ID: 356247
Sample Name: xerox for hycite.htm
Cookbook: default.jbs
Time: 20:06:34
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

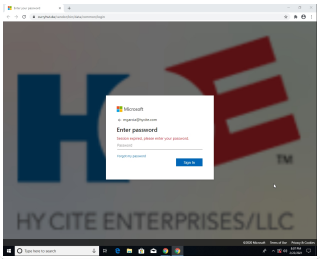
Analysis Report xerox for hycite.htm

Overview

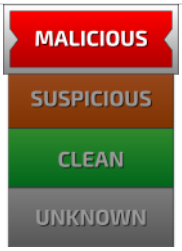
General Information

Sample Name:	xerox for hycite.htm
Analysis ID:	356247
MD5:	158eb35645b71b..
SHA1:	c4d06a2c43fd948..
SHA256:	5873df6b96a855b.

Most interesting Screenshot:



Detection



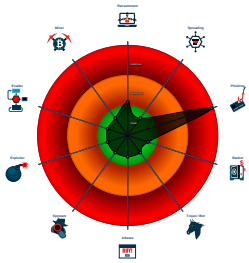
HTMLPhisher

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Phishing site detected (based on fav…
- Yara detected HtmlPhish_10
- Yara detected obfuscated html page
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- Uses Javascript AES encryption / d…
- HTML body contains low number of …
- HTML title does not match URL
- IP address seen in connection with o…
- Invalid 'forgot password' link found
- JA3 SSL client fingerprint seen in co…

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 6436 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'C:\Users\user\Desktop\xerox for hycite.htm' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6632 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1576,9969516566149389704,7036051267904063449,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1696 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

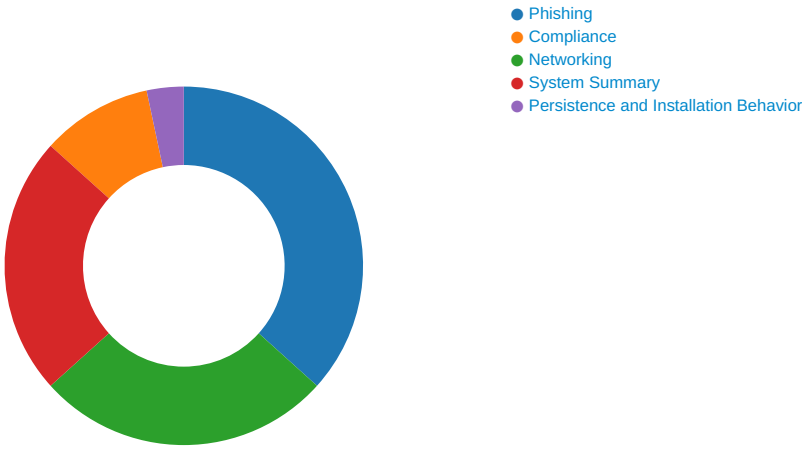
Initial Sample

Source	Rule	Description	Author	Strings
xerox for hycite.htm	JoeSecurity_Obshtml	Yara detected obfuscated html page	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish_10

Yara detected obfuscated html page

Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

Uses Javascript AES encryption / decryption (likely to hide suspicious Javascript code)

Compliance:

Creates a directory in C:\Program Files

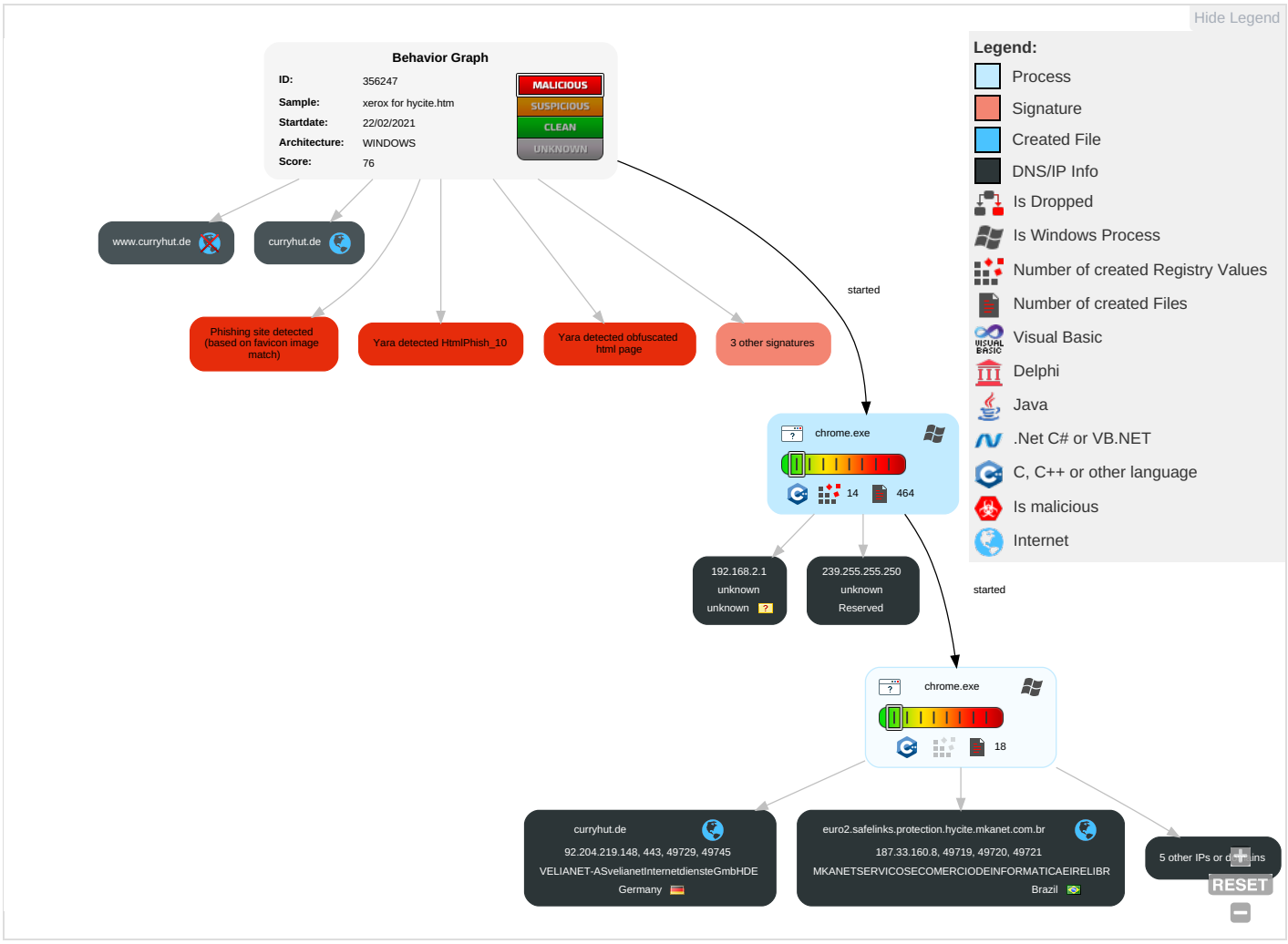
Creates license or readme file

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	Scripting 1	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)	Deobfuscate/Decode Files or Information 1	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)	Scripting 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Carri Billing Fraud

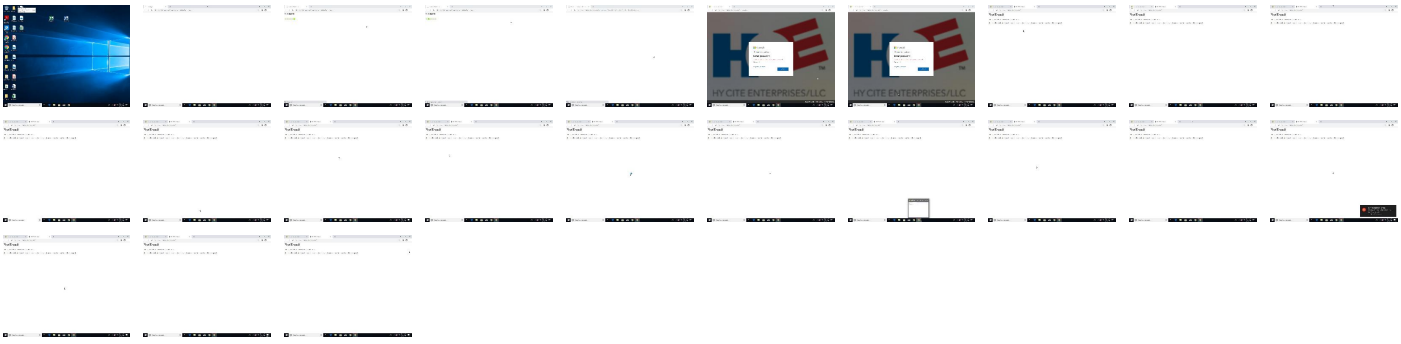
Behavior Graph

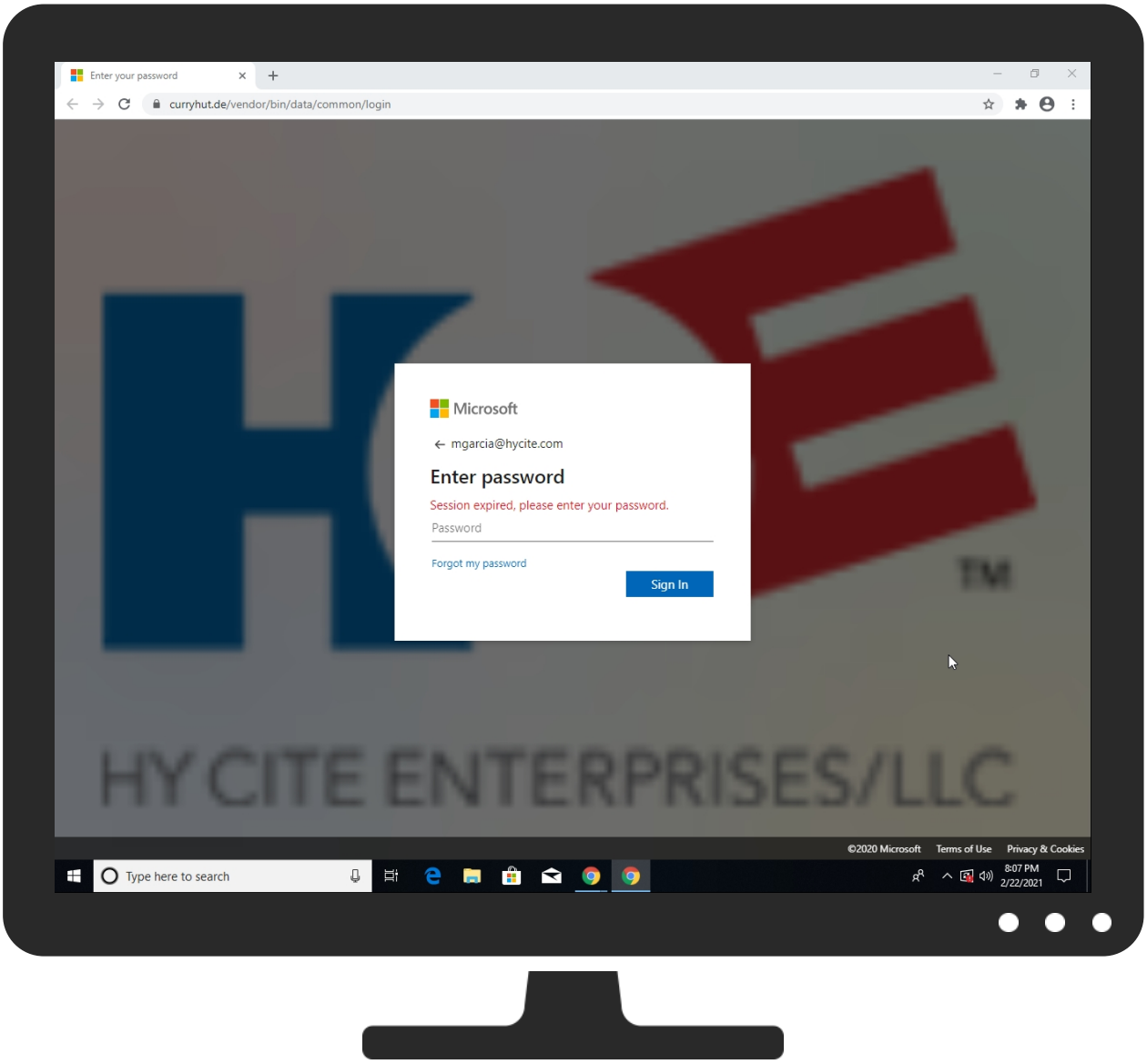


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.curryhut.de/vendor/bin/data/?ss=2&ea=66d67617263696140687963697 4652e636f6d	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://www.curryhut.de/vendor/bin/data?ss=2&ea=66d67617263696140687963697465 2e636f6dEnter	0%	Avira URL Cloud	safe	
http://https://www.curryhut.de/vendor/bin/data/?ss=2&ea=66d67617263696140687963697465 2e636f6d2	0%	Avira URL Cloud	safe	
http://https://www.curryhut.de	0%	Avira URL Cloud	safe	
http://https://www.curryhut.de/vendor/bin/data/?ss=2&ea=66d67617263696140687963697465 2e636f6dEnter	0%	Avira URL Cloud	safe	
http://https://www.curryhut.de/vendor/bin/data?ss=2&ea=66d67617263696140687963697465 2e636f6d	0%	Avira URL Cloud	safe	
http://https://www.curryhut.de/vendor/bin/data/login.php?ss=2&ea=66d67617263696140687963697465 2e636f6d	0%	Avira URL Cloud	safe	
http://https://www.curryhut.de/	0%	Avira URL Cloud	safe	
http://https://curryhut.de/K	0%	Avira URL Cloud	safe	
http://https://www.curryhut.de/vendor/bin/data/files/enc.js	0%	Avira URL Cloud	safe	
http://euro2.safelinks.protection.hycite.mkanet.com.br/inbox/66d67617263696140687963697465 2e636f6d	0%	Avira URL Cloud	safe	
http://https://www.curryhut.de/vendor/bin/data/common/login2	0%	Avira URL Cloud	safe	
http://https://www.curryhut.de/vendor/bin/data/files2/favicon.ico	0%	Avira URL Cloud	safe	
http://https://www.curryhut.de/vendor/bin/data/?ss=2&ea=66d67617263696140687963697465 2e636f6dg	0%	Avira URL Cloud	safe	
http://euro2.safelinks.protection.hycite.mkanet.com.br/inbox/66d67617263696140687963697465 2e636f6d8	0%	Avira URL Cloud	safe	
http://euro2.safelinks.protection.hycite.mkanet.com.br/inbox/66d67617263696140687963697465 2e636f6dEn	0%	Avira URL Cloud	safe	
http://https://www.curryhut.de/vendor/bin/data?ss=2&ea=66d67617263696140687963697465 2e636f6d2	0%	Avira URL Cloud	safe	
http://euro2.safelinks.protection.hycite.mkanet.com.br/inbox/66d67617263696140687963697465 2e636f6d2	0%	Avira URL Cloud	safe	
http://https://www.curryhut.de/vendor/bin/data/common/loginEnter	0%	Avira URL Cloud	safe	
http://https://www.curryhut.de/vendor/bin/data?ss=2&ea=66d67617263696140687963697465 2e636f6dd	0%	Avira URL Cloud	safe	
http://https://www.curryhut.de/vendor/bin/data/login.php?ss=2&ea=66d67617263696140687963697465 2e636f6d2	0%	Avira URL Cloud	safe	
http://https://www.curryhut.de/vendor/bin/data/login.php?ss=2&ea=66d67617263696140687963697465 2e636f6dEnter	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
euro2.safelinks.protection.hycite.mkanet.com.br	187.33.160.8	true	false		unknown
googlehosted.l.googleusercontent.com	142.250.186.33	true	false		high
curryhut.de	92.204.219.148	true	false		unknown
clients2.googleusercontent.com	unknown	unknown	false		high
secure.aadcdn.microsoftonline-p.com	unknown	unknown	false		unknown
www.curryhut.de	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.curryhut.de/vendor/bin/data/common/login	true		unknown
http://https://www.curryhut.de/vendor/bin/data/	true		unknown
http://euro2.safelinks.protection.hycite.mkanet.com.br/inbox/66d67617263696140687963697465 2e636f6d	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.curryhut.de/vendor/bin/data/?ss=2&ea=66d67617263696140687963697465 2e636f6d	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dns.google	695de0af-ffc2-4c28-bc33-7aadafac8e1d.tmp.1.dr, b0afc06f-4b92-4c3f-bc6d-fee8371e7619.tmp.1.dr, e025eb74-386b-44ca-9ec7-b862b5c4620f.tmp.1.dr, 81597e5e-51ec-4e46-99d0-380bb257020f.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.curryhut.de/vendor/bin/data?ss=2&ea=66d67617263696140687963697465 2e636f6dEnter	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.curryhut.de/vendor/bin/data/?ss=2&ea=66d67617263696140687963697465 2e636f6d2	History Provider Cache.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.curryhut.de	Current Session.0.dr, b0afc06f-4b92-4c3f-bc6d-fee8371e7619.tmp.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.curryhut.de/vendor/bin/data/?ss=2&ea=66d67617263696140687963697465 2e636f6dEnter	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.curryhut.de/vendor/bin/data?ss=2&ea=66d67617263696140687963697465 2e636f6d	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.curryhut.de/vendor/bin/data/login.php?ss=2&ea=66d67617263696140687963697465 2e636f6d	Current Session.0.dr, Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.curryhut.de/	Network Action Predictor.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://curryhut.de/K	1aa724cf792052df_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.curryhut.de/vendor/bin/data/files/enc.js	1aa724cf792052df_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.curryhut.de/vendor/bin/data/common/login2	History Provider Cache.0.dr	true	• Avira URL Cloud: safe	unknown
http://https://www.curryhut.de/vendor/bin/data/common/login	Current Session.0.dr, Favicons.0.dr	true		unknown
http://https://www.curryhut.de/vendor/bin/data/files2/favicon.ico	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.curryhut.de/vendor/bin/data/?ss=2&ea=66d67617263696140687963697465 2e636f6dg	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://euro2.safelinks.protection.hycite.mkanet.com.br/inbox/66d67617263696140687963697465 2e636f6d8	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://euro2.safelinks.protection.hycite.mkanet.com.br/inbox/66d67617263696140687963697465 2e636f6dEn	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients2.googleusercontent.com	b0afc06f-4b92-4c3f-bc6d-fee8371e7619.tmp.1.dr, e025eb74-386b-44ca-9ec7-b862b5c4620f.tmp.1.dr	false		high
http://https://www.curryhut.de/vendor/bin/data?ss=2&ea=66d67617263696140687963697465 2e636f6d2	History Provider Cache.0.dr	false	• Avira URL Cloud: safe	unknown
http://euro2.safelinks.protection.hycite.mkanet.com.br/inbox/66d67617263696140687963697465 2e636f6d2	History Provider Cache.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.curryhut.de/vendor/bin/data/common/loginEnter	History.0.dr	true	• Avira URL Cloud: safe	unknown
http://https://www.curryhut.de/vendor/bin/data/	Current Session.0.dr	false		unknown
http://https://www.curryhut.de/vendor/bin/data?ss=2&ea=66d67617263696140687963697465 2e636f6dd	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://www.curryhut.de/vendor/bin/data/login.php?ss=2&ea=66d67617263696140687963697465 2e636f6d2	History Provider Cache.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.curryhut.de/vendor/bin/data/login.php?ss=2&ea=66d67617263696140687963697465 2e636f6dEnter	History.0.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
92.204.219.148	unknown	Germany		29066	VELIANET-ASvelianetInternetdiensteGmbHDE	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
187.33.160.8	unknown	Brazil		53085	MKANETSERVICOSECOMERCIODEINFORMATICAEIRELIBR	false
142.250.186.33	unknown	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356247
Start date:	22.02.2021
Start time:	20:06:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	xerox for hycite.htm
Cookbook file name:	default.jbs
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:	29
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 • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.phis.winHTM@39/189@5/6
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .htm • Browse: https://www.curryhut.de/vendor/bin/data/
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, RuntimeBroker.exe, backgroundTaskHost.exe, UsoClient.exe, audiodg.exe, BackgroundTransferHost.exe, HxTsr.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 13.88.21.125, 184.30.21.144, 168.61.161.212, 142.250.185.206, 142.250.186.174, 172.217.23.109, 74.125.173.135, 74.125.110.104, 104.42.151.234, 2.20.142.210, 2.20.142.209, 142.250.185.131, 92.123.151.195, 142.250.185.202, 142.250.185.234, 142.250.186.42, 142.250.186.74, 142.250.186.138,

142.250.186.170, 172.217.18.106, 172.217.23.106, 216.58.212.138, 172.217.16.138, 142.250.185.106, 142.250.185.138, 142.250.185.170, 23.57.80.111, 51.11.168.160, 8.253.207.120, 8.248.117.254, 67.26.81.254, 8.248.115.254, 8.248.125.254, 51.103.5.159, 142.250.185.195, 142.250.185.227, 173.194.165.167, 173.194.164.171, 92.122.213.247, 92.122.213.194, 74.125.173.233, 74.125.173.230, 52.155.217.156, 20.54.26.129, 173.194.188.167, 173.194.188.168, 74.125.11.9

- Excluded domains from analysis (whitelisted): r3.sn-4g5edne7.gvt1.com, arc.msn.com.nsatc.net, r2.sn-4g5ednsy.gvt1.com, clientservices.googleapis.com, fs-wildcard.microsoft.com.edgekey.net, skypedataprdcoleus15.cloudapp.net, clients2.google.com, audownload.windowsupdate.nsatc.net, update.googleapis.com, watson.telemetry.microsoft.com, www.gstatic.com, au-bg-shim.trafficmanager.net, r1.sn-4g5ednz7.gvt1.com, fs.microsoft.com, r2.sn-4g5edns6.gvt1.com, content-autofill.googleapis.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, secure.aadcdn.microsoftonline-p.com.edgekey.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, r3---sn-4g5edne7.gvt1.com, skypedataprdcolcus17.cloudapp.net, www.googleapis.com, r3---sn-4g5edns6.gvt1.com, ris.api.iris.microsoft.com, r3---sn-4g5ednsr.gvt1.com, store-images.s-microsoft.com, r5---sn-4g5edned.gvt1.com, blobcollector.events.data.trafficmanager.net, r2---sn-4g5ednsy.gvt1.com, clients.l.google.com, r1---sn-4g5ednz7.gvt1.com, au.download.windowsupdate.com.edgesuite.net, r1---sn-4g5edney.gvt1.com, r5.sn-4g5edned.gvt1.com, store-images.s-microsoft.com-c.edgekey.net, r3.sn-4g5ednsr.gvt1.com, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, r2---sn-4g5edns6.gvt1.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, redirector.gvt1.com, e13761.dscg.akamaiedge.net, r4---sn-4g5ednz7.gvt1.com, displaycatalog.mp.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, accounts.google.com, r1.sn-4g5edney.gvt1.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, r4.sn-4g5ednz7.gvt1.com, r3.sn-4g5edns6.gvt1.com, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.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.
- VT rate limit hit for: /opt/package/joesandbox/database/analysis/356247/sample/xerox for hycite.htm

Simulations

Behavior and APIs

Time	Type	Description
20:07:26	API Interceptor	1x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
239.255.255.250	2021-Nouvelle masse salariale-Rapport.html	Get hash	malicious	Browse	
	OneNote rmos@dataflex-int.com.html	Get hash	malicious	Browse	
	Sponsor A Child, Best Online Donation Site, Top NGO - World Vision India.html	Get hash	malicious	Browse	
	barcelona-v-psg-liv-uefa-2021.html	Get hash	malicious	Browse	
	Barcelona-v-PSG-0tv.html	Get hash	malicious	Browse	
	executable.908.exe	Get hash	malicious	Browse	
	executable.908.exe	Get hash	malicious	Browse	
	executable.908.exe	Get hash	malicious	Browse	
	executable.908.exe	Get hash	malicious	Browse	
	executable.908.exe	Get hash	malicious	Browse	
	executable.908.exe	Get hash	malicious	Browse	
	executable.908.exe	Get hash	malicious	Browse	
	executable.908.exe	Get hash	malicious	Browse	
	executable.908.exe	Get hash	malicious	Browse	
	executable.908.exe	Get hash	malicious	Browse	
	executable.908.exe	Get hash	malicious	Browse	
	n8I6klLQIW.exe	Get hash	malicious	Browse	
	M4PzD6DB8W.exe	Get hash	malicious	Browse	
	eWd2XEQ0K4.exe	Get hash	malicious	Browse	
	ZsoqHwHJpN.exe	Get hash	malicious	Browse	
142.250.186.33	Muligheds.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
googlehosted.l.googleusercontent.com	Muligheds.exe	Get hash	malicious	Browse	• 142.250.186.33
	2021-Nouvelle masse salariale-Rapport.html	Get hash	malicious	Browse	• 216.58.209.33
	SOLICITUD DE HERJIMAR, SL (HJM-745022821).exe	Get hash	malicious	Browse	• 216.58.208.161
	#U6211#U662f#U56fe#U7247.exe	Get hash	malicious	Browse	• 216.58.208.161
	OneNote rmos@dataflex-int.com.html	Get hash	malicious	Browse	• 216.58.208.129
	Sponsor A Child, Best Online Donation Site, Top NGO - World Vision India.html	Get hash	malicious	Browse	• 172.217.20.225
	barcelona-v-psg-liv-uefa-2021.html	Get hash	malicious	Browse	• 172.217.20.225
	Barcelona-v-PSG-0tv.html	Get hash	malicious	Browse	• 172.217.20.225
	CONSTRUCCIONES SAN MART#U00cdN, S.A. SOLICITAR. (SMT-14517022021).exe	Get hash	malicious	Browse	• 172.217.20.225
	executable.908.exe	Get hash	malicious	Browse	• 216.58.208.161
	executable.908.exe	Get hash	malicious	Browse	• 216.58.208.161
	executable.908.exe	Get hash	malicious	Browse	• 216.58.208.161
	executable.908.exe	Get hash	malicious	Browse	• 216.58.208.161
	OEVGVSOGAH.dll	Get hash	malicious	Browse	• 216.58.206.65
	executable.908.exe	Get hash	malicious	Browse	• 216.58.206.65
	executable.908.exe	Get hash	malicious	Browse	• 216.58.206.65
	executable.908.exe	Get hash	malicious	Browse	• 216.58.206.65
	executable.908.exe	Get hash	malicious	Browse	• 216.58.206.65
	executable.908.exe	Get hash	malicious	Browse	• 216.58.206.65
	executable.908.exe	Get hash	malicious	Browse	• 216.58.206.65

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VELIANET-ASvelianetInternetdiensteGmbHDE	SecuriteInfo.com.Exploit.Siggen3.10350.857.xls	Get hash	malicious	Browse	• 134.119.186.202
	SecuriteInfo.com.Heur.15875.xls	Get hash	malicious	Browse	• 134.119.186.202
	Sign-979329054_1327186231.xls	Get hash	malicious	Browse	• 134.119.186.202

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	kAZylwSSsf.exe	Get hash	malicious	Browse	• 134.119.186.201
	SecuriteInfo.com.Heur.28224.xls	Get hash	malicious	Browse	• 134.119.186.202
	SecuriteInfo.com.Exploit.Siggen3.10048.21670.xls	Get hash	malicious	Browse	• 134.119.186.202
	SecuriteInfo.com.Exploit.Siggen3.10048.926.xls	Get hash	malicious	Browse	• 134.119.186.202
	SecuriteInfo.com.Exploit.Siggen3.10048.3997.xls	Get hash	malicious	Browse	• 134.119.186.202
	DocuSign_1618411389_250497852.xls	Get hash	malicious	Browse	• 134.119.186.201
	SecuriteInfo.com.Exploit.Siggen3.10048.18578.xls	Get hash	malicious	Browse	• 134.119.186.202
	6d0000.exe	Get hash	malicious	Browse	• 193.42.156.106
	vZKhfBRgSO.exe	Get hash	malicious	Browse	• 134.119.186.200
	hdpnl.exe	Get hash	malicious	Browse	• 134.119.186.202
	SecuriteInfo.com.Exploit.Siggen3.9634.4711.xls	Get hash	malicious	Browse	• 134.119.186.201
	SecuriteInfo.com.Exploit.Siggen3.9634.31858.xls	Get hash	malicious	Browse	• 134.119.186.201
	0zwHgf4MZ6.exe	Get hash	malicious	Browse	• 134.119.186.201
	WlgBUuBdZm.exe	Get hash	malicious	Browse	• 134.119.186.201
	attach-652257188.xls	Get hash	malicious	Browse	• 134.119.186.200
	PFxtDfOJtu.exe	Get hash	malicious	Browse	• 78.138.98.147
	Xi4vVgHekF.exe	Get hash	malicious	Browse	• 37.61.214.188
GOOGLEUS	rad875FE.tmp.exe	Get hash	malicious	Browse	• 34.102.136.180
	SecuriteInfo.com.Trojan.Inject4.6572.17143.exe	Get hash	malicious	Browse	• 34.102.136.180
	IMG_61061_SCANNED.doc	Get hash	malicious	Browse	• 35.200.172.247
	X1(1).xlsm	Get hash	malicious	Browse	• 142.250.186.66
	IMG_6078_SCANNED.doc	Get hash	malicious	Browse	• 35.200.172.247
	fedex.apk	Get hash	malicious	Browse	• 142.250.186.138
	Muligheds.exe	Get hash	malicious	Browse	• 142.250.186.33
	X1(1).xlsm	Get hash	malicious	Browse	• 142.250.186.66
	DHL Document. PDF.exe	Get hash	malicious	Browse	• 34.102.136.180
	ydQ0ICWj5v.exe	Get hash	malicious	Browse	• 35.228.227.140
	r4yGYPyWb7.exe	Get hash	malicious	Browse	• 35.228.227.140
	X1(1).xlsm	Get hash	malicious	Browse	• 142.250.186.66
	aif9fEvN5g.exe	Get hash	malicious	Browse	• 35.228.227.140
	IMG_01670_Scanned.doc	Get hash	malicious	Browse	• 35.200.172.247
	eInvoice.exe	Get hash	malicious	Browse	• 34.102.136.180
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• 34.102.136.180
	SWIFT Payment W0301.doc	Get hash	malicious	Browse	• 35.200.172.247
	Outstanding Invoices.pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	PDF.exe	Get hash	malicious	Browse	• 34.102.136.180
	message_zdm (2).html	Get hash	malicious	Browse	• 172.217.16.150

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
b32309a26951912be7dba376398abc3b	Sponsor A Child, Best Online Donation Site, Top NGO - World Vision India.html	Get hash	malicious	Browse	• 92.204.219.148
	barcelona-v-psg-liv-uefa-2021.html	Get hash	malicious	Browse	• 92.204.219.148
	Barcelona-v-PSG-0tv.html	Get hash	malicious	Browse	• 92.204.219.148
	VM859-7757.htm	Get hash	malicious	Browse	• 92.204.219.148
	Tebling_Resortsac_FILE-HP38XM.htm	Get hash	malicious	Browse	• 92.204.219.148
	Vivaldi.3.5.2115.87.x64.exe	Get hash	malicious	Browse	• 92.204.219.148
	Maersk_BL Draft_copy_Shipping_documents.html	Get hash	malicious	Browse	• 92.204.219.148
	Release Pending messages on account.html	Get hash	malicious	Browse	• 92.204.219.148
	ACH PAYMENT REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 92.204.219.148
	Notice_Admin_Johnstoncompanies_8578.htm	Get hash	malicious	Browse	• 92.204.219.148
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 92.204.219.148

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://r0qp15r0b1rq05rrpbqbrpq5.s3-eu-west-1.amazonaws.com/Ap3dX.html#joetorre@gmail.com	Get hash	malicious	Browse	• 92.204.219.148
	http://https://blog.dericoin.com/wp-includes/shell/ivd/office/office/voicemail/index.php	Get hash	malicious	Browse	• 92.204.219.148
	http://www.secured-mailsharepoint.online/	Get hash	malicious	Browse	• 92.204.219.148
	http://https://alijafari6.wixsite.com/owa-projection-aspx	Get hash	malicious	Browse	• 92.204.219.148
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 92.204.219.148
	http://https://www.canva.com/design/DAESYWKuLHs/avvDNRvDuj_tk82H9Q45ZQ/view?utm_content=DAESYWKuLHs&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 92.204.219.148
	http://quickneasyrecipes.co	Get hash	malicious	Browse	• 92.204.219.148
	http://https://ddghbbf.r.af.d.sendibt2.com/tr/cl/AZ_fzMJRsE3xIeU_QcnTrJNmrQopncatDd-eovbR7xYq9ypiIqtwKWyrTIIdxNfdZBUhEo89L97BvoqW-m0AK8lpY_G1A0R4-OqWFWF7yqRk6lwWGjYQTbxdkNXIPZafVx__3xwAI7RkCXl8CJrNWoLoVVIyiYf1YWtibYMuXAbvq5KxrlLw-G3RcpVIilD2f-TlZx3vckcUFNx1IBpr5JamUxI3ckvzVYmWJV1yS8ZgSAUq_5FOmOxjsnNrYCXLNFt9Ew	Get hash	malicious	Browse	• 92.204.219.148
	http://https://donkoontzdds-my.sharepoint.com:443/:o:/p/paula/EpkEAfrMo1VPgFsywG5EnMwBbr42_dHD8h4N6RCWcat9eA?e=5%3a3JiMMt&at=9	Get hash	malicious	Browse	• 92.204.219.148
37f463bf4616ecd445d4a1937da06e19	SecuriteInfo.com.Heur.15528.xls	Get hash	malicious	Browse	• 92.204.219.148
	Muligheds.exe	Get hash	malicious	Browse	• 92.204.219.148
	DHL_6368638172 documento de recibo,pdf.exe	Get hash	malicious	Browse	• 92.204.219.148
	PDF.exe	Get hash	malicious	Browse	• 92.204.219.148
	pagamento.exe	Get hash	malicious	Browse	• 92.204.219.148
	message_zdm (2).html	Get hash	malicious	Browse	• 92.204.219.148
	Statement-ID28865611496334.vbs	Get hash	malicious	Browse	• 92.204.219.148
	Statement-ID21488878391791.vbs	Get hash	malicious	Browse	• 92.204.219.148
	frank_2021-02-22_02-03.exe	Get hash	malicious	Browse	• 92.204.219.148
	Statement-ID72347595684775.vbs	Get hash	malicious	Browse	• 92.204.219.148
	MR52.vbs	Get hash	malicious	Browse	• 92.204.219.148
	Scan_medcal equipment sample_pdf.exe	Get hash	malicious	Browse	• 92.204.219.148
	rfq02212021.exe	Get hash	malicious	Browse	• 92.204.219.148
	RE ICA 40 Sdn Bhd- Purchase Order#6769704.exe	Get hash	malicious	Browse	• 92.204.219.148
	RFQ-#09503.exe	Get hash	malicious	Browse	• 92.204.219.148
	RFQ_1101983736366355 1101938377388.exe	Get hash	malicious	Browse	• 92.204.219.148
	Offer Request 6100003768.exe	Get hash	malicious	Browse	• 92.204.219.148
	124992436.docx	Get hash	malicious	Browse	• 92.204.219.148
	scarf.exe	Get hash	malicious	Browse	• 92.204.219.148
	Copy_remittnce.exe	Get hash	malicious	Browse	• 92.204.219.148

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

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Reputation:	moderate, very likely benign file
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....I.I6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;/..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....I.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xl@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/l\.cDB0.'.Y...r.[.....vM...o.=....zK..r..I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.077594577114233
Encrypted:	false
SSDEEP:	6:kKhA8oPPbqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:ZAxPW3kPlE99SNxAhUeo+aKt
MD5:	CE513DAD094D650690666EE88181D43C
SHA1:	C618DDEAEC01877AE8562173A5DE59B234B0DECE
SHA-256:	88E8FB761724B23DD3CDD193307C65DD004F1166C8E6739675B77302EA8D1C1C
SHA-512:	BE4C6581EF1E83361F978C37213AEC9CBEC1E69747263EA380B1760B415BEC5BFE1B144173BA65B06462CF383DF9F5C96D45D58F3D1CC1BB06DDA997EAA4BE70
Malicious:	false
Reputation:	low
Preview:	p..... .....e....(..... .....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.e.b.b.a.e.1.d.7.e.a.d.6.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\001102a7-c24d-4173-a7bd-785bc1571c33.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):	155903
Entropy (8bit):	6.051120510599347
Encrypted:	false
SSDEEP:	3072:Zx+9BNyxIauZSIxp/lwiB9oFcbXafIB0u1GOJmA3iuR1:ZxM6b2pB92aqfIlUOoSiuR1
MD5:	68F28349FBC37C84ADDC9C714C600FB6
SHA1:	7923DC398B4058E4514E95A6F3737E52F28F5217
SHA-256:	202A80DD1CF4ACEE07C88AC32B272F1962280519AD521310FDFF8F11E666943E
SHA-512:	33F6FF06FDDA7106E4AEE57A796639DFF26F19E084333CB2DDE1544DD2265CF44B0DD08ECDCE299EB348D970AEFE9CF64EDF3D736A55E470223B57FDBE60967
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\001102a7-c24d-4173-a7bd-785bc1571c33.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.614053244767052e+12,"network":1.614020846e+12,"ticks":96771872.0,"uncertainty":4616108.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016579807"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\17e693f9-593c-4ad3-9b57-0bf545848475.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):	156093
Entropy (8bit):	6.051622549340032
Encrypted:	false
SSDEEP:	3072:Ok+9BNyxIauZSIxp/lwiB9oFcbXafIB0u1GOJmA3iuR1:OkM6b2pB92aqfIlUOoSiuR1
MD5:	E43D8C99FE5F66C5E31CA030FD510EFC
SHA1:	D357A8CCABE058F7751FE447978D3D01683D392B
SHA-256:	D872C12501C3A3031565BD47B634EE518F8C69ABEDB5210D12C3EF5E63A70F20
SHA-512:	46D4FBEED3B360EA524636E3DDF0A06D216848EF840AB7DB6C00EAD43B4BEA0A3361799CC756E721FDAF8ACA3B6709DA02C95F4B1E59A490F4C12494686832D9
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":1.614053244767052e+12,"network":1.614020846e+12,"ticks":96771872.0,"uncertainty":4616108.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016579807"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\2c93ef4b-9f0a-4b67-8e4a-4666324f17e6.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):	164391
Entropy (8bit):	6.081950453540436
Encrypted:	false
SSDEEP:	3072:QZT+9BNyxIauZSIxp/lwiB9oFcbXafIB0u1GOJmA3iuR1:KTM6b2pB92aqfIlUOoSiuR1
MD5:	B72E9C957ADF6317738A854D7CA524ED
SHA1:	AB95B19B133F41FD0AB260C6BAC8F2F30297D354
SHA-256:	D99A0D412B6EC97F2F03A5F2E5C36DE586EDD33D8245669EF053A3EC36A043CB
SHA-512:	E52CB58D77FF7E8F4A9F41A9C7C94BD855ACD3638914D2AA22D7D094CF20F334A8D035EF276F98656141B4A002907F8A7798DDBEE030DF2107DC748729CB485
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":1.614053244767052e+12,"network":1.614020846e+12,"ticks":96771872.0,"uncertainty":4616108.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\36ca6d31-5e37-4d16-b0b9-cc97ec28b742.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):	156250
Entropy (8bit):	6.052170769445067
Encrypted:	false
SSDEEP:	3072:uD+9BNyxIauZSIxp/lwiB9oFcbXafIB0u1GOJmA3iuR1:uDM6b2pB92aqfIlUOoSiuR1
MD5:	EE0653708374FB04E1E9DEFC7176277F
SHA1:	D5D31D9C9317B40E5BFFE620DDAB742945D0B5DB
SHA-256:	3D9D0AB13617AD62144B1202D049BE7069659F68AA1D342D344B54C45CDF246C
SHA-512:	389A39E63ABB373D59543998544072C169F71B702C1D6AAF2C494FD4E34261D31C07AA73BFA28158824A0FC7EF1CA9175F84060F03569EE01951466C39AB2357
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\36ca6d31-5e37-4d16-b0b9-cc97ec28b742.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.614053244767052e+12,"network":1.614020846e+12,"ticks":96771872.0,"uncertainty":4616108.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"132

C:\Users\user\AppData\Local\Google\Chrome\User Data\63850275-7c82-4ea5-8435-7114f72cd700.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	156428
Entropy (8bit):	6.052603250213741
Encrypted:	false
SSDEEP:	3072:uv+9BNyxIauZSlxp/lwiB9oFcbXafIB0u1GOJmA3iuR1:uvM6b2pB92aqfIlUOoSiuR1
MD5:	BEC804C37D4697A6A0BB83061BF1BF50
SHA1:	E29B4A8796339BF8CFA3E3EDF76C2EB3641409E7
SHA-256:	21AC4BF6E7CFD56442EFFEDBBADF6624AD1E4E7B3089A63E843A4898FD2376CD
SHA-512:	CB25941874608145592120B904F0F75F521F965EA0B3C64732393BC683F331B374650EF6C738CE8AA9BF662BD3AD78E6367A32FF2E587B5B2CE7835573320C59
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":1.614053244767052e+12,"network":1.614020846e+12,"ticks":96771872.0,"uncertainty":4616108.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"132

C:\Users\user\AppData\Local\Google\Chrome\User Data\65097fcd-84d4-4cc2-81d3-102cf113f249.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7407477389452826
Encrypted:	false
SSDEEP:	384:JDyth/Q6bAX3VcCR8NhrqvF/3GJfmHnCGSVrAjtJxeDrbKrolmgbgfBtZ6OnntN9:hSSFFizOasenRv383rW/KFjBhJ
MD5:	7F981B69044E92238618848AF1C0B172
SHA1:	C78BFAF029CE7F2CA8E04C73987EB7AF026F7ED8
SHA-256:	43D4686D8AF58E66426AED1E7675EFED7D08B511CABF71C01C31C9D2C65CDC86
SHA-512:	9FEC2BDBAA9ADAB2234FDCD20E59875EEECE35FD0361308EFC6FB97683A1F596C0448F2B69E37A1C04856EF850C14C57275F750708894C39DB0FAFCBAA53D5CA
Malicious:	false
Reputation:	low
Preview:	.q.....*...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...l28.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\7bd0fecb-0671-44ea-b8af-79b2e901fbb1.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.740711148200182
Encrypted:	false
SSDEEP:	384:5Dyth/Q6bAX3VcCR8NhrqvF/3GJfmHnCGSVrAjtJxeDrbKrolmgUegfBtZ6OnntZ:xSSFFizsasenRv383rW/KFjBhr
MD5:	B18768F86885EA71636FBE93B2EC8401
SHA1:	EA801DC84A4FA53C4DD740E56B71E5176595EA1B
SHA-256:	FA4C831DB95F4F5AB0B33B293D577ACCCAFA5EA8EC98BBA7A2DB54D9D9011381
SHA-512:	C78B5446000F586ED75650372A6E5123FEB8050B4FD53621942C57B40F40BAD28B3A619DA19D3B11647E99B1A143750B2AE3DCEFFD9945C0950A05F122786046
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\7bd0fecb-0671-44ea-b8af-79b2e901fbb1.tmp	
Preview:	.t.....*...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...l28.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\..... .m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o .g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\7d0999bb-a852-4fef-b148-451c6f32d392.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):	164391
Entropy (8bit):	6.081951444140935
Encrypted:	false
SSDEEP:	3072:Q/8+9BNyxIauZSIxp/lwiB9oFcbXafIB0u1GOJmA3iuR1:Y8M6b2pB92aqfIlUOoSiuR1
MD5:	38D3653D9D2750B63976CBF6FFC9A5DD
SHA1:	2E199158B337C082AB18513E258CDF915E62A5A9
SHA-256:	6F6620966249077D2B3FB91D0F4A5057E66F0D076D32D62CE87D12C516B27094
SHA-512:	81E0BE5EB834200BF6C5DE574AFDBF2573362BEE2920D96735F0592907BCDBD3EEB69FCEA3686A2BC666CB27E08433B73219CBDB99EBE58E8B08353AF03973 D
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":1.614053244767052e+12,"network":1.614020846e+12,"ticks":96771872.0,"uncertainty":4616108.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"132455951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\81c27780-15e0-4c46-8f6b-5fb750f8a238.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):	156344
Entropy (8bit):	6.052445630249435
Encrypted:	false
SSDEEP:	3072:un+9BNyxIauZSIxp/lwiB9oFcbXafIB0u1GOJmA3iuR1:unM6b2pB92aqfIlUOoSiuR1
MD5:	937ABA308E30F8AF81CFCC894C9E0C0A
SHA1:	4DDEF02A96CB01407F257190572613684717229A
SHA-256:	14D3DF50BB9FEE78F72DC3675D43F1E14931BBEF0CB964E0E8C635994E5F0AA7
SHA-512:	7FBAF258CBD7815E62BA618C08E3E2E29FACA01E8418ACC77BDE20988EE82E9DDDCB4C44207F202AB3CB329C3D3645947DCC64EB07026BD9487A3275A8867A 9A
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":1.614053244767052e+12,"network":1.614020846e+12,"ticks":96771872.0,"uncertainty":4616108.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"132

C:\Users\user\AppData\Local\Google\Chrome\User Data\9dd8c7ba-7749-4c80-a969-9b6b2a10dcbc.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):	164391
Entropy (8bit):	6.081952493641131
Encrypted:	false
SSDEEP:	3072:J/8+9BNyxIauZSIxp/lwiB9oFcbXafIB0u1GOJmA3iuR1:J8M6b2pB92aqfIlUOoSiuR1
MD5:	0DE84C68BCB5824A6E562D88B8D0F53B
SHA1:	4D37B7014A259848D41FF8DE5FE80A3FF3B38A2F
SHA-256:	09428D8CDAB02E3A41757264A5617AA90BD53B0A427C078D0C3E0E0618240E2D
SHA-512:	767981110BDC25685403A954B334D05F3875D507A11CF488706AE8786FCD2DF7F2868CF4BA73045AA098BD19D39AA92ED10248507927DCCAF8CF2443014784D3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\9dd8c7ba-7749-4c80-a969-9b6b2a10dcbc.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.614053244767052e+12,"network":1.614020846e+12,"ticks":96771872.0,"uncertainty":4616108.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016579807"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftIE1G1mkftIE1G1mkftIE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D021294256372C916B8155AC
Malicious:	false
Preview:	sdPC....................s}.....M..2.!..%sdPC....................s}.....M..2.!..%sdPC....................s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\49549b0f-c9a5-40d2-8079-c22f7b317658.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):	5.577654456486878
Encrypted:	false
SSDEEP:	384:+axttLlzIX/1kXqKf/pUZNCgVLH2HfDyrUqQYGm4n:lLl2/1kXqKf/pUZNCgVLH2HfOrU2Gm0
MD5:	D6E4A168E2967B2CA9FA0987B64D2D27
SHA1:	C839B17FFA880742F89F11F87453571FD15A5786
SHA-256:	349A86C8FAA9FF34B6D31306BA1A9D54A1195F87A2221F86711C71AC41927207
SHA-512:	E1672D83FE9189AC978AA956AD49DCD770DE7383D1A1B43D2E1072947C176F99DC36278788F1D3F79DEFE96FC5173AC2ED504C9EF260EC24826D7674285011E
Malicious:	false
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":"13258526841598204","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/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\566188ca-3e3d-4691-84ab-775fc032e1b2.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):	5414
Entropy (8bit):	5.164783808939215
Encrypted:	false
SSDEEP:	48:YcRnUkPklwHjRi2cuqAiRqzbE4lYqlQuoTw0WH3CH3O/s8C1Nfct/9BhUJo3Khmx:nDO/94zbfcVqok0JCKL8VbOTQVuwn
MD5:	C5B0D240F31C46027F012068675A7058
SHA1:	4FF3535901D8B741E048F497C3AAA46F5DCEB6E6
SHA-256:	83749EE6AE5CEF81F264420802F24DA78E3BD67F08CE8C1D0184FA5FD8096A79
SHA-512:	356AA146AD7CFC83E9CDE1B8815BF69A8D893C63976FA5BC70AFAD1829DDBBFA232C688F0FB86E1F7D9C38D2F19C6F463262A3F4A26F0D8F719FD74464DEB0CE
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13258526841920702","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","7355378"],"daily_received_length":["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\6151a037-daac-4c88-b48f-47c7245b2452.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6151a037-daac-4c88-b48f-47c7245b2452.tmp	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4783
Entropy (8bit):	4.951355722833275
Encrypted:	false
SSDEEP:	48:YcRnUkPklwHjRi2crqA8RqTlYqlQuoTw0WH3CH3G/s8C1Nfct/9BhUJo3KhmeSnz:nDOGX4pcV6ok0JCKL8VbOTQVuwn
MD5:	3D60454F7CF0FC2584E19291567A776A
SHA1:	8A8534333C21A670738A14B13780C256F7667179
SHA-256:	3E162EB94163B8AD8D675DA9FE9DFB55E7C953D07ACF2D50B4055F38EBC1DCD5
SHA-512:	3F13035EA2A015E74330F025BFC65FA51DC689544850A1A068CFFC6D80E84077C6922BF02FE22983F69826B8652AB08554179941BCEF75DD18AF996E142BEF08
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13258526841920702","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","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\65dc9078-a0e1-4f0c-b4b3-b362348565cc.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):	5.535569353479038
Encrypted:	false
SSDEEP:	384:+axtELlzIX/1kXqKf/pUZNCgVLH2HfDyrUdHGpnTAQ2Gm44:8Ll2/1kXqKf/pUZNCgVLH2HfOrUBGpnM
MD5:	4F8F876313AB09DFBBDE0E5F1E6B3ADC
SHA1:	3C2EBC2175548D10FD02AA1B3899DABE2A936C90
SHA-256:	F9897AFCAE2858A681E1B093AAC9AF3CADCA047C672EC6E084C356D53FFB9150
SHA-512:	67E8F028986CA9D9DA0FEBC5924FF8509E5FCC881313EB6050CF42325AA1BF41BAFA2ADC0B8F4E813F6EB4759FBFB8E5C6BB4CB948937665D70963B479BE392 1
Malicious:	false
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":"13258526841598204","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/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8a241a21-4cf2-458f-b1f8-ca5795f960ff.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):	5439
Entropy (8bit):	5.16614401528613
Encrypted:	false
SSDEEP:	48:YcRnUkPklwHjRi2c3MOqAiRqzbE4lYqlQuoTw0WH3CH3O/s8C1Nfct/9BhUJo3Kb:nDOs94zbfcVqok0JCKL8O/bOTQVuwn
MD5:	5B1B9138C8CB728F36F21879A12AECF4
SHA1:	1245F527A93F101B6999DA8210BF8AF1DC4CEDB7
SHA-256:	D613B8D69CCE4951B0DAD72CC22BE33F4EA252C6341D3A7EE9D239CEAD4195D7
SHA-512:	372A870D28BCB3E0C56C0E39B21B73F05311BC49EF6CF990C659609F16D7EA0C852648EA7E7465ECD1504A7C776B598C147C759CAEEB39146CF1BB855B96889
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13258526841920702","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","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\917c4f24-2a5b-4fb1-aa7b-7f28003ed308.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):	1205
Entropy (8bit):	5.585873843804817
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\917c4f24-2a5b-4fb1-aa7b-7f28003ed308.tmp	
SSDEEP:	24:YI6H0UhVsTG1KUerkq/HeUeXby2qUeXvS7wUOcWINwU6RUenHQ:YI6UUhVseKUewqPeUer2UefcwUaINwUJ
MD5:	E15046274866142778D9A15FB5EC7B55
SHA1:	FADB93A1031F283EA38BA222871F32491C4CAC99
SHA-256:	BC1ADB44F9285B05ED5C33AE31E28BC022271EC9853EC802B84D1484D3E0E647
SHA-512:	53D480F40A255AC9722FAACF8C7096874669B64E8B6284C1684E8F7835333D013494465396E2192E55352967643766C9342479DCAF6027B1F0AB3D7B16F687C6
Malicious:	false
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_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1645589244.50537,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1614053244.505372},{"expiry":1645589249.29364,"host":"+LCYPikJxOjeTMeNwsPDpkFmxWXugWYr8RjEVTinl5c=","mode":"force-https","sts_include_subdomains":false,"sts_obser

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\94d628e7-228b-4248-96e6-14065bc38f81.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
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.239555354626245
Encrypted:	false
SSDEEP:	6:mQOUcQyq2PWXp+N23iKKdK9RXXTZIFUtp9Qz1ZmwP9QlRkwOWXp+N23iKKdK9RX3:NOFVva5Kk7XT2FUtp9Qz1/P9Qz5f5KkT
MD5:	54653E4213FDFCD417D46F2342CC8C6F
SHA1:	468ECF5715A7F97AD408272AA9C8F2CC9BDAE0B6
SHA-256:	C5026C72B18790F924DBDEAF322EC235DCE2E10673A38F729E9A7A7C7F712AD0
SHA-512:	061C8A62E24B68B38EC6A3356B360599E5935139D716615079FE54BB520D037B2BD9C150E6E0FD221B406E2C2952026760A827F8A6BBD3CF025354FACBE841C8
Malicious:	false
Preview:	2021/02/22-20:07:34.645 1990 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/02/22-20:07:34.648 1990 Recovering log #3.2021/02/22-20:07:34.648 1990 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):	5.185484723464589
Encrypted:	false
SSDEEP:	6:mQycFFc9yq2PWXp+N23iKKdKyDZIFUtp9m11ZmwP9amlRkwOWXp+N23iKKdKyJLJ:N7cAva5Kk02FUtp9m11/P9au5f5KkWJ
MD5:	3755F480F7134DB05E09DEB769FC45DC
SHA1:	E33557DC08A8382A549C099997C011A99976EBDD
SHA-256:	E12102ABC816374599AEFAFFB48F4D0DDF7A5C9206A599D439D0998A10EA1947
SHA-512:	509AFA2F6A892D1000D738AC3A2C429C3E4C363563F96AE0995655D2A7AD8B8CE62B34BCFE843B978430A5D9658366348AE3596B9AD0640912046543AAFE44E8
Malicious:	false
Preview:	2021/02/22-20:07:34.639 1990 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/02/22-20:07:34.640 1990 Recovering log #3.2021/02/22-20:07:34.641 1990 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1aa724cf792052df_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.467541305648812
Encrypted:	false
SSDEEP:	3:m+leH/08RzYrSL37BAIury2AWKu+sRWXM4BA39E+H/lHCQzvlJMWgVKODWuWmHkJ:mTYGLKIOyHsJBS+HgQzv/XROlHGK6t
MD5:	681AB8998CECF177ACB103F0BD78D036
SHA1:	F3D8B3ACE459067139E73168D6386D1C5E7E63BF
SHA-256:	CDE6B76C1B9C4758916D4E8EFCF960A39CFDEA1EA735446A9E3FD8AB84775D50
SHA-512:	E45E52B2F4E446027ABEE622CB17A7DB1E6E68FA717566EF134BA9C712E8CFE89ADCAA964BDC43386A8AECD19D9F2CC218B8691B6C8078D92661D4B6C0CE8ABC
Malicious:	false
Preview:	0\r..m.....N.....$E...._keyhttps://www.curryhut.de/vendor/bin/data/files/enc.js .https://curryhut.de/K..W../.....T.....S=~....Y...s..?{s..0./....m. ..A..Eo.....Fq.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	264
Entropy (8bit):	4.636630429964995
Encrypted:	false
SSDEEP:	3:GLyy/LlHlcet0WFWz/lll50FZz/lllK7u1Zlh/lllsu9KR8lhtOurlh/lllWNRQz:Tg4zQ3zbn3pHkQ+IRwHzCl
MD5:	E72D6C03186A3574C95174086C468826
SHA1:	AD6EAEC03A313E7FFDA6E92329C8A3E6C8F201F9
SHA-256:	9629AAD5DB73B1E8DB1E0413E2E68649AF9FDABD549817041ED9D47D8ADEF8AA
SHA-512:	F110E6FD431FFD3DBEC05BD74C94C7D3CA0E3689EAA2D0C91E65F19C66B6E121124908636BCA107B5A029221CC2959F680563575124E467D1E37CAD210A41F1
Malicious:	false
Preview:	....r...oy retne.....R y.$... .W../.....^}.Np..@ikt../.....-..0..x@ikt../...../...3.KPu../.....KPu../.....&<..\.O$.KPu../.....p..(....KPu../.....q...._.KPu../.....+<P|...X.KPu../.....u..W../.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	1.315788237922013
Encrypted:	false
SSDEEP:	48:TekLLOpEO5J/Kn7U1An2JB4WjmCjPU/NOZTZCjVP:dNwinmB4gmeMOTZeVP
MD5:	D53866800EC84C040AB450BBA1DF6E0C
SHA1:	27D11594128CE981639A3CB08516782FD83A2075
SHA-256:	3E151E1C282174A81F877AA9BC70013AE0ECCB8062461E464FA8B1B2EA92D9AD
SHA-512:	4990E5CBC587F0EE890434BC933AE2C7C26CB5C2CD1F6DA89BC13B4DD238F434671D215B67189183A6423DED0F145F1363B76FC2812230AF4D1A627D29E76A0
Malicious:	false
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):	0.9694325433212604
Encrypted:	false
SSDEEP:	24:HcLgAZOZD/BNfqLbJLbXaFpEO5bNmISHn06Uwp8:H8NOZBNfq5LLOpEO5J/Kn7US8
MD5:	2EEB606AFC283256E37A864A15652DBF
SHA1:	257409835CB54FD7368DC7EF2F94D5C521C8C502
SHA-256:	2B58261F2AB04CBD2E93037792778E0551BBC19F50F764C09B42EAFBC6130775
SHA-512:	A58CA685405D4552CFB07112EFE7A64313B056C3EE24FE91394F2DC6D351018F97F79522BF25FD7D01BC82CD3B3CBC2218A8FA0891B244B3A49634B6E552F03A
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Preview:	....

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):	4386
Entropy (8bit):	3.539655558934335
Encrypted:	false
SSDEEP:	48:34uZHxavA87cAI2B+yKXHqLvA87oImyKpyKXHlXI2BmI2BYUMHYAIs5yKLIpJ:34D5IbXHKkIofXHlXl9lXZHfIsvLIj
MD5:	196FE268D8D0E6D731C00E60F3A1F0B3
SHA1:	8C846AB04D4F5E3EEA5C08B44871C8C85E6D68D2
SHA-256:	6B19C3C93E536F7FA5047B8A49A2E771285E8F1D3AA4F1BF9BD4839CC54CA898
SHA-512:	DFB2A933673517CF4561D152F249A9C75929C78D26B7B337E6A6A0C45D308B8ED26ABBA163EE602B51EBD77F4C079BAB7A0EEE0D9A9D9D9076F0162F611BC5C
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...98370015_59ea_4866_b52a_91ef2f39c5e6.....L..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....7...file:///C:/Users/user/Desktop/xerox%20for%20hycite.htm..... .....h.....`.....8.0....9.0.....0.....v...7...f.i.l.e.:././.C.:./.U.s.e.r.s./.h.a.r.d.z./.D.e.s.k.t.o.p./.x.e.r.o.x .%.2.0.f.o.r.%.2.0.h.y.c.i.t.e...h.t.m.....8.....0.....8..... .....7...file:///C:/Users/user/Desktop/xerox%20for%20hycite.htm.....I..V../.....

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
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:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491A
Malicious:	false
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):	320
Entropy (8bit):	5.164638042060924
Encrypted:	false
SSDEEP:	6:mQCEQ+q2PWXp+N23iKKdK8aPrqIFUtp9lEgZmwP98SQVkwOWXp+N23iKKdK8amLJ:NRQ+va5KkL3FUtp9lEg/P98SQV5f5Kkc

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
MD5:	09647937D58EA056395D5CAA7601694C
SHA1:	268398DAD7C92E5D92803F0EC75C4CA21EDF47BC
SHA-256:	E3DCA8F15FCB797D7A5F60FDF42DF001CCD25D49B586C2D621F36D5306C46F49
SHA-512:	B9BCF415CF8BB26BF9D7F7AA453433A20B18A723A86EB32A7A997C604423E78DB49C7C4130B6A8144EAE204B10D570818B4771A10C7CA5F205BE7C33269D2CF 8
Malicious:	false
Preview:	2021/02/22-20:07:21.927 19bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/02/22-2 0:07:21.928 19bc Recovering log #3.2021/02/22-20:07:21.929 19bc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.203307876731422
Encrypted:	false
SSDEEP:	6:mQV0kSQ+q2PWXp+N23iKKdK8NIFUtp9TF9pgZmwP9TF9pQVkwOWXp+N23iKKdK8n:NV0nQ+va5KkpFUtp9Xpg/P9XpQV5f5Kb
MD5:	DF82AE0F085443DCC05FA52C98A5705E
SHA1:	B6CF66193C14E14A41539C83F5EE99BAAA534925
SHA-256:	48717EFED0C80C76A0587DA1C3D20ACC33A930D16D31DB64EC632EFAB8B94430
SHA-512:	E84236746F0FF9FE1AFBCDC6FF46F2EBBEBCE1AE27F6E1DE45942246CCA3D05C09299B6AEE4C15D303A0DDAF22579524A4D21060DDB85131A2312BF076F187 5
Malicious:	false
Preview:	2021/02/22-20:07:23.959 19bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/02/22-2 0:07:23.961 19bc Recovering log #3.2021/02/22-20:07:23.961 19bc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\comput ed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvuI11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQlOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRITANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.6075203471273571
Encrypted:	false
SSDEEP:	96:yBCwIl+I4I09eh6I5IQ090SIMI9gIu9enIeI0:Irep4UoeL
MD5:	217D0A0A4ABE61A5934C1FE3FA2B7792
SHA1:	8B5E52835954D9822311FCF6371D73875B05D0A9
SHA-256:	233F3AB63D4458EC827A11AD7547FEFBC6D4551AEC843BC1B7B7A400200EB9C0
SHA-512:	4769E21C65736F65BCDDE951C83A9A8C3F3C6D704C8B63F353C0CA7319BCCED2B3F546D1D1EEC24F41B3018A535116001E714661FBBD76E2834CBC29422FBBD
Malicious:	false
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):	0.7750646205077614
Encrypted:	false
SSDEEP:	24:wuyLiXxh0GY/l1rWR1PmCx9fZjsBX+T6Uwa3n:wudBmw6fUt3n
MD5:	5CE751AEDEE6F85FACB54005C6D4FC3D
SHA1:	CE1F37C9933B7F3958CEFB22DD02D857D262E02E
SHA-256:	27C29770EF38217EE14BF60CF686C8F38561E94FE7DC6FC5E050BF7C39290A84
SHA-512:	99FD38677560459AACE5723C6891DF593460D7CA1294076C23AEBF63CBF71E6008F9E1BB93C85CD64A7B5DE1FF272EE15919FEF4D332F60B2544F424E6F66F40
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Preview:	.....A1U..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
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):	5.261056922776248
Encrypted:	false
SSDEEP:	6:mQYFMlyq2PWXp+N23iKKdK25+Xqx8chI+IFUtp9kz1ZmwP97jRkwOWXp+N23iKKN:NYFMIva5KkTXfchI3FUtp9kz1/P9J5fk
MD5:	965D967B37EA3FCFE5575C52A96ECEF0
SHA1:	6EFFD08ABDBE98BB185DBE12CA3A4CBFC737145A
SHA-256:	559E0CC1E221E3A9D04E350B4142E04EFA0251BD79D431D2C32B5C773832BCFF
SHA-512:	0CE66BF49DB446E1B639C6BCCA68094E22805731D6E1F5F4625577C9A4C4B761867CE8709D3DAA7855DD4F8CD20856967C492B58C5655D4002EC80F37AEB229
Malicious:	false
Preview:	2021/02/22-20:07:34.588 1990 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/02/22-20:07:34.608 1990 Recovering log #3.2021/02/22-20:07:34.609 1990 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):	5.214350664865541
Encrypted:	false
SSDEEP:	6:mQUQ9yq2PWXp+N23iKKdK25+XuoIFUtp9AU11ZmwP9alRkwOWXp+N23iKKdK25+Z:NURva5KkTXYFUtp9AU11/P9i5f5KkTXp
MD5:	F18BE1F1820630A216FB6B9DB6129464
SHA1:	E03620239446B9239DEA9DEBC0E31133DD8FD423
SHA-256:	C468FDDB1FB874FA08AFD331DEB956985A84FBB0846D77E841C1A7C6D9EB515A
SHA-512:	882BF3E9C11FD16AF1A056A6AD9754C0D95C3884CAD161B1F66B23457530FBE6B723E2ECDE7B82F572C80DD25573FC2AEAD6CB9FC9B9741245BF0C791AE7F12
Malicious:	false
Preview:	2021/02/22-20:07:34.579 1990 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/02/22-20:07:34.580 1990 Recovering log #3.2021/02/22-20:07:34.581 1990 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):	5.2161491802924385
Encrypted:	false
SSDEEP:	6:mQMyq2PWXp+N23iKKdKWT5g1IdqIFUtp92AFz1ZmwP9yRkwOWXp+N23iKKdKWT5i:Nhva5Kkg5gSRFUtp9311/P9m5f5Kkg5i
MD5:	7946B67226B79A981C30E1C3B9FCB938

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
SHA1:	7633F182096FD44233E998CB5CFFC87D6AD0BD60
SHA-256:	24F13824ACF09BC1FA60081915CA4AD8967DD95D60F9AA69230C40AE730166EE
SHA-512:	B364A8F4D77551853A5F76FE276FA6A2E3EEB340366EFC8E31BD0E95EF93B8C68D5A68510566C3ED4B9B75E779AA4C760430C5BABBF668029793C58A68FF353
Malicious:	false
Preview:	2021/02/22-20:07:34.550 1990 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/02/22-20:07:34.551 1990 Recovering log #3.2021/02/22-20:07:34.552 1990 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\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.45488079341118026
Encrypted:	false
SSDEEP:	3:8Eflm:8
MD5:	4B9AB4DC12D5246329497A76EB553BD5
SHA1:	0415D80E8AE00BEA421DDF7ECC92422F9CDDAEF8
SHA-256:	4B7817C2FA075CACAC79573839087D22190244633E16B68F79BFD22EED638408
SHA-512:	FEA5E89716C972E7972068275B1B6B0C23B3EA68835905899B7424478E357827CEE9340AAB8F02C4658AA8F4F12322BF6686E3540757A00150F2920465B1979B
Malicious:	false
Preview:	.'..(.....qX../.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.5645343605447697
Encrypted:	false
SSDEEP:	48:TdKIf49Cjg02I2BW0kbI60a9Ib0dUaLd7f2wztICI2B+IMFII9Cjk:YIg9eYItbIgIdUqktICIDIMFII9ek
MD5:	9934711535FDB412DC052CC3D9EB4263
SHA1:	675210D99B7929D46694AADE0B45E7DDC8E1C548
SHA-256:	3A959266F6E04EE30935AD5DF6982267D6C5728B0F8353A3E606F70D191DA572
SHA-512:	0697FD1770824B783D8CB81939C64DB1BB69D0EB4054BA3C7C2960133F96216F53295D0D6CB2D88ACD82F66EB3DDB79675B4B2E70DE2A3E38B01B86767BDE15
Malicious:	false
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):	2392
Entropy (8bit):	5.962053592335242
Encrypted:	false
SSDEEP:	48:bCNAlYI7yxkzXH5mGFOZi0uW41zuCqBdnR/S0pIj9CjLCISnIEWI2BMvyz6HtW:b8aYZikzXZhFOFwbqrR9pIj9emIyIxI8
MD5:	5F23260700BEF55A19255334D2B860CB
SHA1:	879820AB2FC1016416761BD401A24BEEA366EB1B
SHA-256:	0A6CF5AF584F2808539523AF8BF63C31899C1C7F6A9922609B4237846010D654
SHA-512:	91FF0658EC5FA7C9701C54408CA589075D193942607831D18CDBA634EEE96BF75BFD872EAB4B3CB3BE00286160314EAD9EA8F01126680171904262A2FAA329EE
Malicious:	false
Preview:	....."..."..bin..common..curryhut..data..de..enter..https..login..password..vendor..www..your.%66d676172636961406879636974652e636f6d..br..com..euro2..http..hycite..inbox..mkanet..protection..safelinks..2..ea..ss..php..c..desktop..file..for..user..htm..users..xerox*..."....2...).%66d676172636961406879636974652e636f6d.....bin.....br.....c.....com.....common.....curryhut.....data.....de.....desktop.....ea.....enter.....euro2.....file.....for.....user.....htm.....http.....https.....hycite.....inbox.....login....mkanet.....password.....php.....protection.....safelinks.....ss.....users. ....vendor.....www.....xerox.!....your..2..."....0.....1.....2.....3.....4.....5.....6.....7.....8.....9.....a.....b.....c.....d.....e..... !....f.....g.....h.....i.....k.....l.....m.....n.....o.....!....p.....r..... !..

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Category:	dropped
Size (bytes):	42076
Entropy (8bit):	0.11655354723484354
Encrypted:	false
SSDEEP:	12:7/z4w4qLBj/563lM4nMWQA9LBjBQZ8fO/:jmqLBg3TbNNTfS
MD5:	56CE5F0DF385DC49B9B03B301A649E98
SHA1:	DD37F8F63FCCC48EEFD9FC59519A5D2BED7D597A
SHA-256:	080D7A0F9384A6CF4B7671B62922E5B9B731D1CB2E1121CDF127539968B11ED6
SHA-512:	26FD3E540416B05C7665ACF2C758A94833F17B3D58C976B7A4991B69D6E53DD98A34B21AB58CBEB23D733D139D86783D263D287F720215656E49451DB84C6BAI
Malicious:	false
Preview:	.....K1..... ....

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):	5.4617422530565
Encrypted:	false
SSDEEP:	48:DZYHGdh3a7GMl8dbIKadbQSefgG+NrS0U9RdiN9aZd:DzNa7GM+dbIKadbQ5fgGyrS0Kd
MD5:	7F0E0706A32AFA8311341B277E52D887
SHA1:	344D5EDB14A63A12DEE253188533DD5BC84F904F
SHA-256:	37D51BC53811CD37DBA8AC628268687B453AFB940C69A83F8B8B69F97CD67ACD
SHA-512:	A0A9D9507C8B54E336108FA1B2CE89E649C9F64C98122BED9B015C1A3CC6BB8C978441F10C2B5924A87FDF398AB689BF274082EA395A8D237800DF0176CCD9E A
Malicious:	false
Preview:	.;.I...*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.Hangout SinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast .RequestIdGenerator..204560000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-02-22 20:07:36.39][INFO][mr.Init] MR instance ID: 84b46e68-a3e1-45ce-b1bf-58bae239ab5d\n","[2021-02-22 20:07:36.39][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-02-22 20:07:36.39][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-02-22 20:07:36.39][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-02-22 20:0 7:36.39][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-02-22 20:07:36.39][INFO][mr.CastProvider] Query enabled: true\n","[2021-02-22 20:07:36.39][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):	332
Entropy (8bit):	5.095835890890869
Encrypted:	false
SSDEEP:	6:mQp+q2PWXp+N23iKKdK8a2jMGIFUtp90sAWZmwP9mVkwOWXp+N23iKKdK8a2jMmd:Np+va5Kk8EFUtp904/P9mV5f5Kk8bJ
MD5:	50CB1AA5089D0BD35214FBDA6748F287
SHA1:	69C50AC4700E9782C1439E7EEB7EF9BF9EAE8456
SHA-256:	15836418A4DAA7075C8762541924B47914821722BF030E9215C014BF8DAB68A7
SHA-512:	DBF2E5A333BC4F512F9718AAD99853CA1A8DDE018473BF576C11896E0152F77D8516D40993FF3A500BC47FF3076A2BA761EC17C2BEBCEADAF57C9B9309775C 7
Malicious:	false
Preview:	2021/02/22-20:07:21.627 1a0c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/0 2/22-20:07:21.629 1a0c Recovering log #3.2021/02/22-20:07:21.635 1a0c 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\Network Action Predictor	
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):	24576
Entropy (8bit):	1.115970434049188
Encrypted:	false
SSDEEP:	96:vOqAuhjspnWOtytdofOqAuhjspnWOKfyS0Ipn:HFALHX
MD5:	E2096092DB3587978D0F95994B183282
SHA1:	39ABDA5CD773B9F1CDE7C6A510A11435D31F20A6
SHA-256:	D68D0695A41BED98B4F2B6169BA3B1900A7A7401D59CFC8A288E0EA17C77C113

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor	
SHA-512:	B3B1B98CA0755F0E120E78B0DFA474A6DE774555844B881B5FEC3FF68215FA342360BBFF6D20D93591FC1866D5B1A1AD2BB6A9E6E7C76622162CF8DE686C281
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....,.....\.t.+.>..,..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	25672
Entropy (8bit):	1.0196526891181517
Encrypted:	false
SSDEEP:	48:xIq7w/qALihje9kqL42WOT/E9qrw/qALihje9kqL42WOT/rt8:xIUOqAuhjspnWOwkOqAuhjspnWOm
MD5:	0725B6929FF47EA7D3E50D4AE3D05047
SHA1:	60AE06F0351335D1830A5CEF807CE7FFB9499DE7
SHA-256:	5FAA36A7B5D821690F11A4CB90EFD19CE9FE6EEF71AB32BB64891538E6B97D30
SHA-512:	3DD58A0AE43A148E3B3E12A431442AA14CE323DA6AF244E64AB3E97593052F316FC1FDFE63B5997F358D65FD6612DFC1C0BA107DC50C3867391620CA21F9A9E F
Malicious:	false
Preview:	....

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):	5.200245407307342
Encrypted:	false
SSDEEP:	6:mQHSQ+q2PWXp+N23iKKdKgXz4rRIFUtp9YgZmwP9aEQVkwOWXp+N23iKKdKgXz4n:NyQ+va5KkgXiuFUtp9Yg/P95QV5f5Kkt
MD5:	4574FA135BA6ADA03C7B9A3914876CC5
SHA1:	88176F5D5F9DEA8241309E813542A0C6BA83BAE9
SHA-256:	4B2B1AEC95652BAE616094CEB4320AEB147458F7FA5DD2B75AF149E25005E422
SHA-512:	817B415E41E1D20C6497CEAFE17AE30B5336AF1223F277A396C8AA28FCAB16CE8EA5ECB8E3207144E0EBADD10258DDF10675AFD704E5E0CD75759D4C6BA58(ED
Malicious:	false
Preview:	2021/02/22-20:07:21.959 19bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/ 02/22-20:07:21.962 19bc Recovering log #3.2021/02/22-20:07:21.963 19bc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Noti fications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljl:5ljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946 B
Malicious:	false
Preview:	..&f.....&f.....&f.....&f.....&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Entropy (8bit):	5.069940999791522
Encrypted:	false
SSDEEP:	6:mQ+5+q2PWXp+N23iKKdKrQMxIFUtp9QZmwP9AVkwOWXp+N23iKKdKrQMFLJ:NW+va5KkCFUtp9Q/P9AV5f5KktJ
MD5:	75A8B2903C89DDAAC596E38C4C453EEC
SHA1:	C8AFFB5A3FB1E11998F67156416C9398E1A0F72D
SHA-256:	CDABE53278A68BE8476DB6E4BF2BB37691703C7899F21BEFDAF11E0A572D787E
SHA-512:	85A12855316CB32190E0A18161AFC21F49E9117285B772B6FC6B643CB7F9015C5DFD0121B8EE4057E04E92301029F92B9C612A9A7C1FA4A2179F25BB6BE5DD20
Malicious:	false
Preview:	2021/02/22-20:07:21.840 1a2c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/02/22-20:07:21.842 1a2c Recovering log #3.2021/02/22-20:07:21.842 1a2c 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):	348
Entropy (8bit):	5.125109236754695
Encrypted:	false
SSDEEP:	6:mQE3N+q2PWXp+N23iKKdK7Uh2ghZIFUtp9jZmwP9XeNVkwOWXp+N23iKKdK7Uh2w:N0Iva5KkIhHh2FUtp9j/P9XG5f5KkIh9
MD5:	8B65E49343244A1859A00A4DA4A27D10
SHA1:	46FD6C7F0D0E1F1526FB9EE31072376B86E4037C
SHA-256:	A7708AE76AB8798EF955A6EFBF92D3BE09DBF0CCB7946AD322871F23CEE2AB2A
SHA-512:	D5495B7B7FE618E1717E6639727CF73F196E4807813A2938BE2094E9E9DFC1BD2C1BBBC55C5EA9329EE9FC457E9C1FD35CE7312D735B960A2400DC5B47D55C58
Malicious:	false
Preview:	2021/02/22-20:07:21.608 19c8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/02/22-20:07:21.609 19c8 Recovering log #3.2021/02/22-20:07:21.611 19c8 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\81597e5e-51ec-4e46-99d0-380bb257020f.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
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.168379886798166
Encrypted:	false
SSDEEP:	6:mQF+q2PWXp+N23iKKdKusNpV/2jMGIFUtp9rZmwP97VkwOWXp+N23iKKdKusNpV0:NF+va5KkFFUtp9r/P97V5f5KkOJ
MD5:	BE2AF2E5925271490BC5790BD4B796FB
SHA1:	C1370863BDC1D6B1ACD9646227B713CB1ED59C5A
SHA-256:	76532114174CC4C138B096F0D1EC9477941CB28D01073495D2A0826B800EC478
SHA-512:	32380E8B02922B32F0DB82431A57BB4BEDF887164DB3DA570A51CEB0B817E683DBED35C1FA7165C2E9CEEF53ACFB313799B6CF46741198235AC758D790A4573 6
Malicious:	false
Preview:	2021/02/22-20:07:21.908 1a2c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/02/22-20:07:21.911 1a2c Recovering log #3.2021/02/22-20:07:21.911 1a2c Reusing old log C:\Users\user\A ppData\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):	432
Entropy (8bit):	5.271902871056194
Encrypted:	false
SSDEEP:	12:NrM+va5KkmiuFUtp92/P9xjMV5f5Kkm2J:Nda5KkSgy2f5Kkr
MD5:	34EBCDE03D8E2C5E00BDC503301102D0
SHA1:	575825F390BF826F8F392D5D516DD542F36CADC9
SHA-256:	4282872D11C2CFB4EE71BCA23AADA422893D9014A0D31C33BE1CE3C6AC141B46
SHA-512:	828EDF960E2AA16EE30597074E5C6D5B657F2942F91D081A97BCA00BEB53461B8FA4F69E3F1088C412046EF94E1C8EDAEB9E30FA1B9453F8A60AB5ACB61AC7 C8
Malicious:	false
Preview:	2021/02/22-20:07:21.952 198c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/02/22-20:07:21.954 198c Recovering log #3.2021/02/22-20:07:21.958 198c 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:	B0A7B194042859056638767 74A2176939A6ED75EF3904E44283A125824BD0BF3
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.238749754402127
Encrypted:	false
SSDEEP:	12:NG0Q+va5KkMFUtp9GX1g/P9GX1QV5f5KkTJ:f5a5KkUgy1j1Sf5Kkl
MD5:	9A4A50A3B330F1B5F45F57CC6FB65331
SHA1:	CB209854373C5C3C2E5549637655E415F9316DCB
SHA-256:	E21AAB3D255E645A66E81BBED54269D40E07A87F51CE734F256E489B1AC455F0
SHA-512:	F4614D183183A78DC66C0188AEC625ED7B6144A82AB775F6D90C76187CCAE61245562410981CDC2225E2A9554FBA459B3A45E2C0279541848E41CBC5D48C9AB
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Preview:	2021/02/22-20:07:39.432 19bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/02/22-20:07:39.433 19bc Recovering log #3.2021/02/22-20:07:39.433 19bc 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\695de0af-ffc2-4c28-bc33-7aadafac8e1d.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
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
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):	5.13663538886584
Encrypted:	false
SSDEEP:	12:NKf+va5KkkGHArBFUtp9Kp/P9KdV5f5KkkGHAryJ:cka5KkkGgPgCu1f5KkkGga
MD5:	F3AE38722BA672EBA9C18A75347323E0
SHA1:	5C63DD75D88DCF3E52CF86AD2467F52B03EF88B6
SHA-256:	DF0C347373D641CFE5AB571117CCEE844C7D901B43989328BB3819709814B97A
SHA-512:	55C709666ECF035D9C4A588500AE0E6D53201AF9E8B2CF70F46C12750861D409BE73477E8499F08E5FA9C6C36CD823D8737E83D57EEDA5DCD01A09A0A1A3024
Malicious:	false
Preview:	2021/02/22-20:07:33.690 1a2c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/02/22-20:07:33.692 1a2c Recovering log #3.2021/02/22-20:07:33.692 1a2c 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):	5.150081665192317
Encrypted:	false
SSDEEP:	12:NKtNyva5KkkGHArqiuFUtp9KkX/P9KkjR5f5KkkGHArq2J:ctNYa5KkkGgCgCkMkjDf5KkkGg7
MD5:	5BAF8F8A3A459EC2BDEC625817B46735

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
SHA1:	52A6E0437A01DFA74BBF68ED0309A2FDA2B9CD59
SHA-256:	5CE3624EA53F3526A35BDA1804810BF74DB8F363870AEE7196F5375E15A2B45F
SHA-512:	CB650F4B3F4B40FBE73CB7A08817C65233803B244801A7056F9652C6230DC8E3499FBD0440438BCC0740AEF39D6A8E85746781C01C63E79FE7232229C44CA8E6
Malicious:	false
Preview:	2021/02/22-20:07:33.720 19c0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/02/22-20:07:33.721 19c0 Recovering log #3.2021/02/22-20:07:33.721 19c0 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
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):	5.211563657737236
Encrypted:	false
SSDEEP:	12:NDaJQ+va5KkkGHArAFUtp9DRg/P9DwQV5f5KkkGHArfJ:Fy5a5KkkGgkgLR4wSf5KkkGgV
MD5:	F0FD5DAD8B36041E4365893BE4BE057C
SHA1:	46B6E2D144993DB33E580CB6F83FA202CD60752F
SHA-256:	275CB33ADA2D0956ECE7F44CF91400F92DBF8D8AC5B326F500972A0B15026483
SHA-512:	3466112243EEAFD1381CC584EBF796CBB64CEDAC463753ABB8E81806A3A96827FD212450F278E6AD96C08F1C80820DFC904BA06E515C0A99DCAF64A3550594C
Malicious:	false
Preview:	2021/02/22-20:07:49.588 19bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/02/22-20:07:49.590 19bc Recovering log #3.2021/02/22-20:07:49.591 19bc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF2124
Malicious:	false
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):	5.209957371629094
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
SSDEEP:	6:mQ8+q2PWXp+N23iKKdKpIFUtp9XZZmwP9XNVkwOWXp+N23iKKdKa/WLJ:NBva5KkmFUtp9XZ/P9Xz5f5KkaUJ
MD5:	3B16214031DBA8670030382D9E01F608
SHA1:	5F55431072847A6057DAF9E4B8287A0682C8076E
SHA-256:	E6971E98A09C7D89132C9C1E5596252F12020440EF318DB428D2F478E33E6244
SHA-512:	40FF6EAE4974CBF69F227440C733CD58C8A68508E609162CB9608DF37FD02CCA2FC9E818882278D3F39E29DC89F2BFF4776EB12AC8D763971324BC88FCCE4DA
Malicious:	false
Preview:	2021/02/22-20:07:21.609 19b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/02/22-20:07:21.611 19b8 Recovering log #3.2021/02/22-20:07:21.611 19b8 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):	5.337140021521106
Encrypted:	false
SSDEEP:	12:NVQ+va5KkkOrsFUtp9REg/P9jQV5f5KkkOrzJ:X5a5Kk+g66Sf5Kkn
MD5:	936F5162DB153CC97FFB57AA73C6A2DA
SHA1:	C8BD26431CFD80420A7698742CBAADF84B6001FC
SHA-256:	BC50321FB08E08C7312C2BDEC91C8CA0D1A34247533772E166A598C363EF5472
SHA-512:	42B457AD27B8227A382F31DB4DEBDB364B0838C2222532689B6C19668210D1E8B791A5897A8AC25A6AFBF468C1300E5B76284039D418ED49DA49811FF14B0F79
Malicious:	false
Preview:	2021/02/22-20:07:36.383 19bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/02/22-20:07:36.384 19bc Recovering log #3.2021/02/22-20:07:36.385 19bc 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):	72
Entropy (8bit):	4.9656107965058105
Encrypted:	false
SSDEEP:	3:Rj3Yd/m891EtFsYh:RUlm80fsYh
MD5:	4999EA64ED7EA8CEC075333C5A989D95
SHA1:	420B0650FA8AA84D08F82674A32A32B5686D9BF0
SHA-256:	F0E023537EB5383B8E359F75D90CF82A5191F5ED25508713E7FD33AF846A9927
SHA-512:	8F703B4584E186918B25BD2A01F62E6B3E3C2D8C65EA1F27E62B908262512602BF7C1D41768088287F66B5378D4E61754BAB19F4F5B1141535E37D8067040F25
Malicious:	false
Preview:	.....F.....)jz-^.....Q`.....v...].....tW...#<.....ty....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b0afc06f-4b92-4c3f-bc6d-fee8371e7619.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	2354
Entropy (8bit):	4.891142603406379
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDHz5s4tRLsNJTsZ9EmsMtkzsSVEyvhX5s83zsEAMH1YhbD:JTnOCXGDHzxtYEXEa+hXLOGyhH
MD5:	37BD6CDA41CD71A3B20DDA3EF0C211A1
SHA1:	7C40A7A72BF93F35ED74F7BD58F3B31E1A0CEC93
SHA-256:	C6CFB9A39BF206F9DCD0FC82A36D587E611E5FE2E3ED9B199E46A64BDC85B204
SHA-512:	84753A29973F6F88F3E072CE8146ED71A4F52E74B1F5815C1A84AABF65310E39B0DF5A5046466CD9CFA58EBE29280BEE120905B8A56F452EC668CDF4C09152F2
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13261118844505253","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13261118844511622","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","suppo

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
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
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):	4.244580303933271
Encrypted:	false
SSDEEP:	3:tUKowNc3jKWZmwv3awNg2ibhR1V8sawNg2ibhR1WGv:mQGz1ZmwP927l7Vv927l7tv
MD5:	282430FD7405448F85E0870D849CA117
SHA1:	258EAB67E8FD3E0B8FD3C54408A226672AEAE460
SHA-256:	01A9B192867AE8BE8D4D6598D3A52EB723C922BD321F2F906CEA349414F7D203
SHA-512:	5057CEC4930DC0DEE7866A8B7CB1FBB42B2EA48DE8EFD8E97A032E10C21DAE3FEE22000436BBF83D26DAB9869F28A43C1959C8FD7E804CB80076141E9219F8 55
Malicious:	false
Preview:	2021/02/22-20:07:32.631 1990 Recovering log #3.2021/02/22-20:07:32.727 1990 Delete type=0 #3.2021/02/22-20:07:32.727 1990 Delete type=3 #2.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e025eb74-386b-44ca-9ec7-b862b5c4620f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e025eb74-386b-44ca-9ec7-b862b5c4620f.tmp	
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\fb42f2be-e238-41b0-a7da-3f02fe7fa994.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):	22614
Entropy (8bit):	5.5354025494105485
Encrypted:	false
SSDEEP:	384:+axtELlzIX/1kXqKf/pUZNCgVLH2HfDyrUdHGynTAQ1Gm4G:8Ll2/1kXqKf/pUZNCgVLH2HfOrUBGynH
MD5:	F0FB346D138C8B79534046C966E4A500
SHA1:	865A30466E87C0C5E7A559D44F1EEB69F1628498
SHA-256:	48A6118A4B96F9961263BCFDDBB8A280D192A2393600A9750BF3B454E60D373F
SHA-512:	4A52142F5841C3AF73C3D241F47C800871BF2BC3C5A84E789389C6D2BB4FF738E98DCE60B8AC4D73F75387C5EB41B00151FE515FE7632852F428D874DB1E5349
Malicious:	false
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":"13258526841598204","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):	5.1812709199931515
Encrypted:	false
SSDEEP:	6:mQcmyq2PWXp+N23iKKdKfrzAdIFUtp9aw1ZmwP9CNRkwOWXp+N23iKKdKfrzILJ:Ncmyva5Kk9FUtp9N/P9iR5f5Kk2J
MD5:	24AD5BAF9C095D154830C453FAE1DE34
SHA1:	76A3FD239B0816D6E7B1368B93A736BB3CFE6590
SHA-256:	0599551873617F79177E76D658479F015E8DC6125B9DBCF354F9F55203BE8086
SHA-512:	809FCFB9D96A9BD1735B98911A371BADCBBFA54294B99F21A98906209E4077E548564E07DFFF2005E699A923B95BFBFCA5C9CB8DDA1818D2E9F0B9E1A023BCB1
Malicious:	false
Preview:	2021/02/22-20:07:34.742 19c0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/02/22-20:07:34.744 19c0 Recovering log #3.2021/02/22-20:07:34.745 19c0 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
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
Size (bytes):	13
Entropy (8bit):	2.8150724101159437
Encrypted:	false
SSDEEP:	3:Yx7:4
MD5:	C422F72BA41F662A919ED0B70E5C3289
SHA1:	AAD27C14B27F56B6E7C744A8EC5B1A7D767D7632
SHA-256:	02E71EB4C587FEB7EE00CE8600F97411C2774C2FC34CB95B92D5538E7F30DA59
SHA-512:	86010ED2B2EEBDCC5A8A076B37703669C294C6D1BFAAEA963E26A9C94B81B4C53EC765D9425E5B616159C43923F800A891F9B903659575DF02F8845521F8DC4
Malicious:	false
Preview:	85.0.4183.121

C:\Users\user\AppData\Local\Google\Chrome\User Data\ShaderCache\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.45488079341118026
Encrypted:	false
SSDEEP:	3:8Eflrt:8
MD5:	414E66CE766CB9A37BE221B0E7A732FA
SHA1:	181D4E278EDB62A0EF4043320C0A78052B32C33B
SHA-256:	B66F8242A5E80B597B6725F811C128CA02512CB067A6A52DE65E402844B8869B
SHA-512:	045404300FC0D7594393B9E81129E989FE4734F111AC70E8C692F604E71DDADC9A615F611B73DBBEBC0D0948D3F2CC59FA8A9FE908A2F089B211CAD3D493805
Malicious:	false
Preview:	.'..(.....kX../ .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\9.19.0\Indexing in Progress	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir6436_269622570\Ruleset Data	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	223592
Entropy (8bit):	4.9638585725691575
Encrypted:	false
SSDEEP:	3072:SRztNSIhnVr91m7Y+VFwPmqSqm2+Sc4Q2PRbKbG5uu5hrExzu6KyGbx+9Omzpj:ShNZDE7nxPC5cVr6xE
MD5:	FCCFC2303ACCE4945A4E5B17FEB074D6
SHA1:	314086BBE1D350CB8850C76D89C00EC6D4E7B0BE
SHA-256:	6139961F1E07AE33628E913D3551469AFB1AD57A29F0520B2281879A44CBC92F
SHA-512:	7F8E9D7919C5A4896113EBFDACC5B9728DC9F56138B163FD92E9CC82B393890B125FADE7586B3A4373B9930311035E5581B14705167070A28FDB5D42D69EA14E
Malicious:	false
Preview:	.....d.....5..... .....`...D.....|.....t..p.....h...d..`.....t...L...T...8...@...<...8...4.....,...(.....uocca.....&.....ozama.....3..0.....0iupb.....@_..H.....g.bat.....`.....onwod.....x.....ennab.....d.....nozam.....(v.....geips.....rekoj.....lgoog.....`.....uotpo.....lreko.....o.....x7.....x.....tf.....H...,.....P...L.....@...<...t...4...0...P...(...0... .....h.....H.....(.....l.....H.....(.....t.....l...h...d...`.....T...P...L...H...X...@...<...8...4...0...,...(...$... .....d.....@..... ....p.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\b6e6bfab-0c09-4863-bb69-4f86ce60f77e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Google\Chrome\User Data\b6e6bfab-0c09-4863-bb69-4f86ce60f77e.tmp	
Category:	dropped
Size (bytes):	156007
Entropy (8bit):	6.051446557943152
Encrypted:	false
SSDEEP:	3072:Ox+9BNyxIauZSIxp/lwiB9oFcbXafIB0u1GOJmA3iuR1:OxM6b2pB92aqfIlUOoSiuR1
MD5:	39CCA4BE37F251955B402BE0BFBC4D92
SHA1:	6D4EA91D5BC46C829BADADC7947FD953374D1529
SHA-256:	ADA22F0DD6A64E7B97946DB6CA2D36431BC2AB8EDFDF039630BC4C42CD04D08A
SHA-512:	0D13AB5A7BBAFBF448B2F7985A28CFB1B456AD0C15AFB4FAA1B11A8EC1FA7152F4E31811458A6C8175F40832BA975270ADAB93B80406EEC0A5627A5E392E087 8
Malicious:	false
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":1.614053244767052e+12,"network":1.614020846e+12,"ticks":96771872.0,"uncertainty":4616108.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016579807"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\cad3c80c-3c40-4eb3-8118-0c082e9dc960.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):	156344
Entropy (8bit):	6.052445630249435
Encrypted:	false
SSDEEP:	3072:un+9BNyxIauZSIxp/lwiB9oFcbXafIB0u1GOJmA3iuR1:unM6b2pB92aqfIlUOoSiuR1
MD5:	937ABA308E30F8AF81CFCC894C9E0C0A
SHA1:	4DDEF02A96CB01407F257190572613684717229A
SHA-256:	14D3DF50BB9FEE78F72DC3675D43F1E14931BBEF0CB964E0E8C635994E5F0AA7
SHA-512:	7FBAF258CBD7815E62BA618C08E3E2E29FACA01E8418ACC77BDE20988EE82E9DDDCB4C44207F202AB3CB329C3D3645947DCC64EB07026BD9487A3275A8867A 9A
Malicious:	false
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":1.614053244767052e+12,"network":1.614020846e+12,"ticks":96771872.0,"uncertainty":4616108.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"132

C:\Users\user\AppData\Local\Google\Chrome\User Data\d8294c39-7fc6-4c5e-ac47-900c793c31f3.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7400818025398928
Encrypted:	false
SSDEEP:	384:fDyth/Q6HXwR8NhrqvF/3GJfmHnCGSVrAjtJxeDrbKrolmgbgfBtZ6OnntNE1JIT:uSFFizOasenRv383rW/KFjBhf
MD5:	ABD1ACA81F290F40A73ED118FF465240
SHA1:	0AFBB8BCC21F65F18068659D4604DDD59334A271
SHA-256:	6020D4D4A23702FF674C0E2C3E0BD68E4720B4D1A8993FF2AE9D99D129323977
SHA-512:	3383BC1AA43DAC62BAF453E3B596B8A4E8FDD1C7CE032F94536611F3D3827CE286AAB5FB3F816868C34B8A92AC0537A0691C2E47F0345CDB0B4D1D8A8611F1 1
Malicious:	false
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...l28.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\fd3d28ad-759d-460c-8dd1-5ac37fa25839.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):	156250
Entropy (8bit):	6.052170769445067

C:\Users\user\AppData\Local\Google\Chrome\User Data\fd3d28ad-759d-460c-8dd1-5ac37fa25839.tmp	
Encrypted:	false
SSDEEP:	3072:uD+9BNyxIauZSIxp/lwiB9oFcbXafIB0u1GOJmA3iuR1:uDM6b2pB92aqfIlUOoSiuR1
MD5:	EE0653708374FB04E1E9DEFC7176277F
SHA1:	D5D31D9C9317B40E5BFFE620DDAB742945D0B5DB
SHA-256:	3D9D0AB13617AD62144B1202D049BE7069659F68AA1D342D344B54C45CDF246C
SHA-512:	389A39E63ABB373D59543998544072C169F71B702C1D6AAF2C494FD4E34261D31C07AA73BFA28158824A0FC7EF1CA9175F84060F03569EE01951466C39AB2357
Malicious:	false
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":1.614053244767052e+12,"network":1.614020846e+12,"ticks":96771872.0,"uncertainty":4616108.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABIt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"132

C:\Users\user\AppData\Local\Temp\13ff4d19-05c1-4fae-8ae1-8e2abb7a6165.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
Preview:	.

C:\Users\user\AppData\Local\Temp\18b0406f-e190-436e-b911-ac4b03219b3f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LIP/....](.A.....l...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\2de9e900-f895-4027-b87e-945b099bfde3.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

C:\Users\user\AppData\Local\Temp\2de9e900-f895-4027-b87e-945b099bfde3.tmp	
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.:.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...l.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\6436_163599434\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.9477608398895883
Encrypted:	false
SSDEEP:	3:SdUoLS6MTYUAZdXtbJXBVGHIVWfE:S/7MTYUATPv8c
MD5:	AFFD907C7BB49B4A7449E67EE49D99C7
SHA1:	3DAEC57822D8C39E0BDE14BCD19B906CED0F55ED
SHA-256:	D5CDD87B76D7E6C3DC16374D41B8350519BE46B978EAC80AB70E6386F6E702FB
SHA-512:	488D45EA5C58C2F27360E86CC50F487AE81F6E5C8D58D82C0155346297AAA542018BBCCAD138972D173E3E822F06D62A95EFDE2426D8823AC1C987214D67D01
Malicious:	false
Preview:	1.869f6197c3fdd474910319ff37ee13b73f8fb8ceeaaa62517e2d056b6a03ff54

C:\Users\user\AppData\Local\Temp\6436_1751050358\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.8680468258162546
Encrypted:	false
SSDEEP:	3:SRkxjWywithugUcdix:SSxqJithuWdix
MD5:	F9F04944035E152D967A9B5D22A45925
SHA1:	043B77352C76F6A78B2E8AA85B88E95B06E71045
SHA-256:	E329E7DF52762639DEA5FF45983940E670AE19C740299F154DB45C8117759F6B
SHA-512:	08DE564F6C178C59DC95D74E26506298654F01A32609F6A756894BE9421ADFA6C2D529B766D277E14E66456DA0C531F066B71057F9DAECFBED8D9923C71BE89
Malicious:	false
Preview:	1.47233fd5797a316715e3023c0b3fcb5960b27b534e94284c4c4853c1aebc1394

C:\Users\user\AppData\Local\Temp\6436_178149882\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.866533712632772
Encrypted:	false
SSDEEP:	3:SpUCQEd2dq8ebEJW2GnnHR:SXQ5Y88EJeR
MD5:	423CB83A2A3B602B0AA82B51B3DA2869
SHA1:	58BC924AF90A89CE87807919F228FE6C915AD854
SHA-256:	0047059C732D70AF8C2F407089237F745838A0FE4F75710ABF1E669B81243E9C
SHA-512:	F80E9B5D544894A667F74CFD0A4D784311299DB080CA6793AABD93B95CF1E2870F74AD38A6386D862580220047F828457240577335C565B7F38B0C6677811660
Malicious:	false
Preview:	1.ffd1d2d75a8183b0a1081bd03a7ce1d140fded7a9fb52cf3ae864cd4d408ceb4

C:\Users\user\AppData\Local\Temp\6436_295851065\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.928261499316817
Encrypted:	false
SSDEEP:	3:STDLGswXEVBcVdBiTDt3zLsW:SPLGLErcVdBiDtf3
MD5:	C00BCE97F21B1AD61EB9B8CD001795EE
SHA1:	8E0392FF3DB267D847711C3F4E0D7468060E1535
SHA-256:	59F06F04230E32E8BC839F45B984D31D611930427B631C963D09E7064A602363

C:\Users\user\AppData\Local\Temp\6436_295851065\manifest.fingerprint	
SHA-512:	9930E44A6ECC62505DBADCEED5E05645909FF09816FB12AAC0414E6D2830AC09758366C3B7D4EDD7839C87EB16DFA4C66D8981AE6237D408B37135C3506F4C2
Malicious:	false
Preview:	1.6f6bc93dcd62dc251850d2ff458fda96083ceb7fbe8eeb11248b8485ef2aea23

C:\Users\user\AppData\Local\Temp\6436_562182264\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.9669759926795995
Encrypted:	false
SSDEEP:	3:SfvHUTa8URTTH/BXDj6:SXD3TfB36
MD5:	E3EDA33A5C956F4FC9C5BBD91FF10252
SHA1:	182B989E299A3EC306622A9DD45C3B74A4DF6077
SHA-256:	6D7A462B703F1617286B65BFE0116F267328BEFC379812BCE774D8C640289647
SHA-512:	A49FF4979FEC3512C44899840CCF8D112806330C93812C515F09953B9B6DBA6B1DAB1828382D634235CF23E093C983AEFA860B7A75FDCB5F3F98DD928D4F47D
Malicious:	false
Preview:	1.d730fdd6875bfda19ae43c639e89fe6c24e48b53ec4f466b1d7de2001f97e03c

C:\Users\user\AppData\Local\Temp\74bae696-64fc-437b-bd1d-a05987b597f1.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
Preview:	.

C:\Users\user\AppData\Local\Temp\scoped_dir6436_180364208\2de9e900-f895-4027-b87e-945b099bfde3.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
Preview:	Cr24.....0..''0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;..._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-I..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\scoped_dir6436_180364208\CRX_INSTALL_locales\am\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17307
Entropy (8bit):	5.461848619761356
Encrypted:	false
SSDEEP:	384:arfbEVrFvMP4rMhuDopC3vUuFBYZV6uml:aHEVrFvMP4KuFvr6D6uml

C:\Users\user\AppData\Local\Temp\scoped_dir6436_180364208\CRX_INSTALL_locales\am\messages.json	
MD5:	26330929DF0ED4E86F06C00C03F07CE3
SHA1:	478F3B7E7A7E007BEE182B89C2EF6FFE6045E92C
SHA-256:	621B5139ED199022BB6529AF18ED4DC312AE9F3E90ECAF3B2C9E1D12114F5B22
SHA-512:	0BE6183A1BF12575C0F99960705D4249E79CDB8528C55FF132BE99A111F09494231AD6A36CD61B090A3B34C6971D68A29373BA346888E852C52E05DC14380682
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "1282768764603190 75": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": ".... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "... ...".. },.. "1802762746589457177": {.. "message": "...".. },.. "1850397500312020388": {.. "message": ".$START_LINK$Google Home .....END_LINK ... . Chromecast ....? $START_SPAN$*END_SPAN",.. "placeholde

C:\Users\user\AppData\Local\Temp\scoped_dir6436_180364208\CRX_INSTALL_locales\ar\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16809
Entropy (8bit):	5.458147730761559
Encrypted:	false
SSDEEP:	192:0IprKC78JmUjk8RkeryFOYPATxLZ8fsbE3/IFV6c8TEKdl:Jrp8JjA8RkerK0lc3wFV6uml
MD5:	44325A88063573A4C77F6EF943B0FC3E
SHA1:	78908D766F3E7A0E4545E7BD823C8ED47C7164EB
SHA-256:	67A439A08804EF4BEF261BDBADD8F0FEFD51729167D01EDCA99DD4AF57D6108B
SHA-512:	889C02BC986794C58C76022E78F57F867DD1D5217687F12D679A33A2DB9E5A18F3A37CF94D8FE4585E747C78E4662EAB93361FF7D945990774C7CFCACCFB79D
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": ".. .. ..".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": "..... .....".. },.. "1850397500312020388": {.. "message": "... .... Chromecast .. $START_LINK$..... Google HomeEND_LINK. $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6436_180364208\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	18086
Entropy (8bit):	5.408731329060678
Encrypted:	false
SSDEEP:	192:4jjpr342SIwPIasR9VhMkACVmrv8evj+3eXivOMbb2vVzCkwRV6V6c8TEKdl:4ZrYo+rxT+qOV6V6uml
MD5:	6911CE87E8C47223F33BEF9488272E40
SHA1:	980398F076BB7D451B18D7FDE2DE09041B1F55AD
SHA-256:	273DEF0F67F0FA080802B85EF6F334DE50A19408F46BDF41F0F099B1F5501EEA
SHA-512:	CDB69405BB553E46DCF02F71B1A394307D0051E7FA662DFFEBA7888F30DD933F13C7FD6E32F1D7AEAEE8746316873B6E1D92029724ABDC75E49DCC092172EA 2
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "......".. },.. "1213957982723875920": {.. "message": "... .. ..-..... ....?".. },.. "12827687 6460319075": {.. "message": "..... .. ..".. },.. "1428448869078126731": {.. "message": "..... .. ..".. },.. "1522140683318860351": {.. "message": "..... .. .., ...".. },.. "155090406471082895 8": {.. "message": "......".. },.. "1636686747687494376": {.. "message": "......".. },.. "18027627 46589457177": {.. "message": ".... .. ..".. },.. "1850397500312020388": {.. "message": "..... .. .. Chromecast . $START_LINK$..... Google Hom eEND_LINK? $START_SPAN$*END_SPAN",.. "p

C:\Users\user\AppData\Local\Temp\scoped_dir6436_180364208\CRX_INSTALL_locales\bn\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19695
Entropy (8bit):	5.315564774032776
Encrypted:	false
SSDEEP:	384:PrUCrcTIOeswIW/Vre/sZn8TFfzheV6uml:IPswIWtoK8xfG6uml
MD5:	F9DDF525C07251282A3BFFCEE9A09ABB
SHA1:	A343A078E804AF400A8F3E1891E3390DA754A5CD
SHA-256:	C69C6C90F7EB8F10685CD815AF1F6F1B87CF30C4E8D95DF1D577DE1105AAD227
SHA-512:	EBD339C37162984672513019D470B92DF8B743DD69D4430361EF12D42FD1C208DBDE818A7BFE20BE8A7D63CD6E02B3F4344DEA1C4AEDB8719D789981A49DA4 C
Malicious:	false

C:\Users\user\AppData\Local\Temp\scoped_dir6436_180364208\CRX_INSTALL_locales\bn\messages.json	
Preview:	{.. "10189845614885205 17": {.. "message": ".... ...".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128 276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... ....".. },.. "1522140683318860351": {.. "message": "..... ... .".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "18027627 46589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "$START_LINK$ Google

C:\Users\user\AppData\Local\Temp\scoped_dir6436_180364208\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15518
Entropy (8bit):	5.242542310885
Encrypted:	false
SSDEEP:	384:drGUBKxMF2ayv8FrIccUVFmwf+7d9VKS3V6uml:dCUBKxMFBy0FE3UzmQ+zkSl6uml
MD5:	A90CF7930E7C3BEC61EE252DEFAD574A
SHA1:	F630CA01114A7BDD39607CB84B8280CCE218A5C6
SHA-256:	A533740E17559E2ADF40B4555C60F21EEC84E92C09CDBC19EED033A0B4DD2474
SHA-512:	598F991B344FA6724617D6CE57BB0D6D64EF86B4F5317BF6AD5EDF43E6B0A385094E7885F7A8FA2B107405B31C3D9F76E92315BC1D9BB52ACD4ECAD342917DE 1
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Es congela".. },.. "1213957982723875920": {.. "message": "Quina de les opcions.seg.ents descriu millor la vostra xarxa?".. },.. "128276876460319075": {.. "message": "Detecci. de dispositius".. },.. "1428448869078126731": {.. "message": "Flu.desa del v.deo".. },.. "1522140683318860351": {.. "message": "S'ha produ.t un error en la connexi.. Torneu-ho a provar.".. },.. "1550904064710828958": {.. "message": "Correcta".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volum".. },.. "1850397500312020388": {.. "message": "Pots veure el Chromecast a l'$START_LINK$aplicaci. Google.HomeEND_LINK?$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "

Static File Info

General

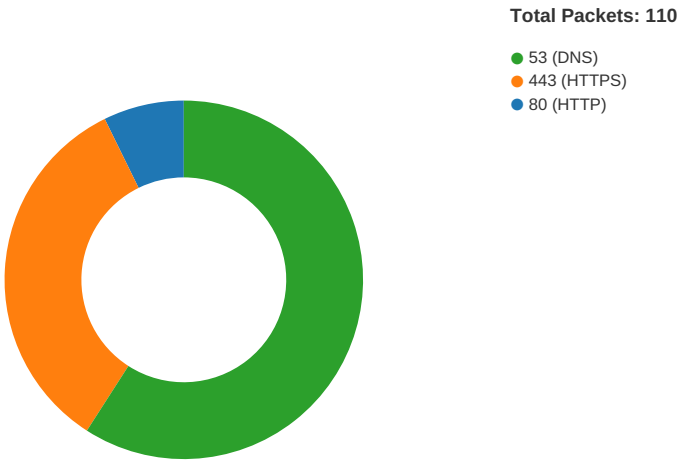
File type:	HTML document, ASCII text, with very long lines, with no line terminators
Entropy (8bit):	3.3765801787304097
TrID:	
File name:	xerox for hycite.htm
File size:	7194
MD5:	158eb35645b71b26b2afd86759768631
SHA1:	c4d06a2c43fd948127d9dfc9880302163cae82ea
SHA256:	5873df6b96a855b79f32aaf44098777bbac335debc6a9eb ee8aadcf50fd7077a
SHA512:	984ff0c97771c1d8dd519bbc4ffad98b8887a1ad9726382 c8c423f9d36f9bb6c9098696bda249754ceffb884b97897 0f5c30a2f30401b7203d50ca569b0a2861
SSDEEP:	192:vaZrL0PWCrd++y5N++y5u++y5t++y5uUZ:gX0eKd +t+O+N+OY
File Content Preview:	<script type='text/javascript'>document.write(unescape(' %3C%2F%64%69%76%3E%0D%0A%3C%70%3E%20 %26%23%36%38%3B%26%23%31%30%31%3B%26 %23%39%37%3B%26%23%31%31%34%3B%2C%20 %3C%62%2F%3E%20%6D%67%61%72%63%69%61 %20%3C%2F%62%3E%0D%0A%3C%70%3E%3C%6 2%72%3E%20%3C%69%6D%

File Icon

Icon Hash:	e8d6a08c8882c461

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:07:24.071218967 CET	49719	80	192.168.2.3	187.33.160.8
Feb 22, 2021 20:07:24.072638988 CET	49720	80	192.168.2.3	187.33.160.8
Feb 22, 2021 20:07:24.294884920 CET	49721	80	192.168.2.3	187.33.160.8
Feb 22, 2021 20:07:24.327040911 CET	80	49720	187.33.160.8	192.168.2.3
Feb 22, 2021 20:07:24.327286959 CET	49720	80	192.168.2.3	187.33.160.8
Feb 22, 2021 20:07:24.328134060 CET	49720	80	192.168.2.3	187.33.160.8
Feb 22, 2021 20:07:24.337913036 CET	80	49719	187.33.160.8	192.168.2.3
Feb 22, 2021 20:07:24.338041067 CET	49719	80	192.168.2.3	187.33.160.8
Feb 22, 2021 20:07:24.560585022 CET	80	49721	187.33.160.8	192.168.2.3
Feb 22, 2021 20:07:24.560734987 CET	49721	80	192.168.2.3	187.33.160.8
Feb 22, 2021 20:07:24.582230091 CET	80	49720	187.33.160.8	192.168.2.3
Feb 22, 2021 20:07:25.373271942 CET	80	49720	187.33.160.8	192.168.2.3
Feb 22, 2021 20:07:25.450663090 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:25.483699083 CET	49720	80	192.168.2.3	187.33.160.8
Feb 22, 2021 20:07:25.494597912 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:25.494755983 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:25.495080948 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:25.540107965 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:25.540448904 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:25.540492058 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:25.540534019 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:25.540569067 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:25.540568113 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:25.540654898 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:25.541966915 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:25.651684999 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:26.150443077 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:26.151288986 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:26.151515007 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:26.194411993 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:26.194442034 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:26.194559097 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:26.194782972 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:26.194899082 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:26.195671082 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:26.195736885 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:26.207608938 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:26.253865957 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:26.260646105 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:26.265500069 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:26.348124027 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.092120886 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.092148066 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.092165947 CET	443	49729	92.204.219.148	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:07:28.092180967 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.092200041 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.092217922 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.092228889 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:28.092233896 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.092252016 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.092259884 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:28.092267990 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.092294931 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:28.092299938 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:28.092323065 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:28.092336893 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:28.137926102 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.137953997 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.137969971 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.137984991 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.138000965 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.138051033 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:28.138102055 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:28.138108015 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:28.138112068 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:28.154431105 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:28.199616909 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.200681925 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.200700998 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.200716972 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.200855017 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:28.278141975 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:28.278647900 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:28.279042959 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:28.280493975 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:28.326262951 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.327388048 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.327409029 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.327423096 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.327562094 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:28.327826023 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.327898979 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:28.329657078 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.329684019 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.329699993 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.329813957 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:28.374990940 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.375015974 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.375031948 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.375051022 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.375087023 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:28.375121117 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:28.377119064 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.377401114 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.377417088 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:28.377423048 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.377438068 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.377496958 CET	49729	443	192.168.2.3	92.204.219.148
Feb 22, 2021 20:07:28.418886900 CET	443	49729	92.204.219.148	192.168.2.3
Feb 22, 2021 20:07:28.418916941 CET	443	49729	92.204.219.148	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:07:14.502975941 CET	49199	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:14.554601908 CET	53	49199	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:15.408704996 CET	50620	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:15.459264994 CET	53	50620	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:07:16.647824049 CET	64938	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:16.699246883 CET	53	64938	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:17.210455894 CET	60152	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:17.274940968 CET	53	60152	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:17.421092987 CET	57544	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:17.469808102 CET	53	57544	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:18.432298899 CET	55984	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:18.492129087 CET	53	55984	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:19.627226114 CET	64185	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:19.676234007 CET	53	64185	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:21.528387070 CET	65110	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:21.579937935 CET	53	65110	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:23.199390888 CET	60831	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:23.250627041 CET	53	60831	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:23.787995100 CET	60100	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:23.793673992 CET	53195	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:23.801304102 CET	50141	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:23.804943085 CET	53023	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:23.845170975 CET	53	60100	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:23.858522892 CET	53	50141	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:23.870347977 CET	53	53023	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:24.065171003 CET	53	53195	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:24.297938108 CET	49563	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:24.371135950 CET	53	49563	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:24.438287973 CET	51352	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:24.489624977 CET	53	51352	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:24.507976055 CET	59349	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:24.574333906 CET	53	59349	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:25.384066105 CET	58823	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:25.449487925 CET	53	58823	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:25.510843992 CET	57568	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:25.561146975 CET	53	57568	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:25.688350916 CET	50540	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:25.747711897 CET	53	50540	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:25.773264885 CET	54366	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:25.850586891 CET	53	54366	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:26.930691957 CET	53034	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:26.980439901 CET	53	53034	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:27.915846109 CET	57762	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:27.967334032 CET	53	57762	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:28.300107956 CET	55435	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:28.363919973 CET	53	55435	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:28.378628016 CET	50713	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:28.446679115 CET	53	50713	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:29.067270041 CET	60633	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:29.118774891 CET	53	60633	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:29.815665007 CET	61292	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:29.872447014 CET	53	61292	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:30.177002907 CET	63619	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:30.225586891 CET	53	63619	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:32.637217999 CET	64910	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:32.685806990 CET	53	64910	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:32.849952936 CET	52123	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:32.914599895 CET	53	52123	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:35.861345053 CET	56338	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:35.926431894 CET	53	56338	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:40.965810061 CET	59420	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:41.014522076 CET	53	59420	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:42.682306051 CET	58784	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:42.730839968 CET	53	58784	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:46.331275940 CET	63978	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:46.383064985 CET	53	63978	8.8.8.8	192.168.2.3
Feb 22, 2021 20:07:51.216880083 CET	62938	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:51.275429964 CET	53	62938	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:07:54.516645908 CET	55708	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:07:54.565469980 CET	53	55708	8.8.8.8	192.168.2.3
Feb 22, 2021 20:08:09.419143915 CET	56803	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:08:09.467907906 CET	53	56803	8.8.8.8	192.168.2.3
Feb 22, 2021 20:08:10.390965939 CET	57145	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:08:10.459222078 CET	53	57145	8.8.8.8	192.168.2.3
Feb 22, 2021 20:08:21.789155006 CET	55359	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:08:21.854593039 CET	53	55359	8.8.8.8	192.168.2.3
Feb 22, 2021 20:08:22.776316881 CET	64124	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:08:22.805123091 CET	49361	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:08:22.833462954 CET	53	64124	8.8.8.8	192.168.2.3
Feb 22, 2021 20:08:22.865431070 CET	53	49361	8.8.8.8	192.168.2.3
Feb 22, 2021 20:08:23.009143114 CET	63150	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:08:23.076881886 CET	53	63150	8.8.8.8	192.168.2.3
Feb 22, 2021 20:08:23.272855997 CET	53279	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:08:23.353293896 CET	53	53279	8.8.8.8	192.168.2.3
Feb 22, 2021 20:08:39.785037041 CET	56881	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:08:39.851264954 CET	53	56881	8.8.8.8	192.168.2.3
Feb 22, 2021 20:08:39.967873096 CET	53642	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:08:40.027687073 CET	53	53642	8.8.8.8	192.168.2.3
Feb 22, 2021 20:08:41.459407091 CET	55667	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:08:41.519071102 CET	53	55667	8.8.8.8	192.168.2.3
Feb 22, 2021 20:09:04.794240952 CET	54833	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:09:04.861943007 CET	53	54833	8.8.8.8	192.168.2.3
Feb 22, 2021 20:09:05.245910883 CET	62476	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:09:05.308207989 CET	53	62476	8.8.8.8	192.168.2.3
Feb 22, 2021 20:09:05.504194021 CET	49705	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:09:05.569509983 CET	53	49705	8.8.8.8	192.168.2.3
Feb 22, 2021 20:09:06.302047968 CET	61477	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:09:06.361855984 CET	53	61477	8.8.8.8	192.168.2.3
Feb 22, 2021 20:09:07.021814108 CET	61633	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:09:07.095335960 CET	53	61633	8.8.8.8	192.168.2.3
Feb 22, 2021 20:09:07.804068089 CET	55949	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:09:07.864908934 CET	53	55949	8.8.8.8	192.168.2.3
Feb 22, 2021 20:09:08.431848049 CET	57601	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:09:08.480484009 CET	53	57601	8.8.8.8	192.168.2.3
Feb 22, 2021 20:09:09.054851055 CET	49342	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:09:09.111901999 CET	53	49342	8.8.8.8	192.168.2.3
Feb 22, 2021 20:09:09.172146082 CET	56253	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:09:09.242182016 CET	53	56253	8.8.8.8	192.168.2.3
Feb 22, 2021 20:09:09.628995895 CET	49667	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:09:09.687954903 CET	53	49667	8.8.8.8	192.168.2.3
Feb 22, 2021 20:09:10.264525890 CET	55439	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:09:10.325346947 CET	53	55439	8.8.8.8	192.168.2.3
Feb 22, 2021 20:09:11.123565912 CET	57069	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:09:11.186183929 CET	53	57069	8.8.8.8	192.168.2.3
Feb 22, 2021 20:09:12.003751040 CET	57659	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:09:12.063678980 CET	53	57659	8.8.8.8	192.168.2.3
Feb 22, 2021 20:09:12.678153038 CET	54717	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:09:12.739409924 CET	53	54717	8.8.8.8	192.168.2.3
Feb 22, 2021 20:09:25.583523035 CET	63975	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:09:25.648850918 CET	53	63975	8.8.8.8	192.168.2.3
Feb 22, 2021 20:09:25.766263962 CET	56639	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:09:25.815227985 CET	53	56639	8.8.8.8	192.168.2.3
Feb 22, 2021 20:09:26.923877001 CET	51856	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:09:26.996449947 CET	53	51856	8.8.8.8	192.168.2.3
Feb 22, 2021 20:10:07.387973070 CET	56546	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:10:07.456281900 CET	53	56546	8.8.8.8	192.168.2.3
Feb 22, 2021 20:10:07.599919081 CET	62152	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:10:07.657546043 CET	53	62152	8.8.8.8	192.168.2.3
Feb 22, 2021 20:10:11.414472103 CET	53470	53	192.168.2.3	8.8.8.8
Feb 22, 2021 20:10:11.479060888 CET	53	53470	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 20:07:23.793673992 CET	192.168.2.3	8.8.8.8	0x5bf0	Standard query (0)	euro2.safe links.prot ection.hyc ite.mkanet.com.br	A (IP address)	IN (0x0001)
Feb 22, 2021 20:07:25.384066105 CET	192.168.2.3	8.8.8.8	0xb457	Standard query (0)	www.curryhut.de	A (IP address)	IN (0x0001)
Feb 22, 2021 20:07:28.300107956 CET	192.168.2.3	8.8.8.8	0x4ea8	Standard query (0)	secure.aad cdn.micros oftonline-p.com	A (IP address)	IN (0x0001)
Feb 22, 2021 20:07:29.815665007 CET	192.168.2.3	8.8.8.8	0x95ce	Standard query (0)	www.curryhut.de	A (IP address)	IN (0x0001)
Feb 22, 2021 20:07:32.849952936 CET	192.168.2.3	8.8.8.8	0xfd08	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
Feb 22, 2021 20:07:24.065171003 CET	8.8.8.8	192.168.2.3	0x5bf0	No error (0)	euro2.safe links.prot ection.hyc ite.mkanet .com.br		187.33.160.8	A (IP address)	IN (0x0001)
Feb 22, 2021 20:07:25.449487925 CET	8.8.8.8	192.168.2.3	0xb457	No error (0)	www.curryhut.de	curryhut.de		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 20:07:25.449487925 CET	8.8.8.8	192.168.2.3	0xb457	No error (0)	curryhut.de		92.204.219.148	A (IP address)	IN (0x0001)
Feb 22, 2021 20:07:28.363919973 CET	8.8.8.8	192.168.2.3	0x4ea8	No error (0)	secure.aad cdn.micros oftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 20:07:29.872447014 CET	8.8.8.8	192.168.2.3	0x95ce	No error (0)	www.curryhut.de	curryhut.de		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 20:07:29.872447014 CET	8.8.8.8	192.168.2.3	0x95ce	No error (0)	curryhut.de		92.204.219.148	A (IP address)	IN (0x0001)
Feb 22, 2021 20:07:32.914599895 CET	8.8.8.8	192.168.2.3	0xfd08	No error (0)	clients2.g oogleuserc ontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 20:07:32.914599895 CET	8.8.8.8	192.168.2.3	0xfd08	No error (0)	googlehost ed.l.googl euserconte nt.com		142.250.186.33	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- euro2.safelinks.protection.hycite.mkanet.com.br

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49720	187.33.160.8	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 20:07:24.328134060 CET	715	OUT	GET /inbox/66d676172636961406879636974652e636f6d HTTP/1.1 Host: euro2.safelinks.protection.hycite.mkanet.com.br 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

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 20:07:25.373271942 CET	1959	IN	HTTP/1.1 302 Found Date: Mon, 22 Feb 2021 19:07:24 GMT Server: Apache X-Powered-By: PHP/5.6.40 Set-Cookie: PHPSESSID=030f992671b79bc5dc4140ffb9867dbf; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache location: https://www.curryhut.de/vendor/bin/data?ss=2&ea=66d67617263696140687963697 4652e636f6d Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 22, 2021 20:07:25.540534019 CET	92.204.219.148	443	192.168.2.3	49729	CN=curryhut.de, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Wed Jun 03 19:30:52 CEST 2020	Mon Aug 02 22:20:21 CEST 2021	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
Feb 22, 2021 20:07:29.993823051 CET	92.204.219.148	443	192.168.2.3	49745	CN=curryhut.de, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Wed Jun 03 19:30:52 CEST 2020	Mon Aug 02 22:20:21 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		

Code Manipulations

Statistics

Behavior

chrome.exe
chrome.exe

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 6436 Parent PID: 996

General

Start time:	20:07:20
Start date:	22/02/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'C:\Users\user\Desktop\xerox for hycite.htm'
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:	moderate

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: 6632 Parent PID: 6436

General

Start time:	20:07:22
Start date:	22/02/2021
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=1576,9969516566149389704,70360 51267904063449,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1696 /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:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly