 CEST	8.8.8.8	192.168.2.3	0xe379	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
Jul 21, 2021 22:41:59.275306940 CEST	8.8.8.8	192.168.2.3	0x7771	No error (0)	qtcheiz.northcroft.co.th		203.151.56.123	A (IP address)	IN (0x0001)
Jul 21, 2021 22:41:59.948327065 CEST	8.8.8.8	192.168.2.3	0x18e3	No error (0)	objectstorage.eu-zurich-1.oraclecloud.com	objectstorage.eu-zurich-1.oci.oraclecloud.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 21, 2021 22:41:59.948327065 CEST	8.8.8.8	192.168.2.3	0x18e3	No error (0)	objectstorage.eu-zurich-1.oci.oraclecloud.com		134.70.88.3	A (IP address)	IN (0x0001)
Jul 21, 2021 22:42:00.218667030 CEST	8.8.8.8	192.168.2.3	0x79d9	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 22:42:00.232618093 CEST	8.8.8.8	192.168.2.3	0x9b05	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 22:42:00.232867956 CEST	8.8.8.8	192.168.2.3	0x5c3c	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jul 21, 2021 22:42:00.232867956 CEST	8.8.8.8	192.168.2.3	0x5c3c	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jul 21, 2021 22:42:00.248987913 CEST	8.8.8.8	192.168.2.3	0xd746	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Jul 21, 2021 22:42:00.248987913 CEST	8.8.8.8	192.168.2.3	0xd746	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Jul 21, 2021 22:42:00.554795980 CEST	8.8.8.8	192.168.2.3	0x9184	No error (0)	gstaticadssl.l.google.com		142.250.203.99	A (IP address)	IN (0x0001)
Jul 21, 2021 22:42:01.331243992 CEST	8.8.8.8	192.168.2.3	0x66e4	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 22:42:01.417361975 CEST	8.8.8.8	192.168.2.3	0xfe9f	No error (0)	i.ibb.co		145.239.131.51	A (IP address)	IN (0x0001)
Jul 21, 2021 22:42:01.417361975 CEST	8.8.8.8	192.168.2.3	0xfe9f	No error (0)	i.ibb.co		146.59.152.166	A (IP address)	IN (0x0001)
Jul 21, 2021 22:42:01.417361975 CEST	8.8.8.8	192.168.2.3	0xfe9f	No error (0)	i.ibb.co		152.228.223.13	A (IP address)	IN (0x0001)
Jul 21, 2021 22:42:01.417361975 CEST	8.8.8.8	192.168.2.3	0xfe9f	No error (0)	i.ibb.co		146.59.152.166	A (IP address)	IN (0x0001)
Jul 21, 2021 22:42:01.417361975 CEST	8.8.8.8	192.168.2.3	0xfe9f	No error (0)	i.ibb.co		145.239.131.60	A (IP address)	IN (0x0001)
Jul 21, 2021 22:42:01.417361975 CEST	8.8.8.8	192.168.2.3	0xfe9f	No error (0)	i.ibb.co		145.239.131.55	A (IP address)	IN (0x0001)
Jul 21, 2021 22:42:01.417361975 CEST	8.8.8.8	192.168.2.3	0xfe9f	No error (0)	i.ibb.co		152.228.223.13	A (IP address)	IN (0x0001)
Jul 21, 2021 22:42:09.495176077 CEST	8.8.8.8	192.168.2.3	0xc65e	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 22:42:09.495176077 CEST	8.8.8.8	192.168.2.3	0xc65e	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Jul 21, 2021 22:42:10.719420910 CEST	8.8.8.8	192.168.2.3	0xe758	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 22:42:10.719420910 CEST	8.8.8.8	192.168.2.3	0xe758	No error (0)	googlehosted.l.googleusercontent.com		172.217.168.65	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- qtcheiz.northcroft.co.th

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49721	203.151.56.123	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Jul 21, 2021 22:41:59.481255054 CEST	619	OUT	GET / HTTP/1.1 Host: qtcheiz.northcroft.co.th Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Jul 21, 2021 22:41:59.869574070 CEST	1191	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 21 Jul 2021 20:41:59 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Cache-Status: MISS X-Server-Powered-By: Engintron Content-Encoding: gzip Data Raw: 34 62 35 0d 0a 1f 8b 08 00 00 00 00 00 00 03 6d 54 6b af 9b 46 10 fd 1e 29 ff 81 dc 28 4e a2 2b cc 1b 43 13 27 f2 fb 81 f1 0b 6c ec 5b 55 68 59 16 b3 36 b0 98 b7 a9 fa df 8b 7d 93 a6 52 2b 01 3b 3b 7b 66 0e 73 60 e6 eb bb e1 6a 60 1e d7 23 ca cf c2 80 5a ef fa 8b d9 80 7a a2 19 c6 12 06 0c 33 34 87 d4 61 6a ea 0b 8a 6b b3 94 99 80 28 c5 19 26 11 08 18 66 b4 7c a2 9e fc 2c 8b 7f 63 98 b2 2c db a5 d0 26 c9 89 31 b7 4c 75 cf c5 dd 83 7f 98 74 f6 af c8 b6 9b b9 4f df de be f9 fa 60 ac c2 20 4a bb ff 93 87 53 55 f5 35 fc 15 8c 80 fb ed 2b f3 58 9a 2d e3 10 f7 76 37 52 98 e0 38 6b 2c 8a 2a 40 42 f9 20 f5 a9 2e 55 e2 c8 25 65 3b 20 10 dc 49 db 77 f7 97 3b 06 7b 9f 1e 90 77 dd 2e f5 f4 f4 99 fa f3 ed 9b bb 9b fa 19 78 5f da 69 1c e0 ec d3 c7 f7 1f 3f 7f 79 3d 84 24 4a 33 0a 85 00 07 3f 30 bf 73 7f 7c f9 19 4a fd 97 2e 41 5e 03 7c 54 95 36 65 11 e7 8c 60 96 66 24 01 27 d4 46 39 5d e7 09 86 3e cd 35 95 02 18 20 18 90 dc 6d 43 12 32 11 53 27 4e 58 c4 91 5c 9e 44 96 71 18 27 87 17 94 d1 3c cb 73 6c 87 e3 69 8e e7 38 86 30 0d 21 aa b8 f6 5d 9e ef 20 cf 7c 92 e0 1a 7d 87 01 46 51 66 63 b7 4b b7 12 94 c6 cd 6b 23 3b bb c5 a8 0b 89 8b 5a 1e c8 e2 ac 0b 5a bf 60 12 27 2a 82 20 f2 34 ab 48 90 16 5d 45 a6 1d 4f 51 68 e8 49 2c ec f0 12 cf 76 94 56 0a 49 93 a1 b9 23 ec 3e c7 09 f1 70 80 9e 1f 62 3c 13 cf 0b 70 84 6c 00 21 4a d3 5f 9c 61 43 d7 f5 48 12 da 31 49 b3 c6 ef e2 a4 51 c0 6e ca ee 3e 44 f9 20 80 0f bc d7 5c 01 39 e1 a8 1d 62 98 90 94 78 19 89 ee f9 ee 52 34 67 cd 33 24 51 63 78 c8 45 c9 43 da 66 43 ee f5 f2 ad 34 03 19 ea 26 9b d9 ac 77 b0 8c b5 65 9b bb be 31 81 92 ce 2e c7 a3 f1 78 a7 0d f4 8d 9e 1a 23 39 4f 6a 15 6f e9 eb e6 a2 6f 39 43 eb 98 de 70 bb 0c b0 5f 75 96 71 d5 59 a5 61 1d bb 76 6f e7 cf 5c 5d 1e f8 33 63 a3 e1 e3 68 b0 1e 99 1a 9e 6a d6 29 e0 e4 e3 e0 a8 61 67 e4 2f 73 57 72 ea 21 3a 82 b3 5a 87 eb 99 60 68 f5 59 ba 4c 5e 9c e4 a5 3c e2 b9 f7 22 f9 e1 7c 3c 09 e6 ea b8 18 ed ca 7a a4 9c 6e 3d 55 1a f4 ea fc a5 38 da 45 1f cb 92 70 4b 71 69 17 5c ad a2 b5 71 15 02 3c 44 13 35 ad 13 6b 67 e4 a5 09 97 76 b9 9e 22 60 02 78 c0 ac a5 c9 8b 6b 2c e0 da 88 ca 91 d8 a3 7b 51 6f 55 94 7e fe b2 49 e0 cb 1c e9 a4 2e f4 9e b6 d6 d1 6d 76 dd f8 f5 c6 4f af 67 72 5d c4 7b fe 45 8c 32 92 79 55 0a 2e ec 4c 2b ad db 05 04 e0 30 75 4f f9 9e 1b c8 bb ad 93 38 ca 39 e0 6f d7 c2 41 3d 62 df c6 61 27 bc 8c 17 b3 e6 43 59 fb 1a 29 87 4a dd f3 d7 fd 76 0c 2f 7d c1 d6 86 fe 18 1b 47 88 8a 09 ed f9 2b 36 ce 25 3f 22 28 1e cc 65 2b b7 4b 61 e2 9a ab 1b 32 64 07 ad 8a 99 a5 69 9d f0 a6 eb 51 35 1d b1 dc 2e 73 8f 52 72 0e ad c4 d3 c5 c0 0c ab fe 21 14 70 b8 cc d8 ad 45 cb bd 1b 29 d7 2b a5 a0 85 a5 a8 5a c5 e4 e5 30 52 43 3d 32 72 0d d5 fc 79 28 66 61 1f 44 60 b5 07 d8 50 41 00 27 ac 75 03 03 a5 6f 76 46 83 eb 72 87 50 2f b8 98 bb 7d 18 cf 52 92 74 ec b1 96 e8 9b bc b0 d4 c9 1c 47 a3 d0 64 c3 fa 14 54 ae 9b ba bb 69 76 88 e4 a0 33 5f 6c 33 31 9d aa 9b a4 6a b4 33 44 33 a4 b7 ce d2 93 d4 79 df d9 01 7f 1d 2d a7 b3 ce 4a 27 95 cf 06 c2 26 da d6 c9 9c 1b 97 c0 26 63 52 5d 96 35 34 Data Ascii: 4b5mTkF)(N+C'l[UhY6}R+;;{fs`j`#Zz34ajk(&f|,c,&1LutO` JSU5+X-v7R8k,*@B .U%e; Iw;{w.x_i?y=$J3?0s\|J.A ^\|T6e`f$'F9]>5 mC2S'NX\Dq'<sli80!] |}FQfcKk#;ZZ`'* 4H]EOQhI,vVI#>pb<pI!J_aCH1IQn>D \9bxR4g3$QcxECfC4 &we1.x#9Ojoo9Cp_uqYavo\]3chj)ag/sWr!:Z`hYL^<"|<zn=U8EpKqi\q<D5kgv"`xk,{QoU~I.mvOgr]{E2yU.L+0uO89oA=b a'CY)Jv/}G+6%?"(e+Ka2diQ5.sRr!pE)+Z0RC=2ry(faD`PA'uovFrP/}RtGdTiv3_l31j3D3y-J'&&cR]54

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
Jul 21, 2021 22:41:59.993089914 CEST	134.70.88.3	443	192.168.2.3	49726	CN=objectstorage.eu-zurich-1.oraclecloud.com, OU=Oracle BMCS ZURICH, O=Oracle Corporation, L=Redwood City, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue May 11 02:00:00 CEST 2021 Thu Sep 24 02:00:00 CEST 2020	Sun Jun 12 01:59:59 CEST 2022 Tue Sep 24 01:59:59 CEST 2030	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 TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jul 21, 2021 22:41:59.993204117 CEST	134.70.88.3	443	192.168.2.3	49727	CN=objectstorage.eu-zurich-1.oraclecloud.com, OU=Oracle BMCS ZURICH, O=Oracle Corporation, L=Redwood City, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue May 11 02:00:00 CEST 2021 Thu Sep 24 02:00:00 CEST 2020	Sun Jun 12 01:59:59 CEST 2022 Tue Sep 24 01:59:59 CEST 2030	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5336 Parent PID: 4364

General

Start time:	22:41:51
Start date:	21/07/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'http://qtcheiz.northcroft.co.th/#ZGFybGFhbmRyaWNAY29sZHdlbGxiYW5rZXIuY29t#aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbQ==#jngdheuy'
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 912 Parent PID: 5336

General

Start time:	22:41:53
Start date:	21/07/2021
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=1552,14705750287286471760,12854902564490349709,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1800 /prefetch:8
Imagebase:	0x7ff77b960000

File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Disassembly