ID: 364098
Cookbook: browseurl.jbs
Time: 21:27:40
Date: 05/03/2021
Version: 31.0.0 Emerald

Table of Contents

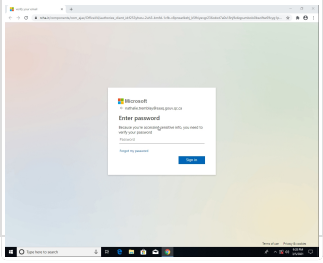
Analysis Report https://analytics.linkre.direct/clickthrou…

Overview

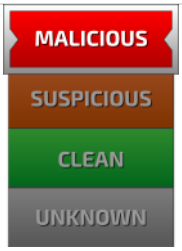
General Information

Sample URL:	https://analytics.linkre.direct/clickthrough?id=CDE9E442CE50D5323CAF39A56&i...y.hotellosmedanos.com.uy/?XAP=bmF0aGFsaWUudHJlbWJsYXlAc2FhcS5nb3V2LnFjLmNh
Analysis ID:	364098
Infos:	

Most interesting Screenshot:



Detection



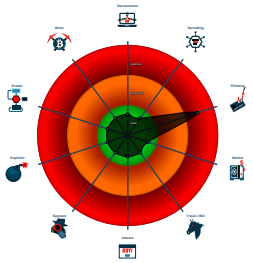
HTMLPhisher

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Phishing site detected (based on fav…
- Yara detected HtmlPhish_10

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 3100 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://analytics.linkre.direct/clickthrough?id=CDE9E442CE50D5323CAF39A56&issuer=interlkp&template=ILNSTATE01&url=http://www.nathalie.tremblay.hotellosmedanos.com.uy/?XAP=bmF0aGFsaWUudHJlbWJsYXlAc2FhcS5nb3V2LnFjLmNh%20' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 4604 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1616,5230389399112637974,4973306169734885708,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1692 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

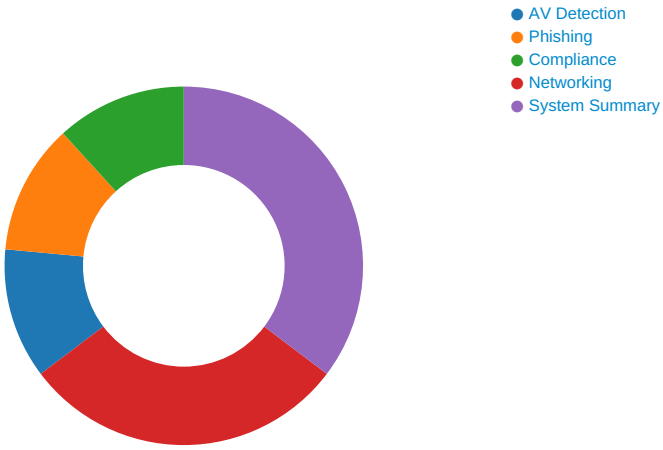
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish_10

Compliance:

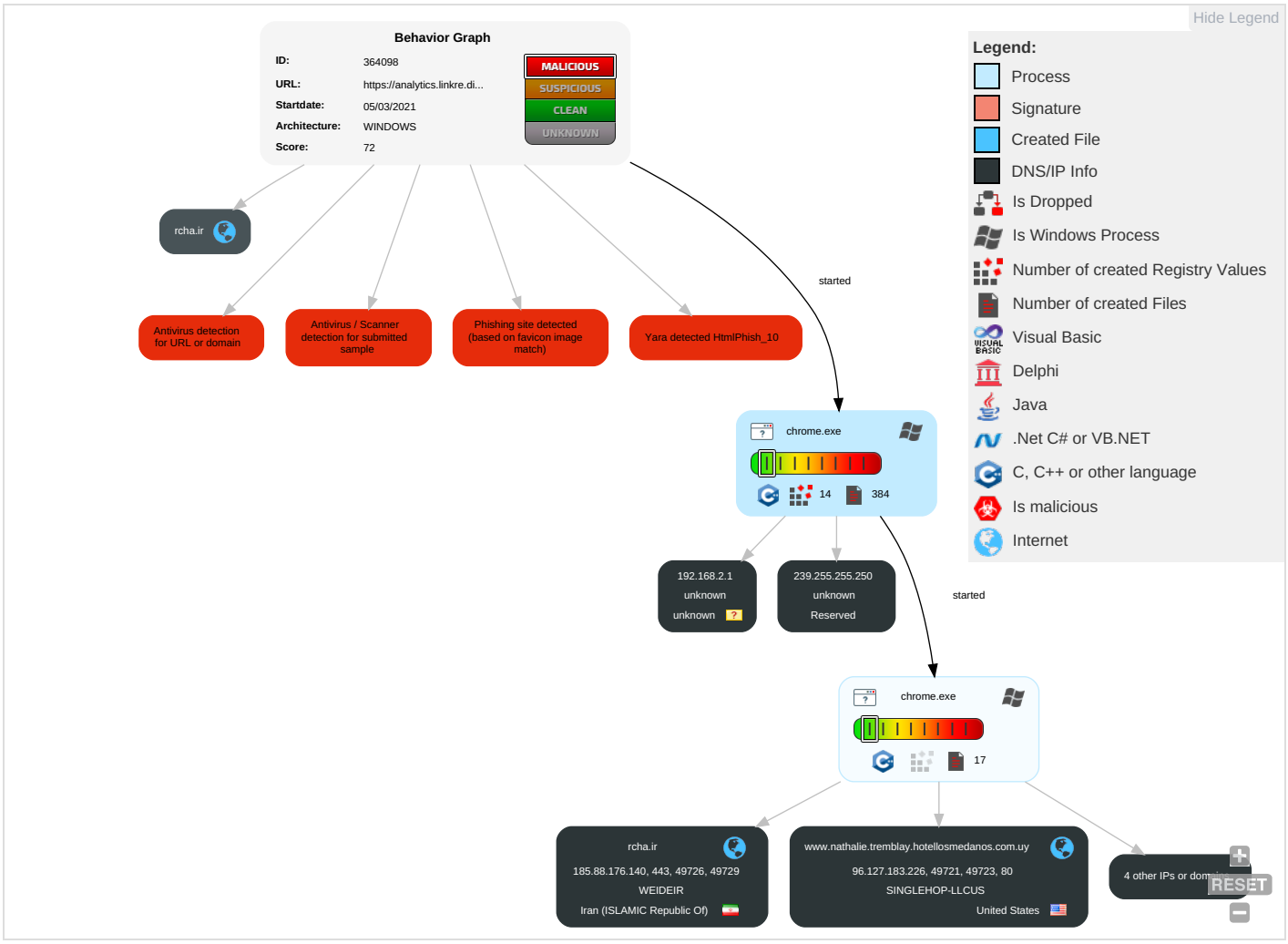
Creates a directory in C:\Program Files

Uses secure TLS version for HTTPS connections

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 Billing Fraud

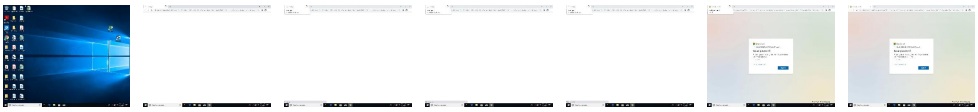
Behavior Graph

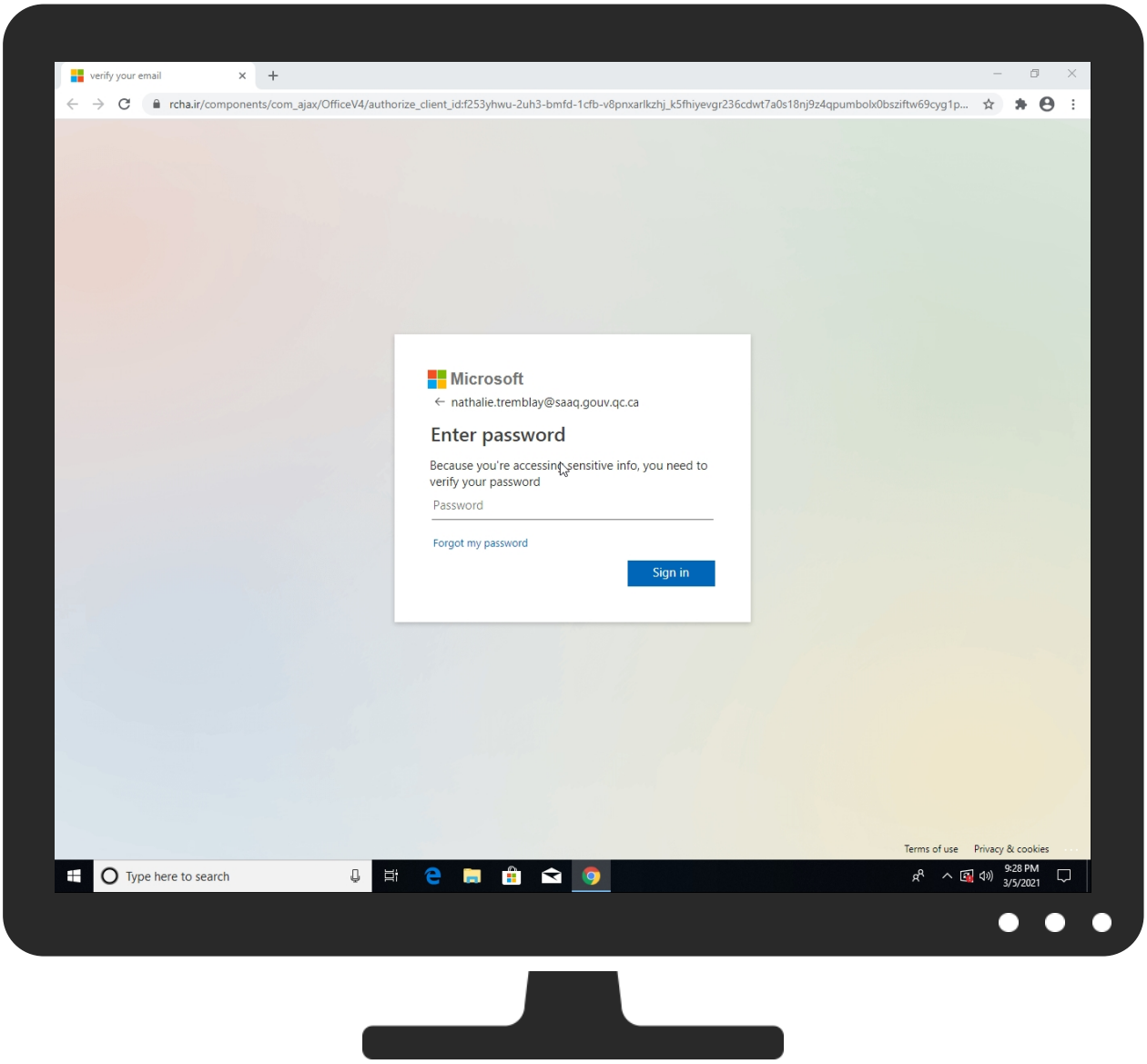


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://analytics.linkre.direct/clickthrough?id=CDE9E442CE50D5323CAF39A56&issuer=interlkp&template=ILNSTATE01&url=www.nathalie.tremblay.hotellosmedanos.com.uy/?XAP=bmF0aGFsaWUudHJlbWJsYXIAc2FhcS5nb3V2LnFjLmNh%20	0%	Avira URL Cloud	safe	
http://https://analytics.linkre.direct/clickthrough?id=CDE9E442CE50D5323CAF39A56&issuer=interlkp&template=ILNSTATE01&url=www.nathalie.tremblay.hotellosmedanos.com.uy/?XAP=bmF0aGFsaWUudHJlbWJsYXIAc2FhcS5nb3V2LnFjLmNh%20	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
rcha.ir	0%	Virustotal		Browse
analytics.linkre.direct	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://rcha.ir/components/com_ajax/OfficeV4/authorize_client_id:f253yhwu-2uh3-bmfd-1cfb-v8pnxarlkzhj_k5fhiyevgr236cdwt7a0s18nj9z4qpumbolx0bsziftw69cyg1puq5r38lakdnmhxej24ov78p3xc6dokf9i2re7wlvnzgqsbu105h4jmayt?data=bmF0aGFsaWUudHJlbWJsYXlAc2FhcS5nb3V2LnFjLmNh	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://analytics.linkre.direct/clickthrough?id=CDE9E442CE50D5323CAF39A56&issuer=interlkp&template=I	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://rcha.ir/components/com_ajax/OfficeV4/images/favicon.ico	0%	Avira URL Cloud	safe	
http://https://rcha.ir:443	0%	Avira URL Cloud	safe	
http://https://rcha.ir/components/com_ajax/OfficeV4?08909598527009&email=bmF0aGFsaWUudHJlbWJsYXlAc2FhcS5nb3	0%	Avira URL Cloud	safe	
http://www.nathalie.tremblay.hotellosmedanos.com.uy/?XAP=bmF0aGFsaWUudHJlbWJsYXlAc2FhcS5nb3V2LnFjLmNh	0%	Avira URL Cloud	safe	
http://https://rcha.ir/components/com_ajax/OfficeV4/authorize_client_id:f253yhwu-2uh3-bmfd-1cfb-v8pnxarlkzh	0%	Avira URL Cloud	safe	
http://https://rcha.ir/components/com_ajax/OfficeV4/?08909598527009&email=bmF0aGFsaWUudHJlbWJsYXlAc2FhcS5nb	0%	Avira URL Cloud	safe	
http://www.nathalie.tremblay.hotellosmedanos.com.uy/?XAP=bmF0aGFsaWUudHJlbWJsYXlAc2FhcS5nb3V2LnFjLmN	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
rcha.ir	185.88.176.140	true	false	• 0%, Virustotal, Browse	unknown
analytics.linkre.direct	143.204.90.56	true	false	• 0%, Virustotal, Browse	unknown
www.nathalie.tremblay.hotellosmedanos.com.uy	96.127.183.226	true	false		unknown
googlehosted.l.googleusercontent.com	172.217.23.33	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high

Contacted URLs

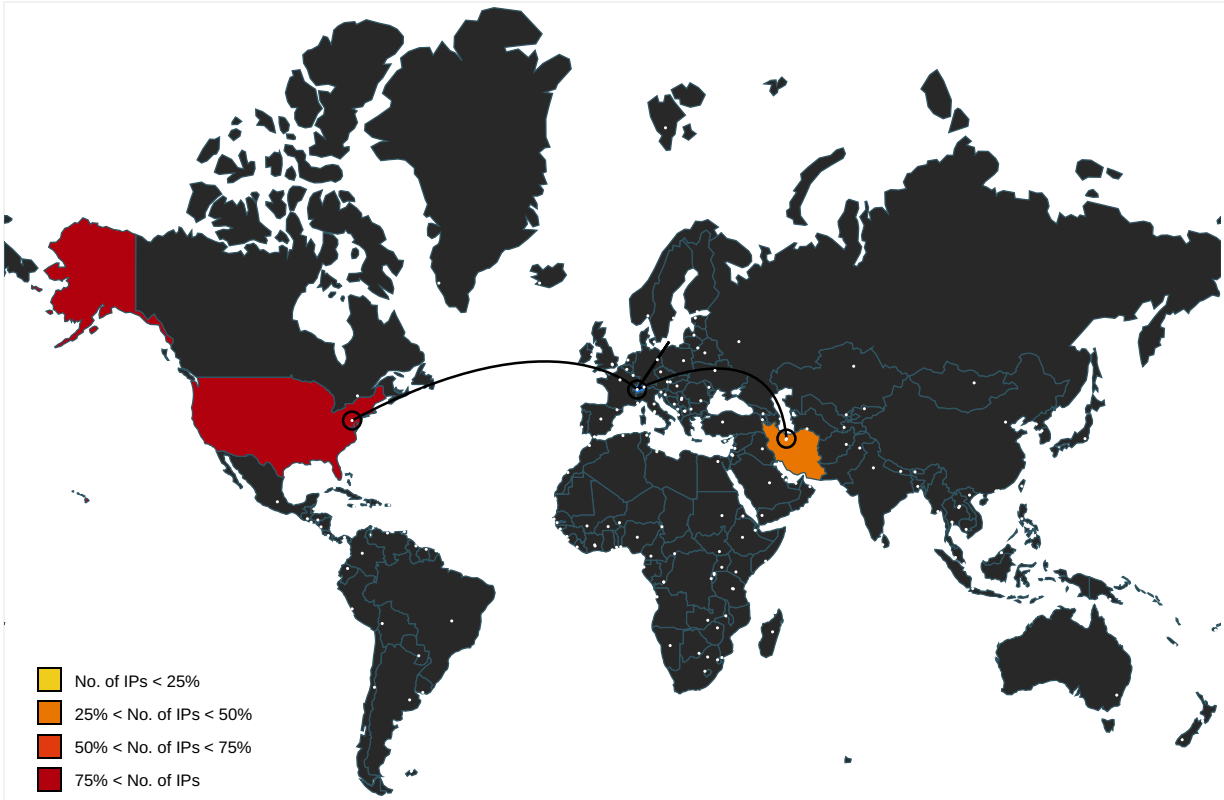
Name	Malicious	Antivirus Detection	Reputation
http://www.nathalie.tremblay.hotellosmedanos.com.uy/?XAP=bmF0aGFsaWUudHJlbWJsYXlAc2FhcS5nb3V2LnFjLmNh	false	• Avira URL Cloud: safe	unknown
http://https://rcha.ir/components/com_ajax/OfficeV4/authorize_client_id:f253yhwu-2uh3-bmfd-1cfb-v8pnxarlkzhj_k5fhiyevgr236cdwt7a0s18nj9z4qpumbolx0bsziftw69cyg1puq5r38lakdnmhxej24ov78p3xc6dokf9i2re7wlvnzgqsbu105h4jmayt?data=bmF0aGFsaWUudHJlbWJsYXlAc2FhcS5nb3V2LnFjLmNh	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://analytics.linkre.direct/clickthrough?id=CDE9E442CE50D5323CAF39A56&issuer=interlkp&template=I	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dns.google	c07a7b6e-a366-4a96-b276-abd1c1b7eb0e.tmp.1.dr, f100c073-8ff6-4aa0-ae19-94a17b740845.tmp.1.dr, 3cc5e6bc-70b2-4fc3-a8bc-837fee4852c1.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rcha.ir/components/com_ajax/OfficeV4/images/favicon.ico	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients2.googleusercontent.com	c07a7b6e-a366-4a96-b276-abd1c1b7eb0e.tmp.1.dr	false		high
http://https://rcha.ir:443	e5c080a1-79d3-4018-bc7c-12d19559d84f.tmp.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://rcha.ir/components/com_ajax/OfficeV4?08909598527009&email=bmF0aGFsaWUudHJlbWJsYXlAc2FhcS5nb3	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://rcha.ir/components/com_ajax/OfficeV4/authorize_client_id:f253yhwu-2uh3-bmfd-1cfb-v8pnxarlkzh	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://rcha.ir/components/com_ajax/OfficeV4/?08909598527009&email=bmF0aGFsaWUudHJlbWJsYXlAc2FhcS5nb	History.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://www.nathalie.tremblay.hotellosmedanos.com.uy/?XAP=bmF0aGFsaWUudHJlbWJsYXlAc2FhcS5nb3V2LnFjLmN	History.0.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
239.255.255.250	unknown	Reserved		unknown	unknown	false
185.88.176.140	rcha.ir	Iran (ISLAMIC Republic Of)		201691	WEIDEIR	false
172.217.23.33	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
96.127.183.226	www.nathalie.tremblay.hotellosmedanos.com.uy	United States		32475	SINGLEHOP-LLCUS	false
143.204.90.56	analytics.linkre.direct	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	364098
Start date:	05.03.2021
Start time:	21:27:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 23s
Hypervisor based Inspection enabled:	false
Report type:	light

Cookbook file name:	browseurl.jbs
Sample URL:	http://https://analytics.linkre.direct/clickthrough?id=CDE9E442CE50D5323CAF39A56&issuer=interlkp&template=ILNSTATE01&url=www.nathalie.tremblay.hotellosmedanos.com.uy/?XAP=bmF0aGFsaWUudHJlbWJsYXlAc2FhcS5nb3V2LnFjLmNh
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:	mal72.phis.win@29/162@5/7
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 93.184.220.29, 20.190.160.132, 20.190.160.129, 20.190.160.134, 20.190.160.71, 20.190.160.136, 20.190.160.6, 20.190.160.2, 20.190.160.4, 52.147.198.201, 51.103.5.186, 51.104.139.180, 52.255.188.83, 104.43.193.48, 142.250.185.238, 172.217.22.237, 172.217.22.206, 173.194.187.170, 74.125.173.39, 216.58.207.163, 104.43.139.144, 23.211.6.115, 184.30.24.56, 216.58.207.170, 172.217.20.234, 172.217.23.42, 172.217.23.74, 172.217.22.202, 172.217.22.234, 216.58.207.138, 51.104.144.132, 51.103.5.159, 2.20.142.210, 2.20.142.209 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, cs9.wac.phicdn.net, arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, clientservices.googleapis.com, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, vip1-par02p.wns.notify.trafficmanager.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, r1---sn-4g5e6nlk.gvt1.com, clients2.google.com, ocsp.digicert.com, redirector.gvt1.com, login.live.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, client.wns.windows.com, fs.microsoft.com, accounts.google.com, dual-a-0001.a-msedge.net, r5.sn-4g5e6nz7.gvt1.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, www.googleapis.com, r1.sn-4g5e6nlk.gvt1.com, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, r5---sn-4g5e6nz7.gvt1.com, blobcollector.events.data.trafficmanager.net, clients.l.google.com, ams2.current.a.prd.aadg.trafficmanager.net, vip2-par02p.wns.notify.trafficmanager.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtQueryVolumeInformationFile calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\04d757ca-3fda-4cc7-b3d3-68b8e1843619.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):	355944
Entropy (8bit):	6.0155373679196025
Encrypted:	false
SSDEEP:	6144:ljHVRzIHn+ieNryi8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB8:7R7LNryPxzurRDn9nfNxF4ijZVtilB8
MD5:	51EB4B532900BB2EDEF22D9FDAA327CE
SHA1:	49BAD71C194FC2957CC2A8B88B72D64D99BA016A
SHA-256:	501A7B9FC60AA6B88742D0A333275A881FC10AFCADFDF0BB50AB835E32206386
SHA-512:	789AB2873D440DE62662759F8F6A3BC4AF2E3EADC4B75AB8D10F89B1F983F2196F248EE2CC4FD23D865A744D94B6E07A80FC7A5BB1413734843C04EED8216B7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\04d757ca-3fda-4cc7-b3d3-68b8e1843619.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.615008510888287e+12,"network":1.614976112e+12,"ticks":105834567.0,"uncertainty":4434227.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075932336"},"policy":{"last_statistics_update":"13259482107786

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\05c678c8-1b11-49be-aa42-5c3403927172.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):	874
Entropy (8bit):	5.558349025694059
Encrypted:	false
SSDEEP:	12:YdDZ6Hk3O+UAnIvld06cY8rNgmh4r+UAnIElIWcNnYj+UAnIECm/bR7N+UAnI785:YT6H0UhHPkG1KUe9aUeC87wUavRUeIQ
MD5:	A21E50B55226C8B20E3695712A2AC9E6
SHA1:	52DF28905534E207CDE785EB740DC974C9B60DB6
SHA-256:	C30FD4C762FFE176B9382E395DA990FC4D3B41BE86E4FC406F6A5BB0AB979757
SHA-512:	E3D9DEC39459658CA25C3D2F851C23C615E4F061A1634F9915290151821E191768B56D3E142CFD12DFB62F9D84D9C30518E5A980265BA2A78ADB83C8AE48528E
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1633013028.743725,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477028.743728},{"expiry":1633013040.850112,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477040.850115},{"expiry":1646544510.858642,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1615008510.858645},{"expiry":1633013028.952627,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477028.95263}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\605e53c3-bd07-4dbb-8533-f0b2e83c04f7.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):	22614
Entropy (8bit):	5.535851435979107
Encrypted:	false
SSDEEP:	384:0gvttLlSHLXK1kXqKf/pUZNCgVLH2HfDFrU4HGwnTHLqyo4t:TLlyK1kXqKf/pUZNCgVLH2HfZrUsGwnd
MD5:	B671168C609FD70329D2484A2EDD624F
SHA1:	2FCD59F528608B5AEEABD162714A316EFD5398C0
SHA-256:	AED53BE468C3E5ACF42BD9AC48399C77180CFB0944F8C7BF666218A16F4FF5CA
SHA-512:	48249C238486A154AC66CC0F3F56D1B8D7D5F433CC502BA463B2C24788347C70208D129AB0A6A59FA91DB2DCC7D768DB05151D75405FBEC9316A63646A765F0
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":"13259482107880647","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\882a1c61-fced-405b-b68e-8332d89bf744.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):	16763
Entropy (8bit):	5.578166380455861
Encrypted:	false
SSDEEP:	384:0gvtULlSHLXK1kXqKf/pUZNCgVLH2HfDFrUfNqLo4D:KLlyK1kXqKf/pUZNCgVLH2HfZrUook
MD5:	DCE32077EBF2B8F9AC3F36BC4BFCDA11
SHA1:	2F58CD3BB7EDF6946E701DCC7B9DF6DB97C0E068
SHA-256:	4253DBC391F694FC6A555E0F018F059EE6F2D41D42825CCFE42B451BD29B7814
SHA-512:	9BAE3530F0DEF9F19BF363209AB1ED2F1A1E6400837FAC59D9A5A499A6D4189CFCAA5255D6736B91E53474087D0A01AF59EABF9EFECA5B71A627E07850690378
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":"13259482107880647","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	333
Entropy (8bit):	5.190236908245124
Encrypted:	false
SSDEEP:	6:mhHjyq2P923iKKdK9RXXTZIFUtpyVu1ZmwPy4RkwO923iKKdK9RXX5LJ:Cuv45Kk7XT2FUtpyk1/PyA5L5Kk7XVJ
MD5:	F7AA4A9C5DB944495012CFAAA303A586
SHA1:	04045226E8BC1CEA93F55EE6883045C814553CD0
SHA-256:	D16AF753261F9ECCB34AC886EDEEBB085126497647E87CF44F89170075C457D3
SHA-512:	467542FAAB2D1E4AD7BF583B4D8221084FAAD1A02E877D71667A0AE28BA049E919E8C3D29367F1EB46A25AD8E074669DFAE290F7B9909B943CDA6CBB2F99A1CE
Malicious:	false
Reputation:	low
Preview:	2021/03/05-21:28:47.720 e10 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/03/05-21:28:47.765 e10 Recovering log #3.2021/03/05-21:28:47.767 e10 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):	317
Entropy (8bit):	5.156848591395452
Encrypted:	false
SSDEEP:	6:mh1VFlyq2P923iKKdKyDZIFUtpy3j1ZmwPy31RkwO923iKKdKyJLJ:C1VOv45Kk02FUtpy3j1/Py3D5L5KkWJ
MD5:	1D8046B1B7B3217E2D748FD2FCDD948A
SHA1:	39A0063D6183DE035012114803C9F1265D57AA4A
SHA-256:	8247527C6F1248267F730CAEB5340BB001230DBBC80B089B25DF49F3B20C0432
SHA-512:	BCDB1E769902C85C30472F9AD7ED754E42E8B6413A2F40051BD44B583C81E245DAD81578ED5160179E8DEAF3A2A18261FCC4380C7B86A98460F80003B691F7C
Malicious:	false
Reputation:	low
Preview:	2021/03/05-21:28:47.702 e10 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/03/05-21:28:47.704 e10 Recovering log #3.2021/03/05-21:28:47.704 e10 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	12288
Entropy (8bit):	1.1048974207667022
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
SSDEEP:	24:TLyqJLbXaFpEO5bNmISHn06UwXEmDBdT4rtEy8FinP:TekLLOpEO5J/Kn7UpmD32DP
MD5:	439F62784DE0FD7F8B0BBDEF7CCE3C54
SHA1:	59041DF5725D476775B94E70CE734B4ADE28A46C
SHA-256:	B41ED40A2A05F73FA4E3FF59E0F20E466A0E60A500A3F546A1ED7658ADBC35B8
SHA-512:	A99D0C79A82965FF4AE96CC063EE9145108AD27A06B11EFA24DBCA03BD4DFF8B187B22A0268996F3EC8AF8E7D5DF807FF722910E19B63B32689C0DA268076EA 1
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):	0.9697265185157276
Encrypted:	false
SSDEEP:	24:cIL4rtEy8CqLbJLbXaFpEO5bNmISHn06Uwm8:cI+fq5LLOpEO5J/Kn7UR8
MD5:	5CDD687C33A1B2F308758564BD53B798
SHA1:	F81C7A79A43A600F3E86A7A09AE094EBA8CF7ACD
SHA-256:	56EE8988C8C52499AA3C6E443AE245568B9774EB386B12D6B1A2502C4ADF3D0C
SHA-512:	37510C51BB0B500B599CD814042FE95C0AF70FF2531A871B9BBF52CB17927F5EC0F5C4F5D486BBF372E97FD84BD8EA40A6A17FE38ECF79E92FC01C9CF179FB4 5
Malicious:	false
Reputation:	low
Preview:	.....6..... ....

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):	1787
Entropy (8bit):	4.438301027478149
Encrypted:	false
SSDEEP:	48:34uOcbexec002YxucW+CZmrwVlt7mklekW:34yl0NEdgwVlckI/
MD5:	C2C5F883AA88263CD572843ABA71C913
SHA1:	B3AF306D41CD3D9FF2C03C77C3811E74BBD8C97F
SHA-256:	1C23BAC054950DE58B1A70E4E6104695E56C630F9C299C6C6AE50E6C2498CDF0
SHA-512:	DFEE4CCD9EA40CDB731EFBCA70E6D9D09AF7C138B1DF0FB82BE040782BF891130245370807DC7D6DDE232A9D24608180A036CF3C68C96E0D40F21C05B1795A F8
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...388b3cb4_2737_4cde_8f7f_e610807cebe4.....RW$..... .....5..0.....&...{2F4F8386-A58B-4B0C-A17B-2FAAF764E551}.....https://rcha.ir/components/com_ajax/Off iceV4/authorize_client_id:f253yhwu-2uh3-bmfd-1cfb-v8pnxarlkzhj_k5fhiyevgr236cdwt7a0s18nj9z4qpumbolx0bsziftw69cyg1puq5r38lakdnmhxej24ov78p3xc6dokf9i2re 7wlvnzgqsbu105h4jmayt?data=bmF0aGFsaWUudHJlbWJsYXlAc2FhcS5nb3V2LnFjLmNh....T...P.....H.....h.....`.....p.....x.....p.....$.. x...%..x.....h.t.t.p.s.:.//.r.c.h.a...i.r./.c.o.m.p.o.n.e.n.t.s./.c.o.m._.a.j.a.x./.O.f.f.i.c.e.V.4./.a.u.t.h.o.r.i.z.e._.c.l.i.e.n.t._.i.d.:.f.2.5.3.y.h.w.u.-.2.u.h.3.- .b.m.f.d.-.1.c.f.b.-.v.8.p.n.x.a

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
SHA-512:	884C0D3594390E2FC0AEAB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C
Malicious:	false
Reputation:	low
Preview:	SNSS....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	319
Entropy (8bit):	5.152898898570193
Encrypted:	false
SSDEEP:	6:mhKlM+q2P923iKKdK8aPrqIFUtpyEZmwPyATpMVkwO923iKKdK8amLJ:CKlM+v45KkL3FUtpyE/PyQpMV5L5KkQJ
MD5:	C58312BA75BDAE1CB70D6F4E7CD8A450
SHA1:	97924C5F711D1DCC7D040D7537EEC18DCA7BEFCF
SHA-256:	E21B5039334020900A99847B7485AB5F5BBE934F18120BF8CBE4B28E430F9812
SHA-512:	B5740B580CFDBFE6261273F338A8F1A65A7A0D94C7EB4AAC6574CEA5A761F9493A472C035C9CC7AE2CA31E43405DCD9AAA853CD6C39E62434A42222AD763A6 6B
Malicious:	false
Reputation:	low
Preview:	2021/03/05-21:28:28.186 2fc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/03/05-21 :28:28.187 2fc Recovering log #3.2021/03/05-21:28:28.188 2fc 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:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Size (bytes):	319
Entropy (8bit):	5.175337898317946
Encrypted:	false
SSDEEP:	6:mhHFlq2P923iKKdK8NIFUtpyS9ZmwPyBFzkwO923iKKdK8+eLJ:Cuv45KkpFUtpyS9/Pyzz5L5KkqJ
MD5:	E4B992DC839E179E0CFD5807683A19B0
SHA1:	CFC3228493413F446E9A8E94FE4A404FA497A6F2
SHA-256:	F65B6D194C7FBB32840BD08C8BE04AED2B257E89F4F353BE72CC10699A93D47F
SHA-512:	B989BC7B98BA51B3968BE1F59755C688EB3C988B0B98AF381676E671C03D49D787006FBF5A881BA0F371A255085BA45F65A5046A17BAC736FE51F3CB5D1FD109
Malicious:	false
Reputation:	low
Preview:	2021/03/05-21:28:30.370 384 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/03/05-21:28:30.375 384 Recovering log #3.2021/03/05-21:28:30.376 384 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:GbylJnlTwGB7V9Hne4qasKxXltmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRITANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkIjEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	16384

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Entropy (8bit):	2.353243505550162
Encrypted:	false
SSDEEP:	48:yBmw6fUh2nxucm/+k1k4nw1Ok0GTXUBdsxxWhHxucaufkhcO:yBC62nMmIk4wsnGTkvuiHwwnO
MD5:	B8CD62B6762AA5068FC273849F60EC80
SHA1:	638E7DDAE618C166718E19E47AB2C655E8E1A038
SHA-256:	68CC02C37797D4CF999A55E31073B508DE5138B0F48FF8DBAE755C55531B377C
SHA-512:	8800CF3BE65881A18904947B4B18C2984022441911DEF0F5540C3759DB9AFA74D73D469D7DCF63B0F670003D7466D2AE17475A08FCC83A5F12228683F1CA00BB
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16972
Entropy (8bit):	0.7779501076885739
Encrypted:	false
SSDEEP:	24:UOOayLiXxh0GY/l1rWR1PmCx9fZjsBX+T6Uwrt3n:4adBmw6fUe3n
MD5:	C6D83D054CA9466B3D22639EDB1E6F56
SHA1:	05524E2A95C8932BE8A14558B04EF632780DE586
SHA-256:	1AD6BCA48CECADEF399080CFA7035177F0D1D273F134B3EC0986F0961A0175E7
SHA-512:	F9B17966772E8DCBC6E7C8EC8B502F32D9C8C29A6AF982C88B06B80C45DE1F1FFBC282F7F61AE0508603C2E90D310DEBA9B2BBBFC5F04C180764049488F973 4
Malicious:	false
Reputation:	low
Preview:	.....91..... ....

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):	371
Entropy (8bit):	5.23359688975627
Encrypted:	false
SSDEEP:	6:mhU4yq2P923iKKdK25+Xqx8chI+IFUtpyuj1ZmwPypMjRkwO923iKKdK25+Xqx8E:CU9v45KkTXfchI3FUtpyuj1/PypMF5Lk
MD5:	7FA727BDC8B3798666C87934754BD021
SHA1:	1116EBF7F4EAADB19AEB8A58851B79DFE75B7835
SHA-256:	D1C4AB49C6F7A5C0E9D578040E92F08808E412F7B6EF15BD3256F09AC5446EF1
SHA-512:	5A51961137FA9B38DB46FA0F062017495B546C523098CCB7F91FF315EF56EBCFEB99E691A272BD7DDF4EF73409C76B366EFC64AB4DECA34B35956B368F8871B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Preview:	2021/03/05-21:28:47.243 e10 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/03/05-21:28:47.266 e10 Recovering log #3.2021/03/05-21:28:47.268 e10 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):	357
Entropy (8bit):	5.174513796372333
Encrypted:	false
SSDEEP:	6:mhj9yq2P923iKKdK25+XuoIFUtpyAVT1ZmwPyAeRkwO923iKKdK25+XuxWLJ:CjAv45KkTXYFUtpyAR1/PyA65L5KkTXp
MD5:	11B6D5BA4BA9D43B805C0719F3CCEF63
SHA1:	5FFD6D2AE81579E1D7BA9C4FFD7EACC0B1A370AB
SHA-256:	18AF7EB8147CD06EB33629D122721519B2F4020021F934C274AAC195E0E7F647
SHA-512:	43EB806D7086FD978933DE1BD62F95C5FF996C635EB2FAD2EBCA9DB505AB57AEAABE5B65ECFD654945FC69021471BD2125DD5CF887071B26204F7CD44E0321E
Malicious:	false
Reputation:	low
Preview:	2021/03/05-21:28:47.168 e10 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/03/05-21:28:47.170 e10 Recovering log #3.2021/03/05-21:28:47.171 e10 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.264405962816196
Encrypted:	false
SSDEEP:	6:mhc+q2P923iKKdKWT5g1IdqIFUtpyKdZmwPy8hVkwO923iKKdKWT5g1I3ULJ:Chv45Kkg5gSRFUtpye/Py8v5L5Kkg5gZ
MD5:	9D3E9CC15F3B8A06133ADA07AB56D64E
SHA1:	0185B01A264428390A4A5FC780480B4BBB376CBE
SHA-256:	68782853916BEC9C329100C189560DFDA5230455AD78BFBEE38B39E91CD29B64
SHA-512:	C0A2EEB84E8386E90FBBFB82E4772CC297A7620FE9FB2B732073EAE2617C98D22B5CD6402366B26A9FF98FD1E54B3C3F808FBD3B160FA8960EED487ABD97074D
Malicious:	false
Reputation:	low
Preview:	2021/03/05-21:28:46.773 1ab8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/03/05-21:28:46.858 1ab8 Recovering log #3.2021/03/05-21:28:46.870 1ab8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.7589891406855308
Encrypted:	false
SSDEEP:	48:TB2kIm8xucufhTfikyf5fvJO72UjOUVuxucFCykY:kJ3IfhTfLyf5fv82Uz0DCyp
MD5:	57D53539225744D0DC4D970E656BECEA
SHA1:	84DEC241B8C59289149033C6D46C9FE006130217
SHA-256:	8016C11D98DB28169F11E5DD495B34C1DE071FAFE81F7A964E4F501124B73364
SHA-512:	5404EDB8D5971866E065B5D85EA37ECB77100AB6F1673A8EE3DF34CB45CB7934CD1DC055742E2A7BE6899C82C9190A7572724A9EE6E73360D69A356B71DB92A2
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Category:	dropped
Size (bytes):	3360
Entropy (8bit):	6.238931634872428
Encrypted:	false
SSDEEP:	48:ur5mrZj7tIKRfcIOEbegNMIYZXvdNykj/f0PR0+E0XxucI0UxNcMp:uQr4IXIgNeZOeXYR1EqvxcMp
MD5:	15F85442FDAA9E82C67FA1A377E67CD7
SHA1:	B2C4EDEAA9DFF0D05B7070E3C0A87427AE47E517
SHA-256:	CBF4AFECB1ECA962E23770E3EBA5B1A68AE0691645444D455BFDEC5005CAD00A
SHA-512:	5FD20ECA78590EE3520340912C365D61209D6F6EB2FD67F199CF45AF8034A9C93F97809A2DE914D2EC6E705FC4C840900B1A8CF2DBBA328CB442CB9BADC312 1
Malicious:	false
Reputation:	low
Preview:	.....".'..analytics.,bmf0agfsawuudhjlbwjsyxlac2fhcs5nb3v2lnfjlmnh..cde9e442ce50d5323caf39a56..clickthrough..com..direct..email..hotellosmedanos..http..https..id. .ilnstate01..interlkp..issuer..linkre..nathalie..template..tremblay..url..uy..verify..www..xap..your..08909598527009..ajax..components..ir..officev4..rcha..1cfb..2uh3..au thorize..bmfd..client..data..id:f253yhwu.lk5fhiyevgr236cdwt7a0s18nj9z4qpumbolx0bsziftw69cyg1puq5r38lakdnmhxej24ov78p3xc6dokf9i2re7wlvnzgqsbu105h4jmayt ..v8pnxarlkzhj*...'....08909598527009.....1cfb.....2uh3.....ajax.....analytics.....authorize. .0.,bmf0agfsawuudhjlbwjsyxlac2fhcs5nb3v2lnfjlmnh.....bmfd.!....cde9e44 2ce50d5323caf39a56.....clickthrough.....client."....com.....components.....data.#....direct.....email.....hotellosmedanos.....http.....https.....id.....id:f253yhwu.$....i lnstate01.....interlkp.....ir.....issuer...p.lk5fhiyevgr236cdwt7a0s18nj9z4qpumbolx0bsziftw69cyg1puq5r38lakdnmhxej24ov78p3xc6dokf9i2re7wlvnzgqsbu105h4jmayt.%

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):	0.04751802633184638
Encrypted:	false
SSDEEP:	6:40p7T5/l1+IW3+5Tpg9bNFlEwtCS/lC/l3n:VDqfV9qLipS/m3n
MD5:	501DF8BC105A9EA101A7B6BA691E36AB
SHA1:	A61E4893D044340876086ECE5946CBE5AD40F99B
SHA-256:	BA1373A323AA36AADB4C7A1298C6F5A64C6DDDF24443A7094D4C0BC095405630
SHA-512:	5F77F45B2EE1CE263052B878B67A854D5072712C41D5C3D2A6ED65B56AF03A37E5494CD5953ADBB8FC0E26FBA1116E535DF3FE6A3AF930DADFE96A07E452F9/ 7
Malicious:	false
Reputation:	low
Preview:	.....B'..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.458370951147012
Encrypted:	false
SSDEEP:	48:TZ0Gp5a7nM28dbvJZSsbQSefgGs4ZGNrS0U9RdiN97h:TJa7nMNdbvJZSsbQ5fgGsxrS0Vh
MD5:	A3982CCBD4BD284E6648EC20722C81B5
SHA1:	B7922652C2CB285ADB3E405E7112F383AA4B464E
SHA-256:	581B386FBE87D7F910AA9474F9FA15F94D8D7F9B786280DA3A0CE3E444392ED1
SHA-512:	8D3E3DF0FB684D1ACACB8DDF69482DEAE90D9BBDDBE279133D05A80E85B84998801BD367B2003655452337F4E360E8C01C5FDDF7131A621FFD36794C96DAEE CE
Malicious:	false
Reputation:	low
Preview:	I.....*.....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..537641000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-03-05 21:28:50.63][INFO][mr.Init] MR instance ID: e0fbe334-021e-4eef-90f5-fecec4fc7142\n","[2021-03-05 21:28:50.65][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-03-05 21:28:50.65][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-03-05 21:28:50.65][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-03-05 21:28:50.65][I NFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-03-05 21:28:50.65][INFO][mr.CastProvider] Query enabled: true\n","[2021-03-05 21:28:50.67][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Entropy (8bit):	5.1769789889848665
Encrypted:	false
SSDEEP:	6:mhG0FN+q2P923iKKdK8a2jMGIFUtpyG4X5ZmwPyGlWNVkwO923iKKdK8a2jMmLJ:CG0FIv45Kk8EFUtpyGW/PyG85L5Kk8bJ
MD5:	AE448AC2DCAEF7771AC6F63E14176F33
SHA1:	35BBE417C6E7B28993F1FB254951A7B7582EF884
SHA-256:	897D963211F75803F27283352A4D0C667F1A48E9FB5CF04A3BC7EB6DD3EF8301
SHA-512:	0822A2EBB0B3CD14F78D4A5607D0D4440866926C1734092E7A44299118B378D671B976BCB704E8D6D87EF5C0C1F1105A05213CF81F9E8085F8A34AC8BDF8884C
Malicious:	false
Reputation:	low
Preview:	2021/03/05-21:28:27.939 1128 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/03/05-21:28:27.942 1128 Recovering log #3.2021/03/05-21:28:27.944 1128 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	333
Entropy (8bit):	5.144021452376432
Encrypted:	false
SSDEEP:	6:mhgMq2P923iKKdKgXz4rRIFUtpyuZmwPy8FkwO923iKKdKgXz4q8LJ:CgMv45KkgXiuFUtpyu/Pyw5L5KkgX2J
MD5:	D85D5A36122DE19209C6E598C9C6026E
SHA1:	EDFDC4E98DA01B36C43F20083635218E4E5CC0A8
SHA-256:	6DF7375CF3C98FB06D88F90617D7D3DB237B7585BA0F15C79EEA347AD8C0C0F9
SHA-512:	B4F4AA73FF660F8CFDF0DFCFD5C5F445F78DB1D7CCE1C5B2883E2F5C23B0FB5388665B38186DD6044C7CDFBDA59DAB1000D31A2F2D012664E8ED63FB90C9EBC
Malicious:	false
Reputation:	low
Preview:	2021/03/05-21:28:28.208 384 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/03/05-21:28:28.211 384 Recovering log #3.2021/03/05-21:28:28.213 384 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\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljl:5ljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946B
Malicious:	false
Reputation:	low
Preview:	..&f.....&f.....&f.....&f.....&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	322
Entropy (8bit):	5.138287173873681
Encrypted:	false
SSDEEP:	6:mh2LKN+q2P923iKKdKrQMxIFUtpyaLXZmwPyQUxNVkwO923iKKdKrQMFLJ:C2v45KkCFUtpyaLX/PyQm5L5KktJ
MD5:	174ED96B0AB7ADA1CBBFAF61E67D67D9
SHA1:	2E74F31BED0D91AFB8FFDC1E87D4127EBEF83C3A
SHA-256:	557A73CB1FB400B8432087F9B8A8032A1B0AFCC038436446DD8514B37D007163
SHA-512:	8C06C49530FBEA3A153A56211C9DB2761BC27AB84864B2FD5AF1FFEEC6E4FC7DBEA289B46A6C1EA5C57156942686207A2CDAA9BF0360C1ECC43273646132F0D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Preview:	2021/03/05-21:28:28.124 1778 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/03/05-21:28:28.125 1778 Recovering log #3.2021/03/05-21:28:28.126 1778 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):	350
Entropy (8bit):	5.125573565833931
Encrypted:	false
SSDEEP:	6:mhG04q2P923iKKdK7Uh2ghZIFUtpyGRvYNJZmwPyGRUuPDkwO923iKKdK7Uh2gnd:CG04v45KkIhHh2FUtpyGRANJ/PyGRUce
MD5:	9F679A2FDDEC3EC0EDF3F062D3D9B522
SHA1:	7C5AF62A498EDCE48F94FD67167328D59AAF52E9
SHA-256:	4C4B40B6BD494FF5C46462826E8C884B5C67E43A6E68A874C3070704B1306733
SHA-512:	431A50158D03DD989921D2608C26151F4B038FEB7A73EB4033DC4C2E947A7563EF626A24630F272CD6E014804B5F5C0F6A4AD90A9F66C24A15729141BCFD8AA
Malicious:	false
Reputation:	low
Preview:	2021/03/05-21:28:27.859 1220 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/03/05-21:28:27.860 1220 Recovering log #3.2021/03/05-21:28:27.861 1220 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\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):	429
Entropy (8bit):	5.215182172998502
Encrypted:	false
SSDEEP:	6:mh3FXL9+q2P923iKKdKusNpV/2jMGIFUtpy/WZmwPyO9VkwO923iKKdKusNpV/23:CdL9+v45KkFFUtpy/W/PyYV5L5KkOJ
MD5:	B09B550DA9EEA37E28531E929DDB3EF0
SHA1:	9893BED27970E1E96A7EBA692DDF1CBCC1C7F274
SHA-256:	1E95D275CA3EDCAE853B294465DB820107C5E6DC1501D5D2F144B194F5C0CA6A
SHA-512:	A8373F8B0207476E3D156CC2EE4BDE7514E8DB3A21A9E80229A9F3C535156081D4ED420C98B97514432920B9068495DF694C3D6F8436CFE715B19A01CC2FD7D
Malicious:	false
Reputation:	low
Preview:	2021/03/05-21:28:28.172 2cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/03/05-21:28:28.173 2cc Recovering log #3.2021/03/05-21:28:28.175 2cc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	434
Entropy (8bit):	5.216204053905406
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
SSDEEP:	6:mhjUPIq2P923iKKdKusNpqz4rRIFUtpyzZmwPy3bkwO923iKKdKusNpqz4q8LJ:CoPIv45KkmiuFUtpyz/PyL5L5Kkm2J
MD5:	26D290EA0143B01FAEC3244CC03AF3C4
SHA1:	1790A150DEDA9C471F563D9E1219DB112DEFD2F3
SHA-256:	4F6C95E3A1805FC30447E882761252F560E30E93E7E297C3A61148AF359B0F47
SHA-512:	55890E04FE42C9E40FBCABECF809FE0315CCAA341E216DA5302D077D549F989F189F82C3FAE146C45947BDBA0CA5DD951ABE115EB24F19BF80B82DA9C0A9E0F1
Malicious:	false
Reputation:	low
Preview:	2021/03/05-21:28:28.209 11b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/03/05-21:28:28.211 11b0 Recovering log #3.2021/03/05-21:28:28.213 11b0 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):	417
Entropy (8bit):	5.298969684334981
Encrypted:	false
SSDEEP:	6:mhTaOq2P923iKKdKusNpZQMxIFUtpydqZmwPydWkwO923iKKdKusNpZQMFLJ:Cjv45KkMFUtpydq/PydW5L5KkTJ
MD5:	BF23FF0E1F7DFDAA898FE4D2A731E734
SHA1:	D3EFD85E96D95956909C202CAD6DD725AFBE9237
SHA-256:	3753EB690CB2A58B01B329A351FA9EE2CF424673E2AD0824CE3871610DEB0249
SHA-512:	212E742FF31D552EB92AFB5A0DB957917F5E1F1DC4D95A8E69FB84A2254BFC7F373DB583DC8080BB9F84412659D78ADB5F3E7D527FDBCE1B0252771FBA9771A
Malicious:	false
Reputation:	low
Preview:	2021/03/05-21:28:44.657 384 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/03/05-21:28:44.659 384 Recovering log #3.2021/03/05-21:28:44.659 384 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\gfdkimpbcpahaombhbimeihdjnejgicl\def\f100c073-8ff6-4aa0-ae19-94a17b740845.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.956993026220225
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5rAcJksDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdVAsBdLJlyH7E4f3K33y
MD5:	0C03D530AC97788D62D27B2802C34D83
SHA1:	20F78B6B32D98FA52846C70DF78E4E5CEF663E2D
SHA-256:	7941FADA9867DAAE08EBC196BAFC6952DD506842C3E7D8FB14DF9D4E402D894B
SHA-512:	D5905C124060997A14322D12DECE5C00C63F7174743C740C974D00E88B03F203909CC2AC972B2759E8087B0B10F6306C6E66BF853319B5AC96907F34C8456C80
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542588505091","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\3cc5e6bc-70b2-4fc3-a8bc-837fee4852c1.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.976576189225149
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5OV/sDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdysBdLJlyH7E4f3K33y
MD5:	5886A009EB58EE06A16EFD6D1BA9A046
SHA1:	A867B5052F3FBB811693DF8CE3FDAA794F2F2E40
SHA-256:	9E3392126DE2D81D019E0AB3E17F20BADD0EC9FBD944BCB7C4DAF449D937D496
SHA-512:	D24F30A2E35F903AC10AACC4425C58BECB1C6BE2BA30A3C2B9D9D46CE04914AA71F55B3B16ED89081AD65A7090C77F5DC4A258B7B98D71E6A994D176536FB 27
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542597817103","port":443,"protocol_str":"quic"}],"isol ation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.175056210237422
Encrypted:	false
SSDEEP:	12:Cgf+v45KkkGHArBFUtpys9L2W/PysVV5L5KkkGHAryJ:K45KkkGgPgjLbL5KkkGga
MD5:	9DC083B3D3A149A807AE2C62F172D675
SHA1:	9C3014799D15228D4CC3FC3209B2D6B127ABB2A9
SHA-256:	5CF80E08E8AA777D861C961A63BD8A90B4D63AFD62C9AD19D8238C1303A7174B
SHA-512:	C98E39CBCCBAD6F82AB40E05E2B52DB8425BD220687B86D7DC617DC7A653C470E5C11692FC6E5CD7605CAB48A6AB866D1B44E145D56F8C35F0D7307E5CBA7 95
Malicious:	false
Reputation:	low
Preview:	2021/03/05-21:28:47.307 2cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Local Storage\leveldb/MANIFEST-000001.2021/03/05-21:28:47.312 2cc Recovering log #3.2021/03/05-21:28:47.314 2cc Reusing old log C:\Users\user\AppD ata\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):	434
Entropy (8bit):	5.205597667922483
Encrypted:	false
SSDEEP:	12:CBMM+v45KkkGHArqiuFUtpys9/PyshjMV5L5KkkGHArq2J:Td45KkkGgCgd2L5KkkGg7
MD5:	5EC919F531A8D40F868DE9C65145E150
SHA1:	9D15D50512D2F34020ED898803A539967A183C00

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
SHA-256:	4B4EA8BB3257C208B958B0AC74AA5C944510DEC19460E34CD994AA8BF09D3AEF
SHA-512:	A35E455C076CD0ACE15C560D349F6F25E7EA2F9F69748AC10EA3A5C8CD1C23CE2065C42740C90B8664E654AD08A6A7A762B1AA907CAA3DFCB256FCE079E8F AA
Malicious:	false
Reputation:	low
Preview:	2021/03/05-21:28:47.308 128c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/03/05-21:28:47.314 128c Recovering log #3.2021/03/05-21:28:47.315 128c Reusing old log C:\Users\user\ AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	420
Entropy (8bit):	5.147746659626076
Encrypted:	false
SSDEEP:	12:CueijM+v45KkkGHArAFUtpyuepw/PyueZMMV5L5KkkGHArfJ:1d45KkkGgkgT2L5KkkGgV
MD5:	53133997CE0A4EE7F8180571CE287598
SHA1:	F2B8FBBCE7B7A225701A4FC07A09C0DB97337D8A
SHA-256:	83AF604130639DC3E2692FB8E61E8FE38B5AAB7E6B9B92159EE6552D9A1181B7
SHA-512:	D65850C0002796D1A2676DD50086B5DE3A6AA7DC263FBA1E3DCE6EF9F11D9FB5597D9BC1F407CADEC2393B6593E67CFC150382F66775993E0C0537E8F19FAE A
Malicious:	false
Reputation:	low
Preview:	2021/03/05-21:29:03.006 128c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/03/05-21:29:03.007 128c Recovering log #3.2021/03/05-21:29:03.008 128c 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:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF21 24
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Category:	dropped
Size (bytes):	326
Entropy (8bit):	5.150322153967675
Encrypted:	false
SSDEEP:	6:mhGt4q2P923iKKdKpIFUtpyGC/JZmwPyGlPDkwO923iKKdKa/WLJ:CGt4v45KkmFUtpyGeJ/PyG1D5L5KkaUJ
MD5:	A37C0DB5E48EEA7FBCB0319C14A95388
SHA1:	28467CB3D02A6863C052F7FF9558B7FA600B7746
SHA-256:	28843FF57AABE0683DDC221E5A910C6B3F38ACA657633FF17ADF50061A26E0F0
SHA-512:	C1EE968590B47D494EF235BEE0D4DA45A14B59B08E2BA4FE285B8CB441D1114A91966CE4E1CF61BC5A6137CA6DD08D278B20BCCA6109BEE25F7E27167D5FB2E0
Malicious:	false
Reputation:	low
Preview:	2021/03/05-21:28:27.900 1220 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/03/05-21:28:27.905 1220 Recovering log #3.2021/03/05-21:28:27.908 1220 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):	401
Entropy (8bit):	5.237118236807892
Encrypted:	false
SSDEEP:	12:CJT9+v45KkkOrsFUtpyJVb2W/PyJVb9V5L5KkkOrzJ:a+45Kk+g0VgVVL5Kkn
MD5:	B71A509CB2F2E107D34FFA938A07ACEA
SHA1:	C561865F05B8D7996ED5230C8BF825C57A52CDA5
SHA-256:	FB8E5DA6237B9995E6EC714190302A0416CB8433177BFC9B6EDC76BA8881C367
SHA-512:	FE487C6BCAD94FF17D1B6A0D683E96047EB3AA1127BA2E703060B7DF0B590EEEF7561F2AE293538ED4C88F8FACA2B55F55C43353C5F2FD3F0215CF4231480BDB
Malicious:	false
Reputation:	low
Preview:	2021/03/05-21:28:50.700 2cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/03/05-21:28:50.702 2cc Recovering log #3.2021/03/05-21:28:50.702 2cc 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):	60
Entropy (8bit):	4.763501280039721
Encrypted:	false
SSDEEP:	3:eiuSlllFel59N8OngE6:N/6jB/6
MD5:	1FE9E6952CB5D39E24F899D8236B1F63
SHA1:	90C521CD6D6A9DA5F4F2B26B13C6743552E57E90
SHA-256:	021986AA8D6C5C40FD58F13B4EF8BB29D39694EE87F6BF7B830313292946B6C7
SHA-512:	257D04F92FDB36631D8AF0D7821A856713C384FBAEEC40693E97E2F0B86E2C6C391E5C65397D813C1DA602254C3276B148DD5AA20650AB592CC26B64CB5F544
Malicious:	false
Reputation:	low
Preview:	....z..pLC.8.....>..TX.0.....K...<.....C\)Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a01910a8-303c-48fb-8247-31d2edbe0aaf.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):	22613
Entropy (8bit):	5.535912430543056
Encrypted:	false
SSDEEP:	384:0gvttLlSHLXK1kXqKf/pUZNCgVLH2HfDFrU4HGDnTHLqWo4g:TLlyK1kXqKf/pUZNCgVLH2HfZrUsGDnM
MD5:	9AF13898237861A00FE4019F1A862506
SHA1:	08CEC7995BCB99AE8A0D7737E8CAB2B58B0F7B7C
SHA-256:	6B4624C698B6457E426CA9A1AE1D0FCFE2464DA679626F69AB56C9049B5FA0F0
SHA-512:	BA08BCC437DA5665E89F48CC0C05DB8DEF6FA6305B92397B88D5D2C37B7B170E2CDDC2E07E123C28A3916689221B9C12A42951C787A297A1F33A86BFDA02A72

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a01910a8-303c-48fb-8247-31d2edbe0aaf.tmp	
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":"13259482107880647","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\b52055f5-6b47-4cff-b5b4-42400747a172.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\c07a7b6e-a366-4a96-b276-abd1c1b7eb0e.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):	2693
Entropy (8bit):	4.871599185186076
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD
MD5:	829D5654ADF098AD43036E24C47F2A94
SHA1:	506C8BA397509BA0357787950C538C1879047DF3
SHA-256:	4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211
SHA-512:	D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DBCAA
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c16374d8-cc39-4d71-985a-178a681da92d.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):	5556
Entropy (8bit):	5.1722425236033995
Encrypted:	false
SSDEEP:	96:nlFPPv4HQsnjSVpIk0JCKL8BkO11BbOTQVuwn:nlp4H1SvC4KEkOx
MD5:	F46947D0792A2C0AC515DFAAE2EA556E
SHA1:	F385155D74A15260B8F9ED06F879FEDA5EEC0F33
SHA-256:	B5151097CB11D95706677189252864 7C365644E7833BA82159EFAC44EDDE6A92
SHA-512:	443B32C2442AEB261779A881E5CCE86FCBCC71F28833E85A0803D7B574DAAF707DD2A9B01FB5E2EB867037C4438E108C61D37C1BB1BA41AFAA62BB7E8A4E6499
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c16374d8-cc39-4d71-985a-178a681da92d.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13259482108133249","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcom e_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":1 0,"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","1538886"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.629516710945991
Encrypted:	false
SSDEEP:	3:tUKIjmFUEHQgZmwv3yjC2V8syjC2WGv:mhqFUEH5ZmwPy22Vvy22tv
MD5:	293B87D8995F28D17BF255F286CF07A5
SHA1:	07838B45BE321B5C2EBD705ADE1B697B5AED58FB
SHA-256:	A7C8EB1CB2A62996D774221C4688C98C321E06BD0C3FDDD9A5767D28DF4C318D
SHA-512:	88DE07B74299890ACC7274984520C2C60B4D6B46D0AECB967F0779D746F76008FF78A01829CE434BC8E4A7787D3286A6676ACD132E3083B7318306352D319C39
Malicious:	false
Reputation:	low
Preview:	2021/03/05-21:28:46.443 1ab8 Recovering log #3.2021/03/05-21:28:46.527 1ab8 Delete type=0 #3.2021/03/05-21:28:46.527 1ab8 Delete type=3 #2.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e5c080a1-79d3-4018-bc7c-12d19559d84f.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):	4960
Entropy (8bit):	4.961442674217402
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e5c080a1-79d3-4018-bc7c-12d19559d84f.tmp	
SSDEEP:	96:nlFPoG4pSVpIk0JCKL8BkO11BbOTQVuwn:nlF4pSvC4KEkOx
MD5:	967AA353BE1F3D335734B8491B142ACD
SHA1:	4ED49E7F3772D4E2A858556DD5162BC9B3D586E1
SHA-256:	98CAE79B4EE6E281897491F0E257453BB64637AF7AD0F34EFA8C2C3939CF73A0
SHA-512:	22D7CE2D0A668E58989DEA622DF76D233BDAAEB502909E1D9D08A23910EEE515BF780A95B4518A612857D81BA50C30B981956932C73E68789E8B6DF7022A6C5
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13259482108133249","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	337
Entropy (8bit):	5.207429501549222
Encrypted:	false
SSDEEP:	6:mhMOq2P923iKKdKfrzAdIFUtpysd9ZmwPysdPkwO923iKKdKfrzILJ:CMOv45Kk9FUtpyM/Pys5L5Kk2J
MD5:	D6A0CBFB444AE20EFA084238C6B54C0B
SHA1:	36EF02F6C37DA4E638463CC1ACC5BB5173A0AEDE
SHA-256:	A79F2D64DF4470E0CA78A2D96DFEBD6DF301E42606A6D2D7525059A0FBB9A5A1
SHA-512:	B6D0ACE52730C23B0809BF1BB4665DB276522475A120A26558FA1C09AFAEAE23AE6C9C07FCA4358A5AB326FB5DBF51C0E26255DAB88D30AFC462723E232D50D
Malicious:	false
Reputation:	low
Preview:	2021/03/05-21:28:48.235 384 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/03/05-21:28:48.246 384 Recovering log #3.2021/03/05-21:28:48.246 384 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
Preview:	85.0.4183.121

C:\Users\user\AppData\Local\Google\Chrome\User Data\d70c950e-de5d-48f3-8e51-bbe3cfc47fb5.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7409296116839013
Encrypted:	false
SSDEEP:	384:TTIXr5agJFabWNTrovvl3YnRkHtgGkDrOJDrx4d59YrSrma9KVrLLEOlFzNq1jyh:ca19mVggAe3XtpgfnqJKrRPFj
MD5:	AAB75C30B3578FB9B86F9EE3E3CDE42A
SHA1:	33121D1ADC7BC51228C7DC47C4B5964A91BDEB05
SHA-256:	8DB04FD7A58FCCBBDCC1C477380490B6339C8E02BF451FC5985E76769B534EEA
SHA-512:	D71C6DD49307DB0437BA9150FFB1EB70CF92C8C279011363E7AFDDCDD4BC9D3A83A4C0BF5FE321FDB1941D270C846D72244C35DDF4DFF4DB912812ADAA286C9
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...u38.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\f8d7ebac-c94e-48a0-bc7d-9933b42dc052.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):	355944
Entropy (8bit):	6.0155372710883865
Encrypted:	false
SSDEEP:	6144:tjHVRzIHn+ieNryi8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB8:zR7LNryPxzurRDn9nfNxF4ijZVtilB8
MD5:	9DBE3FC9D57B3B76A2AB226940566708
SHA1:	B458A8A4F696E179194D52A3EC89909B24460CB4
SHA-256:	457A038D2DED099521C8F9026EAE50E654FA310878A1F2D77E5CE5680814B170
SHA-512:	A8A94D73A449E0CB67DE6270D5BB5FB9B4B2FD15A5A359D4F3418944B177FA191E474792B383F90AD0D71328D4D3C24D019C868C8516E73D18A0B39B0D895EF
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":1.615008510888287e+12,"network":1.614976112e+12,"ticks":105834567.0,"uncertainty":4434227.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13259482107786

C:\Users\user\AppData\Local\Google\Chrome\User Data\fde43cc8-91e8-45b7-97ae-9d34e5d1b811.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):	355944
Entropy (8bit):	6.015537052953158
Encrypted:	false
SSDEEP:	6144:7jHVRzIHn+ieNryi8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB8:FR7LNryPxzurRDn9nfNxF4ijZVtilB8
MD5:	9ED2465ADFCE6CDC4FCE961B2800E351
SHA1:	D69D5F98DC58C33BEF93FAA4BF060F9B48523510
SHA-256:	8707EF0E788C489FB25A5C5E79215FA3862155DC236CFF9D8B9E21015C4F40C0
SHA-512:	93439537D42E7D34CA904860183F499054DFD1EC99F43103E3708AB3788D81A978A75903C6F501A286D43B905BE5128E665C59906A83E208152C7CD893F8E9F5
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":1.615008510888287e+12,"network":1.614976112e+12,"ticks":105834567.0,"uncertainty":4434227.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13259482107786

C:\Users\user\AppData\Local\Temp\1e07c26f-1556-4e52-80cb-fc5aa046621c.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\39927738-4091-4f41-a9a1-06ce1246f630.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\a420a1c1-b52d-4afc-a6f0-9cf9445330b4.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F332688
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L]....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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\c72b5704-f23e-4a4c-b271-107f9d615d97.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

C:\Users\user\AppData\Local\Temp\c72b5704-f23e-4a4c-b271-107f9d615d97.tmp	
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L\....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v....;.._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&..._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....I-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-I..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F770C
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... . ... Chrome".. },.. "app_name": {.. "message": "..... . ... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "...., ...".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "...., ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CEB4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "Connecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D84885B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\cs\messages.json	
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed .".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5 E0A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_u navailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be comp leted.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB805 52
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_una vailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "The trans action could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	787
Entropy (8bit):	4.973349962793468
Encrypted:	false
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWlOGAOf+XD:WguYpCZnpEZbGoD
MD5:	05C437A322C1148B5F78B2F341339147
SHA1:	AB53003A678E44A170E73711FBD9949833BBF3AA
SHA-256:	A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070
SHA-512:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavail able": {.. "message": ". ...."".. },.. "craw_connect_to_network": {.. "message": "..... .. .."".. },.. "iap_unavailable": {.. "message": ".. ...."".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."".. },.. "please_sign_in": {.. "message": "..... ... Chrome."".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\en\messages.json	
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\en_GB\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	661
Entropy (8bit):	4.450938335136508
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyZnLAOfTY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OGAOffD
MD5:	82719BD3999AD66193A9B0BB525F97CD
SHA1:	41194D511F1ACC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE018
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "Los pagos en la aplicaci.n no est.n disponibles en este momento.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\es_419\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	637
Entropy (8bit):	4.47253983486615
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34GLO03OyZnLAOfTYiJD:1HEvaC6WYpcDeEFxq8Zp4LlOGAOfvD

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\es_419\messages.json	
MD5:	6B2583D8D1C147E36A69A88009CBEBC7
SHA1:	4D4DEEB4BE6AA0181825F3371A761ABC5B4D5937
SHA-256:	6659BC3705311D7641A73995DCFEA80C7734F2F4EBBC3787B3892A240348324F
SHA-512:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA3
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "En este momento, Pagos En-Apps no est. disponible.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\et\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	595
Entropy (8bit):	4.467205425399467
Encrypted:	false
SSDEEP:	12:1HEJfPGGGfPG+WYpU34Ze7z+dgrW9O8ZpU34ZwZz03OyZnLAOfTYgoLIR:1HEdvqlWYpTeObk8ZpT/OGAOfuLIR
MD5:	CFF6CB76EC724B17C1BC920726CB35A7
SHA1:	14ED068251D65A840F00C05409D705259D329FFC
SHA-256:	C85800BF45942FCC7FD6B1DF929C25F9CC2A977A6678966BD03D4B6B69889AFD
SHA-512:	53D7D01BB30C0306DE65A79FD9551D2E8C1F71F4F45F71906B009071CB3E0F231E6A50FDD78773E9B4DE94085BC7B97F829842FA21A89A2080D33458B745C46F
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome'i veebipoe maksed".. },.. "app_name": {.. "message": "Chrome'i veebipoe maksed".. },.. "craw_app_unavailable": {.. "message": "Rakendus pole praegu saadaval.".. },.. "craw_connect_to_network": {.. "message": "Looge .hendus v.rguga.".. },.. "iap_unavailable": {.. "message": "Rakendusesisesed maksed ei ole praegu saadaval.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logige Chrome'i sisse.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\fi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.595421267152647
Encrypted:	false
SSDEEP:	12:1HEJRuzGGRuz+WYpU34ujSBu+dgYO8ZpU34J+Bu03OyZnLAOfTY5HN:1HEFcWYpPNa8ZpD+FOGAOfEHN
MD5:	3A01FEE829445C482D1721FF63153D16
SHA1:	F3EAAADDC03F943FC88B30B67F534AA13E3336DD
SHA-256:	0BDE54B20845124113383B6EB81E43A0F05E4EB0C44BEE3C1DFAC4CC5FEC2836
SHA-512:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BEAD8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Storen maksut".. },.. "app_name": {.. "message": "Chrome Web Storen maksut".. },.. "craw_app_unavailable": {.. "message": "Sovellus ei ole t.ll. hetkell. k.ytett.viss..".. },.. "craw_connect_to_network": {.. "message": "Muodosta verkkoyhteys.".. },.. "iap_unavailable": {.. "message": "Sovelluksen sis.iset maksut eiv.t ole t.ll. hetkell. k.ytett.viss..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Kirjaudu sis..n Chromeen.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\fil\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	658
Entropy (8bit):	4.5231229502550745
Encrypted:	false
SSDEEP:	12:1HEJADlbGGADlb+WYpU34hTUT+dgHfZAFFZO8ZpU34hTjzeT03OyZnLAOfTYHfvF:1HEYah6WYp7TUSoxOS8Zp7TOsOGAOfqV
MD5:	57AF5B654270A945BDA8053A83353A06
SHA1:	EEEF7A4F869F97CF471A05D345E74F982D15E167
SHA-256:	EC002ED92359F67818B49455DFC579E140368E6A004080AF022FD4F57F6B03F2
SHA-512:	5F0AE839FCF3F4EA48FF41A76655AE0F3821564AFD5D42FBB9FBB9A38E8D8F7BB5E9B6F71064588CD441261F644095A44A755C134CE546D506D9A21E488BAF52
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\fil\messages.json	
Preview:	{.. "app_description": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "app_name": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Kasalukuyang hindi available ang app.".. },.. "craw_connect_to_network": {.. "message": "Mangyaring kumonekta sa isang network.".. },.. "iap_unavailable": {.. "message": "Kasalukuyang hindi available ang Mga Pagbabayad na In-App.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Mangyaring mag-sign in sa Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\fr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	677
Entropy (8bit):	4.552569602149629
Encrypted:	false
SSDEEP:	12:1HEJALf/nbGGALf/nb+WYpU34Owdgbyb+dgdQjO8ZpU34ITQpGnbyb03OyZnLAO8:1HE4Hna1Hn6WYpNdgpY8ZpSTQwnBOGAh
MD5:	8D11C90F44A6585B57B933AB38D1FFF8
SHA1:	3F9D44EA8807069A32AACA2AAAD02FD892E6CC90
SHA-256:	599491F8C52B945C16C441ADF45BFD45AFAE046DA07757D97C56AF4DE75ED3B5
SHA-512:	D7EF7F5AD7EF1A1595825D79B69E2B1E988AD3CF1F3881496FCCD30F241E4E9C6E457F9F5D0F855DE3536DB7A40C3E1C55946B50D3F556F4A35285066A0CD6F
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "app_name": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "craw_app_unavailable": {.. "message": "Application indisponible pour le moment.".. },.. "craw_connect_to_network": {.. "message": "Veuillez vous connecter . un r.seau.".. },.. "iap_unavailable": {.. "message": "Les paiements via l'application ne sont pas disponibles pour le moment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Veuillez vous connecter . Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\hi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.791154467711985
Encrypted:	false
SSDEEP:	24:1HEs07J0JWYp9vnCSVLP8Zp6CsOGAOf8SLm:Wh7qgYp1CMLUph1GiSLm
MD5:	E376D757C8FD66AC70A7D2D49760B94E
SHA1:	1525C5B1312D409604F097768503298EC440CC4D
SHA-256:	8106D98C4F8DA16DB698444409558E29CC96735E188BFA303C333A5D99231C1D
SHA-512:	673F3F259AF2946E4F49BBED14A2A70D44BF9FDA9D7A71DC9172BA9B7B3C7F7062B16D29682B638D485B0520ED6F99E7A735F28C7C719B539559005B69FA7555
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome ... .".. },.. "app_name": {.. "message": "Chrome ... .".. },.. "craw_app_unavailable": {.. "messa ge": "..... .. ..".. },.. "craw_connect_to_network": {.. "message": "..... ....".. },.. "iap_unavailable": {.. "message": "..-.. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... Chrome ... .".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\hr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	618
Entropy (8bit):	4.56999230891419
Encrypted:	false
SSDEEP:	12:1HEJGiimxmbZGGGiimxmbZ+WYpU34OBOEuhopIO+dgcapZO8ZpU34GiiZrMrQphK:1HE4H4TH8WYpNjTta28ZpQVLP0SOGAOK
MD5:	8185D0490C86363602A137F9A261CC50
SHA1:	5BD933B874441CEACB9201CCC941FF67BAED6DC0
SHA-256:	A2B2EC359A9DD9DCCCE02859CE1E738BD30FAA4A05F1DC522893FFDF722BBC15
SHA-512:	D7629978FC031EA5F716F9C1065FB2FEAB48C15F10CD68830DC966FA1002C03DDC7ACDE314C7D075F9F3A0A68552A6ACBCCDEE24CF20B6C3DD1BCE6562D0 6E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "app_name": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "craw _app_unavailable": {.. "message": "Aplikacija trenuta.no nije dostupna.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se s mre.om.".. },.. "iap_unavailable": {.. "message": "Pla.anje u aplikaciji trenuta.no nije dostupno.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be comple ted.".. },.. "please_sign_in": {.. "message": "Prijavite se na Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\hu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\hu\messages.json	
Category:	dropped
Size (bytes):	683
Entropy (8bit):	4.675370843321512
Encrypted:	false
SSDEEP:	12:1HEJVJiGGVJi+WYpU34Hpo9O+dgMmfgijO8ZpU34Huo9O03OyZnLAOfTYBIAYm:1HEVrk5WYpQzTUg/8ZpwoXOGAOfYIAd
MD5:	85609CF8623582A8376C206556ED2131
SHA1:	1E16EB70DB5E59BB684866FF3E3925C2DEF25A12
SHA-256:	32A249749F12ADB6A220BF9ADC272C7E5D9AD5497A38B0086D961E3ABA17FBC6
SHA-512:	27883430865D3CFA6EDFE8C6CE1442BD96150B5CE520CCF7D556A330CAA6392C712B47BD86F7350E174876BC681F6DEC94D1312402655B0AF90883A2899EC78
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. },.. "app_name": {.. "message": "Chrome Internetes .ruh.z Fizet.si r endszere".. },.. "craw_app_unavailable": {.. "message": "Az alkalmaz.s jelenleg nem .rhet. el.".. },.. "craw_connect_to_network": {.. "message": "K.rj.k, csatlako zzon egy h.l.zathoz.".. },.. "iap_unavailable": {.. "message": "Az alkalmaz.son bel.li fizet.s jelenleg nem .rhet. el.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Jelentkezzen be a Chrome-ba.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\id\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	604
Entropy (8bit):	4.465685261172395
Encrypted:	false
SSDEEP:	12:1HEJs25bGGs25b+WYpU34ORBHAeSJ+dgkmO8ZpU34s22C/SzFAs03OyZnLAOfTYR:1HEBaA6WYpaHFH8ZptOYOGAOf2D
MD5:	EAB2B946D1232AB98137E760954003AA
SHA1:	60BDC2937905B311D2C9844DF2D639D7AC9F7F67
SHA-256:	C6E8800450602DE0F39FE9F6854472383813FB454B08ABAE7E25A9167CE004C3
SHA-512:	970FEC9A9EF0BAF7F693C4C5977F3B47914579C5B5414FCE9DBB5E4574659A5BB9AD2DE0CC886B368F49C019785AF7D2D7FE82F71341F039EADC399ED776CA 2
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pembayaran Chrome Webstore".. },.. "app_name": {.. "message": "Pembayaran Chrome Webstore".. },.. "cr aw_app_unavailable": {.. "message": "Aplikasi tidak tersedia saat ini.".. },.. "craw_connect_to_network": {.. "message": "Sambungkan ke jaringan.".. },.. "iap_unavailable": {.. "message": "Pembayaran Dalam Aplikasi saat ini tidak tersedia.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be co mpleted.".. },.. "please_sign_in": {.. "message": "Harap masuk ke Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\it\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	603
Entropy (8bit):	4.479418964635223
Encrypted:	false
SSDEEP:	12:1HEJsqd/bGGsqd/b+WYpU34OcX4+dgUvIO8ZpU34vq703OyZnLAOfTYsD:1HEXd/aKd/6WYpZrv58ZpskOGAOfzD
MD5:	A328EEF5E841E0C72D3CD7366899C5C8
SHA1:	2851ED658385804E87911643F5A4200B1FB26E13
SHA-256:	CD891C45F7586FB4A2514205A11F260E4A6D4482FA03D901909DD9F57BE0536D
SHA-512:	E47297896E981774EC3B59D41B89D6BA9333F6B4435EB9727D8645A46B10C7D408ADE06844871FA757382FBE7E645276449DB7B1B23BC59C9A71A5CB5A5ECC5
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamenti Chrome Web Store".. },.. "app_name": {.. "message": "Pagamenti Chrome Web Store".. },.. "craw_app_una vailable": {.. "message": "App al momento non disponibile.".. },.. "craw_connect_to_network": {.. "message": "Collegati a una rete.".. },.. "iap_unavailable": {.. "message": "La funzione Pagamenti In-App non . al momento disponibile.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accedi a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\ja\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	697
Entropy (8bit):	5.20469020877498
Encrypted:	false
SSDEEP:	12:1HEJ07uGG07u+WYpU34DB+dgnsVztO8ZpU34MwiB03OyZnLAOfTYmSH:1HEcnDNWYp1kxU8Zp2wiqOGAOfpSH
MD5:	9B3A5D473C3F2BBFAEECE94A07A940B8
SHA1:	61BACA342CF766BBA15C7B4D892A0E7DAC9405AA

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\ja\messages.json	
SHA-256:	706312A4A2AEF3317223F141EB2B82685345B7EED444F16BB4DF3A272716DA1F
SHA-512:	94F6FEE9A11BD890AB8211C98D1CC142348961EBCF756F66477A3E3A76519804B70BE0AE4E551739F8AFE32D7ADE6EDE04EF6B9B9EED03E3A857E6058EEDD4C6
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome ....".. },.. "app_name": {.. "message": "Chrome ....".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "..... ".. },.. "iap_unavailable": {.. "message": "..... ".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Chrome .... ".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\ko\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	631
Entropy (8bit):	5.160315577642469
Encrypted:	false
SSDEEP:	12:1HEJ1GG1+WYpU34K3aT+dgh8d0HTO8ZpU34KaNkaT03OyZnLAOfTY/YeHx:1HEajWYpc3aSl0Hq8Zpc6kasOGAOfyYA
MD5:	9F6B4D82A70C74CA751E2EAE70FAB5CF
SHA1:	0534F125FFCE8222277CF2BE3401C59DAF9217F8
SHA-256:	D1467B8D037114403E8F4EFC52E88C4A7FEB96126BE4CFF883FEFF1084EF7E68
SHA-512:	ED9319830314385D09C06F62EE34186E8CA576C857981205E4468A28B3ACD2AB03384E77B866032C324ABDD97A56EFD08E2D6E0C79D563578B3EC52517819BD8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome . ... ..".. },.. "app_name": {.. "message": "Chrome . ... ..".. },.. "craw_app_unavailable": {.. "message": ".. .. ..".. },.. "craw_connect_to_network": {.. "message": "..... .....".. },.. "iap_unavailable": {.. "message": ".. .. ..".. },.. "jwt_retrieve_failed": {.. " message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Chrome. .....".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\lt\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	665
Entropy (8bit):	4.66839186029557
Encrypted:	false
SSDEEP:	12:1HEJpqHnkGGpqHnk+WYpU346M+dgV6O8ZpU34WzSWz03OyZnLAOfTYx:1HELqHtKqHPWYpM3A8ZpwGzOGAOfg
MD5:	4CA644F875606986A9898D04BDAE3EA5
SHA1:	722A10569E93975129D67FBDB75B537D9D622AD1
SHA-256:	7C311AB751D840D750C11553C083785813E079C1D464FE568A98C9E3EF3DB96C
SHA-512:	E575E3D0622F5BD4B6C0EE79128A1B1F1882195670139D1983F4377D847141B8FB8EBB8BCED82AF3A220ED07D3577AFBE085BADC0E9C7678292B80E3EC5D3444
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema".. },.. "app_name": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema".. },.. "craw_app_unavailable": {.. "message": "Programa .iuo metu negalima.".. },.. "craw_connect_to_network": {.. "message": "Prisijunkite prie tinklo.".. },.. "iap_unavailable": {.. "message": "Mok.jimai programoje .iuo metu negalimi.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prisijunkite prie .Chrome..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\lv\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	671
Entropy (8bit):	4.631774066483956
Encrypted:	false
SSDEEP:	12:1HEJFhVbGGFhVb+WYpU34wDoz+dgGedBO8ZpU34wF03OyZnLAOfTYGYID:1HENQKkWYp2Doy/em8Zp2WOGAOfRYID
MD5:	C5CE2C51391EAFD3DA9E4C71549A3C28
SHA1:	1F67FF6EF6E90C0CE3AAF56ED543A3EFD381574D
SHA-256:	1FA1DF2CA8516DEF490FB8484E9AA498ACFF80EEF5C9258FFE42D3678E6C7DED
SHA-512:	C85F6281E682F52BC2147DEA7E2F3BB4DC48D98BADA8687B05C6C7271C78EA7F5431CD51671A4184C9AE004FC53C016E3C594697F483195CCBA08A93821EEF
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome interneta veikala maks.jumu sist.ma".. },.. "app_name": {.. "message": "Chrome interneta veikala maks.jumu s ist.ma".. },.. "craw_app_unavailable": {.. "message": "Lietotne pagaid.m nav pieejama.".. },.. "craw_connect_to_network": {.. "message": "L.dzu, izveidojiet savienojumu ar t.klu.".. },.. "iap_unavailable": {.. "message": "Maks.jumi lietotn.s pa.laik nav pieejami.".. },.. "jwt_retrieve_failed": {.. "message": "The transacti on could not be completed.".. },.. "please_sign_in": {.. "message": "L.dzu, pierakstieties p.rl.k. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\nb\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.555032032637389
Encrypted:	false
SSDEEP:	12:1HEJhiOGGhiO+WYpU34OHSN+dgFjdGFZO8ZpU34JgdN03OyZnLAOfTYiD:1HEDiHIitWYpCYJ8ZpD1OGAOfRD
MD5:	93C459A23BC6953FF744C35920CD2AF9
SHA1:	162F884972103A08ADB616A7EB3598431A2924C5
SHA-256:	2CD700AEB57D89C2E73333D0702556EE3FF3863516170F85669BC680FCBDC4E0
SHA-512:	F76E6E8D8499306883C3EC1E774F7E8BB6B601096DA5A14D17D3E7D5732829542041E42B7350466589291ADCC83FB065FD591B4E20CFCF8EDC586E128ECBFCE
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Nettmarked-betalinger".. },.. "app_name": {.. "message": "Chrome Nettmarked-betalinger".. },.. "craw_app _unavailable": {.. "message": "Appen er utilgjengelig for .yeblikket.".. },.. "craw_connect_to_network": {.. "message": "Du m. koble til et nettverk.".. },.. "iap _unavailable": {.. "message": "Betaling i app er ikke tilgjengelig for .yeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Du m. logge p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\nl\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	615
Entropy (8bit):	4.4715318546237315
Encrypted:	false
SSDEEP:	12:1HEJJQGkbGGJQGkb+WYpU34OQKJT+dgiXUmvFZO8ZpU34g7JT03OyZnLAOfTYMD:1HErxkaqxk6WYptndXI8ZpTOGAOfbD
MD5:	7A8F9D0249C680F64DEC7650A432BD57
SHA1:	53477198AEE389F6580921B4876719B400A23CA1
SHA-256:	92BE7C2DC9CFBE5A65E9CE6488D364C8D7EC19E7B67A31E4D43C1CB2B169671C
SHA-512:	969AB979546A741C0F3EDBEEB21BABA375FA8870D4FB9248CDD4C305736E332E10CAB7B64C5C078E60EC0CD73848101B390BE8F44B89C310058AF4C1CA3C8A A7
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalingen via Chrome Web Store".. },.. "app_name": {.. "message": "Betalingen via Chrome Web Store".. },.. "cr aw_app_unavailable": {.. "message": "App momenteel niet beschikbaar.".. },.. "craw_connect_to_network": {.. "message": "Maak verbinding met een netwerk.".. },.. "iap_unavailable": {.. "message": "In-app-betalingen is momenteel niet beschikbaar.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log in bij Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\pl\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	636
Entropy (8bit):	4.646901997539488
Encrypted:	false
SSDEEP:	12:1HEJbiVbGGbiVb+WYpU34OBHlBi9+dgQUg6O8ZpU34bdbfiIu03OyZnLAOfTYR5k:1HE5iVauiV6WYpIAYr8ZpxFiaOGAOfIC
MD5:	0E6194126AFCCD1E3098D276A7400175
SHA1:	E8127B905A640B1C46362FA6E1127BE172F4A40F
SHA-256:	E2699F98C511B18A2AFB82EAE9A4804B646C4FF1077D80E77C17A3943A6373C2
SHA-512:	A71F7C7BFBBF1E37E699601AF2E095C56CBA91F90CB7556477DF31D01B83ADFB1271E1775C9BA299FF6875BBFC2B6AB47488CC88E33DEF2F6F2E0E5AC687B7 77
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "app_name": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Aplikacja jest obecnie niedost.pna.".. },.. "craw_connect_to_network": {.. "message": "Po..cz si. z sieci..".. },.. "iap_unavailable": {.. "message": "P.atno.ci w ramach aplikacji s. teraz niedost.pne.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be com pleted.".. },.. "please_sign_in": {.. "message": "Zaloguj si. w Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\pt_BR\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	636
Entropy (8bit):	4.515158874306633
Encrypted:	false

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\pt_BR\messages.json	
SSDEEP:	12:1HEJsc/bGGsc/b+WYpU34OLw+dgn/KzO8ZpU34FjIBMwGRO03OyZnLAOfTYN+KcY:1HEb/a8/6WYp4mZ8Zp7cKlOGAOf2tD
MD5:	86A2B91FA18B867209024C522ED665D5
SHA1:	63DEC245637818C76655E01FCB6D59784BC7184E
SHA-256:	6374880FDD1F8AF1EE8AEA6A06B73BE0AB265AFCEB4FE6F08BDE3B3989264B21
SHA-512:	DA6DBDE5028756421C2904F605632EE98831A25A1247E6238A931629B94CE8A00FD76F4235F118D2167304BD60F2C06B2AD78E54FF6CE53F8C38DF8C7B5AFCE4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamentos da Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos da Chrome Web Store".. },.. "craw _app_unavailable": {.. "message": "Aplicativo indispon.vel no momento.".. },.. "craw_connect_to_network": {.. "message": "Conecte-se a uma rede.".. },.. "iap_unavailable": {.. "message": "No momento, os Pagamentos no aplicativo n.o est.o dispon.veis.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Fa.a login no Google Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\pt_PT\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	622
Entropy (8bit):	4.526171498622949
Encrypted:	false
SSDEEP:	12:1HEJsZUkbGGsZUkb+WYpU34OAE+dgqxKzO8ZpU34rEpBfvPO03OyZnLAOfTYLD:1HEmUka5Uk6WYpFvdxZ8ZpSTnPlOGAOS
MD5:	750A4800EDB93FBE56495963F9FB3B94
SHA1:	8BFB915488A4EB3CB33D68E2E59F1F8447DB7D61
SHA-256:	C1C94F65FABAF17DEF98A8587711A56D61B1E5607500E9B01F2824DB109F9E83
SHA-512:	2AEDEF5793406221BE76AF22031CE8C30AB5FAEAED09BB394C153E2EBE990C89C1A2A73B40D8A92842641AFCA8C77FFD808A2058602D3646FD8DAE2844406F4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamentos via Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos via Chrome Web Store".. },.. "cr aw_app_unavailable": {.. "message": "Aplica..o atualmente indispon.vel.".. },.. "craw_connect_to_network": {.. "message": "Ligue-se a uma rede.".. },.. "iap_unavailable": {.. "message": "Os Pagamentos na app est.o atualmente indispon.veis.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicie sess.o no Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\ro\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.61125938671415
Encrypted:	false
SSDEEP:	12:1HEJqJrJZGGqJrJZ+WYpU344HIx2Z+dgrVPlZO8ZpU34qT7hl3O03OyZnLAOfTYU:1HEC4D8WYpKow8WV68ZpKhoOGAOfoVGD
MD5:	98D43E4B1054A65DF3FA3CC40AB6FB6D
SHA1:	46E0A21C4DA2BB5D4D8F837AE211C1B6FA26E7E2
SHA-256:	113A13900CBA62FE8AED06751971C23A80A99B47F9BE219CF884D57DB19611D9
SHA-512:	A76DC53912A4F46714926B9EA2B22E909540E447F61F6DD72607AB7B3BB5D4A9B39E525B04C33AEC53BA813D14AC1FB5827275B2524E52B693E83171E1CD146
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pl..i prin Magazinul web Chrome".. },.. "app_name": {.. "message": "Pl..i prin Magazinul web Chrome".. },.. "cr aw_app_unavailable": {.. "message": ".n prezent, aplica.ia nu este disponibil..".. },.. "craw_connect_to_network": {.. "message": "Conecteaz.-te la o re.ea.".. },.. "iap_unavailable": {.. "message": "Pl..ile .n aplica.ie nu sunt disponibile momentan.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be c ompleted.".. },.. "please_sign_in": {.. "message": "Conecteaz.-te la Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\ru\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	744
Entropy (8bit):	4.918620852166656
Encrypted:	false
SSDEEP:	12:1HEJ7OJHZMSl3ZGG7OJHZMSl3Z+WYpU34zWJ2F+dgVtLSv/TO8ZpU347NWjT03On:1HElOJHZMq4uOJHZMq8WYpdWJ/YGHq8m
MD5:	DB2EDF1465946C06BD95C71A1E13AE64
SHA1:	FB4F3ECE9ECECEBBC6CA2A592A15FB9C1FDFB811
SHA-256:	FBAF22CE6E16DE174CED8CB5EA3098CCA1C3426A2111FF33BD3E64DA64ED67AB
SHA-512:	4E0CF00BAEF1757548DEB17BBE1AF55770A0A0F7351779EF55C7DEFA6D112D0227B8865C2C22E0EC62E6E2F1C8E1632A2D0CE6828D25C5ABBF143C990116F62
Malicious:	false

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\ru\messages.json	
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ....-..... Chrome".. },.. "app_name": {.. "message": "..... ....-..... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... .....".. },.. "craw_connect_to_network": {.. "message": "..... . .....".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... . Chrome".. }.. }..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\sk\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.640777810668463
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34ORO+dgmmCO8ZpU34yH7u2Z03OyZnLAOfTYCUAi0D:1HEl4G8WYpetPmD8ZpcH7aOGAOfzUeD
MD5:	8DF215D1EFBDABB175CCDD68ED8DCB0A
SHA1:	2B374462137A38589A73FDD00A84CBDC7E50F9F4
SHA-256:	7FA16AF97E6CFC52EC6008EB679D3F30E7E0C24F9EF2D18A9228EAF4DED9D63B
SHA-512:	C0E623343BDAEB4731800D183B59F2FCFE285F0C7153EC99641FD84F2F2DCFE47D21E73F3D28B1240340453C5668EB0AFFBE087AAB62F1C88CD2A40CC44E59 D
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplik.cia moment.lne nie je dostupn..".. },.. "craw_connect_to_network": {.. "message": "Pripojte sa k sieti..".. },.. "iap_unavailable": {.. "message": "Platby v aplik.cii moment.lne nie s. k dispoz.cii.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prihl.ste sa do prehliada.a Chrome..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\sl\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	617
Entropy (8bit):	4.5101656584816885
Encrypted:	false
SSDEEP:	12:1HEJGcyvmbZGGGcyvmbZ+WYpU34OBOEtf+dgca1ZO8ZpU34GcQArERff03OyZnLh:1HE4cyY4TcyY8WYpNoWa1w8ZpQcQ6AfK
MD5:	3943FA2A647AECEDFD685408B27139EE
SHA1:	0129DD19D28373359530B3B477FE8A9279DABB7D
SHA-256:	18AFF072EE0DF7C3495045435C752A805606E6D5D462EF2321C443F1773F4B3A
SHA-512:	42E62B3855611FF2E1D39C11404CB1A09825EE4CA6A8ACB3FF538B4574388F549E3BD79137DD4DC128A8DC44DD270D7D878E4AAD20DA8250A5C25297B0DEC0 D
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pla.ila v spletni trgovini Chrome".. },.. "app_name": {.. "message": "Pla.ila v spletni trgovini Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikacija trenutno ni na voljo.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se z omre.jem.".. },.. "iap_unavailable": {.. "message": "Pla.ila v aplikacijah trenutno niso na voljo.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prijavite se v Chrome..".. }..}..

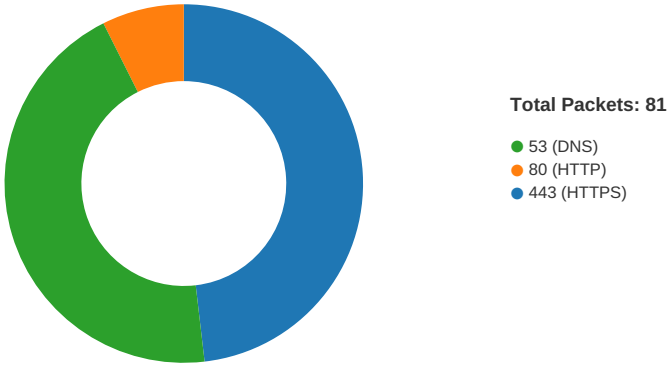
C:\Users\user\AppData\Local\Temp\scoped_dir3100_196228870\CRX_INSTALL_locales\sr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	743
Entropy (8bit):	4.913927107235852
Encrypted:	false
SSDEEP:	12:1HEJssbdOGGssbdO+WYpU347xBP+dgcucO8ZpU34s1muP03OyZnLAOfTYzDYD:1HEKsb59sbTWYplx4Xud8Zpy1mNOGAOv
MD5:	D485DF17F085B6A37125694F85646FD0
SHA1:	24D51D8642CDC6EFD5D8D7A4430232D8CDE25108
SHA-256:	7FFDE34C58E7C376C042DE64DEF6481DAE32BE8B70F0B18EDF536290CBE0C818
SHA-512:	0DDECFD860E99290B6C3AAA04F510272AE081CF2D93ED5832D9D6378EC9D36177FFBE213471247FB94721EA34A83E7665669200047091D0FDE134E3D763217E7
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... . Chrome ...-.....".. },.. "app_name": {.. "message": "..... . Chrome ...-.....".. },.. "craw_app_unavailable": {.. "message": "..... .. ..".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": "..... . ...".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... .. . Chrome..".. }..}..

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 21:28:30.529370070 CET	49710	443	192.168.2.5	143.204.90.56
Mar 5, 2021 21:28:30.530083895 CET	49711	443	192.168.2.5	143.204.90.56
Mar 5, 2021 21:28:30.570487022 CET	443	49710	143.204.90.56	192.168.2.5
Mar 5, 2021 21:28:30.570590019 CET	49710	443	192.168.2.5	143.204.90.56
Mar 5, 2021 21:28:30.570967913 CET	49710	443	192.168.2.5	143.204.90.56
Mar 5, 2021 21:28:30.570986032 CET	443	49711	143.204.90.56	192.168.2.5
Mar 5, 2021 21:28:30.571075916 CET	49711	443	192.168.2.5	143.204.90.56
Mar 5, 2021 21:28:30.571398973 CET	49711	443	192.168.2.5	143.204.90.56
Mar 5, 2021 21:28:30.609294891 CET	443	49710	143.204.90.56	192.168.2.5
Mar 5, 2021 21:28:30.612494946 CET	443	49710	143.204.90.56	192.168.2.5
Mar 5, 2021 21:28:30.612536907 CET	443	49710	143.204.90.56	192.168.2.5
Mar 5, 2021 21:28:30.612603903 CET	49710	443	192.168.2.5	143.204.90.56
Mar 5, 2021 21:28:30.612828970 CET	443	49710	143.204.90.56	192.168.2.5
Mar 5, 2021 21:28:30.616230965 CET	443	49711	143.204.90.56	192.168.2.5
Mar 5, 2021 21:28:30.616277933 CET	443	49710	143.204.90.56	192.168.2.5
Mar 5, 2021 21:28:30.616353989 CET	49710	443	192.168.2.5	143.204.90.56
Mar 5, 2021 21:28:30.616394997 CET	443	49710	143.204.90.56	192.168.2.5
Mar 5, 2021 21:28:30.622241020 CET	443	49711	143.204.90.56	192.168.2.5
Mar 5, 2021 21:28:30.622284889 CET	443	49711	143.204.90.56	192.168.2.5
Mar 5, 2021 21:28:30.622320890 CET	443	49711	143.204.90.56	192.168.2.5
Mar 5, 2021 21:28:30.622370958 CET	49711	443	192.168.2.5	143.204.90.56
Mar 5, 2021 21:28:30.625823021 CET	443	49711	143.204.90.56	192.168.2.5
Mar 5, 2021 21:28:30.625895977 CET	49711	443	192.168.2.5	143.204.90.56
Mar 5, 2021 21:28:30.625986099 CET	443	49711	143.204.90.56	192.168.2.5
Mar 5, 2021 21:28:30.656161070 CET	49710	443	192.168.2.5	143.204.90.56
Mar 5, 2021 21:28:30.666078091 CET	49711	443	192.168.2.5	143.204.90.56
Mar 5, 2021 21:28:30.883579016 CET	49710	443	192.168.2.5	143.204.90.56
Mar 5, 2021 21:28:30.884234905 CET	49711	443	192.168.2.5	143.204.90.56
Mar 5, 2021 21:28:30.884325981 CET	49711	443	192.168.2.5	143.204.90.56
Mar 5, 2021 21:28:30.884443045 CET	49710	443	192.168.2.5	143.204.90.56
Mar 5, 2021 21:28:30.884871006 CET	49710	443	192.168.2.5	143.204.90.56
Mar 5, 2021 21:28:30.923767090 CET	443	49710	143.204.90.56	192.168.2.5
Mar 5, 2021 21:28:30.923901081 CET	443	49710	143.204.90.56	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 21:28:30.924179077 CET	443	49710	143.204.90.56	192.168.2.5
Mar 5, 2021 21:28:30.924218893 CET	443	49710	143.204.90.56	192.168.2.5
Mar 5, 2021 21:28:30.924261093 CET	49710	443	192.168.2.5	143.204.90.56
Mar 5, 2021 21:28:30.924266100 CET	443	49711	143.204.90.56	192.168.2.5
Mar 5, 2021 21:28:30.924304008 CET	443	49711	143.204.90.56	192.168.2.5
Mar 5, 2021 21:28:30.924333096 CET	443	49710	143.204.90.56	192.168.2.5
Mar 5, 2021 21:28:30.924489021 CET	443	49711	143.204.90.56	192.168.2.5
Mar 5, 2021 21:28:30.924575090 CET	49711	443	192.168.2.5	143.204.90.56
Mar 5, 2021 21:28:30.962594032 CET	443	49710	143.204.90.56	192.168.2.5
Mar 5, 2021 21:28:30.965137959 CET	49710	443	192.168.2.5	143.204.90.56
Mar 5, 2021 21:28:31.856132984 CET	443	49710	143.204.90.56	192.168.2.5
Mar 5, 2021 21:28:31.856173992 CET	443	49710	143.204.90.56	192.168.2.5
Mar 5, 2021 21:28:31.856342077 CET	49710	443	192.168.2.5	143.204.90.56
Mar 5, 2021 21:28:32.021970987 CET	49721	80	192.168.2.5	96.127.183.226
Mar 5, 2021 21:28:32.116255045 CET	49723	80	192.168.2.5	96.127.183.226
Mar 5, 2021 21:28:32.166032076 CET	80	49721	96.127.183.226	192.168.2.5
Mar 5, 2021 21:28:32.166237116 CET	49721	80	192.168.2.5	96.127.183.226
Mar 5, 2021 21:28:32.166459084 CET	49721	80	192.168.2.5	96.127.183.226
Mar 5, 2021 21:28:32.260433912 CET	80	49723	96.127.183.226	192.168.2.5
Mar 5, 2021 21:28:32.260591030 CET	49723	80	192.168.2.5	96.127.183.226
Mar 5, 2021 21:28:32.310167074 CET	80	49721	96.127.183.226	192.168.2.5
Mar 5, 2021 21:28:32.339148998 CET	80	49721	96.127.183.226	192.168.2.5
Mar 5, 2021 21:28:32.341679096 CET	80	49721	96.127.183.226	192.168.2.5
Mar 5, 2021 21:28:32.341787100 CET	49721	80	192.168.2.5	96.127.183.226
Mar 5, 2021 21:28:32.650701046 CET	49726	443	192.168.2.5	185.88.176.140
Mar 5, 2021 21:28:32.799983978 CET	443	49726	185.88.176.140	192.168.2.5
Mar 5, 2021 21:28:32.800088882 CET	49726	443	192.168.2.5	185.88.176.140
Mar 5, 2021 21:28:32.800333977 CET	49726	443	192.168.2.5	185.88.176.140
Mar 5, 2021 21:28:32.950866938 CET	443	49726	185.88.176.140	192.168.2.5
Mar 5, 2021 21:28:32.958789110 CET	443	49726	185.88.176.140	192.168.2.5
Mar 5, 2021 21:28:32.958826065 CET	443	49726	185.88.176.140	192.168.2.5
Mar 5, 2021 21:28:32.958847046 CET	443	49726	185.88.176.140	192.168.2.5
Mar 5, 2021 21:28:32.958925962 CET	49726	443	192.168.2.5	185.88.176.140
Mar 5, 2021 21:28:32.966206074 CET	49726	443	192.168.2.5	185.88.176.140
Mar 5, 2021 21:28:32.966362953 CET	49726	443	192.168.2.5	185.88.176.140
Mar 5, 2021 21:28:33.112881899 CET	443	49726	185.88.176.140	192.168.2.5
Mar 5, 2021 21:28:33.112915993 CET	443	49726	185.88.176.140	192.168.2.5
Mar 5, 2021 21:28:33.112945080 CET	443	49726	185.88.176.140	192.168.2.5
Mar 5, 2021 21:28:33.113013983 CET	49726	443	192.168.2.5	185.88.176.140
Mar 5, 2021 21:28:34.533004045 CET	443	49726	185.88.176.140	192.168.2.5
Mar 5, 2021 21:28:34.536761999 CET	49726	443	192.168.2.5	185.88.176.140
Mar 5, 2021 21:28:34.721977949 CET	443	49726	185.88.176.140	192.168.2.5
Mar 5, 2021 21:28:34.781977892 CET	443	49726	185.88.176.140	192.168.2.5
Mar 5, 2021 21:28:34.782027960 CET	443	49726	185.88.176.140	192.168.2.5
Mar 5, 2021 21:28:34.782078028 CET	443	49726	185.88.176.140	192.168.2.5
Mar 5, 2021 21:28:34.782121897 CET	443	49726	185.88.176.140	192.168.2.5
Mar 5, 2021 21:28:34.782164097 CET	443	49726	185.88.176.140	192.168.2.5
Mar 5, 2021 21:28:34.782172918 CET	49726	443	192.168.2.5	185.88.176.140
Mar 5, 2021 21:28:34.782198906 CET	49726	443	192.168.2.5	185.88.176.140
Mar 5, 2021 21:28:34.782208920 CET	443	49726	185.88.176.140	192.168.2.5
Mar 5, 2021 21:28:34.782243013 CET	443	49726	185.88.176.140	192.168.2.5
Mar 5, 2021 21:28:34.782257080 CET	49726	443	192.168.2.5	185.88.176.140
Mar 5, 2021 21:28:34.787007093 CET	49729	443	192.168.2.5	185.88.176.140
Mar 5, 2021 21:28:34.792929888 CET	443	49726	185.88.176.140	192.168.2.5
Mar 5, 2021 21:28:34.792996883 CET	49726	443	192.168.2.5	185.88.176.140
Mar 5, 2021 21:28:34.793410063 CET	49726	443	192.168.2.5	185.88.176.140
Mar 5, 2021 21:28:34.934766054 CET	443	49729	185.88.176.140	192.168.2.5
Mar 5, 2021 21:28:34.934904099 CET	49729	443	192.168.2.5	185.88.176.140
Mar 5, 2021 21:28:34.935309887 CET	49729	443	192.168.2.5	185.88.176.140
Mar 5, 2021 21:28:34.940102100 CET	443	49726	185.88.176.140	192.168.2.5
Mar 5, 2021 21:28:35.035116911 CET	443	49726	185.88.176.140	192.168.2.5
Mar 5, 2021 21:28:35.035171986 CET	443	49726	185.88.176.140	192.168.2.5
Mar 5, 2021 21:28:35.035212994 CET	443	49726	185.88.176.140	192.168.2.5
Mar 5, 2021 21:28:35.035249949 CET	443	49726	185.88.176.140	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 21:28:35.035262108 CET	49726	443	192.168.2.5	185.88.176.140
Mar 5, 2021 21:28:35.035300970 CET	49726	443	192.168.2.5	185.88.176.140
Mar 5, 2021 21:28:35.035319090 CET	443	49726	185.88.176.140	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 21:28:20.638066053 CET	52704	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:20.683839083 CET	53	52704	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:20.807349920 CET	52212	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:20.853509903 CET	53	52212	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:21.424921989 CET	54302	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:21.470757961 CET	53	54302	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:21.582918882 CET	53784	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:21.628843069 CET	53	53784	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:23.020544052 CET	65307	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:23.077889919 CET	53	65307	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:23.312150002 CET	64344	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:23.359699011 CET	53	64344	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:23.990434885 CET	62060	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:24.036526918 CET	53	62060	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:24.067426920 CET	61805	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:24.113558054 CET	53	61805	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:24.376693964 CET	54795	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:24.422516108 CET	53	54795	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:25.258682013 CET	49557	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:25.304707050 CET	53	49557	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:26.198920012 CET	61733	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:26.245188951 CET	53	61733	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:27.182519913 CET	65447	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:27.228482008 CET	53	65447	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:28.749618053 CET	52441	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:28.798636913 CET	53	52441	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:30.392946959 CET	65296	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:30.440571070 CET	53	65296	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:30.462289095 CET	63183	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:30.470494986 CET	60151	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:30.471281052 CET	56969	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:30.471679926 CET	55161	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:30.508290052 CET	53	63183	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:30.527618885 CET	53	60151	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:30.538242102 CET	53	56969	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:30.546590090 CET	53	55161	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:30.952383041 CET	54757	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:31.014496088 CET	53	54757	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:31.127414942 CET	49992	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:31.193890095 CET	53	49992	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:31.522294998 CET	55016	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:31.569622993 CET	53	55016	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:31.866206884 CET	64345	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:32.020395041 CET	53	64345	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:32.288140059 CET	57128	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:32.304951906 CET	54791	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:32.344791889 CET	50463	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:32.353071928 CET	53	57128	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:32.353605986 CET	53	54791	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:32.649404049 CET	53	50463	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:33.283380032 CET	50394	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:33.330468893 CET	53	50394	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:34.167732954 CET	58530	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:34.224210978 CET	53	58530	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:35.188199997 CET	54450	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:35.236918926 CET	53	54450	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:37.372731924 CET	59261	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 21:28:37.427321911 CET	53	59261	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:40.512517929 CET	51649	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:40.567047119 CET	53	51649	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:46.658322096 CET	65086	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:46.726337910 CET	53	65086	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:49.328857899 CET	56432	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:49.411672115 CET	53	56432	8.8.8.8	192.168.2.5
Mar 5, 2021 21:28:49.878458023 CET	52929	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:28:49.940731049 CET	53	52929	8.8.8.8	192.168.2.5
Mar 5, 2021 21:29:12.476490021 CET	64317	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:29:12.526350975 CET	53	64317	8.8.8.8	192.168.2.5
Mar 5, 2021 21:29:15.543040037 CET	61004	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:29:15.591815948 CET	53	61004	8.8.8.8	192.168.2.5
Mar 5, 2021 21:29:16.202105999 CET	56895	53	192.168.2.5	8.8.8.8
Mar 5, 2021 21:29:16.259794950 CET	53	56895	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 5, 2021 21:28:30.470494986 CET	192.168.2.5	8.8.8.8	0x8a9e	Standard query (0)	analytics.linkre.direct	A (IP address)	IN (0x0001)
Mar 5, 2021 21:28:31.866206884 CET	192.168.2.5	8.8.8.8	0x6eec	Standard query (0)	www.nathalie.tremblay.hotellosmedanos.com.uy	A (IP address)	IN (0x0001)
Mar 5, 2021 21:28:32.344791889 CET	192.168.2.5	8.8.8.8	0x39ff	Standard query (0)	rcha.ir	A (IP address)	IN (0x0001)
Mar 5, 2021 21:28:37.372731924 CET	192.168.2.5	8.8.8.8	0x7626	Standard query (0)	rcha.ir	A (IP address)	IN (0x0001)
Mar 5, 2021 21:28:46.658322096 CET	192.168.2.5	8.8.8.8	0x73ac	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
Mar 5, 2021 21:28:21.470757961 CET	8.8.8.8	192.168.2.5	0x4ae9	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 21:28:30.527618885 CET	8.8.8.8	192.168.2.5	0x8a9e	No error (0)	analytics.linkre.direct		143.204.90.56	A (IP address)	IN (0x0001)
Mar 5, 2021 21:28:30.527618885 CET	8.8.8.8	192.168.2.5	0x8a9e	No error (0)	analytics.linkre.direct		143.204.90.33	A (IP address)	IN (0x0001)
Mar 5, 2021 21:28:30.527618885 CET	8.8.8.8	192.168.2.5	0x8a9e	No error (0)	analytics.linkre.direct		143.204.90.90	A (IP address)	IN (0x0001)
Mar 5, 2021 21:28:30.527618885 CET	8.8.8.8	192.168.2.5	0x8a9e	No error (0)	analytics.linkre.direct		143.204.90.12	A (IP address)	IN (0x0001)
Mar 5, 2021 21:28:32.020395041 CET	8.8.8.8	192.168.2.5	0x6eec	No error (0)	www.nathalie.tremblay.hotellosmedanos.com.uy		96.127.183.226	A (IP address)	IN (0x0001)
Mar 5, 2021 21:28:32.649404049 CET	8.8.8.8	192.168.2.5	0x39ff	No error (0)	rcha.ir		185.88.176.140	A (IP address)	IN (0x0001)
Mar 5, 2021 21:28:37.427321911 CET	8.8.8.8	192.168.2.5	0x7626	No error (0)	rcha.ir		185.88.176.140	A (IP address)	IN (0x0001)
Mar 5, 2021 21:28:46.726337910 CET	8.8.8.8	192.168.2.5	0x73ac	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 21:28:46.726337910 CET	8.8.8.8	192.168.2.5	0x73ac	No error (0)	googlehosted.l.googleusercontent.com		172.217.23.33	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.nathalie.tremblay.hotellosmedanos.com.uy

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49721	96.127.183.226	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Mar 5, 2021 21:28:32.166459084 CET	1504	OUT	GET /?XAP=bmF0aGFsaWUudHJlbWJsYXlAc2FhcS5nb3V2LnFjLmNh HTTP/1.1 Host: www.nathalie.tremblay.hotellosmedanos.com.uy 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
Mar 5, 2021 21:28:32.339148998 CET	1505	IN	HTTP/1.1 302 Found Date: Fri, 05 Mar 2021 20:28:32 GMT Server: Apache Location: https://rcha.ir/components/com_ajax/OfficeV4?08909598527009&email=bmF0aGFsaWUudHJlbWJsYXlAc2FhcS5nb3V2LnFjLmNh Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8

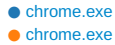
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 5, 2021 21:28:37.974232912 CET	185.88.176.140	443	192.168.2.5	49743	CN=rcha.ir CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Mar 02 23:59:48 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Jun 01 00:59:48 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 21:28:38.121798038 CET	185.88.176.140	443	192.168.2.5	49745	CN=rcha.ir CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Mar 02 23:59:48 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Jun 01 00:59:48 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 3100 Parent PID: 3536

General

Start time:	21:28:26
Start date:	05/03/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://analytics.linkre.direct/clickthrough?id=CDE9E442CE50D5323CAF39A56&issuer=interlkp&template=ILNSTATE01&url=http://www.nathalie.tremblay.hotellosmedanos.com.uy/?XAP=bmF0aGFsaWUudHJlbWJsYXlAc2FhcS5nb3V2LnFjLmNh%20'
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: chrome.exe PID: 4604 Parent PID: 3100

General

Start time:	21:28:28
Start date:	05/03/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1616,5230389399112637974,4973306169734885708,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1692 /prefetch:8
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly