ID: 344868
Cookbook: browseurl.jbs
Time: 11:01:06
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

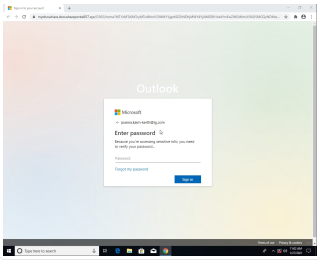
Analysis Report http://bkbizwwqfqstgcsbkbizwwqfqstgc…

Overview

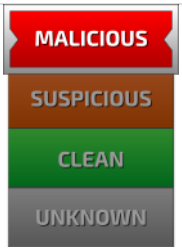
General Information

Sample URL:	http://bkbizwwqfqstgcsbkbizwwqfqstgcs.lk8ftr.com/e/am9hbm5hLmthaW0ta2VydGhAaWcuY29t
Analysis ID:	344868

Most interesting Screenshot:



Detection



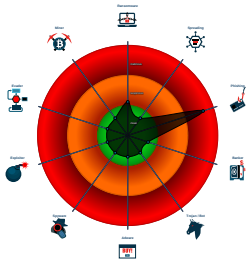
HTMLPhisher

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Phishing site detected (based on fav…
- Yara detected HtmlPhish_10
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- Invalid T&C link found

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 5752 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'http://bkbizwwqfqstgcsbkbizwwqfqstgcs.lk8ftr.com/e/am9hbm5hLmthaW0ta2VydGhAaWcuY29t' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 464 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1532,15419587561947641969,2247414398812328316,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1724 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

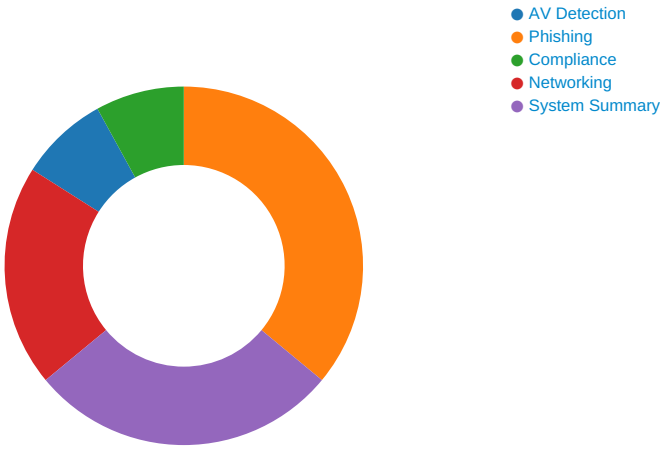
Yara Overview

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

Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

Compliance:

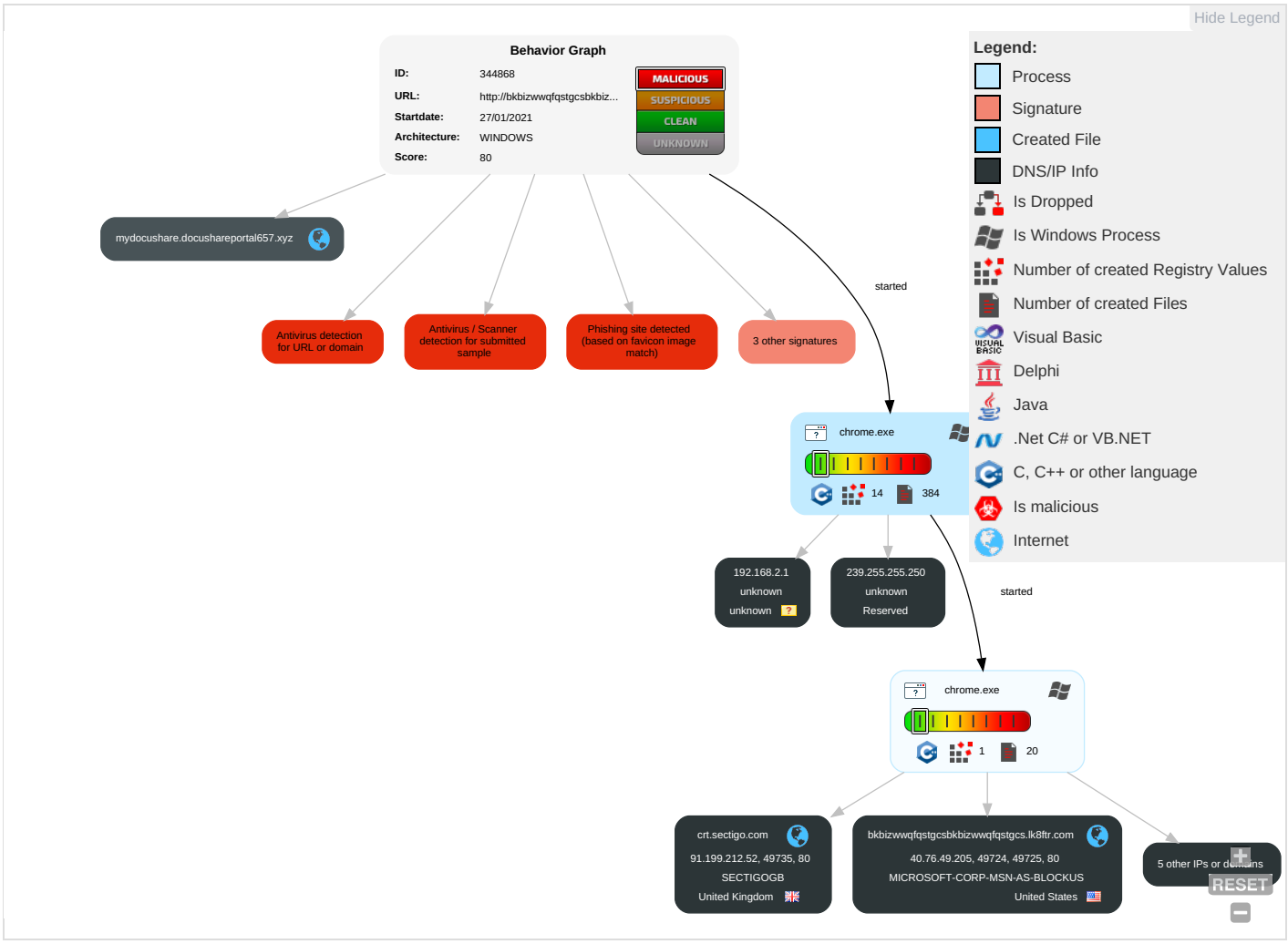
Creates a directory in C:\Program Files

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 Billin Fraud

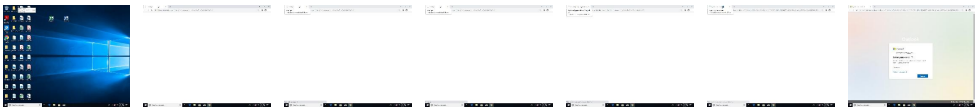
Behavior Graph

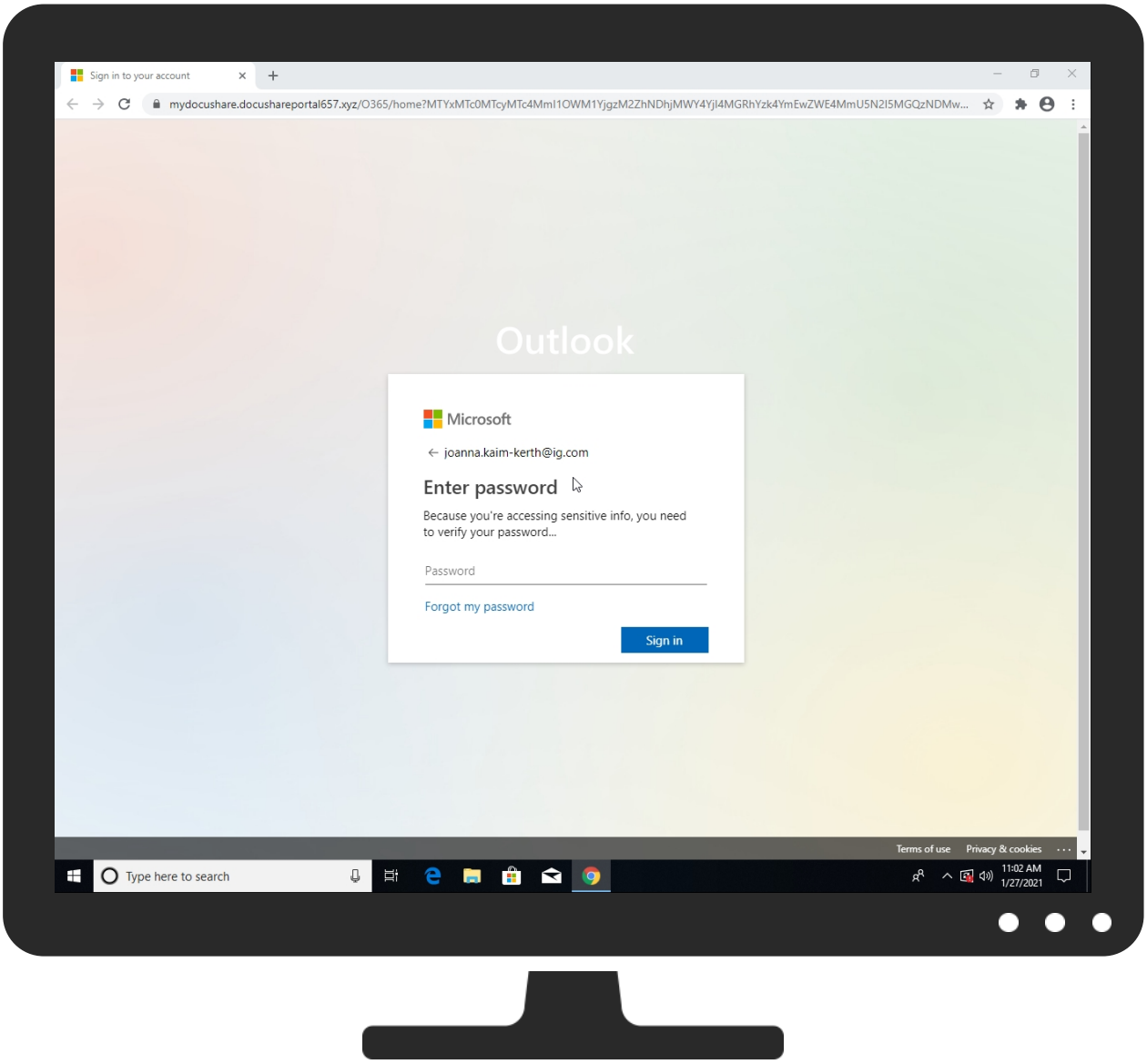


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://bkbizwwqfqstgcsbkbizwwqfqstgcs.lk8ftr.com/e/am9hbm5hLmthaW0ta2VydGhAaWcuY29t	1%	Virustotal		Browse
http://bkbizwwqfqstgcsbkbizwwqfqstgcs.lk8ftr.com/e/am9hbm5hLmthaW0ta2VydGhAaWcuY29t	0%	Avira URL Cloud	safe	
http://bkbizwwqfqstgcsbkbizwwqfqstgcs.lk8ftr.com/e/am9hbm5hLmthaW0ta2VydGhAaWcuY29t	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://bkbizwwqfqstgcsbkbizwwqfqstgcs.lk8ftr.com/e/am9hbm5hLmthaW0ta2VydGhAaWcuY29t	100%	UrlScan	phishing brand: onedrive microsoft	Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
mydocushare.docushareportal657.xyz	0%	Virustotal		Browse
crt.sectigo.com	1%	Virustotal		Browse
zerossl.crt.sectigo.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://mydocushare.docushareportal657.xyz/O365/home?MTYxMTc0MTcyMTc4MmI1OWM1YjgzM2ZhNDhjMWY4YjI4MGRhYzk4YmEwZWE4MmU5N2I5MGQzNDMwNDIxNjdlMzM5MzkwZDczMmMwZDBiYzkyMg==&data=am9hbm5hLmthaW0ta2VydGhAaWcuY29t&email=joanna.kaim-kerth@ig.com&MTYxMTc0MTcyMWExZTE4OGY1ZTFlNTA0ZjViN2NkMDRhNzdhODlhMWY1NzRkZDE3OGE5OGUyZGZhMTFlMDgzZTJjYmFjMzYzMjM3NjNhOTc5MA==%3D	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://mydocushare.docushareportal657.xyz/O365/home?MTYxMTc0MTcyMTc4MmI1OWM1YjgzM2ZhNDhjMWY4YjI4MGRhYzk4YmEwZWE4MmU5N2I5MGQzNDMwNDIxNjdlMzM5MzkwZDczMmMwZDBiYzkyMg==&data=am9hbm5hLmthaW0ta2VydGhAaWcuY29t&email=joanna.kaim-kerth@ig.com&MTYxMTc0MTcyMWExZTE4OGY1ZTFlNTA0ZjViN2NkMDRhNzdhODlhMWY1NzRkZDE3OGE5OGUyZGZhMTFlMDgzZTJjYmFjMzYzMjM3NjNhOTc5MA==%3D	100%	UrlScan	phishing brand: onedrive microsoft	Browse
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://bkbizwwqfqstgcsbkbizwwqfqstgcs.lk8ftr.com	0%	Avira URL Cloud	safe	
http://https://mydocushare.docushareportal657.xyz/O365/home?MTYxMTc0MTcyMTc4MmI1OWM1YjgzM2ZhNDhjMWY4YjI4MGR	0%	Avira URL Cloud	safe	
http://https://mydocushare.docushareportal657.xyz/O365/?joanna.kaim-kerth	0%	Avira URL Cloud	safe	
http://bkbizwwqfqstgcsbkbizwwqfqstgcs.lk8ftr.com/e/am9hbm5hLmthaW0ta2VydGhAaWcuY29t23S	0%	Avira URL Cloud	safe	
http://https://mydocushare.docushareportal657.xyz/O365/proceed?email=joanna.kaim-kerth	0%	Avira URL Cloud	safe	
http://https://mydocushare.docushareportal657.xyz/O365/lib/img/favicon.ico	0%	Avira URL Cloud	safe	
http://zerossl.crt.sectigo.com/ZeroSSLRSADomainSecureSiteCA.crt	0%	Avira URL Cloud	safe	
http://bkbizwwqfqstgcsbkbizwwqfqstgcs.lk8ftr.com/e/am9hbm5hLmthaW0ta2VydGhAaWcuY29tS	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bkbizwwqfqstgcsbkbizwwqfqstgcs.lk8ftr.com	40.76.49.205	true	false		unknown
mydocushare.docushareportal657.xyz	52.188.166.242	true	false	• 0%, Virustotal, Browse	unknown
crt.sectigo.com	91.199.212.52	true	false	• 1%, Virustotal, Browse	unknown
googlehosted.l.googleusercontent.com	172.217.22.225	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
zerossl.crt.sectigo.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

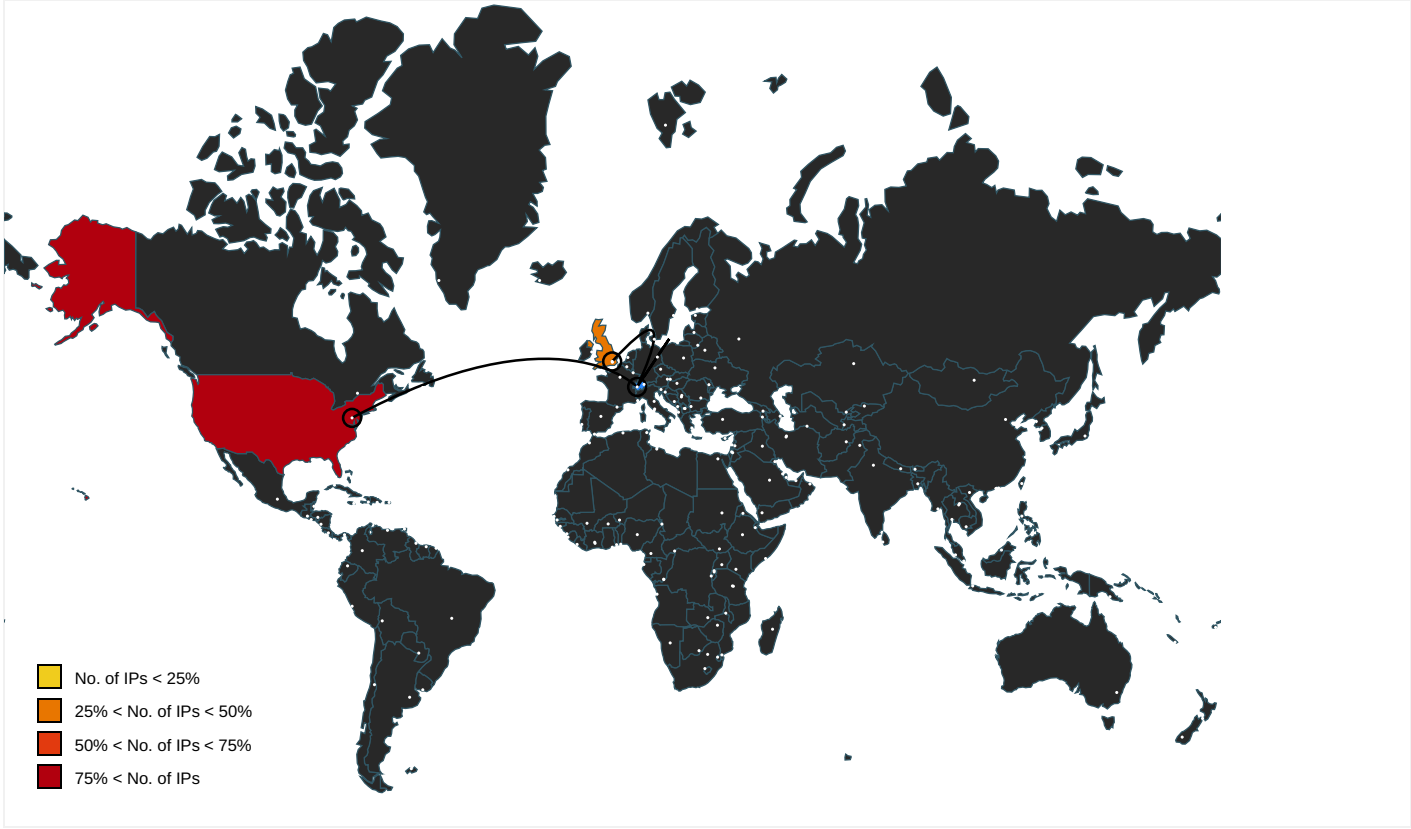
Name	Malicious	Antivirus Detection	Reputation
http://bkbizwwqfqstgcsbkbizwwqfqstgcs.lk8ftr.com/e/am9hbm5hLmthaW0ta2VydGhAaWcuY29t	true		unknown
http://https://mydocushare.docushareportal657.xyz/O365/home?MTYxMTc0MTcyMTc4MmI1OWM1YjgzM2ZhNDhjMWY4YjI4MGRhYzk4YmEwZWE4MmU5N2I5MGQzNDMwNDIxNjdlMzM5MzkwZDczMmMwZDBiYzkyMg==&data=am9hbm5hLmthaW0ta2VydGhAaWcuY29t&email=joanna.kaim-kerth@ig.com&MTYxMTc0MTcyMWExZTE4OGY1ZTFlNTA0ZjViN2NkMDRhNzdhODlhMWY1NzRkZDE3OGE5OGUyZGZhMTFlMDgzZTJjYmFjMzYzMjM3NjNhOTc5MA==%3D	true	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://zerossl.crt.sectigo.com/ZeroSSLRSADomainSecureSiteCA.crt	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	71a93ce5-c5db-43e1-9b45-27c90a52ea2b.tmp.1.dr, 5920a891-a4d7-4969-ac23-7026941eaf9f.tmp.1.dr, 4d17712d-d8aa-4e1c-accd-8c3693b5068c.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://bkbizwwqfqstgcsbkbizwwqfqstgcs.lk8ftr.com	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://mydocushare.docushareportal657.xyz/O365/home?MTYxMTc0MTcyMTc4MmI1OWM1YjgzM2ZhNDhjMWY4YjI4MGR	Current Session.0.dr, Favicons.0.dr, History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://mydocushare.docushareportal657.xyz/O365/?joanna.kaim-kerth	Favicons.0.dr, History.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://bkbizwwqfqstgcsbkbizwwqfqstgcs.lk8ftr.com/e/am9hbm5hLmthaW0ta2VydGhAaWcuY29t23S	History Provider Cache.0.dr	true	• Avira URL Cloud: safe	unknown
http://https://clients2.googleusercontent.com	4d17712d-d8aa-4e1c-accd-8c3693b5068c.tmp.1.dr	false		high
http://https://mydocushare.docushareportal657.xyz/O365/proceed?email=joanna.kaim-kerth	Favicons.0.dr, History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://mydocushare.docushareportal657.xyz/O365/lib/img/favicon.ico	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://bkbizwwqfqstgcsbkbizwwqfqstgcs.lk8ftr.com/e/am9hbm5hLmthaW0ta2VydGhAaWcuY29tS	History.0.dr	true	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.22.225	unknown	United States		15169	GOOGLEUS	false
91.199.212.52	unknown	United Kingdom		48447	SECTIGOGB	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
40.76.49.205	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.188.166.242	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344868
Start date:	27.01.2021
Start time:	11:01:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://bkbizwwqfqstgcsbkbizwwqfqstgcs.lk8ftr.com/e/am9hbm5hLmthaW0ta2VydGhAaWcuY29t
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:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.phis.win@29/164@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): 104.42.151.234, 104.43.139.144, 216.58.207.174, 172.217.23.35, 172.217.23.78, 172.217.20.237, 173.194.187.70, 173.194.187.106, 52.255.188.83, 172.217.23.74, 172.217.23.10, 172.217.23.42, 172.217.22.234, 216.58.207.170, 172.217.20.234, 23.210.248.85, 51.132.208.181, 67.27.159.254, 67.26.83.254, 67.27.157.126, 8.241.122.254, 67.27.158.126 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, r1---sn-4g5e6nsk.gvt1.com, clientservices.googleapis.com, r5---sn-4g5e6nsr.gvt1.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, clients2.google.com, redirector.gvt1.com, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, accounts.google.com, content-autofill.googleapis.com, r1.sn-4g5e6nsk.gvt1.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, www.googleapis.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, clients.l.google.com, r5.sn-4g5e6nsr.gvt1.com, skypedataprdcolwus16.cloudapp.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtQueryVolumeInformationFile calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:02:00	API Interceptor	1x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\10BDC45B4A27319429BBC4F08A4E8A10	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1753
Entropy (8bit):	7.54155945514523

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\10BDC45B4A27319429BBC4F08A4E8A10	
Encrypted:	false
SSDEEP:	48:m4qXYiteL8B0wtUJgVXpxi4sVQmjPOZphFRl12:StO+0mrZn/T5R+
MD5:	58AA23107C8D5AEDEABD0D5E32578592
SHA1:	C81A8BD1F9CF6D84C525F378CA1D3F8C30770E34
SHA-256:	21ACC1DBD6944F9AC18C782CB5C328D6C2821C6B63731FA3B8987F5625DE8A0D
SHA-512:	ED89CA15A1A6150246A3A92EEF6E1E962928BCB2E70FA802513581076C907F276CA0639E700FB4BA7E20F2276A0184D8C19168C9E466CCDA5FE2500D16B8C43
Malicious:	false
Reputation:	low
Preview:	0...0.....lU.....0...*.H.....0..1.0...U....US1.0...U....New Jersey1.0...U....Jersey City1.0...U....The USERTRUST Network1.0,..U...%USERTrust RSA Certification Authority0...2001300000000Z..3001292359595Z0K1.0...U....AT1.0...U....ZeroSSL1*0(..U...!ZeroSSL RSA Domain Secure Site CA0.."0...*.H.....0.....is~..1.#.m...T.....!.~].R|?1..l.Y8^g~KV.u..7.5Zd..L.,$..m....Mf.....!t..C..q...L8}.*.....8...N..h..kw..@...._.....=$._.d...Y..B.oPR..Z.'<.....^...T.c.....q.+{@.5.....A...F..|2E...E.e..Pt.....Vu..J..j.u...5../.]..\..;..w..%5-.V..^x$.....(g..0...mZ'...;.`.r3..}.*c...C.u.;.L..7t...>.D....B.f...tJ..."Y..bf:!...'.{...r2n..]tU.....F.....Ex;6E.....-5E*....X.....B.y9.$....g.....|..OxR..WOaU.'.8y..B...--....jG.iV'4%:KI.J.v.i.-o....."m.z.Wc..%9J.~h.i.H.@...#....Ui.(KBU.....u0..q0...U.#..0...Sy.Z.+J.T.....f.0...U.....xh...h.=r._.>....0...U.....0...U.....0.....0...U.%..0...+.....+.....0"..U. ..0.0...+.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\10BDC45B4A27319429BBC4F08A4E8A10	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	274
Entropy (8bit):	3.0967437244190994
Encrypted:	false
SSDEEP:	3:kkFkl1lN/Nl1fllXlE/lYoTZELDcqElXlije9DZlOJE5Yol2luN7MS1g15lquGlb:kKKyY4qMUjKFgJE5Y7EyUWOJ9jn/
MD5:	6677654241D55C7AD6A02F5FF8257302
SHA1:	454CF3DD973E8ACF5B7D9938C21F34BC762EE232
SHA-256:	D3E506C02ABDE6C155E27CC699121B00308F3BAAB11E129BAD4F2EB9F30A8D6B
SHA-512:	E7BCA81056F170D35DD40E41AED4A2046C1D211177013CE59BE41F91DE981C81AE08923B672F7A7877693A5BBF781674432AE9B2E22317B85C8265FBEDA7D71
Malicious:	false
Reputation:	low
Preview:	p..... ....._.....(..... .....6....@8.....h.t.t.p.:././.z.e.r.o.s.s.l...c.r.t...s.e.c.t.i.g.o...c.o.m./.Z.e.r.o.S.S.L.R.S.A.D.o.m.a.i.n.S.e.c.u.r.e.S.i.t.e.C.A...c.r.t...".5.e.3.2.1.c.8.0.-.6.d.9."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\6974601f-1ef4-4c82-b000-f276cacc3c43.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):	163493
Entropy (8bit):	6.081306729007913
Encrypted:	false
SSDEEP:	3072:7EBu2w0rBlQ96umxmsP6tttYVj4Un8FcbXafIB0u1GOJmA3iuRx:IV1lAumJe8UqaqfllUOoSiuRx
MD5:	D8B035E4073537B42F127E7EFBE35502
SHA1:	FBDFAF6293C1F52B6266EB896AE853FA25451B72
SHA-256:	6CDCDC48CC20D6088E8135546CE6F029AA2F7711D0B2FB7286BB5E1C027C0386
SHA-512:	4806E275DC9C18D8EC0D9BA174E788E10A509EC11AFC440D94C8DB48510CA5ABCEFD837D19A45DF0126DF777A534D54C9F04002310A5C0881FF54FE1E5A45FB
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":1.611774117874456e+12,"network":1.61174172e+12,"ticks":98904365.0,"uncertainty":4831919.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Google\Chrome\User Data\7f45b162-b131-484a-bc0f-70074afcfcc7.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):	163493
Entropy (8bit):	6.081307111526059
Encrypted:	false
SSDEEP:	3072:GEBu2w0rBlQ96umxmsP6tttYVj4Un8FcbXafIB0u1GOJmA3iuRx:9V1lAumJe8UqaqfllUOoSiuRx
MD5:	5DA1C1AEB0BD2FC20493366F3963AF99
SHA1:	0AC83F811F0D2C267BB7E41A2399C6FDC57269A1
SHA-256:	BD3857BABD17F613FF6BFA64938E3B82D973576552AF6B4A72ABF927687CE387

C:\Users\user\AppData\Local\Google\Chrome\User Data\7f45b162-b131-484a-bc0f-70074afcfcc7.tmp	
SHA-512:	0A30910704657D75B9D27D3F51D681B96CF97394E8936A80B5EC9202A0F3778693A98D266C5A6C8B00D7A91AB1283550385D572A1AA8F692D8F75EEC677E2A0C
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":1.61174117874456e+12,"network":1.61174172e+12,"ticks":98904365.0,"uncertainty":4831919.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016775315"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftlE1G1mkftlE1G1mkftlE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D021294256372C916B8155AC
Malicious:	false
Reputation:	low
Preview:	sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0f290be4-cb6e-4cc9-8582-321788e92cd7.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\1a523365-b044-44ca-8325-21d5072656cf.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):	5.53601623729171
Encrypted:	false
SSDEEP:	384:iDot6LlLdXf1kXqKf/pUZNCgVLH2HfDnrUxHGtnTYufi49:ALlFf1kXqKf/pUZNCgVLH2HfLrUlGtnf
MD5:	A6C864580EE917B038C134A6125EF62F
SHA1:	055B7D5E65A9AEEFE9FAA7171BE9D2405A6ED9FA
SHA-256:	4BC454EDC2E27B0E9693B21D4972E24E2C89CB43600C7247B6D36424CF78B0FC
SHA-512:	AB84D02665891149E7F469018E9D5A3A4C9444CF61F8AE1E93FAA1F45EB4BDE233B833D9547615E3A11E6E11B46C59007B00264ABAA8F180E259CC5714EE7D57
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":"13256247714768912","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\1ad3a9d3-b54a-4fe4-a11a-dd26144d8360.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):	1038
Entropy (8bit):	5.559932495202013
Encrypted:	false
SSDEEP:	24:YI6H0UhVsTG1KUerkq/HeUeXby2qUeXvnd7wU9JRUenHQ:YI6UUhVseKUewqPeUer2Uefn9wU9vUew
MD5:	AA1F3066D11175447367E62FF3B36CCD
SHA1:	C2B746B8596C66A05586916FD67C718B61E35BA0
SHA-256:	3B54E4CF03DCCCB0CFE5628101EA0D9F0C12BBE200F07A73FF709BFE9A3B37BE
SHA-512:	F4E35854F22EAB1C1FC34D52BF40577B3F60D1A2B1CF3C28822EA32C0A8C9C447044E7858DDA20357BB0520CBE78E132C14E7C536FF6F366523333FA69FFDF1
Malicious:	false
Reputation:	low

Preview:

{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains"
:true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_inc
lude_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mo
de":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+
6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1643310119.655767,"host":"8/RrMmQlCD2Gsp
14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1611774119.65577},{"expiry":1633014077.462534,"host
":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2ef254dd-bbd0-4703-9172-fb11790ea0f0.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):	5.535842786341347
Encrypted:	false
SSDEEP:	384:iDot6LlLdXf1kXqKf/pUZNCgVLH2HfDnrUxHGQnTYuyi4R:ALlFf1kXqKf/pUZNCgVLH2HfLrUlGQnU
MD5:	77C378CE8CCF8A727A4375E7A5477CC0
SHA1:	68323530993ED452384709FFC1BB5B947E634000
SHA-256:	D490FC9946443B6F0965B2E2BA32AB8921B7151F87989E8A23BACB13AB0303A5
SHA-512:	E2F67D8EEF0351010B68C43095E2F60FAD83065689CFC69A234C91BDEF7A2ACEF120703274401872BAF682A2D97DEF6F03657DC39DB03C4A8DD7E7909AA8E3F
Malicious:	false
Reputation:	low

Preview:

{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy
stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":
[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13256247714768912","location":5,"manifest":{"a
pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and
themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt
l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVG
ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4801c30c-0a4e-4686-a8d2-9cd9a564b936.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):	5280
Entropy (8bit):	5.009847268361959
Encrypted:	false
SSDEEP:	96:nVaFqX4pcV/ok0JCAGRWL84/k51dbOTQVuwn:nVaa4pcM41YRk5X
MD5:	9F300CC77C7B74B2FC48C56D07784BAE
SHA1:	2952ACF8FAF1DB76EB44C72E0744D8526B816DA6
SHA-256:	350588F0262258B3DD4F2833433657B5B905B5355778F7603AEE9D0324E78A6F
SHA-512:	AAD6E5388AE70CA1E1F6EEB8BC3D7F31B261CB20CB28CEF462861742F46555427CEC8EE2B4C7CA975B187E00DE34C91B49C967537D3C33B291BCEF23BE6C3F7
Malicious:	false
Reputation:	low

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13256247715018140","alternate_error_pages":{"backup":true},"announcement_notification_ser
vice_first_run_time":"13245951485614034","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","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4d17712d-d8aa-4e1c-accd-8c3693b5068c.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4d17712d-d8aa-4e1c-accd-8c3693b5068c.tmp	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\603a971c-cba7-4424-86e0-a9f2fcea195e.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):	5877
Entropy (8bit):	5.204891201212644
Encrypted:	false
SSDEEP:	96:nVaF7M4HUsg4cV/ok0JCAGRWL84/k51dbOTQVuwn:nVaO40s5cM41YRk5X
MD5:	3C4EB7EF303BA862D407BEBA79E838DB
SHA1:	647862DFEFF014EACCA4FB9ECBB70B2C78943341
SHA-256:	409E3C1C86A4E3AA4DB6B1E0C07D615BF26C9F38B674D69BE5DF6F408B157B3E
SHA-512:	290BAA120561FABE26FB5F34B14395C5EF98EB71C305CBB07FFD2E3BD7F79A2F27558F2ED8E33667FF2DB521D6C102344BF69AFE813EE7A7BAC266F3AB588D8 5
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13256247715018140","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.170739094803277
Encrypted:	false
SSDEEP:	6:mBhCDi+q2PWXp+N23iKKdK9RXXTZIFUtp+hGHZmwP+hcUHVkwOWXp+N23iKKdK9l:OAG+va5Kk7XT2FUtp+cH/P+LV5f5Kk73
MD5:	4FDD29A21EF9FB72BBF3CA6774DDD36C
SHA1:	4603E3A7C7AEC7A836C6E7ED5E115BF1B4141CFE
SHA-256:	8A26ABA93FA15574BBDC5830B2B947A51CDFBA7FCDB38F9E06F5F64CA87699DD
SHA-512:	BBC026B9D3E70CD8B0656BAEABC2133BA5212AAB78B4AF38C7D58F43791A8ABFBEED5EA623122EAF3134452CED87F44854B7A9D1D2E0A2B27EFD6CA21FBA 2260
Malicious:	false
Reputation:	low
Preview:	2021/01/27-11:02:12.081 1b9c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/01/27-11:02:12.082 1b9c Recovering log #3.2021/01/27-11:02:12.083 1b9c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.16459912724566

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Encrypted:	false
SSDEEP:	6:mBhSM3FN+q2PWXp+N23iKKdKyDZIFUtp+hS2qZmwP+hSmVkwOWXp+N23iKKdKyJd:OEM33+va5Kk02FUtp+E2q/P+EmV5f5K1
MD5:	35C13041CEF46041CC268128DC3D93C8
SHA1:	24C9BCF5FE299E45559A865982BAFCA53573FA0B
SHA-256:	B5454378ECCBA1E209C2202E0BC5CB889F725D36E1E53634D7D6EB34862538C3
SHA-512:	EC660CD0CAAFEE66F953A5B02BAD43D7CB0C6C14DA5D4085DCF61C5231DAD7CA20074511BF0BCD60E946D68146785356B88A4B54FE391784E310873EE115E8 1
Malicious:	false
Reputation:	low
Preview:	2021/01/27-11:02:12.076 1b9c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/01/27-11 :02:12.077 1b9c Recovering log #3.2021/01/27-11:02:12.078 1b9c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatab ase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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):	1.1531069239325096
Encrypted:	false
SSDEEP:	24:TLyqJLbXaFpEO5bNmISHn06UwHETz3Bu0C+gAZOZD/FxbP:TekLLOpEO5J/Kn7Uh3xdVNOZbbP
MD5:	622994682A631B746C62B5DD2DAA95EA
SHA1:	880512767EE04F5719C8B93C8DC0F4D304572175
SHA-256:	CE56AF09057F58B23F6933ACDCDA0FDA3C5FDA69A594DA53C1E7D5E82AD5520F
SHA-512:	48DEC01A2E77C13581A0DA233E3BE6AE8EA2BCDBFEAC94ACAC9F826D7A15032B6C8880BF44F45BEB0FBDEB85E784818500885C16A09F5B8292A6721593B8B7 DA
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):	0.9671341119983462
Encrypted:	false
SSDEEP:	24:rrcLgAZOZD/1qLbJLbXaFpEO5bNmISHn06UwF8:rr8NOZ1q5LLOpEO5J/Kn7Uu8
MD5:	F562B1D75008C22CA33CC10A3EAB35DD
SHA1:	F1C8302066787F0FA44B28AE646048B2D6F3D6FB
SHA-256:	E5DB8FEB2135F42BCA59646ABF149DE04A132813729D03E6A57AA6DF4121D524
SHA-512:	088639E94223BE471C68A47F759EA2FF828BF34F716A2556A94CE74B07117076FEA34BB30C0E87484C6D1260B96ECDAE4D237328B31B59486C146549100F32D9
Malicious:	false
Reputation:	low
Preview:	.....ES..... ....

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):	2681
Entropy (8bit):	4.147297053320382
Encrypted:	false
SSDEEP:	48:345+maxigHa/JBz6y36hHikBi3BV2IY4oJulDbpAxey3yq+k849y6V:3458HqLpYHjsx84ITyXuy6V
MD5:	9F68858A80D74613E1A99FA942D229B7
SHA1:	42886341AC6AC431C5F77D2711F09767EB610B30
SHA-256:	247E4CC6A79AC55B814965B1FE9269C76CD887832F371ABF2D43D8F8D8A1828C
SHA-512:	756DB6FB1B6430F287C361A41CFBBEB4659ACAEF033737F231E806D8D8756102EEDC0CF7570F9308D3BE41122DFAB45E9EA82D837EFAA97C4562B99BE69DE8 B2

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...b37ede36_819e_4167_85f1_d62bbb415ccb.....K..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....S...http://bkbizwwqfqstgcsbkbizwwqfqstgcs.l k8ftr.com/e/am9hbm5hLmthaW0ta2VydGhAaWcuY29t.....h.....`.....g.....g...P.....h.....S ...h.t.t.p.:./.b.k.b.i.z.w.w.q.f.q.s.t.g.c.s.b.k.b.i.z.w.w.q.f.q.s.t.g.c.s...l.k.8.f.t.r...c.o.m./.e./.a.m.9.h.b.m.5.h.L.m.t.h.a.W.0.t.a.2.V.y.d.G.h.A.a.W.c.u.Y.2.9.t..... ...8.....0.....8..... .....S...http://bkbizwwqfq

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.212218308646966
Encrypted:	false
SSDEEP:	6:mCryq2PWXp+N23iKKdK8aPrqIFUtpAAAz1ZmwPAAAlRkwOWXp+N23iKKdK8amLJ:TWva5KkL3FUtplAz1/PlAz5f5KkQJ
MD5:	470BBFAFE3582F3B283E4AF949933F19
SHA1:	95715B38E7986652D3478AD4A6A56015A5CE4419
SHA-256:	2DE5CC5F1BE06EC273DF1F2332BB522004D55059E146CD61133C3F469E912C27
SHA-512:	B7018F4A17301991C8EAA5D72A53AEC516C8C59B69679DFDC4ADA827BFFC230914B7C4B735F9B1D50670578292A9C767EE4989BE3A01AE1C4F2CB6F629D928 A
Malicious:	false
Reputation:	low
Preview:	2021/01/27-11:01:55.058 e94 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/01/27-11 :01:55.060 e94 Recovering log #3.2021/01/27-11:01:55.060 e94 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Reputation:	low
Preview:	.f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f. 5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.. .....f.5.....f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.237114757327194
Encrypted:	false
SSDEEP:	6:m4Mq2PWXp+N23iKKdK8NIFUtpOFHZmwPOFVkwOWXp+N23iKKdK8+eLJ:RMva5KkpFUtpO5/POT5f5KkqJ
MD5:	B3D266F04857FEA16A72DEFF0E441DC4
SHA1:	B3C045D980F4D73EB207867676DF202A6466B8ED
SHA-256:	21D871305D9A180A758130314CACA1178C2702464A0E03EC67466061A316E708
SHA-512:	19B8C8E48C9700F4397D5913A8619753C0C14130C6CCF93A33C51B2545851B5D89845B1D85FEB5E920F4277919265DAD376B33A29C203C7A5E442A7FBDDE0AE
Malicious:	false
Reputation:	low
Preview:	2021/01/27-11:01:57.085 864 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/01/27-11 :01:57.086 864 Recovering log #3.2021/01/27-11:01:57.086 864 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\1.0.0.5_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):	17938
Entropy (8bit):	6.061511031838911
Encrypted:	false
SSDEEP:	384:ahlZ97TC4hNLFkQF/4H/vo3c93yaM5ZAVGnLMeP3rrBsuzfccHyfXRH0MVEPT:ahlvS2Fk5ooNM5Zg+YePRgpXRHLVA
MD5:	58E0F46E53B12F255C9DCFD2FC198362
SHA1:	24E3904DED013ED70FFC033CFA4855FBB6C41C19
SHA-256:	F82EEF4F80D86F5DEF0F40F91FFB6453E1706CA5FD8A7172EDB19C4B17E2F330
SHA-512:	1AC83CDFF124E4C0281FBBFC0A919AA177F1524AB85434D82E5A87DDDF7CAC26A761C5E6249566626054C62D6B0F46A51AAC1F6E64C260F50832AE1D5F0A49 C
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["vyABSKu1ssLnoQtj8Nqw6CjEthL33alh0QYBLzRg9+E=","DGWrOFQ2mF53Fk3FM5jLCV5sKg1DgRTF750mXhpKaoM=","f8vmSL13lL5/ sEk/UBo2z9BTE1au+kMnftvxebWlLfQ=","g6BagkGM3fYVfhX6pe9v+WIhrxb6KJyr1H8KEdf3iQc=","6GdjKPovCi9TAL74Kj/R6GzGC1RVsWCb0lMtrG41ElU=","vttVT0ok782 96FZBpoJgEIMmZmATBpKLrC5wr6RiPIg=","5dwwmOMAg6GXh2x6hn99MsZgiXJCxgTnwFdiMmcl2/0=","lQFxytl8i5cYLqNLbSnc45XXd/jEIuKwO1nAvNh5/WE="," qETF6aAOXwVcduPggf/FGrY8l2ALwdIswKxFJWG2JpQ=","+fjs95t/ESSgtcK9SzZOIcY/aemUr2l/yYI07esfjbk=","H+r4m51qI4G0z8YtAibc3/AGYvPK9qT14BbGvmM4/y4=", "Qz4vtomAqVrAeKIcJ/zbVi5yDpFiY+F7tP/FTdoAKwU=","k110zqa69JMO5T4RH/nBdkCVX9l/98Gd7K2dnRuyFyg=","+QrRx4Pz8wbz4ef9ch1Q2aAQDZbv0r64NMy j9z0qaaE=","6q/tcYekY7TN66ZdPx4ALLcteRLQJqFy0wgcIqL6fFU=","djipPPtOAFsToDpKDbadLJLGQiCzTkN2qsRbzvKijBo=","uHEm1DVxHADroGNWHjmdfpdN UgtHXDQ0zfTmdqtJgYo=","1C2E0Gz2nqKFG3ghcQEVyiTYI4rTYNnrpsHQY9J7BfI=","swYZ8T85/4tzx26dfC0RKxMiHwnjqJoxtn0Mb8NdcjI=","AuXwavx8SOtkg FhnRlnM4rolw243Ryh2ktL0QZRDLoE=","oG0S5XUkjBtAHts9X+uQt5MTsf

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
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
Entropy (8bit):	1.810032082410456
Encrypted:	false
SSDEEP:	48:yBmw6fUXcWL3BV2IY4XQuRyDtjI90R4dGncW/3BV2IY4w7+pI:yBCMDx84XQKyh090B3x84w7+pI
MD5:	B01EDB223F72B9FCCE9A5F8B53CAE802
SHA1:	2A197F82430C6B8D4A523DE51102658CB74544DD
SHA-256:	4DA553A493F3CCB467F0A1B93600A9E8ACDC8BDD0D7D250E4FDA0B56AEB3B72D
SHA-512:	1349EB781DE3C0B3066375AE082748E4D109096C48468A1D8E16FB8C32DC5DBD79F2EDCDA9E741A9463574CBEC5524F604AE9162821FF30981FAC0181593E23
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):	0.7748039149858267
Encrypted:	false
SSDEEP:	24:v8yyLiXxh0GY/l1rWR1PmCx9fZjsBX+T6Uwf3n:v8ydBmw6fUQ3n
MD5:	23F1E034AFF720E5E78E52D2E21854E7
SHA1:	40409202CC14BAC752A8C8E04F656F1A8589A3D6
SHA-256:	FBF0B5E6A90DB1C3EAE130ECC1E9D6C083FA2F669DEE93BC38A58F00FD018A3D
SHA-512:	8238656C3FE6298CCBEEDB380423ED69E0056B5366D87A5883DB02779F73F03AC4F2E6E2E772DA527EE64D8D302FB634328E1C1F61E84FDC8CEAED65A398E4 4
Malicious:	false
Reputation:	low
Preview:	.....P.mY..... ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
Reputation:	low
Preview:	.f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.209567102133011
Encrypted:	false
SSDEEP:	6:mBhQy3+q2PWXp+N23iKKdK25+Xqx8chI+IFUtp+hQsZmwP+hQXVkwOWXp+N23iKG:Or+va5KkTXfchI3FUtp+5/P+CV5f5KkI
MD5:	7FB0D9E52295F26BE482377A45126DDC
SHA1:	A653EBC4315E1885CD6D0F246B0EA4B26719D706
SHA-256:	386009E30E75784C0ADB3D39C1A94F82FA2D58D16ACEAAF7D423DEF805217A78
SHA-512:	BC38FF39B52924A1FFB6712B12F34FDAFC45576E8CBA5F28EBCC536974796EFDCCF181FB9F727848460E9F9C29C4C0701E3929766379586F4E296D621522D390
Malicious:	false
Reputation:	low
Preview:	2021/01/27-11:02:12.050 1b9c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/01/27-11:02:12.052 1b9c Recovering log #3.2021/01/27-11:02:12.053 1b9c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.212142831896276
Encrypted:	false
SSDEEP:	6:mBhsi+q2PWXp+N23iKKdK25+XuoIFUtp+h2ZZmwP+h2NVkwOWXp+N23iKKdK25+Z:Od+va5KkTXYFUtp+g/P+QV5f5KkTXHJ
MD5:	65EFACE4B837AE44DCA7D6F43888C947
SHA1:	E4DE83A2F8E2D75F1F8F74AC63A830EB6C0BD25C
SHA-256:	6111477CA7F73688AB811FE878ECF1D10155521F05FEF6223EE21A4A6645AE8B
SHA-512:	B62537E218A306AB9DDE600E815D1237B932090E9476B09E29240A9276CB94183E1E54D7B1E1896A0C8BBA226BD56078DA8F839D58C6F2910CD06F71AA861048
Malicious:	false
Reputation:	low
Preview:	2021/01/27-11:02:12.045 1b9c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/01/27-11:02:12.046 1b9c Recovering log #3.2021/01/27-11:02:12.046 1b9c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.1906803283778995
Encrypted:	false
SSDEEP:	6:m6ADM+q2PWXp+N23iKKdKWT5g1IdqIFUtpHzAgZmwPHzADMVkwOWXp+N23iKKdKn:zcM+va5Kkg5gSRFUtpHzJ/PHzcMV5f5N
MD5:	5D5753C5E97CB179610290E56F916257
SHA1:	CF7D6E1A925DBAEB9BA33716A410C5C3EA798E25
SHA-256:	14AD0527F7697D3264B4BE6A2015B7932D2FBF01C043A719FFDC2C85E024E683
SHA-512:	EB599F3422187C84A486D437F10EDBAAB3B0B0E208C9496C97A0C646C441E044FE50AADB4DDF1DAE57C3570BEC3C391D27502C008B34F0E782AF3AE3A3B44E7C
Malicious:	false
Reputation:	low
Preview:	2021/01/27-11:02:11.508 178c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/01/27-11:02:11.733 178c Recovering log #3.2021/01/27-11:02:11.733 178c 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.6434024967377274
Encrypted:	false
SSDEEP:	48:TJcWR2zf3BV2IY4MOyog+9RpO3BV2IY4KcWoY78:torx84pNR97Ox84K/78
MD5:	B4E25B61406C2BD26EBF6CEFB24511DE
SHA1:	A0844B6DE9E8E188EE4A39481C899594C3B29330
SHA-256:	19E8E1CBB086B0862446CFCEEE0A7711A1913E962541980C6517414E4FFF99A4
SHA-512:	80E7E948EA211864B78DA405D956B255E6DCC16313BDF4D5FEC0C1F7C5109A5F88D58484B71516C6AE8A19A5216E51F5C6E4EC11ACBE521ED4F623D62DA7231
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2902
Entropy (8bit):	6.162225623774973
Encrypted:	false
SSDEEP:	48:h188z8CYC87mk2tUYIv70LVMQZw3KBIOHOIgcWhI63BV2IY4sIfPIk90icD:hL83mJUdwLVMQZw3KLHOdJ/x84sgP90B
MD5:	8B1DA4F28896569750036C74C38CDD83
SHA1:	3872B19FDB99F9E6D97980595EBFB6C11251872C
SHA-256:	83649AD64DC1B29B5FF90950E6E74438E62A2D24FD16402C9B12616D809020B4
SHA-512:	5890B9BD0FE304AA635228A98A87ECCF3E8C4E69831D418E9A20821AA1A41BE0B5DEDE6CB861252DC41EF6714904EFFA6A8741EBD2B3BD56B3763C5B66B883E9
Malicious:	false
Reputation:	low
Preview:	".....ac...cou..nt..com..docushareportal657..https..ig..i..n..joanna..kaim..kerth..mydocushare..o365..s.ig..n..to..xyz..y..ou..r..email..proceed. am9hbm5hlmtha w0ta2vydghaawcuy29t..data..home.nmtyxmtc0mtcymtc4mmi1owm1yjgzm2zhndhjmwy4yji4mgrhyzk4ymewzwe4mmu5n2i5mgqzndmwndixnjdlmzm5mzkwzdczm mmwzdbiyzkymg.nmtyxmtc0mtcymwexzte4ogy1ztflnta0zjvin2nkmdrhnzdhodlhmwy1nzrkzde3oge5oguyzgzhmtflmdgzztjjymfjmzyzmjm3njnhotc5ma..bkbizwwqfqstg csbkbizwwqfqstgcs..e..http..lk8ftr*........ac...cou..nt...$. am9hbm5hlmthaw0ta2vydghaawcuy29t..".."..bkbizwwqfqstgcsbkbizwwqfqstgcs.....com.....data.....docushareportal657.....e.....email.....home.....http.....https.....ig.....i..n.....joanna.....kaim.....kerth.....lk8ftr...r.nmtyxmtc0mtcymtc4mmi1owm1yjgzm2zhndhjmwy4yji4mgrhyzk4ymewzwe4mmu5n2i5mgqzndmwndixnjdlmzm5mzkwzdczmmmwzdbiyzkymg...r.nmtyxmtc0mtcymwexzte4ogy1ztflnta0zjvin2nkmdrhnzdhodlhmwy1nzrkzde3oge5oguyzgzhmtflmdgz ztjjymfjmzyzmjm3njnhotc5ma.....mydocushare...

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):	0.04761656801783401
Encrypted:	false
SSDEEP:	3:d3llu/fllpNllGfllUNllztFllGflltFllPMRgSWbNFl/l/4ltNll/llOlZTPlG:djk6Ag9bNFlWCj/lKnwKl3n
MD5:	7F99274944AD9ED0F5403620F807F427
SHA1:	91A73C8426E35D03A008ED4419606E2C90D7CD30
SHA-256:	5FDB225B1DD177DDDBB5AC10C620C738A49B0267C27A584A6C10BD2D5B071E7B
SHA-512:	0BD368B2F4EE416A01888A85C55C575D601CC4EDDD575DB5F09E35A7F60C3C67B5DA1926331219694B012B73310C09A13C2E1D6272656F4AAF4E0AC58A41665
Malicious:	false
Reputation:	low
Preview:	.....zy..... ....

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):	5.457843963459808
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
SSDEEP:	48:IZxGS11a7tMz8dbOWNWbQSefgG0NrS0U9RdiN91s:IbPa7tMAdbOWNWbQ5fgG0rS0bs
MD5:	42702D68629959033A1FFD4BB42D29CE
SHA1:	F9812EF32CE4403EBBC9AEB539003032734EF817
SHA-256:	0A0233FF45858F5F162401EA9FDE0AB4926BD5CCF5CFD27906CC6091A08DF9BC
SHA-512:	608B0B48BB893DE878410A888B7345E155CD0C16E06AB9DFA45567AEEC19317AFECE28610F62048E1765EC11A85C86A19519C20F716E5DD15E51B8ED7EB7B4F
Malicious:	false
Reputation:	low
Preview:	I>j....*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..560277000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-01-27 11:02:13.01][INFO][mr.Init] MR instance ID: 8d8df070-b879-46d1-99c1-e0f0581a7a35\n","[2021-01-27 11:02:13.01][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-01-27 11:02:13.01][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-01-27 11:02:13.01][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-01-27 11:02:13.01][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-01-27 11:02:13.02][INFO][mr.CastProvider] Query enabled: true\n","[2021-01-27 11:02:13.02][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	329
Entropy (8bit):	5.247302305395246
Encrypted:	false
SSDEEP:	6:mjOq2PWXp+N23iKKdK8a2jMGIFUtpRHZZmwPTTPkwOWXp+N23iKKdK8a2jMmLJ:xva5Kk8EFUtp7/PTT5f5Kk8bJ
MD5:	5209249BCFFA9DB9D0F2C08615054755
SHA1:	9748517F0D78DCEF7620AA4D32A059804A067CD0
SHA-256:	2F9BCC7AB776B1F2712E5EAA3C3B106181D6BDF604C68938EF8F537F91FA593B
SHA-512:	F198C972B0B5D56DCE77FAFABD7DA894F3869A95557A4B39770B96F0E6A35E96B6100F433B0E3105B01A766CB552D40D222CCBD116692039F0384709EA58483D
Malicious:	false
Reputation:	low
Preview:	2021/01/27-11:01:54.892 864 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/01/27-11:01:54.895 864 Recovering log #3.2021/01/27-11:01:54.897 864 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.160457238881649
Encrypted:	false
SSDEEP:	6:m1Vq2PWXp+N23iKKdKgXz4rRIFUtpXgZmwPXIkwOWXp+N23iKKdKgXz4q8LJ:WVva5KkgXiuFUtpXg/PXI5f5KkgX2J
MD5:	A322FCCD8DE6A681589B7BB755722AD1
SHA1:	735F34ABB0783A4A0CCABCEAC73095EC19F551CB
SHA-256:	AB4298634A51EB4EF7A127C9DF6B4F005C3547F48CA2518D78AEF79D0321431D
SHA-512:	512D1CFDAD8863D58DE55C4543323BA205AF014ADAF83D6E7F45B92D640C958FD8A5AA49F2B88C87F4624FBB3E9D5C07BD203B5B9FFC12459FBD4952FE053F1
Malicious:	false
Reputation:	low
Preview:	2021/01/27-11:01:55.078 12e0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/01/27-11:01:55.079 12e0 Recovering log #3.2021/01/27-11:01:55.079 12e0 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:	3:5ljljljljljl:5ljljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946B

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Malicious:	false
Reputation:	low
Preview:	..&f.....&f.....&f.....&f.....&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.167060282654658
Encrypted:	false
SSDEEP:	6:mRjyq2PWXp+N23iKKdKrQMxIFUtpWv1ZmwPWE1RkwOWXp+N23iKKdKrQMFLJ:GOva5KkCFUtpWv1/PWED5f5KktJ
MD5:	8696B3955CF67DB9F6237755DE43EFC4
SHA1:	913DD5A6BDDDF082EAC5680852E8C4D6A78BE034
SHA-256:	E2187F325B721BBCF0CB856F51F89BFAC1C1451409D0F79333B82716E3DE99E6
SHA-512:	967958A36BEB0F5B1CC794290FB2397DBC9A4389196696BC4EF865F2532F5A2B8A4222C3EEE6C0D735286B934644F3713B803A633574715764734E3BA3A45952
Malicious:	false
Reputation:	low
Preview:	2021/01/27-11:01:54.991 e94 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/01/27-11:01:54.993 e94 Recovering log #3.2021/01/27-11:01:54.994 e94 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	345
Entropy (8bit):	5.186369638881622
Encrypted:	false
SSDEEP:	6:mffQL+q2PWXp+N23iKKdK7Uh2ghZIFUtpYEG1ZmwPYnoXAQLVkwOWXp+N23iKKdb:6va5KkIhHh2FUtpI1/P9XD5f5KkIhHLJ
MD5:	BE9043342EECE6C069719014D41B7174
SHA1:	D9D8FB421DAF6319AAE48BFCDED2528362046E8D
SHA-256:	F45009F4309D2C757722A05CC55988CBEBEC22045403AEDE09AEBBAEAEA980D7
SHA-512:	E4831EC19FA044F9FEA87B81CC654AC06FA758DDAA76913BB01E88BAE2ACF516EA8AA0CE0442B3DB29F21207F9BE136503746E7B7CA992D93E7AE5A66612FADE
Malicious:	false
Reputation:	low
Preview:	2021/01/27-11:01:54.762 6c8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/01/27-11:01:54.770 6c8 Recovering log #3.2021/01/27-11:01:54.771 6c8 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\5920a891-a4d7-4969-ac23-7026941eaf9f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.234895576651389
Encrypted:	false
SSDEEP:	6:myyq2PWXp+N23iKKdKusNpV/2jMGIFUtpu1ZmwP4RkwOWXp+N23iKKdKusNpV/23:Uva5KkFFUtpu1/PA5f5KkOJ
MD5:	AA818C761D52DCC1379F5F06EBDE838E
SHA1:	0DEB57EA2D7D6D8C1E75570F4F9A2BBC7D50A4E8
SHA-256:	F99DA606EE4E8FF774E167C47DCAF496F059928A94040DF9339B289DCAE19472
SHA-512:	CB9CE50B008875F2801BD78163CB0D960D607FE944C96A56FBEE5149FA71B79FC9EE19AD4D270C6656CBFCDAF20256F0C52C6F66FD34364EB3B5DCF06742BD E4
Malicious:	false
Reputation:	low
Preview:	2021/01/27-11:01:55.030 e94 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Local Storage\leveldb/MANIFEST-000001.2021/01/27-11:01:55.031 e94 Recovering log #3.2021/01/27-11:01:55.031 e94 Reusing old log C:\Users\user\AppD ata\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.288653907561449
Encrypted:	false
SSDEEP:	6:mKjyq2PWXp+N23iKKdKusNpqz4rRIFUtpUc/1ZmwPbS1RkwOWXp+N23iKKdKusN9:gva5KkmiuFUtpUc/1/POD5f5Kkm2J
MD5:	468633F13E4735C44BD9B6F4C311B8D3
SHA1:	B5F67D3282C10AF21D95ED5EBC75A44DC65D52C1
SHA-256:	937CEB131E945B2C0D3669EB2F1F65F91FDFBB28A1F1ADAB5575B431F66B8B66
SHA-512:	917C6DBD9EA0FA878395314A52E90CA0DCA9523CA4DA69E4703C96FFA58F5ADC7319BC14E3C0194BBAA08EF02964830E14E06D949CE2428AFE90A30EC18EE0 10
Malicious:	false
Reputation:	low
Preview:	2021/01/27-11:01:55.081 e94 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Platform Notifications/MANIFEST-000001.2021/01/27-11:01:55.083 e94 Recovering log #3.2021/01/27-11:01:55.084 e94 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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.2498548076038
Encrypted:	false
SSDEEP:	6:mq+Iq2PWXp+N23iKKdKusNpZQMxIFUtp5IZmwP5QkwOWXp+N23iKKdKusNpZQMFd:kIva5KkMFUtpG/P65f5KkTJ
MD5:	45C8436D4921B3D94A0F879E559C1424
SHA1:	BC43D5B713DDAE98BA18D7557F0364B7770C6EBD
SHA-256:	18F15F1698E61B01DF10B9A1254B977A44CA056376BF7052D0E6A388BFB52150
SHA-512:	4A0F8DF5727ACD3A479F29C375BD93CE3A481C2DEC10F9F6A2ECFFA70E249915C2FDF69261D375B09298D8DF083A18DBB13C897E9C65E1F385C7120C932E80
Malicious:	false
Reputation:	low
Preview:	2021/01/27-11:02:11.229 864 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/01/27-11:02:11.230 864 Recovering log #3.2021/01/27-11:02:11.230 864 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\71a93ce5-c5db-43e1-9b45-27c90a52ea2b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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):	430
Entropy (8bit):	5.1047640813978425

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Encrypted:	false
SSDEEP:	12:ZVva5KkkGHArBFUtp1Sg/P1SI5f5KkkGHAryJ:Z5a5KkkGgPgiDSf5KkkGga
MD5:	958535600210B4335F59496719F7A52F
SHA1:	3FB171E5FED2C486879FDF8C0700C755789703E3
SHA-256:	8FB4A4E1F2BF306D4F2EBBF59A58CE4E6C7794364BB3304F96EAD9C25C8E01AF
SHA-512:	5DAA03AE7B2C4D5B9D61D7A0423E66154871383AECF209E8BB1ED98EB12F2695EA815D0BD8FB1EFDF35E083104831B97A65E751225AC23B9E2E41068429062B
Malicious:	false
Reputation:	low
Preview:	2021/01/27-11:02:11.616 12e0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/01/27-11:02:11.617 12e0 Recovering log #3.2021/01/27-11:02:11.617 12e0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.18525524163612
Encrypted:	false
SSDEEP:	12:iva5KkkGHArqiuFUtpd+/PP5f5KkkGHArq2J:oa5KkkGgCg4f5KkkGg7
MD5:	D4E34E24330CCD566DC58809CB544A60
SHA1:	E5A40A0D149136974320C9392408FC286B0499A6
SHA-256:	FE5E6D64795C11217B0AC63C7E699AF40AF5C33B164A9143BA739A6F9D73997B
SHA-512:	3FB7B8B6DE843D29152DEAD594EC711680EAD8E7C14DA89A0BC7418932738D58D2E4A191DFD7C331F58709AE7D1D61FA481E5992C3443B7B8C44CAC558543E4
Malicious:	false
Reputation:	low
Preview:	2021/01/27-11:02:11.676 1778 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/01/27-11:02:11.677 1778 Recovering log #3.2021/01/27-11:02:11.678 1778 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):	418
Entropy (8bit):	5.14624571216414
Encrypted:	false
SSDEEP:	12:hVva5KkkGHArAFUtprFtg/PrFtI5f5KkkGHArfJ:7a5KkkGgkgnGAf5KkkGgV
MD5:	164D6FB7558FF9119B3B2F319DCF3DCC
SHA1:	68D067127556F5A7699DF24285E3FFBFAC7D7803
SHA-256:	5FE921E59BA9A69242278B0382EF6352359FADC2491390B10C12EA7E993E9E06
SHA-512:	B01D51EEC8A7F55A7DD5925E7CBC58C24F5DE1F3A0FE1BE8F158F26B51DABF43F1F8AE700376E79D27E787226BDF515F7C71C38109F2B0F883C3AB8EBC16944
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Preview:	2021/01/27-11:02:27.009 16d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/01/27-11:02:27.010 16d4 Recovering log #3.2021/01/27-11:02:27.010 16d4 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
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.216304836685733
Encrypted:	false
SSDEEP:	6:mfL+q2PWXp+N23iKKdKpIFUtpYlQ5ZmwPYtNVkwOWXp+N23iKKdKa/WLJ:Hva5KkmFUtpek/PS5f5KkaUJ
MD5:	2CD0818D4A608EC1D9D6A7A25A473C7E
SHA1:	AC0509E4EB3231F1892DCEE1C236408A5E2416B9
SHA-256:	25723AFBFFC84DEE3B580F3CECDE255CC4C7B08E2B6B443F9E4984FDB54B762F
SHA-512:	A2ADA0FDA1B6431DE78BFB568DD732C08F4FDD4EC3A750615B34810BF53858B1A4957BBEAD95A402A2B4E01A2DDBE98145E5A8AEA7520C9FB24EA72E9A629 13A
Malicious:	false
Reputation:	low
Preview:	2021/01/27-11:01:54.770 1778 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/01/27-11:01:54.773 1778 Recovering log #3.2021/01/27-11:01:54.774 1778 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):	402
Entropy (8bit):	5.326831027186087
Encrypted:	false
SSDEEP:	12:OnVva5KkkOrsFUtp+ug/P+VI5f5KkkOrzJ:O5a5Kk+g4CIf5Kkn
MD5:	B2E5BD09E513D1617B52E7ACA6414E93
SHA1:	8E0178F558A7ECABA3404BD7AAC9F77AB7E47FE6
SHA-256:	886FA7DA8C8F30F315DDD06EC1F7129C9E17AEBDE711CDAA8DCDD1E91176F653
SHA-512:	8411215581CC2D35108E4BBEDB51049ED75C3BB5C9FA973A88C5F4BAA8A4218445C83EAABEC5AC08AC73B4C19491F8E15C3636FE1781B891ADE5B490085A62 E
Malicious:	false
Reputation:	low
Preview:	2021/01/27-11:02:12.994 16d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/01/27-11:02:12.995 16d4 Recovering log #3.2021/01/27-11:02:12.996 16d4 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):	48

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Entropy (8bit):	4.605388542207535
Encrypted:	false
SSDEEP:	3:DOblOidFDBOZbX:DObUidFDBOZbX
MD5:	8264FFDDC9E008AA08F440F5B780A995
SHA1:	6FB31093DE358AD9FCFAFB7B14DCD57DF71F85E3
SHA-256:	9836FBCB92A32E18FB3C05FB5359DDEE9F0096688AD13CB969FF70DC637E9F5E
SHA-512:	BBFA2A9068FC0771F799ECF284D3AAE5EC2EA97309E0D0F0D9B8B155DEA7C420D5D2F811C92D250BCB6C73E58F2CC3BC1FF7489911F17B305C08046E2DE19A 83
Malicious:	false
Reputation:	low
Preview:	.....\V.....+.;.....o.[. .....n+.>..

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.4204023051400565
Encrypted:	false
SSDEEP:	3:tUKTAcURddEAgZmwv3VAcTluSs0V8sVAcTluSs0WGv:mbcURdWAgZmwPWcJuSs0VvWcJuSs0tv
MD5:	B00019599DAC691D25E3BFB5C145D85E
SHA1:	892811DED301A6FFC703D9B535601802F9EE1CA4
SHA-256:	A808D865486304E260D2AB91D4A10FA61D7E52FC004410C165F2EE0FB3473C02
SHA-512:	4902B77E2ED78CA7787CDA89DA32071C2D769764AA152E1FC33C533FC56D6D2B45639E8E326A5C1A466F3F64B56E1AD10909B1D5DE05EA4E1D0E336598326C7
Malicious:	false
Reputation:	low
Preview:	2021/01/27-11:02:07.914 178c Recovering log #3.2021/01/27-11:02:07.961 178c Delete type=0 #3.2021/01/27-11:02:07.961 178c Delete type=3 #2.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f9b9ae81-c85c-4916-8e56-5dc5afc3e42f.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):	5.578114711794002
Encrypted:	false
SSDEEP:	384:iDot/LlLdXf1kXqKf/pUZNCgVLH2HfDnrUUuZi4LU:1LlFf1kXqKf/pUZNCgVLH2HfLrUvZi/
MD5:	F36B93A1359B0E8265FD1A4DAA718303
SHA1:	3BEFEE5EADCB001ED32BB24E69FF6DDEBB6FFA27
SHA-256:	5F40A436C60ACF13BD8BEE08DB208CC5591EDB7C04A14D2046D4503F1846E3F9
SHA-512:	99064D3B30D6FE281C1091E50118D352421231DCA48E89A04B2307E346B1F6CADCA38CBB4527482C2CBB36729CD8C1F48376C60CE76352B9C18971D1887E810A
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":"13256247714768912","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.146206988153457
Encrypted:	false
SSDEEP:	6:mBgVq2PWXp+N23iKKdKfrzAdIFUtp+ZgZmwP+ZIkwOWXp+N23iKKdKfrzILJ:OgVva5Kk9FUtp+Zg/P+ZI5f5Kk2J
MD5:	FBABA2E88B99CEF24E181052B482761E
SHA1:	4FE85EFB9B2DA72D23CFA58CE0A890D7261849B1
SHA-256:	911464154D2480A68B84F967CAD11AA4D0A5DCFEC0337E290E662A65A177865B
SHA-512:	86874700758FD2087EE129AD8902588DD59B16813D8E1E3EC8E9073339260EF01EFC0EFCB733E217DE609FB18959ADC0ADA274DE918C16C834783B1A5ED377F
Malicious:	false
Reputation:	low
Preview:	2021/01/27-11:02:12.180 16d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/01/27-11:02:12.181 16d4 Recovering log #3.2021/01/27-11:02:12.181 16d4 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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\b4fcaf44-6683-4ee3-a654-1f81e2525e5a.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):	163493
Entropy (8bit):	6.08130710906914
Encrypted:	false
SSDEEP:	3072:7ZBf2w0rBlQ96umxmsP6tttYVj4Un8FcbXafIB0u1GOJmA3iuRx:dg1lAumJe8UqaqfIlUOoSiuRx
MD5:	333E17FB526BBFCEFB72984163E290D1
SHA1:	EE62DAA26CD24A9FE4863B810DB699603D911E72
SHA-256:	641735AA271612DA72D33D8CDE77EDC268D66327A364D59E0D94FDD56E461D70
SHA-512:	94AF264F82AD079BEB77407DF5DE880DA1E10D212C3088623FB680912675C82BB01306545656E9D7CAD8AA2C6A4DF105688A14BE131F32B677C439987820EBA7
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":1.61177411787456e+12,"network":1.61174172e+12,"ticks":98904365.0,"uncertainty":4831919.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Google\Chrome\User Data\d1b9b9b1-bc9b-4e8e-8a4b-ffaf9f413a3e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7514853105932104
Encrypted:	false
SSDEEP:	384:DvCBF7kKXHgNMNVrmvZD3a9vWH3uGGJrE3dVxanb3ar4VmQL0TddtKObT9NY11Mn:aepF+7CqceHFXH4/rKbKFbxlX
MD5:	9E3C30C6985E6264B93D7E3386AFDB2C
SHA1:	79F72C25DD10212A60C32A1C7EC9BE1682F32365
SHA-256:	A157F6DBAE4BBF387386543AF216F77AD0820D0E6F64DC1424243D3AEB726FF9
SHA-512:	1AE7A492AE849A19D2DFD07589743811A38D6426D4A3E3E4C692D9EBF98235AE5B74BDE160EC31ABDA634D3FB87BCFAB7B6A0103D4E81BFD06FB22E52770AACF
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..../8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Temp\0da42cc6-128b-4ba3-9e1e-04c3e2e639d8.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\0da42cc6-128b-4ba3-9e1e-04c3e2e639d8.tmp	
Preview:	.

C:\Users\user\AppData\Local\Temp\59e48edb-4a38-4908-bb87-233755c51147.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	300953
Entropy (8bit):	7.973503294353402
Encrypted:	false
SSDEEP:	6144:0sb1v/4nxPbqqBbWbFsw+wh3bC5NFv++S/hup0XcaxlnJ9:7l/4nxPZbOFsw+y3d+S6WnX
MD5:	1FE8E0AEB768437A23CEEAE6053E5822
SHA1:	5529A275644B729009E22035F6125879450F4ABB
SHA-256:	25A2F515CEC98CF2ACF11B34C59723D76820A4B5734E223D7EBEA55E5A851468
SHA-512:	45C8EEC35301495EB9DCE36B32F1CA2E9A7B167CAB52D3E026E2617134067C38CCE1463DEC18C1657A6984FBB8F342336E29E8BF6280C0533CB67CA56812320
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.....L.18..Y.~..%...~._.....O\..p,...eY.0=.!..+.SoZA7...:t.G...VZ<..d....MN.....T..{1\.T...P,...i...NrD...e.2..u....5.....1.n.Zu.E...!..XR..j.:.E.gUw.-s7:T.c_...(.i..iU.).M=yF<..`.....F...@)..IK.. b.4.o..mC'...N.*@OtT...`.&|.8.M;.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.I....{.K@]6.LIP/....](.A.....e..;.<LQ0{^....=m.V.#....a.NL.....%...p.@.4....Q.Fw...dUoCq....RI.G.,2.....[..T'.....''ct.).s#.(/.D..C..4..RKf.W....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-I..`.Q.{...H0F.!...L..\.j.1.d.....==v.....-

C:\Users\user\AppData\Local\Temp\7d28b7c8-f361-4c2a-88be-b95ba2757ac5.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\ef369371-97ee-430a-90eb-cba128e4b063.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;..._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....I-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-I..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\59e48edb-4a38-4908-bb87-233755c51147.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	300953

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\59e48edb-4a38-4908-bb87-233755c51147.tmp	
Entropy (8bit):	7.973503294353402
Encrypted:	false
SSDEEP:	6144:0sb1v/4nxPbqqBbWbFsw+wh3bC5NFv++S/hup0XcaxlnJ9:7l/4nxPZbOFsw+y3d+S6WnX
MD5:	1FE8E0AEB768437A23CEEAE6053E5822
SHA1:	5529A275644B729009E22035F6125879450F4ABB
SHA-256:	25A2F515CEC98CF2ACF11B34C59723D76820A4B5734E223D7EBEA55E5A851468
SHA-512:	45C8EEC35301495EB9DCE36B32F1CA2E9A7B167CAB52D3E026E2617134067C38CCE1463DEC18C1657A6984FBB8F342336E29E8BF6280C0533CB67CA56812320
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.....L.18..Y.~..%...~._.....O\..p,...eY.0=.!..+.SoZA7...:t.G...VZ<..d....MN.....T..{1\.T...P,...i...NrD...e.2..u....5.....1.n.Zu.E...!..XR..j.:.E.gUw.-s7:T.c_...(.i..iU.).M=yF<..`.....F...@)..IK.. b.4.o..mC'...N.*@OtT...`.&|.8.M;.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.I....{.K@]6.LIP/....](.A.....e..;.<LQ0{^....=m.V.#....a.NL.....%...p.@.4....Q.Fw...dUoCq....RI.G.,2.....[..T'....."ct.).s#.(/.D..C..4..RKf.W....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...H0F.!...L..\.j.1.d.....==v.....-

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	886
Entropy (8bit):	4.799570700992651
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyIDEK:1HE7n4gn8WYpYrbhz8ZpotHOPjsrdaD
MD5:	0F604F138A921EE7270C45E520621C30
SHA1:	E2BA940AF44609BEAC49B603EB1C379E43F4AAEB
SHA-256:	A149D52858570C9544E33B183915556230B7F66CF4ABAD4DDB00B1409476FBE1
SHA-512:	D87C8C7D0C998B37E34B7E4E6F5212FF4A0588C15F1273A55CD36B4A6FB13B7FDAE4F3B23EA469E7ACAF22B8BF53EB67476D897B96CA5C15C113EC078071A6D
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": "..... .. .., ...-.....".. },.. "please_sign_in": {.. "message": "...., ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	705
Entropy (8bit):	4.576619033098666
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyFJKtOi2V2Te:1HE5baib6WYpm31Lt0Z8Zp8pxOaKtwVl
MD5:	DDD77BA67108D8D88D66E35AA72A8048
SHA1:	F9C217728E756728B788C969F5101484D0557065
SHA-256:	3DB4D2B1586C020EC679C09148DB226DBB23857D326BECBB6CC48976036C391F
SHA-512:	6CA88083CECF6166503A1441BE8BB726CF08DEA8CFD61F1E81A970FE623284039FB9A530990E8E2008A4B1128399022AFE4F517E85CC7B069B670F5BA659F4F6
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": "No s'ha pogut completar la transacci.. Torneu-ho a provar m.s tard.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	663
Entropy (8bit):	4.771803710371731
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyN+/sFfmSYWc:1HEl4G8WYpdt8Zpq5TOT0FfmR
MD5:	B587AF92ECD087AAE3EF210364960844
SHA1:	AD78B31888863D3F0EC0D8CDCA316EDE9EBD7543
SHA-256:	9796A230BA459EF31E3D102B02575B73D6F1C812BF11F4D1E55B17C17891D2C5

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\CRX_INSTALL_locales\cs\messages.json	
SHA-512:	D2771ABB1174C3B6AF70BA1640837DE1B28137319307841B12A7D03C0A605AAECFC93069026A3906B289BAE12D33F4457FB54D7D27ABC5DC674C5C4C1E9F7CE 1
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "Transakci nebylo mo.n. dokon.it. Zkuste to znovu pozd.ji.".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	642
Entropy (8bit):	4.533570611298554
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyNz31m8tbYzD:1HErMKfqMKVWYpM6lL8ZpDNOOQ84D
MD5:	639CEF5231701AE13F81DBB67730BB95
SHA1:	E249FE0C70B0F85B033730719B6D1B30F0B04431
SHA-256:	6C71F9D37006245D0E2E956D6D2C1815FFEB43236DD3D427A02F8DD348AC93C5
SHA-512:	D040D25ADD9666050544F9173EF61E044F7EBBAE8C528FC4077880734141205AAE60566668E6854D0B9C8D59924E22D1665D2C93085ED7F7E1F4DA91B951F09E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_unavailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "Transaktionen kunne ikke gennemf.res. Pr.v igen senere.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	701
Entropy (8bit):	4.598783840405771
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603Oy91Lj8SYJ6K:1HEzWWYp3Bewv8Zp7k4OALlhj
MD5:	6E1B49ABC0AA5C1E2764E48EB1EA256A
SHA1:	604E76C89D4763C002C51908CEFE8C11AF7CBBE5
SHA-256:	B692DB1A249223E62E62DE9725334039419B5942AF715669F0F0F4BDEDAC5733
SHA-512:	EE527D48178D09D66120C0D1EA2584A7397404109A074AC09487D6AE8507A593193B31D3197C2418A162BB3E7DCC46FA5844D4951BB09650FC2A4AA10EAB8110
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_unavailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "Die Transaktion konnte nicht abgeschlossen werden. Bitte versuchen Sie es sp.ter erneut.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	875
Entropy (8bit):	4.920210350678433
Encrypted:	false
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWlOBINZXD:WguYpCZnpEZb6fD
MD5:	41BB0DB6EC99E4664C6E2247EC704151
SHA1:	BF2268F9A77218384F1F73951F98829296318452
SHA-256:	90FC75C419D7359C2241F54562177252655526F3074E7E419E36F5C473843842
SHA-512:	738F7C254825E0D00D4BDF909FA6957D5A6027BCBCDF76F1385210FA5F908C2C94C038B6DF4309C68774C96B84447079AAF514F46519E60876BE4A8F4ABC9E60
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": ". ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": ".. ....".. },.. "jwt_retrieve_failed": {.. "message": "... ....".. },.. "please_sign_in": {.. "message": "..... ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	617
Entropy (8bit):	4.481995064086158
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOtiCsHTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOthFD
MD5:	64CBD0878A320F70E8F9DC2AD540C8DE
SHA1:	E95BC23E053C078BA4C269B2F75C22159450C2F2
SHA-256:	E99F26D0540E2C71802716B24668D9B4611E9BC429CD681606963E095D18EDFD
SHA-512:	10BAF5423314EF0352FD56D3649CF73713BE8D5EE8A2E21E7E02AAA46EE92635A1EEF87DC62D3E999A1B3704720C51D3281FB28CB9523395EB5A21C4AB3C6D0 A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unava ilable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed. Please try again later.". },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	617
Entropy (8bit):	4.481995064086158
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOtiCsHTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOthFD
MD5:	64CBD0878A320F70E8F9DC2AD540C8DE
SHA1:	E95BC23E053C078BA4C269B2F75C22159450C2F2
SHA-256:	E99F26D0540E2C71802716B24668D9B4611E9BC429CD681606963E095D18EDFD
SHA-512:	10BAF5423314EF0352FD56D3649CF73713BE8D5EE8A2E21E7E02AAA46EE92635A1EEF87DC62D3E999A1B3704720C51D3281FB28CB9523395EB5A21C4AB3C6D0 A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unava ilable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed. Please try again later.". },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	696
Entropy (8bit):	4.469493700399435
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyFJhwtOLLY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OahwtyD
MD5:	B4B479436878DA0B032F1B656B310637
SHA1:	F525EDB5B376CE665280DB32EFE3684CE6DC10DC
SHA-256:	3B3DEB56AD7A5F85ED5AB944172B715A5F5F49E3C5A0F7915DB879BF8ACCFEE0
SHA-512:	56C5CCA31DFF155E608723EFEBE01B421DFA3AB43EDFB586778BD76C6EB1AAF57CF904BDE0EA0FB5E912CCB445788136DE319653A882DC2E844046847D201B 0D
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": "No se ha podido completar la transacci.n. Vuelve a intentarlo m.s tarde.".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	667
Entropy (8bit):	4.49547663693789
Encrypted:	false

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\CRX_INSTALL_locales\es_419\messages.json	
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34GLO03OyFJ2tOLLYiJD:1HEvaC6WYpcDeEFxq8Zp4LlOa2t4D
MD5:	807730218B74CA040AD8DD01E5B2E0D8
SHA1:	ADA0042296C448DCD5C2B22F520C9304526FE9AD
SHA-256:	2823F6DDBF6905D9F4459091A85073644E64B5F7AAAA7FC435495C50DC5ECE68
SHA-512:	5ED86C91A0A435417CB0EDF984AA4DF2177BE37C27D0C805147CEB11ABF75C642416443DB88049A538F63BED9CCCBA95973DAC795498A1A7E022DD6ED36204 2
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": "No se pudo completar la transacci.n. Vuelve a intentarlo m.s tarde.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	609
Entropy (8bit):	4.483029436148137
Encrypted:	false
SSDEEP:	12:1HEJfPGGGfPG+WYpU34Ze7z+dgrW9O8ZpU34ZwZz03OyQQUe1YgoLIR:1HEdvqlWYpTeObk8ZpT/O3QU1LIR
MD5:	B5DF9CEA0A2FEAE9816F8D41470D744E
SHA1:	65C86CD677A68FF7E11A789EAB078FB932A9E157
SHA-256:	AD75B59775C8F6688FFA9F0453868999996E04B9EE9645721765D1C731D04578
SHA-512:	10C30393C29829FFC535559C57B31EBDCC370ABB5C2ED2A6F04E9CC5590FB8587DAB330E4E9367F3E762314EFE913802B98821136D17E9B9A437B56885F259F8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome'i veebipoe maksed".. },.. "app_name": {.. "message": "Chrome'i veebipoe maksed".. },.. "craw_app_unavail able": {.. "message": "Rakendus pole praegu saadaval.".. },.. "craw_connect_to_network": {.. "message": "Looge .hendus v.rguga.".. },.. "iap_unavailable": {.. "message": "Rakendusesisesed maksed ei ole praegu saadaval.".. },.. "jwt_retrieve_failed": {.. "message": "Tehingut ei saa l.pule viia. Proovige hiljem uuesti.".. },.. "please_sign_in": {.. "message": "Logige Chrome'i sisse.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	673
Entropy (8bit):	4.6221501785662396
Encrypted:	false
SSDEEP:	12:1HEJRuzGGRuz+WYpU34ujSBu+dgYO8ZpU34J+Bu03Oy0EyOxAxWeY5HN:1HEFcWYpPNa8ZpD+FO4zxAWHN
MD5:	50EF678CECF0C82675B9DF64CC3CF72E
SHA1:	F9D9A994530C86C1A99B6D104E86666AB56AD4DA
SHA-256:	7F5B921E0D0B01D8D3287D3293729BFFF07ABC7DBCB1227134823A404DF29E83
SHA-512:	62A96C70F496CEA0FF0765E4ED7E014F1A2C7B394F7438C887C094C62885F5B9CD2822B0A9BB83C45471076CA5CF47954C0D5C46D4B45AA7AD5910D57CD2AF4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Storen maksut".. },.. "app_name": {.. "message": "Chrome Web Storen maksut".. },.. "craw_app_unavail able": {.. "message": "Sovellus ei ole t.ll. hetkell. k.ytett.viss..".. },.. "craw_connect_to_network": {.. "message": "Muodosta verkkoyhteys.".. },.. "iap_unavai lable": {.. "message": "Sovelluksen sis.iset maksut eiv.t ole t.ll. hetkell. k.ytett.viss..".. },.. "jwt_retrieve_failed": {.. "message": "Tapahtumaa ei voi suorittaa loppuun. Yrit. my.hemmin uudelleen.".. },.. "please_sign_in": {.. "message": "Kirjaudu sis..n Chromeen.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	692
Entropy (8bit):	4.519947404204655
Encrypted:	false
SSDEEP:	12:1HEJADlbGGADlb+WYpU34hTUT+dgHfZAFFZO8ZpU34hTjzeT03OytnmHQnJvYHf9:1HEYah6WYp7TUSoxOS8Zp7TOsO4wXX2w
MD5:	0CA8EE1D816E684D781E7DF18C18455D
SHA1:	F711596B4049CBAA99296AD3755CCC0E79D47051
SHA-256:	CA9739F4FA8514C8669AE6221842B1F5D148BD80492888CECBA7410CB32225A8
SHA-512:	3BE7CA9E781E0D0BF17F3E894FD75CF7FCCCB0BEEB9A0FC7C17D3F5BC142B662ACFDC7254AA75D2AF9933D0FB70057297E29E8A5815F29469906F9DC8F3390 2E
Malicious:	false

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\CRX_INSTALL_locales\fil\messages.json	
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "app_name": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Kasalukuyang hindi available ang app.".. },.. "craw_connect_to_network": {.. "message": "Mangyaring kumonekta sa isang network.".. },.. "iap_unavailable": {.. "message": "Kasalukuyang hindi available ang Mga Pagbabayad na In-App.".. },.. "jwt_retrieve_failed": {.. "message": "Hindi makumpleto ang transaksyon. Pakisubukang muli sa ibang pagkakataon.".. },.. "please_sign_in": {.. "message": "Mangyaring mag-sign in sa Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	708
Entropy (8bit):	4.573921094123133
Encrypted:	false
SSDEEP:	12:1HEJALf/nbGGALf/nb+WYpU34Owdgbyb+dgdQjO8ZpU34ITQpGnbyb03Oynha3Gg:1HE4Hna1Hn6WYpNdgpY8ZpSTQwnBOshi
MD5:	BE3C2C2BF4551641D84A60EC9F1E6E15
SHA1:	AAB0C8097A5B35FA40F2B137E1889677CB105B40
SHA-256:	DDDDAA9A83C34BF2874CBBE0214351C15E2620C0DC3863B2B79C4ACF9C2A4637
SHA-512:	4F263F78B61075525FA94493FB5C6297A53395F61E630E2DE81F14393BD2D5B3E687F35BF321C1009C0AF9A230A0C49D188F68AA7F2E4F61F3358596A86A6C2D
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": "Impossible de finaliser la transaction. Veuillez r.essayer plus tard.".. },.. "please_sign_in": {.. "message": "Veuillez vous connecter . Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	955
Entropy (8bit):	4.664681647654927
Encrypted:	false
SSDEEP:	24:1HEs07J0JWYp9vnCSVLP8Zp6CsOjSvzdlmLzSLm:Wh7qgYp1CMLUph1jSv3mLzSLm
MD5:	8CFF82EB516A180F2BFA22DA0B18D9E7
SHA1:	87053836FFDB4103302D17D221BC76C8DB842A28
SHA-256:	EA0020B530B3E047559248C076B54E90EFEF6A233DA130D5F43445C25BCB2008
SHA-512:	DEADC807AE4F254A4A73D31A12C2BC274D0E2E25413A36DCEF565B155BA72037BD3A14B5067A8B0325A86CB126C3B223A7DDFC66D5981CB48F1975E962AFBE E6
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": "...-... ....".. },.. "please_sign_in": {.. "message": "..... Chrome ... .".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	633
Entropy (8bit):	4.602004893403632
Encrypted:	false
SSDEEP:	12:1HEJGiimxmbZGGGiimxmbZ+WYpU34OBOEuhopIO+dgcapZO8ZpU34GiiZrMrQphc:1HE4H4TH8WYpNjTta28ZpQVLP0SOv3XD
MD5:	5A777479C6072C009FF6EEEDD167B205
SHA1:	D4B509E3AD07A7EABEB32E7EF06166D5A60D4B54
SHA-256:	1650A45BF772FA06F99EB68015FD356B8BCC1DD4AEE0A4213C626BA2216D9D43
SHA-512:	8E13AD3DF747E6F082D813E4BC5321F1AB1A6D8C203EB9E0A01EF8B5B496DE74F5FCAE956239C85A18DD26399847177325FAADD84C60AC507818E9F26BBB53 D
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": "Transakcija nije dovr.ena. Poku.ajte ponovo kasnije.".. },.. "please_sign_in": {.. "message": "Prijavite se na Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\CRX_INSTALL_locales\hu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	710
Entropy (8bit):	4.727128297637916
Encrypted:	false
SSDEEP:	12:1HEJVJiGGVJi+WYpU34Hpo9O+dgMmfgijO8ZpU34Huo9O03OyeFRLpzS0suYBIAd:1HEVrk5WYpQzTUg/8ZpwoXODpFGIAd
MD5:	C3AD6A15FC6370A3D3E18A313AB22237
SHA1:	E1FB9248DA5E0607882DBCC1819DE5B67F8614F5
SHA-256:	F895E3D151B52E817531C21F877689109B92EC2DA5F0F1A677CC8219A6315373
SHA-512:	F3DEDD20971FCAC9FED5C403E6452C0562148BFD08F81128161F83459A2686127590E997B584F89FA250666C9A82EB3F0C561DA0CCFA1444DC1796DA4404AA0
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": "A tranzakci.t nem siker.lt befejezni. Pr.b.lja .jra k.s.bb.".. },.. "please_sign_in": {.. "message": "Jelentkezzen be a Chrome-ba.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	617
Entropy (8bit):	4.445455113766944
Encrypted:	false
SSDEEP:	12:1HEJs25bGGs25b+WYpU34ORBHAeSJ+dgkmO8ZpU34s22C/SzFAs03OyN4KolFYjt:1HEBaA6WYpaHFH8ZptOYODhuD
MD5:	8B27E83CA394C9D73B58C33910881F01
SHA1:	007F3DFA6CACB4D96D5C057930A8D45241F9908F
SHA-256:	EE050F8DE5EC6F49D4B8E5CE1A432BDE43B4EAFA0963C045D8A097AB622D96E8
SHA-512:	EF1ACFADA29E971E6468804D63AE490C7046B20B946B39F572BC1FF5BAB480C93F97C85E5DC3484EC1A0C3A4CA35FBBF3C217102A9EA269B7AE353C17C5CFF BA
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": "Transaksi tidak dapat diselesai kan. Coba lagi nanti.".. },.. "please_sign_in": {.. "message": "Harap masuk ke Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	622
Entropy (8bit):	4.505455493845955
Encrypted:	false
SSDEEP:	12:1HEJsqd/bGGsqd/b+WYpU34OcX4+dgUvIO8ZpU34vq703OynjbeQfL6CYsD:1HEXd/aKd/6WYpZrv58ZpskOsjhDD
MD5:	DCA488BB7ACBBDC0FF63246899F85933
SHA1:	9408CEF9B8C2EB24E66700E7CD6405A232803EDE
SHA-256:	43267C5F695BCD2A31360D6B03699EFD27D9F53215479042642F42F8612EB7BB
SHA-512:	484793E3F366EBBCC59625BDA5BEAF4B4A0FB58E9CAEB9700BC5A7B74F7ED13B51E72AF46ACD609C137AF84E776FEC3ECF9B256C58F7B5731C8871D3DCD0A CDB
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": "Impossibile completare la transazione. Riprova pi. tardi.".. },.. "please_sign_in": {.. "message": "Accedi a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	778
Entropy (8bit):	5.228857160227492
Encrypted:	false

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\CRX_INSTALL_locales\ja\messages.json	
SSDEEP:	12:1HEJ07uGG07u+WYpU34DB+dgnsVztO8ZpU34MwiB03Oypv/Ik589dwttYmSH:1HEcnDNWYp1kxU8Zp2wiqOoIk589QnSH
MD5:	5FB01096BE49765965AE2148455ADD74
SHA1:	BA73186A0A0D81A20D2830432DEDA52A0527C9A1
SHA-256:	C6BE17C57BB3500A02F98F8A218B120F63D4F29BAE2A960210DC14656D37CBE3
SHA-512:	4A365178D73EA46C9FC6E7A28D1EF13FD89F8E42239231D9DDFE9BF2CA68713C015FC4C76AE25A6497D9287EF693E4A317596AF5A4063B863828F0C13BD1504
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": "....."... },.. "please_sign_in": {.. "message": "Chrome ....."... }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	669
Entropy (8bit):	5.2871011966880666
Encrypted:	false
SSDEEP:	12:1HEJ1GG1+WYpU34K3aT+dgh8d0HTO8ZpU34KaNkaT03OyhMcg/QeHTY/YeHx:1HEajWYpc3aSl0Hq8Zpc6kasOeMcgIeY
MD5:	087B93BE3016C3C7CBB1753C38E337EF
SHA1:	01F9EAB9C8E614DDAC5AE7CAEB564E4803586753
SHA-256:	F49A563FD4545BE61DBB720325E4DF86E2C6674F9EBC53C24E190F291E44E364
SHA-512:	4B9301150BD8601D1D70DD6F4403762D7D7D538DD97E088B73A5281820D017987F8607385DFD1D14DF49E68F99F399B1A700D39BFB71CBFA1265E1033F84F752
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": "... ...."... },.. "please_sign_in": {.. "message": "Chrome. ....."... }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	686
Entropy (8bit):	4.727132438660756
Encrypted:	false
SSDEEP:	12:1HEJpqHnkGGpqHnk+WYpU346M+dgV6O8ZpU34WzSWz03OyFMm/FYx:1HELqHtKqHPWYpM3A8ZpwGzOCu
MD5:	FC774504DD2DCE69B8DD55AFC02AF58D
SHA1:	1D31DC3F3DA200AC24026B2F542BB30B52CE6B16
SHA-256:	6F976F9ED367A7B85CE9B1DE0CB3B228E9E983E3FBBA4D3CD35A59BCA58EDBBC
SHA-512:	8A832DFCB0326D731FDC7D0D33F59724239A1BAB6E9780C8032925E411C184062F71710D217B9F4FA079D5247BED051897EBA12AE2A7AEE148C903B445D736D
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": "Nepavyko u.baigti operacijos. V.liau bandykite dar kart..".. },.. "please_sign_in": {.. "message": "Prisijunkite prie .Chrome..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	699
Entropy (8bit):	4.685697694118083
Encrypted:	false
SSDEEP:	12:1HEJFhVbGGFhVb+WYpU34wDoz+dgGedBO8ZpU34wF03OyNrEuIjYGYID:1HENQKkWYp2Doy/em8Zp2WOZuIBYID
MD5:	4FDBF2298A69836E8F76B3374E20DDA7
SHA1:	445DFC32C1D748D3B100D1211D2A2ABCD26C5834
SHA-256:	5E3FEFF17B28742EE0D5882D94C7A31D13CDB1D9C1524FE69F045AB109B2A173
SHA-512:	5058F9AE32F655DE90BB4FEA9FA2D75494D3E11E7AB6EA54F6A78D8AF12CC386B1CC789DB9C1308C716DFBBCC04697676D57CBC5922125532E0555D765E7A17
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\CRX_INSTALL_locales\lv\messages.json	
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": "Transakciju n evar.ja pabeigt. L.dzu, v.l.k m..iniet v.lreiz.".. },.. "please_sign_in": {.. "message": "L.dzu, pierakstieties p.rl.k. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	644
Entropy (8bit):	4.587522520391651
Encrypted:	false
SSDEEP:	12:1HEJhiOGGhiO+WYpU34OHSN+dgFjdGFZO8ZpU34JgdN03OyN3L8AebYiD:1HEDiHIitWYpCYJ8ZpD1OcL8TD
MD5:	8DF502C935CB5F2C61F7B9EFD6426CF5
SHA1:	31D25CF9B1DC6CDBA07203C107AA1233987D6FFF
SHA-256:	AB56E763119222142A2A69B694238E7C2069F03D909623B7DA25BEAB87494A8A
SHA-512:	3E3F4C956863355282B2C6F31419950A325490027FC839D3881897B7B102DE35953DDD33F417AD8BD89544801A1B378D436C871A592F428DE236BA9B682F5B5B
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": "Transaksjonen kunne ikke fullf.res. Pr.v p. nytt senere.".. },.. "please_sign_in": {.. "message": "Du m. logge p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	642
Entropy (8bit):	4.477340419637416
Encrypted:	false
SSDEEP:	12:1HEJJQGkbGGJQGkb+WYpU34OQKJT+dgiXUmvFZO8ZpU34g7JT03OyjnpSglzYMD:1HErxkaqxk6WYptndXI8ZpTOQ7D
MD5:	F7739EB95F617BFC907FD1D245B49329
SHA1:	D7E6850E8EE0743726BB9CBFE0CDC68F2272D188
SHA-256:	D614E1F67703BC80B0DBEB0896C87E31466E3E3E668A41364EEA7478A8049CB2
SHA-512:	F3E5386F3A70FE8E55FF4CD64F4A6B988F9B3890A6155EBAFCCB09DE128A538DCC1083A3B3CD83977A87B7C20CBCFDA15E072591631784196B004C18917231B
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": "De transactie kan niet worden voltooid. Probeer het later opnieuw.".. },.. "please_sign_in": {.. "message": "Log in bij Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	666
Entropy (8bit):	4.731175547924324
Encrypted:	false
SSDEEP:	12:1HEJbiVbGGbiVb+WYpU34OBHlBi9+dgQUg6O8ZpU34bdbfiIu03OyFLQz9NnuOYk:1HE5iVauiV6WYpIAYr8ZpxFiaOEt50D
MD5:	B0329570F687126C3D9D26FD4279A107
SHA1:	DCF852F8E558C9445AE3598B814226D8C756932B
SHA-256:	9A50EB2C558B250F198F3D1EED232056D3BF8C4463DCEFF37D99579381C84118
SHA-512:	CFB4EC0E5FFD21EC85F7EB47F9B2D394C7C7F59B7BA425B8B0FC8C38D9B844AFA12E3003FED3A588BF694547B4316A891FA26C5EB75CBD473FBE57759F37B9 ED
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": "Nie uda.o si. zrealizowa. transakcji. Spr.buj ponownie p..niej.".. },.. "please_sign_in": {.. "message": "Zaloguj si. w Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\CRX_INSTALL_locales\pt_BR\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\CRX_INSTALL_locales\pt_BR\messages.json	
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	667
Entropy (8bit):	4.5430939640446315
Encrypted:	false
SSDEEP:	12:1HEJsc/bGGsc/b+WYpU34OLw+dgn/KzO8ZpU34FjIBMwGRO03OyFK46XEn6IkYNX:1HEb/a8/6WYp4mZ8Zp7cKlOZ46U6IptD
MD5:	F39681D5543FB19D168EEBE59277C73B
SHA1:	B279538A6B837A0930CD4CD86200792B58E10454
SHA-256:	619631AA6317854DF7FE928288E3A13B2AEAEFAB2F2B46F019F68856E1B02B1E
SHA-512:	E4F93BC1FEC189B3CFC7BC9B68DD2E4CBF54495D98C58053FCBCCD31CB6951AA4D5C008B9044EF98CD5040518918A810ED22D200FA267D1AB34564DA021B33C
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": "N.o foi poss.vel concluir a transa..o. Tente novamente mais tarde.".. },.. "please_sign_in": {.. "message": "Fa.a login no Google Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	661
Entropy (8bit):	4.57627334449273
Encrypted:	false
SSDEEP:	12:1HEJsZUkbGGsZUkb+WYpU34OAE+dgqxKzO8ZpU34rEpBPPO03OyFK46XEn6IkYLD:1HEmUka5Uk6WYpFvdxZ8ZpSTPPlOZ46I
MD5:	EFCAC911642CA7FAF70B8807891387D4
SHA1:	9F603B7AE7A06D83540B4C6B2EF5955C8ECB7C26
SHA-256:	0327B23F28CEC110209093E1305FF1EFE550C04AE977C31A3E1D5AFB2098BD7F
SHA-512:	72F337AE3BBB1B53C75CB0BD10A2322DF520A9F02E69B641EC6DB50907EFD89BE16576D3FA891BB1C100195522C19C1DB947C7ABB1B2974B2759D52E36E8951
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamentos via Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos via Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Aplica..o atualmente indispon.vel.".. },.. "craw_connect_to_network": {.. "message": "Ligue-se a uma rede.".. },.. "iap_unavailable": {.. "message": "Os Pagamentos na Aplica..o est.o atualmente indispon.veis.".. },.. "jwt_retrieve_failed": {.. "message": "N.o foi poss.vel concluir a transa..o. Tente novamente mais tarde.".. },.. "please_sign_in": {.. "message": "Inicie sess.o no Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	668
Entropy (8bit):	4.650567255288544
Encrypted:	false
SSDEEP:	12:1HEJqJrJZGGqJrJZ+WYpU344HIx2Z+dgrVPlZO8ZpU34qT7hI3O03Oy/r6rjJSZR:1HEC4D8WYpKow8WV68ZpKhoOWr6rj8CY
MD5:	AC696B33EC1AFDAE3A4A3E2029E92CCB
SHA1:	2B1D6F49C25A082C876E98C71DF96CAF4D1A1681
SHA-256:	E7829B9A2FC8F518340A97A09C537608DB005EB265B670581682728E0FB0DA41
SHA-512:	A4CCFF6C003083889C3305C4A3E466E76D242746543367E5555A694A6921C93017494BF55E8D09BB693A6EB540E8B12A1773E8A5EB6A3C0FFD97188BB712B4A7
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pl..i prin Magazinul web Chrome".. },.. "app_name": {.. "message": "Pl..i prin Magazinul web Chrome".. },.. "craw_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": "Tranzac.ia nu s-a putut finaliza. .ncearc. din nou mai t.rziu.".. },.. "please_sign_in": {.. "message": "Conecteaz.-te la Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\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):	783
Entropy (8bit):	4.868660175371157
Encrypted:	false
SSDEEP:	24:1HElOJHZMq4uOJHZMq8WYpdWJ/YGHq8ZptNWgOIF5x07ZqD:WlT7uTgYp6hvptNe85e7UD

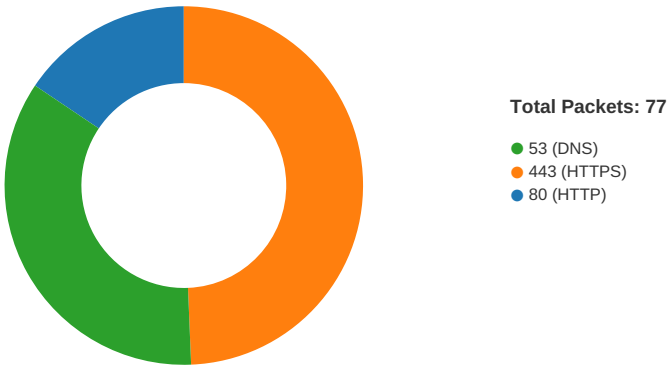
C:\Users\user\AppData\Local\Temp\scoped_dir5752_1870413338\CRX_INSTALL_locales\ru\messages.json	
MD5:	7A151C71B963B0547E30005DF632B5A2
SHA1:	AB9D0B08786AF05AEAE7DAD971934B82C21D38D5
SHA-256:	6FE9E5A1B0C425766582273747F85911C40D8EE125CD609209BA1E3C706EF6E8
SHA-512:	37699BF04408A5EC4FED3321188B6FECCC04D1D713305DABE1BE826D131DA180D1B92C138428BA2411E551B01F75B3A4C2597BB83DB4C59782C169642A5BE6F1
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": "..... ....".. },.. "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
Jan 27, 2021 11:01:59.930124044 CET	49724	80	192.168.2.3	40.76.49.205
Jan 27, 2021 11:01:59.930840015 CET	49725	80	192.168.2.3	40.76.49.205
Jan 27, 2021 11:02:00.055089951 CET	80	49724	40.76.49.205	192.168.2.3
Jan 27, 2021 11:02:00.055182934 CET	49724	80	192.168.2.3	40.76.49.205
Jan 27, 2021 11:02:00.055452108 CET	49724	80	192.168.2.3	40.76.49.205
Jan 27, 2021 11:02:00.055514097 CET	80	49725	40.76.49.205	192.168.2.3
Jan 27, 2021 11:02:00.055608034 CET	49725	80	192.168.2.3	40.76.49.205
Jan 27, 2021 11:02:00.233864069 CET	80	49724	40.76.49.205	192.168.2.3
Jan 27, 2021 11:02:00.426493883 CET	80	49724	40.76.49.205	192.168.2.3
Jan 27, 2021 11:02:00.468161106 CET	49724	80	192.168.2.3	40.76.49.205
Jan 27, 2021 11:02:00.580089092 CET	49733	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:00.580580950 CET	49734	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:00.706485987 CET	443	49733	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:00.706594944 CET	49733	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:00.706736088 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:00.706785917 CET	49733	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:00.706830978 CET	49734	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:00.706975937 CET	49734	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:00.831967115 CET	443	49733	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:00.832015991 CET	443	49733	52.188.166.242	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 11:02:00.832081079 CET	49733	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:00.832225084 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:00.832259893 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:00.832387924 CET	49734	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:00.986680984 CET	49735	80	192.168.2.3	91.199.212.52
Jan 27, 2021 11:02:01.046876907 CET	80	49735	91.199.212.52	192.168.2.3
Jan 27, 2021 11:02:01.046987057 CET	49735	80	192.168.2.3	91.199.212.52
Jan 27, 2021 11:02:01.047938108 CET	49735	80	192.168.2.3	91.199.212.52
Jan 27, 2021 11:02:01.108164072 CET	80	49735	91.199.212.52	192.168.2.3
Jan 27, 2021 11:02:01.108222961 CET	80	49735	91.199.212.52	192.168.2.3
Jan 27, 2021 11:02:01.108258963 CET	80	49735	91.199.212.52	192.168.2.3
Jan 27, 2021 11:02:01.108421087 CET	49735	80	192.168.2.3	91.199.212.52
Jan 27, 2021 11:02:01.186446905 CET	49734	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:01.186968088 CET	49733	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:01.187180042 CET	49734	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:01.314080000 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:01.314116955 CET	443	49733	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:01.314146042 CET	443	49733	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:01.314172029 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:01.314273119 CET	49733	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:01.314380884 CET	49734	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:01.365077972 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:01.851849079 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:01.857069969 CET	49734	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:02.042488098 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.420418978 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.423475027 CET	49734	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:03.610234022 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.619668007 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.619695902 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.619716883 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.619739056 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.619827032 CET	49734	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:03.619884014 CET	49734	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:03.717464924 CET	49734	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:03.717806101 CET	49733	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:03.718765974 CET	49743	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:03.719501972 CET	49744	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:03.720633030 CET	49745	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:03.721461058 CET	49746	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:03.734030962 CET	80	49735	91.199.212.52	192.168.2.3
Jan 27, 2021 11:02:03.734119892 CET	49735	80	192.168.2.3	91.199.212.52
Jan 27, 2021 11:02:03.736008883 CET	49735	80	192.168.2.3	91.199.212.52
Jan 27, 2021 11:02:03.796300888 CET	80	49735	91.199.212.52	192.168.2.3
Jan 27, 2021 11:02:03.844399929 CET	443	49743	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.844549894 CET	49743	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:03.844682932 CET	443	49744	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.844775915 CET	49744	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:03.844929934 CET	49743	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:03.845098019 CET	49744	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:03.846617937 CET	443	49745	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.846698999 CET	49745	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:03.847327948 CET	49745	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:03.847754955 CET	443	49746	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.847826958 CET	49746	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:03.848056078 CET	49746	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:03.848076105 CET	443	49733	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.848093987 CET	443	49733	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.848157883 CET	49733	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:03.849642992 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.849669933 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.849695921 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.849716902 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.849737883 CET	443	49734	52.188.166.242	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 11:02:03.849764109 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.849786043 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.849807024 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.849831104 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.849833012 CET	49734	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:03.849852085 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.849873066 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.849874973 CET	49734	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:03.849881887 CET	49734	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:03.849885941 CET	49734	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:03.849895000 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.849912882 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.849915981 CET	49734	443	192.168.2.3	52.188.166.242
Jan 27, 2021 11:02:03.849939108 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.849961042 CET	443	49734	52.188.166.242	192.168.2.3
Jan 27, 2021 11:02:03.849976063 CET	49734	443	192.168.2.3	52.188.166.242

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 11:01:50.840328932 CET	60831	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:01:50.893268108 CET	53	60831	8.8.8.8	192.168.2.3
Jan 27, 2021 11:01:52.403717995 CET	60100	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:01:52.454443932 CET	53	60100	8.8.8.8	192.168.2.3
Jan 27, 2021 11:01:53.445796967 CET	53195	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:01:53.494249105 CET	53	53195	8.8.8.8	192.168.2.3
Jan 27, 2021 11:01:56.147114992 CET	50141	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:01:56.200053930 CET	53	50141	8.8.8.8	192.168.2.3
Jan 27, 2021 11:01:57.729832888 CET	57568	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:01:57.779095888 CET	53	57568	8.8.8.8	192.168.2.3
Jan 27, 2021 11:01:58.662338018 CET	50540	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:01:58.713258982 CET	53	50540	8.8.8.8	192.168.2.3
Jan 27, 2021 11:01:59.852078915 CET	55435	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:01:59.852992058 CET	50713	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:01:59.854695082 CET	56132	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:01:59.858181953 CET	58987	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:01:59.863797903 CET	56579	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:01:59.865586042 CET	60633	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:01:59.917294025 CET	53	60633	8.8.8.8	192.168.2.3
Jan 27, 2021 11:01:59.922698975 CET	53	55435	8.8.8.8	192.168.2.3
Jan 27, 2021 11:01:59.925090075 CET	53	50713	8.8.8.8	192.168.2.3
Jan 27, 2021 11:01:59.926542997 CET	53	56579	8.8.8.8	192.168.2.3
Jan 27, 2021 11:01:59.926574945 CET	53	58987	8.8.8.8	192.168.2.3
Jan 27, 2021 11:01:59.938957930 CET	53	56132	8.8.8.8	192.168.2.3
Jan 27, 2021 11:02:00.273794889 CET	61292	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:02:00.326251030 CET	53	61292	8.8.8.8	192.168.2.3
Jan 27, 2021 11:02:00.492366076 CET	63619	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:02:00.513531923 CET	64938	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:02:00.556478024 CET	53	63619	8.8.8.8	192.168.2.3
Jan 27, 2021 11:02:00.578030109 CET	53	64938	8.8.8.8	192.168.2.3
Jan 27, 2021 11:02:00.919447899 CET	61946	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:02:00.980880022 CET	53	61946	8.8.8.8	192.168.2.3
Jan 27, 2021 11:02:01.226584911 CET	64910	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:02:01.289071083 CET	53	64910	8.8.8.8	192.168.2.3
Jan 27, 2021 11:02:02.115696907 CET	52123	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:02:02.177409887 CET	53	52123	8.8.8.8	192.168.2.3
Jan 27, 2021 11:02:03.412729979 CET	58784	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:02:03.463485956 CET	53	58784	8.8.8.8	192.168.2.3
Jan 27, 2021 11:02:03.795404911 CET	63978	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:02:03.863229990 CET	53	63978	8.8.8.8	192.168.2.3
Jan 27, 2021 11:02:04.976211071 CET	62938	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:02:05.039833069 CET	53	62938	8.8.8.8	192.168.2.3
Jan 27, 2021 11:02:05.519339085 CET	55708	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:02:05.581937075 CET	53	55708	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 11:02:08.806193113 CET	58306	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:02:08.875327110 CET	53	58306	8.8.8.8	192.168.2.3
Jan 27, 2021 11:02:13.473110914 CET	64124	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:02:13.542752981 CET	53	64124	8.8.8.8	192.168.2.3
Jan 27, 2021 11:02:23.019772053 CET	49361	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:02:23.078474998 CET	53	49361	8.8.8.8	192.168.2.3
Jan 27, 2021 11:02:26.715765953 CET	63150	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:02:26.765803099 CET	53	63150	8.8.8.8	192.168.2.3
Jan 27, 2021 11:02:39.941783905 CET	53279	53	192.168.2.3	8.8.8.8
Jan 27, 2021 11:02:39.993582964 CET	53	53279	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 11:01:59.852078915 CET	192.168.2.3	8.8.8.8	0x6321	Standard query (0)	bkbizwwqfq stgcsbkbiz wwqfqstgcs .lk8ftr.com	A (IP address)	IN (0x0001)
Jan 27, 2021 11:02:00.513531923 CET	192.168.2.3	8.8.8.8	0x7fd	Standard query (0)	mydocushar e.docushar eportal657.xyz	A (IP address)	IN (0x0001)
Jan 27, 2021 11:02:00.919447899 CET	192.168.2.3	8.8.8.8	0x4bca	Standard query (0)	zerossl.cr t.sectigo.com	A (IP address)	IN (0x0001)
Jan 27, 2021 11:02:05.519339085 CET	192.168.2.3	8.8.8.8	0xaebb	Standard query (0)	mydocushar e.docushar eportal657.xyz	A (IP address)	IN (0x0001)
Jan 27, 2021 11:02:08.806193113 CET	192.168.2.3	8.8.8.8	0x99dd	Standard query (0)	clients2.g oogleuserc ontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 11:01:59.922698975 CET	8.8.8.8	192.168.2.3	0x6321	No error (0)	bkbizwwqfq stgcsbkbiz wwqfqstgcs .lk8ftr.com		40.76.49.205	A (IP address)	IN (0x0001)
Jan 27, 2021 11:02:00.578030109 CET	8.8.8.8	192.168.2.3	0x7fd	No error (0)	mydocushar e.docushar eportal657.xyz		52.188.166.242	A (IP address)	IN (0x0001)
Jan 27, 2021 11:02:00.980880022 CET	8.8.8.8	192.168.2.3	0x4bca	No error (0)	zerossl.cr t.sectigo.com	crt.sectigo.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 11:02:00.980880022 CET	8.8.8.8	192.168.2.3	0x4bca	No error (0)	crt.sectigo.com		91.199.212.52	A (IP address)	IN (0x0001)
Jan 27, 2021 11:02:05.581937075 CET	8.8.8.8	192.168.2.3	0xaebb	No error (0)	mydocushar e.docushar eportal657.xyz		52.188.166.242	A (IP address)	IN (0x0001)
Jan 27, 2021 11:02:08.875327110 CET	8.8.8.8	192.168.2.3	0x99dd	No error (0)	clients2.g oogleuserc ontent.com	googlehosted.l.googleuserc ontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 11:02:08.875327110 CET	8.8.8.8	192.168.2.3	0x99dd	No error (0)	googlehost ed.l.googl euserconte nt.com		172.217.22.225	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- bkbizwwqfqstgcsbkbizwwqfqstgcs.lk8ftr.com
- zerossl.crt.sectigo.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49724	40.76.49.205	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 11:02:00.055452108 CET	108	OUT	GET /e/am9hbm5hLmthaW0ta2VydGhAaWcuY29t HTTP/1.1 Host: bkbizwwqfqstgcsbkbizwwqfqstgcs.lk8ftr.com 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
Jan 27, 2021 11:02:00.426493883 CET	191	IN	HTTP/1.1 200 OK Date: Wed, 27 Jan 2021 10:02:00 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/8.0.1 X-Powered-By: PHP/8.0.1 Content-Length: 139 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 20 3d 20 22 68 74 74 70 73 3a 2f 2f 6d 79 64 6f 63 75 73 68 61 72 65 2e 64 6f 63 75 73 68 61 72 65 70 6f 72 74 61 6c 36 35 37 2e 78 79 7a 2f 4f 33 36 35 2f 3f 6a 6f 61 6e 6e 61 2e 6b 61 69 6d 2d 6b 65 72 74 68 40 69 67 2e 63 6f 6d 22 3c 2f 73 63 72 69 70 74 3e 0a Data Ascii: <script type="text/javascript">window.location.href = "https://mydocushare.docushareportal657.xyz/O365/?joanna.kaim-kerth@ig.com"</script>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49735	91.199.212.52	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 11:02:01.047938108 CET	993	OUT	GET /ZeroSSLRSADomainSecureSiteCA.crt HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Microsoft-CryptoAPI/10.0 Host: zerossl.crt.sectigo.com
Jan 27, 2021 11:02:01.108222961 CET	994	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 27 Jan 2021 10:02:01 GMT Content-Type: application/pkix-cert Content-Length: 1753 Connection: keep-alive Last-Modified: Thu, 30 Jan 2020 00:00:00 GMT ETag: "5e321c80-6d9" X-CCACDN-Mirror-ID: sscrl2 Cache-Control: max-age=14400, s-maxage=3600 X-CCACDN-Proxy-ID: mcdpinlb6 X-Frame-Options: SAMEORIGIN Accept-Ranges: bytes Data Raw: 30 82 06 d5 30 82 04 bd a0 03 02 01 02 02 10 6c 55 ab db d0 07 92 c7 9d 07 0c d8 11 9e d6 bf 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0c 05 00 30 81 88 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 13 30 11 06 03 55 04 08 13 0a 4e 65 77 20 4a 65 72 73 65 79 31 14 30 12 06 03 55 04 07 13 0b 4a 65 72 73 65 79 20 43 69 74 79 31 1e 30 1c 06 03 55 04 0a 13 15 54 68 65 20 55 53 45 52 54 52 55 53 54 20 4e 65 74 77 6f 72 6b 31 2e 30 2c 06 03 55 04 03 13 25 55 53 45 52 54 72 75 73 74 20 52 53 41 20 43 65 72 74 69 66 69 63 61 74 69 6f 6e 20 41 75 74 68 6f 72 69 74 79 30 1e 17 0d 32 30 30 31 33 30 30 30 30 30 30 30 5a 17 0d 33 30 30 31 32 39 32 33 35 39 35 39 5a 30 4b 31 0b 30 09 06 03 55 04 06 13 02 41 54 31 10 30 0e 06 03 55 04 0a 13 07 5a 65 72 6f 53 53 4c 31 2a 30 28 06 03 55 04 03 13 21 5a 65 72 6f 53 53 4c 20 52 53 41 20 44 6f 6d 61 69 6e 20 53 65 63 75 72 65 20 53 69 74 65 20 43 41 30 82 02 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 82 02 0f 00 30 82 02 0a 02 82 02 01 00 86 69 73 7e a3 b5 31 d8 23 e1 6d dd a4 13 d3 54 15 f5 02 eb dc 03 21 b5 7e 5d 1d 52 7c 3f 31 eb 9e 09 6c d1 59 38 5e 67 7e 4b 56 8f 75 90 b2 37 0c 35 5a 64 a5 be 4c 10 2c 24 18 c4 6d 89 8c c1 c5 92 4d 66 02 83 9d f7 e1 21 74 f9 cb 43 02 c1 71 b1 7f ab 4c 38 7d 91 2a c6 ff 89 a9 e8 e4 a1 b9 b2 da 10 85 09 89 9a 38 b7 ce f7 4e e4 9d d1 68 f9 0d 6b 77 0e da 40 1b c4 f7 e6 5f ef fb 1a cd f2 e6 fc 3d 24 a8 5f 95 64 83 0f a3 59 fe 0a 42 d3 6f 50 52 c3 ab c9 85 5a 15 27 3c be a3 1c 00 03 5e 9b ec e2 54 cd 63 03 ad c7 dc 90 b5 ba 71 c1 2b 7b 40 96 35 f8 80 ab 99 12 41 e8 1b 8a 46 df e3 7c 32 45 f4 9b 1c 45 05 65 1c 8c 50 74 a0 09 97 ba 1a 56 75 e0 0e 4a ad 93 6a 9d 75 dd e4 08 35 dd ef 88 2f f3 5d c6 f7 5c fb 0a 3b 06 c8 9f 77 a0 92 25 35 2d d4 80 56 c3 e9 5e 78 24 c8 19 de b4 a6 a2 d6 1b cf df 28 67 15 fb 30 a6 ed 0a 6d 5a 27 fa be 85 3b f6 60 ad 72 33 1a e7 7d c8 9e 2a 63 98 05 b1 43 86 75 b9 3b a4 4c 03 bd 37 74 12 bd da 3e 97 44 dd 84 b6 d2 e4 42 eb a3 66 0c be 8d 74 4a b5 a5 8c 22 59 0d 91 62 66 3a 21 e6 12 b4 27 80 7b ed 88 d9 08 72 32 6e 9a ad 5d 74 55 f8 89 a4 c8 e3 46 ba ce 0b c8 06 dc 45 78 3b 36 45 f7 1a 1f bd de af b7 2d 35 45 2a 81 04 f9 ac 58 09 84 c9 85 c7 be ab 42 00 79 39 95 24 a1 d6 f9 93 67 b1 ec ff 86 bb 82 7c e9 b4 b5 e7 4f 78 52 e6 1c 57 4f 61 55 e9 27 99 38 79 13 1f 42 04 a8 a9 2d 2d 96 db 02 81 6a 47 fe 69 56 27 34 25 3a 4b 49 c0 4a ab 76 c6 b6 69 18 2d 6f ee fe 83 86 e7 a9 cb 22 6d 9f 7a 92 57 63 e8 06 25 39 4a a9 7e 68 04 69 c1 48 9b 40 c1 a6 e3 88 23 c8 d0 ea 0e 55 69 f9 28 4b 42 55 07 f7 1f 02 03 01 00 01 a3 82 01 75 30 82 01 71 30 1f 06 03 55 1d 23 04 18 30 16 80 14 53 79 bf 5a aa 2b 4a cf 54 80 e1 d8 9b c0 9d f2 b2 03 66 cb 30 1d 06 03 55 1d 0e 04 16 04 14 c8 d9 78 68 a2 d9 19 68 d5 3d 72 de 5f 0a 3e dc b5 86 86 a6 30 0e 06 03 55 1d 0f 01 01 ff 04 04 03 02 01 86 30 12 06 03 55 1d 13 01 01 ff 04 08 30 06 01 01 ff 02 01 00 30 1d 06 03 55 1d 25 04 16 30 Data Ascii: 00lU0*H010UUS10UNew Jersey10UJersey City10UThe USERTRUST Network1.0,U%USERTrust RSA Certification Authority0200130000000Z3001292359595Z0K10UAT10UZeroSSL1*0(U!ZeroSSL RSA Domain Secure Site CA0"0*H0is~1#mT!~]R|?1lY8^g~KVu75ZdL,$mMf!tCqL8}*8Nhkw@_=$_dYBoPRZ'<^Tcq+{@5AF|2EEePtVuJju5/]\;w%5-V^x$(g0mZ';`r3}*cCu;L7t>DBftJ"Ybf:!'{r2n]tUFEx;6E-5E*XBy9$g|OxRWOaU'8yB--jGiV'4%:KIJvi-o"mzWc%9J~hiH@#Ui(KBUu0q0U#0SyZ+JTf0Uxhh=r_>0U0U00U%0

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
Jan 27, 2021 11:02:05.844063044 CET	52.188.166.242	443	192.168.2.3	49754	CN=*.docushareportal657.xyz	CN=ZeroSSL RSA Domain Secure Site CA, O=ZeroSSL, C=AT	Wed Jan 20 01:00:00 CET 2021	Wed Apr 21 01:59:59 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
Jan 27, 2021 11:02:05.916349888 CET	52.188.166.242	443	192.168.2.3	49755	CN=*.docushareportal657.xyz	CN=ZeroSSL RSA Domain Secure Site CA, O=ZeroSSL, C=AT	Wed Jan 20 01:00:00 CET 2021	Wed Apr 21 01:59:59 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

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5752 Parent PID: 4852

General

Start time:	11:01:53
Start date:	27/01/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'http://bkbizwwqfqstgcsbkbizwwqfqstgcs.lk8ftr.com/e/am9hbm5hLmthaW0ta2VydGhAaWcuY29t'
Imagebase:	0x7ff77b960000
File size:	2150896 bytes

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

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: chrome.exe PID: 464 Parent PID: 5752

General

Start time:	11:01:55
Start date:	27/01/2021
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=1532,15419587561947641969,2247414398812328316,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1724 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly