ID: 532647
Cookbook: browseurl.jbs
Time: 15:34:08
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

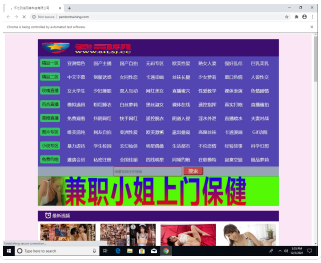
Windows Analysis Report http://pentontraining.com

Overview

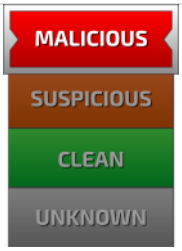
General Information

Sample URL:	http://pentontraining.com
Analysis ID:	532647
Infos:	

Most interesting Screenshot:



Detection



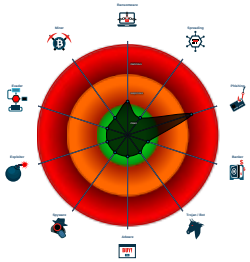
HTMLPhisher

Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish10
- Suspicious form URL found
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5448 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "http://pentontraining.com MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6160 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1624,18296224567106023194,6347225086560399399,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1932 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

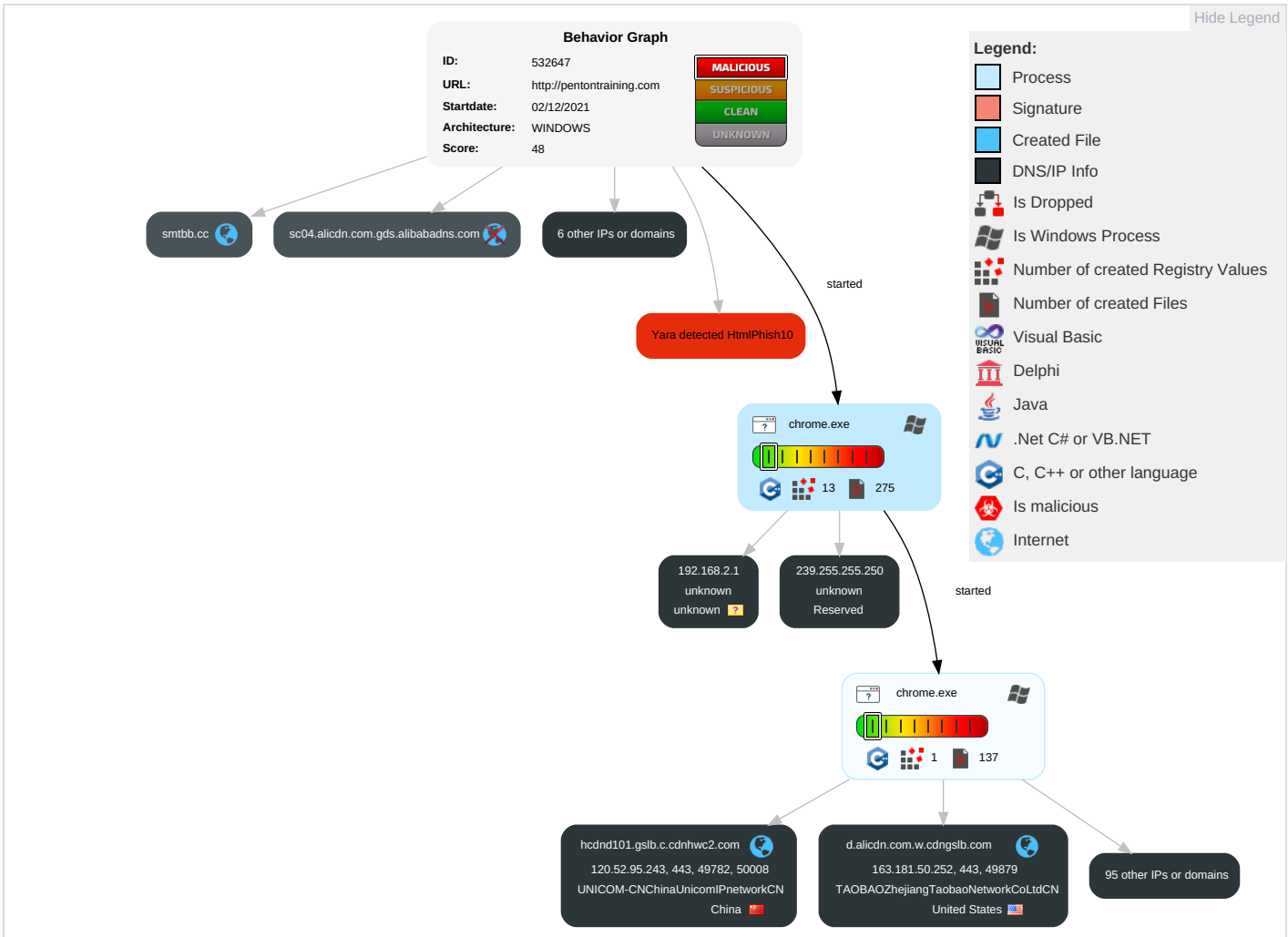
Phishing:

Yara detected HtmlPhish10

Mitre Att&ck Matrix

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

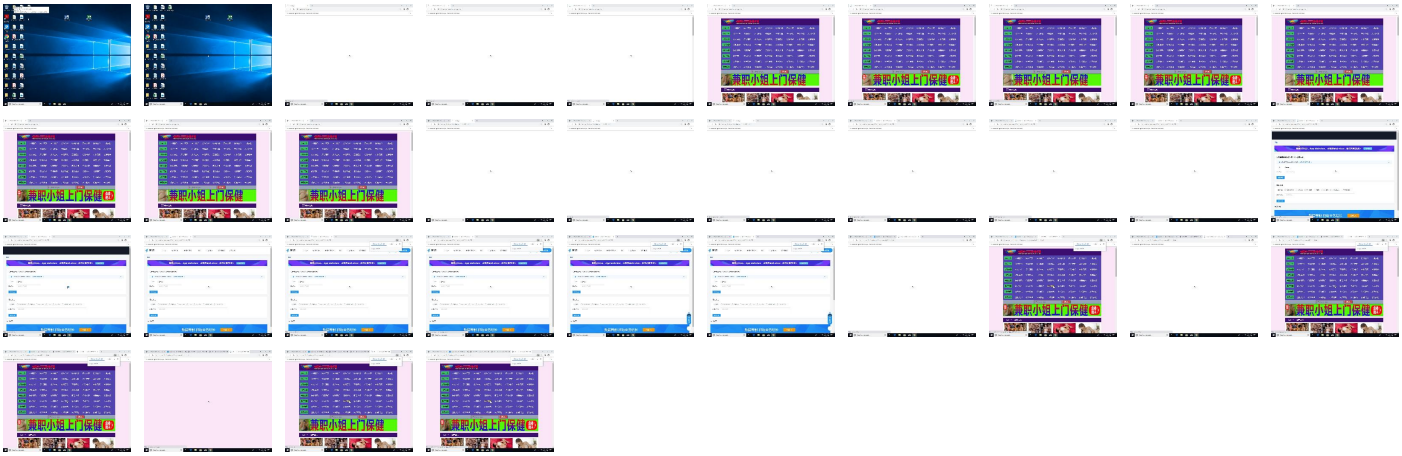
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://pentontraining.com	0%	Virustotal		Browse
http://pentontraining.com	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://pentontraining.com/	0%	Virustotal		Browse
http://pentontraining.com/	0%	Avira URL Cloud	safe	
http://fmlb.netlbtu.com/images/2021/11/23/dmm15659.jpg	0%	Avira URL Cloud	safe	
http://pentontraining.com/2$	0%	Avira URL Cloud	safe	
http://fmlb.netlbtu.com/images/2021/11/23/jr17173.jpg	0%	Avira URL Cloud	safe	
http://https://smtbb.cc:2022	0%	Avira URL Cloud	safe	
http://www.pentontraining.com/2$	0%	Avira URL Cloud	safe	
http://https://www.govguangxi.cn:4443	0%	Avira URL Cloud	safe	
http://https://02qyjs.com:2021	0%	Avira URL Cloud	safe	
http://fmlb.netlbtu.com/images/2021/7/27/dmm7543.jpg	0%	Avira URL Cloud	safe	
http://fmlb.netlbtu.com/images/2021/11/23/dmm15656.jpg	0%	Avira URL Cloud	safe	
http://www.pentontraining.com/tj.js	0%	Avira URL Cloud	safe	
http://fmlb.netlbtu.com/images/2021/11/23/dmm15643.jpg	0%	Avira URL Cloud	safe	
http://fmlb.netlbtu.com/images/2021/11/23/jr17172.jpg	0%	Avira URL Cloud	safe	
http://fmlb.netlbtu.com/images/2021/11/23/jr17171.jpg	0%	Avira URL Cloud	safe	
http://fmlb.netlbtu.com/images/2021/11/23/dmm15644.jpg	0%	Avira URL Cloud	safe	
http://fmlb.netlbtu.com/images/2021/11/23/dmm15657.jpg	0%	Avira URL Cloud	safe	
http://www.pentontraining.com/common.js	0%	Avira URL Cloud	safe	
http://www.pentontraining.com/favicon.ico	0%	Avira URL Cloud	safe	
http://fmlb.netlbtu.com/images/2021/11/23/dmm15658.jpg	0%	Avira URL Cloud	safe	
http://fmlb.netlbtu.com/images/2021/11/23/dmm15662.jpg	0%	Avira URL Cloud	safe	
http://https://www.govzhajian.cn:12443	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://fmlb.netlbtu.com/images/2021/11/23/hey4569.jpg	0%	Avira URL Cloud	safe	
http://fmlb.netlbtu.com/images/2021/11/23/dmm15661.jpg	0%	Avira URL Cloud	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://fmlb.netlbtu.com/images/2021/11/23/cc16500.jpg	0%	Avira URL Cloud	safe	
http://fmlb.netlbtu.com/images/2021/11/23/dmm15655.jpg	0%	Avira URL Cloud	safe	
http://fmlb.netlbtu.com/images/2021/11/23/hey4568.jpg	0%	Avira URL Cloud	safe	
http://fmlb.netlbtu.com/images/2021/11/23/cc16498.jpg	0%	Avira URL Cloud	safe	
http://fmlb.netlbtu.com/images/2021/11/23/dmm15660.jpg	0%	Avira URL Cloud	safe	
http://fmlb.netlbtu.com/images/2021/11/23/hey4570.jpg	0%	Avira URL Cloud	safe	
http://fmlb.netlbtu.com/images/2021/11/23/cc16499.jpg	0%	Avira URL Cloud	safe	
http://fmlb.netlbtu.com/images/2021/11/23/hey4567.jpg	0%	Avira URL Cloud	safe	
http://https://2021tupian.com:2021	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
at.alicdn.com.danuoyi.alicdn.com	47.246.46.252	true	false		high
fragment.tmall.com.danuoyi.alicdn.com	47.246.2.234	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtbb.cc	172.247.112.220	true	false		unknown
na61-na62.wagbridge.work.alibabacorp.com.gds.alibabadns.com	203.119.207.130	true	false		unknown
icon.cnzz.com.danuoyi.tbcache.com	58.215.157.250	true	false		unknown
hm.e.shifen.com	103.235.46.191	true	false		unknown
pentontraining.com	154.81.191.203	true	false		unknown
gxb.mmstat.com.gds.alibabadns.com	47.246.136.160	true	false		unknown
all.cnzz.com.danuoyi.tbcache.com	58.215.157.250	true	false		unknown
gm.gds.mmstat.com	47.246.136.160	true	false		unknown
d2cb5ad7002c4066.huaweisafedns.com	183.131.207.66	true	false		unknown
a.cnzz.com.gds.alibabadns.com	203.119.216.77	true	false		unknown
g.alicdn.com.danuoyi.alicdn.com	79.133.177.252	true	false		high
www.pentontraining.com	154.81.191.203	true	false		unknown
vip.70qn.com	222.186.129.233	true	false		unknown
log-api.aplus.emas-poc.com	101.132.251.31	true	false		unknown
et2-na61-na62.wagbridge.alibaba.tanx.com.gds.alibabadns.com	203.119.214.125	true	false		unknown
q.gds.cnzz.com	106.11.84.7	true	false		high
default.cn.zb.wagbridge.umeng.alibabacorp.com.gds.alibabadns.com	59.82.29.248	true	false		unknown
cagnon2x.slt.sched.tdnsv8.com	61.176.194.20	true	false		unknown
02qyjs.com	23.224.122.132	true	false		unknown
img.alicdn.com.danuoyi.alicdn.com	47.246.49.251	true	false		high
accounts.google.com	172.217.168.45	true	false		high
sycdn.comtucdncom.com	172.67.42.54	true	false		unknown
na61-na62.wagbridge.alibaba.tanx.com.gds.alibabadns.com	203.119.169.41	true	false		unknown
hcdnd101.gslb.c.cdnhwc2.com	120.52.95.243	true	false		unknown
2021tupian.com	23.224.122.133	true	false		unknown
d.alicdn.com.w.cdngslb.com	163.181.50.252	true	false		unknown
pic.laoyaimg.com	213.159.203.19	true	false		unknown
crt.sectigo.com	91.199.212.52	true	false		unknown
clients.l.google.com	142.250.203.110	true	false		high
daka.70qn.com	23.225.154.19	true	false		unknown
fmlb.netlbtu.com	172.67.25.30	true	false		unknown
googlehosted.l.googleusercontent.com	142.250.203.97	true	false		high
z.gds.cnzz.com	106.11.84.4	true	false		high
hzvs2.cnzz.com	unknown	unknown	false		high
s13.cnzz.com	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
c.cnzz.com	unknown	unknown	false		high
icon.cnzz.com	unknown	unknown	false		high
www.cnzz.com	unknown	unknown	false		high
gxb.mmstat.com	unknown	unknown	false		unknown
ia.51.la	unknown	unknown	false		high
cdn.wuxiqiangheng.com	unknown	unknown	false		unknown
js.users.51.la	unknown	unknown	false		high
www.umeng.com	unknown	unknown	false		high
www.govguangxi.cn	unknown	unknown	false		unknown
g.alicdn.com	unknown	unknown	false		high
z3.cnzz.com	unknown	unknown	false		high
z7.cnzz.com	unknown	unknown	false		high
info.umeng.com	unknown	unknown	false		high
hqs2.cnzz.com	unknown	unknown	false		high
sc04.alicdn.com	unknown	unknown	false		high
z13.cnzz.com	unknown	unknown	false		high
cnzz.mmstat.com	unknown	unknown	false		unknown
q3.cnzz.com	unknown	unknown	false		high
hm.baidu.com	unknown	unknown	false		high
s4.cnzz.com	unknown	unknown	false		high
gm.mmstat.com	unknown	unknown	false		unknown
img.alicdn.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
at.alicdn.com	unknown	unknown	false		high
act.umeng.com	unknown	unknown	false		high
uweb.umeng.com	unknown	unknown	false		high
d.alicdn.com	unknown	unknown	false		high
fragment.tmall.com	unknown	unknown	false		high
new.cnzz.com	unknown	unknown	false		high
s5.cnzz.com	unknown	unknown	false		high
a.cnzz.com	unknown	unknown	false		high
node.www.umeng.com	unknown	unknown	false		high
w.cnzz.com	unknown	unknown	false		high
passport.umeng.com	unknown	unknown	false		high
www.govzhajian.cn	unknown	unknown	false		unknown
s.umeng.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://pentontraining.com/	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.pentontraining.com/	false		unknown
http://fmlb.netlbtu.com/images/2021/11/23/dmm15659.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.govguangxi.cn:4443/ty/x-5825-34-1.html	true		unknown
http://https://smtbb.cc:2022/index.php/vod/type/id/uCCCCS.html	true		unknown
http://fmlb.netlbtu.com/images/2021/11/23/jr17173.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.govguangxi.cn:4443/ty/x-5830-33-1.html	true		unknown
http://https://smtbb.cc:2022/index.php/vod/type/id/HCCCCS.html	true		unknown
http://fmlb.netlbtu.com/images/2021/7/27/dmm7543.jpg	false	• Avira URL Cloud: safe	unknown
http://fmlb.netlbtu.com/images/2021/11/23/dmm15656.jpg	false	• Avira URL Cloud: safe	unknown
http://www.pentontraining.com/tj.js	false	• Avira URL Cloud: safe	unknown
http://fmlb.netlbtu.com/images/2021/11/23/dmm15643.jpg	false	• Avira URL Cloud: safe	unknown
http://fmlb.netlbtu.com/images/2021/11/23/jr17172.jpg	false	• Avira URL Cloud: safe	unknown
http://fmlb.netlbtu.com/images/2021/11/23/jr17171.jpg	false	• Avira URL Cloud: safe	unknown
http://fmlb.netlbtu.com/images/2021/11/23/dmm15644.jpg	false	• Avira URL Cloud: safe	unknown
http://fmlb.netlbtu.com/images/2021/11/23/dmm15657.jpg	false	• Avira URL Cloud: safe	unknown
http://www.pentontraining.com/common.js	false	• Avira URL Cloud: safe	unknown
http://www.pentontraining.com/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://fmlb.netlbtu.com/images/2021/11/23/dmm15658.jpg	false	• Avira URL Cloud: safe	unknown
http://fmlb.netlbtu.com/images/2021/11/23/dmm15662.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.govguangxi.cn:4443/ty/x-5829-34-1.html	true		unknown
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt	false	• URL Reputation: safe	unknown
http://fmlb.netlbtu.com/images/2021/11/23/hey4569.jpg	false	• Avira URL Cloud: safe	unknown
http://https://smtbb.cc:2022/index.php/vod/type/id/0CCCCS.html	true		unknown
http://fmlb.netlbtu.com/images/2021/11/23/dmm15661.jpg	false	• Avira URL Cloud: safe	unknown
http://fmlb.netlbtu.com/images/2021/11/23/cc16500.jpg	false	• Avira URL Cloud: safe	unknown
http://new.cnzz.com/v1/login.php?siteid=1280563498	false		high
http://fmlb.netlbtu.com/images/2021/11/23/dmm15655.jpg	false	• Avira URL Cloud: safe	unknown
http://www.pentontraining.com/	true		unknown
http://fmlb.netlbtu.com/images/2021/11/23/hey4568.jpg	false	• Avira URL Cloud: safe	unknown
http://fmlb.netlbtu.com/images/2021/11/23/cc16498.jpg	false	• Avira URL Cloud: safe	unknown
http://https://smtbb.cc:2022/	true		unknown
http://fmlb.netlbtu.com/images/2021/11/23/dmm15660.jpg	false	• Avira URL Cloud: safe	unknown
http://https://uweb.umeng.com/v1/login.php?siteid=1280563498	false		high
http://fmlb.netlbtu.com/images/2021/11/23/hey4570.jpg	false	• Avira URL Cloud: safe	unknown
http://fmlb.netlbtu.com/images/2021/11/23/cc16499.jpg	false	• Avira URL Cloud: safe	unknown
http://fmlb.netlbtu.com/images/2021/11/23/hey4567.jpg	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
203.119.216.77	a.cnzz.com.gds.alibabadns.com	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
183.131.207.66	d2cb5ad7002c4066.huaweisafedns.com	China		136190	CHINATELECOM-ZHEJIANG-JINHUA-IDCJINHUAZHEJIANGProvince	false
91.199.212.52	crt.sectigo.com	United Kingdom		48447	SECTIGOGB	false
154.81.191.203	pentontraining.com	Seychelles		35916	MULTA-ASN1US	false
203.119.214.125	et2-na61-na62.wagbridge.alibaba.tanx.com.gds.alibabadns.com	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
59.82.60.44	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
59.82.60.43	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.203.97	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
47.246.2.234	fragment.tmall.com.danuoyi.alicdn.com	United States		24429	TAOBAOZhejiangTaobaoNetworkCoLtdCN	false
106.11.84.4	z.gds.cnzz.com	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
23.224.122.132	02qyjs.com	United States		40065	CNSERVERSUS	false
23.224.122.133	2021tupian.com	United States		40065	CNSERVERSUS	false
106.11.84.7	q.gds.cnzz.com	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
104.22.0.86	unknown	United States		13335	CLOUDFLARENETUS	false
59.82.31.92	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
101.132.251.31	log-api.aplus.emas-poc.com	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
218.94.207.228	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
47.246.136.160	gxb.mmstat.com.gds.alibabadns.com	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	false
103.235.46.191	hm.e.shifen.com	Hong Kong		55967	BAIDUBeijingBaiduNetcomScienceandTechnologyCoLtd	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.67.42.54	sycdn.comtucdncom.com	United States		13335	CLOUDFLARENETUS	false
172.67.25.30	fmlb.netlbtu.com	United States		13335	CLOUDFLARENETUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
23.225.154.19	daka.70qn.com	United States		40065	CNSERVERSUS	false
79.133.177.252	g.alicdn.com.danuoyi.alicdn.com	Russian Federation		43882	SOTLINE-ASRU	false
59.82.31.209	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
172.247.112.220	smtbb.cc	United States		40065	CNSERVERSUS	false
47.246.49.251	img.alicdn.com.danuoyi.alicdn.com	United States		24429	TAOBAOZhejiangTaobaoNetworkCoLtdCN	false
61.176.194.20	cagnon2x.slt.sched.tdnsv8.com	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
222.186.129.233	vip.70qn.com	China		23650	CHINANET-JS-AS-APASNumberforCHINANETjiangsuprovinceba	false
47.246.46.252	at.alicdn.com.danuoyi.alicdn.com	United States		24429	TAOBAOZhejiangTaobaoNetworkCoLtdCN	false
203.119.207.130	na61-na62.wagbridge.work.alibabacorp.com.gds.alibabadns.com	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
120.52.95.243	hcdnd101.gslb.c.cdnhwc2.com	China		133119	UNICOM-CNChinaUnicomIPnetworkCN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
58.215.157.250	icon.cnzz.com.danuoyi.tbcache.com	China		23650	CHINANET-JS-AS-APASNumberforCHINANETjiangsuprovinceba	false
203.119.175.170	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
59.82.29.248	default.cn.zb.wagbridge.umeng.alibabacorp.com.gds.alibabadns.com	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
203.119.169.41	na61-na62.wagbridge.alibaba.tanx.com.gds.alibabadns.com	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
163.181.50.252	d.alicdn.com.w.cdngslb.com	United States		24429	TAOBAOZhejiangTaobaoNetworkCoLtdCN	false
106.11.43.154	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
213.159.203.19	pic.laoyaimg.com	Russian Federation		12389	ROSTELECOM-ASRU	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532647
Start date:	02.12.2021
Start time:	15:34:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	**http**://pentontraining.com
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	12
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:	mal48.phis.win@35/202@57/43
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://www.cnzz.com/stat/website.php?web_id=1280563498 • Browse: https://smtbb.cc:2022/index.php/vod/type/id/uCCCCS.html • Browse: https://smtbb.cc:2022/index.php/vod/type/id/0CCCCS.html • Browse: https://smtbb.cc:2022/index.php/vod/type/id/HCCCCS.html
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF 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\30D802E0E248FEE17AAF4A62594CC75A	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\30D802E0E248FEE17AAF4A62594CC75A	
Size (bytes):	1559
Entropy (8bit):	7.399832861783252
Encrypted:	false
SSDEEP:	48:B4wgi+96jf8TXJgnXpxi4sVtcTtrdoh+S:KiIq0eZnep
MD5:	ADAB5C4DF031FB9299F71ADA7E18F613
SHA1:	33E4E80807204C2B6182A3A14B591ACD25B5F0DB
SHA-256:	7FA4FF68EC04A99D7528D5085F94907F4D1DD1C5381BACDC832ED5C960214676
SHA-512:	983B974E459A46EB7A3C8850EC90CC16D3B6D4A1505A5BCDD710C236BAF5AADC58424B192E34A147732E9D436C9FC04D896D8A7700FF349252A57514F588C6A
Malicious:	false
Reputation:	low
Preview:	0...0.....}[Q&.v...t...S..0...*.H.....0..1.0...U....US1.0...U....New Jersey1.0...U....Jersey City1.0...U....The USERTRUST Network1.0,..U...%USERTrust RSA Certification Authority0...181102000000Z..301231235959Z0..1.0...U....GB1.0...U....Greater Manchester1.0...U....Salford1.0...U....Sectigo Limited1705..U....Sectigo RSA Domain Validation Secure Server CA0.."0...*.H.....0.....s3..< ....E..>..?.A.20.l.....-?.M.....b..Hy...N..2%.....P?.L.@*.9.....2A.&.#z. ... .<.Do.u..@.2.....#>...o]Q.j.i.O.ri..Lm.....~... ...7x...4.V.X....d[.7..(h.V...\.....$..0.....z...B.....J.....@..o.BJd..0....'Z..X.....c.oV...`4.t....._.....n0..j0...U.#..0...Sy.Z.+J.T.....f.0...U.....^.T...w.....a.0...U.....0...U.... ...0.....0...U.%..0...+.....+.....0...U. ..0.0...U. .0...g.....0P..U...I0G0E.C.A.?http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl0v..+.....j0h0?..+.....0..3http://crt.usertrust.com/USERTrustRSAAddTrustCA.crt0%..+.....0.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\30D802E0E248FEE17AAF4A62594CC75A	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	282
Entropy (8bit):	3.12263295853183
Encrypted:	false
SSDEEP:	3:kkFklZnNl1fllXlE/lPbXx8bqlF8tlije9DZl2i9XYolzIllMltuN7ANJbZ15lqa:kKVjXxp9jKFIlaYM2+/LOjA/
MD5:	01C5B4BE774EA5B3151CD33F3945B1CF
SHA1:	A5AA6D8CEE7C765B0685D2F45432FAE24722C7A0
SHA-256:	0D2104A133C94F962A6D341C22F67BC19CB3970237DF08C8A514849D4F3DCD20
SHA-512:	0CF4DC8F74B0BDA52E03EC65BA699F529C01800E90D020E2D6418C9AEEE88E7AEAB4B253ED1E0C3B7885B08A631AB05DE500B024F274C50ECE0F8B6AF5E61DC5
Malicious:	false
Reputation:	low
Preview:	p..... .....l7.B....(..... .....@u.>r..@8.....h.t.t.p.:././.c.r.t...s.e.c.t.i.g.o...c.o.m./.S.e.c.t.i.g.o.R.S.A.D.o.m.a.i.n.V.a.l.i.d.a.t.i.o.n.S.e.c.u.r.e.S.e.r.v.e.r.C.A...c.r.t...".5.b.d.b.9.3.8.0.-.6.1.7."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\08e61189-f1b0-4eb3-be80-4777ca8fffbb.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):	399235
Entropy (8bit):	6.04764967547862
Encrypted:	false
SSDEEP:	6144:YMWT5jsSyAiP5i3aRG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinX:YMHSmc3aRGNPUZ+w7wJHyEtAW+
MD5:	F0A71DA2A6EF9381AC730E9F8578382C
SHA1:	B5B74745EAD4782E53C402A32039BEB7723FF50E
SHA-256:	13D4FF414741DA020F6494659C8B47DE50219B10BE614EBEBFD4E4E4E3F10258
SHA-512:	FB122D91047DB0AA590C6463C3B583EC26FC54E331C53E4DBD7CFA9E98676CA1712050E21FE77BBA4E131C802840715E94C299CA88DD8E872448E4FDA9E0A4D
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":1.638488114000646e+12,"network":1.638455715e+12,"ticks":167985729.0,"uncertainty":3993797.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\124f9881-5c2c-4966-b675-aa8715c3bedd.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.748889407168919
Encrypted:	false
SSDEEP:	384:h3tyK0PNQXAuVn52pNar/vOG3luQdHYtGRorzQO8xdIkQnrvWmDgzgqaWJOoE6N7:RGeZZKoxJgengqUIPXG+KYG65H

C:\Users\user\AppData\Local\Google\Chrome\User Data\124f9881-5c2c-4966-b675-aa8715c3bedd.tmp	
MD5:	410B05D976D84787EC2431B4BA961B14
SHA1:	9016F65A9AAFFE12FC15F3C9FE0AF98E3837388A
SHA-256:	8EBE7392F594473A78BBCA67B8617DA3386C1F3D9DB6CFF4647FD5D7A95600B6
SHA-512:	46521524CF3E97A9E5C4BA3CFAE1952EB4B1E94C1B9FED2831A0F21A3FDC226C4967FC15D71A984491E716CC58A005A7D02C492C7CEB670CCE68C8C2396EC 9
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....L.8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\3be92e81-6ed3-4897-a73e-7b2fcbc26794.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):	390872
Entropy (8bit):	6.027303852312546
Encrypted:	false
SSDEEP:	6144:HMWT5jsSyAiP5i3aRG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinX:HMHSmc3aRGNPUZ+w7wJHyEtAW+
MD5:	C8F2C3021C730335911C136EBB49BF2A
SHA1:	AB969D45B4D08E6F3826A1592709B0C0E62192FA
SHA-256:	CC80EED6A27DCA34832B6A3B512A2606BACEFBE05FEE55A3EA38E7E3798141D9
SHA-512:	D8DAB82C3866433598BAD2CFA9067F211A5149CCC8DBE107E8ADBAC596C0EFC808ECEA76CD873FD3014367EA27027306ED079F62FD8DCBB9718A0A981C8B7 8A
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"use r":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time": {"network_time_mapping":{"local":1.638488114000646e+12,"network":1.638455715e+12,"ticks":167985729.0,"uncertainty":3993797.0}},"os_crypt":{"encrypted_key":"RF BBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OU Dn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfi V1Q9wriZb5iS+jYbOXKVX44kAAAABYJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_man ager":{"os_password_blank":true,"os_password_last_changed":"13245952488002404"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\3efc8743-a7af-4fc3-b165-03feae4e617b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7481346932167363
Encrypted:	false
SSDEEP:	384:H3tyK0PNUAv2pNar/vOG3luQdHYtGRorzQO8xdlkQnrvWmDgzgqaWJOoE6Nb1KD4:XeZZKoxJgengqUIPXG+KYG65/
MD5:	C1276BA2F9F2432BD620AEE38F9CF7A3
SHA1:	4C20C2E9D83A74C367D2F0155FE7EEAE95B30D3A
SHA-256:	189A1C54A2F724B635F9F7233FDD5F7141CF2B8E2E97181727AA52FB9BC16F85
SHA-512:	B6726A145B29C36CA500C176285D4EAC4B2BD488B74EEC7ABA530E991370542B6F5602F96A731653A31FF5210374E735BE49DBD557F88BEFAD654F0A55AD9C8
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....L.8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\47562235-76ac-401b-8983-e71748058cf4.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7488429513003507
Encrypted:	false
SSDEEP:	384:R3tyK0PNQXAuVn52pNar/vOG3luQdHYtGRorzQO8xdlkQnrvWmD39zgqaWJOoE6+:hGeZZKoMJgengqUIPXG+KYG65k
MD5:	0A6F0D20EA3DB64D4F5CFE429101D524

C:\Users\user\AppData\Local\Google\Chrome\User Data\47562235-76ac-401b-8983-e71748058cf4.tmp	
SHA1:	392DBD441C54E7F0A5D9C5A682325A5F342648DC
SHA-256:	3C9072ECCA72800162DEFF0B148C528D327755D7A1052260347D22730A9F8112
SHA-512:	C8F57AC0FCB40C4174297593A8C81BA7651915B0205301DDA4460D9B906DCB620EFF55F7ED9A0491A4ABA2DED1DA8E1A062ADB9E9EC1A936E4B529340F3A45C
Malicious:	false
Reputation:	low
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....L.8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\4ddc14b7-42c9-43b6-89eb-485a7cc0281a.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):	399236
Entropy (8bit):	6.047650034452815
Encrypted:	false
SSDEEP:	6144:RMWT5jsSyAiP5i3aRG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinX:RMHSmc3aRGNPUZ+w7wJHyEtAW+
MD5:	0AAFA6632417A589799B2A812B153203
SHA1:	EC2350C78D67589D6064226F2A83DB9B8896096C
SHA-256:	3460D5B263ADFC46F2069D7BBDBE7CD9A09414642B4EE52860B783237AC57316
SHA-512:	86B334CC3065063B978D99F0E7E4B2EFC70FD10AF6AB576E7FE1C3C62C5788FFA20ED216E8C4A8749BAF689E83AE0C0931BFC1F1485A93E292B8FA995D97C634
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":1.638488114000646e+12,"network":1.638455715e+12,"ticks":167985729.0,"uncertainty":3993797.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488002404"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\5a86453f-ac3c-4886-b4e5-dc07d6b4e231.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):	390768
Entropy (8bit):	6.027114393917184
Encrypted:	false
SSDEEP:	6144:aMWT5jsSyAiP5i3aRG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinX:aMHSmc3aRGNPUZ+w7wJHyEtAW+
MD5:	CE39597F410058DAE818F31AEA8ACA55
SHA1:	A43615A63B4CF855754DFDE4BEF7F45CD46F291A
SHA-256:	81C3A31BBE8C51DB661B6B73024297F63A7833D54E54F0E86C2228C7BC9EDDE8
SHA-512:	BD24ED5B89FB209A8E2652E392F525F88B518B454EEA17B3414BDF90252D025B2AC57070EE0E7487D8D45178BF2E7DD3EEEDB839E3F1C23E802EB2E669D3FF37
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":1.638488114000646e+12,"network":1.638455715e+12,"ticks":167985729.0,"uncertainty":3993797.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488002404"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\755ed427-0fc7-40f8-92f5-6da49c49694c.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):	390958
Entropy (8bit):	6.0274176864989295
Encrypted:	false
SSDEEP:	6144:NMWT5jsSyAiP5i3aRG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinX:NMHSmc3aRGNPUZ+w7wJHyEtAW+
MD5:	030039C99D2B3C056720BF239B37CAF5

C:\Users\user\AppData\Local\Google\Chrome\User Data\755ed427-0fc7-40f8-92f5-6da49c49694c.tmp	
SHA1:	C662E5B4326D34ED4A7176387BFAA37F41699C80
SHA-256:	CE18F71B81F3D833C715DC55FCB244B20C23EFA3C94F467165311FFDE26C6716
SHA-512:	3DEE7BB6E4F29FE1CCF328763FA133C1529321839925353F4EE751D41D8D08CA352A8705B3065C97237FE852559D09177A41A234A10C034FB9C69550BA8E492A
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":1.638488114000646e+12,"network":1.638455715e+12,"ticks":167985729.0,"uncertainty":3993797.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488002404"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\84f3e848-7cbe-4c9f-905e-444e7bf7e5a8.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):	390768
Entropy (8bit):	6.027114393917184
Encrypted:	false
SSDEEP:	6144:aMWT5jsSyAiP5i3aRG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinX:aMHSmc3aRGNPUZ+w7wJHyEtAW+
MD5:	CE39597F410058DAE818F31AEA8ACA55
SHA1:	A43615A63B4CF855754DFDE4BEF7F45CD46F291A
SHA-256:	81C3A31BBE8C51DB661B6B73024297F63A7833D54E54F0E86C2228C7BC9EDDE8
SHA-512:	BD24ED5B89FB209A8E2652E392F525F88B518B454EEA17B3414BDF90252D025B2AC57070EE0E7487D8D45178BF2E7DD3EEEDB839E3F1C23E802EB2E669D3FF37
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":1.638488114000646e+12,"network":1.638455715e+12,"ticks":167985729.0,"uncertainty":3993797.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488002404"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\98887ec1-f4ef-4010-9976-662ee4c9d38e.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):	399236
Entropy (8bit):	6.047649770453321
Encrypted:	false
SSDEEP:	6144:3MWT5jsSyAiP5i3aRG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinX:3MHSmc3aRGNPUZ+w7wJHyEtAW+
MD5:	A521579CA194321980ACFF683CE483D8
SHA1:	0FE120D45CE2DF507F53E903D11EF1B9314984CC
SHA-256:	AE332F703AACEB22FCCD3A7E954DF7F3B9CC1EDFFC2B46D6C0C15215980435D7
SHA-512:	69D8D45A073359B43E1F1315CF80EED05CEF47A07A6E6756D1EA98851973759F22F30833DE00AED2754B786FF4604734884604DFD7E58A6021D1190A05BCD5BF
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":1.638488114000646e+12,"network":1.638455715e+12,"ticks":167985729.0,"uncertainty":3993797.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488002404"},"plugins":{"metadata":{"adobe-flash-player":{"disp

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):	40
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXEwozZHn:+EwozZHn
MD5:	BEBB369FF4A565B19D5E0BC83CD176AE
SHA1:	A6F07666F8DDDF61E5AACE533129BFB541A8A769

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

SHA-256:	8018F98553432706436A31FFD1E743018C3B7F1AA8D34B2FA18F494A4CFCEB19
SHA-512:	5D2F9F6E9502517AFF4673C3157D57046D4E38D70B5E228F468FB820363E559087D1A2F2E4006B4589BF3F175A4507F1FA3D7BE5FC34F9FA39EB17757DAEC17F
Malicious:	false
Reputation:	low
Preview:	sdPC......................y3..M.Y.NbD.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0d3d935d-09db-4177-8b6e-a45fd5a11835.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.5770945037337425
Encrypted:	false
SSDEEP:	384:ZottULlBYXm1kXqKf/pUZNCgVLH2HfDQrU9By+44g:tLl0m1kXqKf/pUZNCgVLH2HfsrUu1H
MD5:	1203C3FD17A8DEB9B30CF93ED477073D
SHA1:	130AEB29FAB5303816534F720E133CB684DFFD59
SHA-256:	4EC4B68412A796A291D33671BBD0F53EE2A94A5B8EF247A4C09998F72868547E
SHA-512:	0BFD363F3A08B25A4ADDDD1A6EC94A0FFFC95F12ECE208AF083B094774F52DF5ACC53A65DDF2C8303DB0D521DF8B231DCD4B23D611EA1A7A9437BA62BA5F AD0
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13282961711991619","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\1f6fccd9-5133-457f-897e-3774f76a72d3.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):	5146
Entropy (8bit):	4.978868955443446
Encrypted:	false
SSDEEP:	96:nTXbNegk9paAKIvjxk0JCKL8lkz1fKbOTQVuwn:nTXbNk9p9r4KekzBA
MD5:	7994B2468C5F611E4229765AEDB6E6D3
SHA1:	7BD7E5EF32818FF156211F9E3348647EE3BA9A63
SHA-256:	BC52D82535D884016E02C249EDEF54E90C4C3668A5FEBEA5B5C5BAC8DF98C8D5
SHA-512:	F59B7DC4CDFCE76BD710FE1B9AF550BC94DEBFE914D6593AE057E18D0D76F6D04190D13A942F2A354B5B60EA8E0A72A61EEC829262DD8B5332C35BCE0CABD 3AD
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13282961712527985","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2b78b0bf-e220-4329-b656-a22639d02eb5.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):	708
Entropy (8bit):	5.565174885477947
Encrypted:	false
SSDEEP:	12:Y5SybhUzQd+UAnIFdWYoIy9+UAnIO+YmY4CM2vN+UAnIZmeSrxEQ+UAnIYsQ:YMPzNUPoDsU3m4CM2YUcrxeUesQ
MD5:	B9E8401EE98D1E98A2973931FD758EFC
SHA1:	76E39E8DEF7E53C0698A55A9E7DDA53656C09C4C
SHA-256:	50A4D4E3E0C5237592B053BA626BB33EAF8374A30F997CF5A63EFBFBBC83C038
SHA-512:	CC8AC61FA69E3E23541EF44434FE061298FE701BA13851DB5D93E00E2069A1C71DC51505DEF6BA4AE8830AB4725DB5F65F47ACF14B9E498372AD07CA9B22AA 4
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2b78b0bf-e220-4329-b656-a22639d02eb5.tmp	
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1670024119.948557,"host":"KGyVyOzcH38WQtFj4DzXbgPV6WlJ6jEXlGCy7bQqxP0=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1638488119.948562},{"expiry":1670024116.932907,"host":"dB37gun4g0pYnpLvPJ85IXXrTzlvNN7CKVwSG+Hf4es=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1638488116.932913},{"expiry":1670024119.856428,"host":"vA9oKLb+VzFjdrV+bccuN8QaVNSXslt1MFtqqYkyfZI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1638488119.856433},{"expiry":1670024119.436192,"host":"7QT/HAN40NvtLf/i7IKTHV6PBeq7825X4YD7PSA5F3s=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1638488119.436195}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\524770a2-c214-4a6a-be0c-859903b25d5b.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):	5146
Entropy (8bit):	4.978868955443446
Encrypted:	false
SSDEEP:	96:nTXbNegk9paAKIvjxk0JCKL8lkz1fKbOTQVuwn:nTXbNk9p9r4KekzBA
MD5:	7994B2468C5F611E4229765AEDB6E6D3
SHA1:	7BD7E5EF32818FF156211F9E3348647EE3BA9A63
SHA-256:	BC52D82535D884016E02C249EDEF54E90C4C3668A5FEBEA5B5C5BAC8DF98C8D5
SHA-512:	F59B7DC4CDFCE76BD710FE1B9AF550BC94DEBFE914D6593AE057E18D0D76F6D04190D13A942F2A354B5B60EA8E0A72A61EEC829262DD8B5332C35BCE0CABD3AD
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13282961712527985","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5a86327c-82e2-4666-bc74-58f077047343.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):	708
Entropy (8bit):	5.566382763677624
Encrypted:	false
SSDEEP:	12:YabhUzQd+UAnIXmWYoIy9+UAnIO+YmYI34CM2vN+UAnIuvmeSrxEQ+UAnIYsQ:YnzNUdDsU3yI34CM2YUQvUrxeUesQ
MD5:	7CC9D446F40682F629494BC1A2ED59C5
SHA1:	C351A8D1FBE2F986C51EA64A6449C009550BA630
SHA-256:	8EA1D2C062371D26150D68BC1F7A41D6B368DDD2BFF9E2B435657271737FA671
SHA-512:	BD395DAF663F3B389D3B0D346760FF0F27C4084C0AFB0B52168E4AC821AFABC532E18A8EAA7B00E599A80CDD44CFDEA5CF8823846113FD06699A3D9F4F8073 7
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1670024177.089697,"host":"KGyVyOzcH38WQtFj4DzXbgPV6WlJ6jEXlGCy7bQqxP0=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1638488177.089703},{"expiry":1670024116.932907,"host":"dB37gun4g0pYnpLvPJ85IXXrTzlvNN7CKVwSG+Hf4es=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1638488116.932913},{"expiry":1670024171.935458,"host":"vA9oKLb+VzFjdrV+bccuN8QaVNSXslt1MFtqqYkyfZI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1638488171.935465},{"expiry":1670024119.436192,"host":"7QT/HAN40NvtLf/i7IKTHV6PBeq7825X4YD7PSA5F3s=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1638488119.436195}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5aa07afc-1669-4cc1-96a9-c08648641c7b.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):	708
Entropy (8bit):	5.566682820886664
Encrypted:	false
SSDEEP:	12:YDbhUzQd+UAnIWBWYoIy9+UAnIO+YmYI34CM2vN+UAnIuvmeSrxEQ+UAnIYsQ:YWzNUVDsU3yI34CM2YUQvUrxeUesQ
MD5:	6CC79BB3B161A5E399018BC918FBDEED
SHA1:	CDD6C85A0956BDBD49C94512666E5A56BE1CF82A
SHA-256:	B76F63E17FD345F84F343E6DC9B6562A3212550F5DB40EA4854309F962FAD39D
SHA-512:	D24319CFD94982B4E91C62442F01ED46E38419835862E8CDD7B83C5864DC7375C792BAFE7DB2AA2287306059CA7FA48547DC18319E2EC7D3F01D1F490D938CF
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5aa07afc-1669-4cc1-96a9-c08648641c7b.tmp

Preview:	{"expect_ct":[],"sts":[{"expiry":1670024171.049553,"host":"KGyVyOzcH38WQtFj4DzXbgPV6WlJ6jEXlGCy7bQqxP0=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1638488171.049561},{"expiry":1670024116.932907,"host":"dB37gun4g0pYnpLvPJ85IXXrTzlvNN7CKVwSG+Hf4es=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1638488116.932913},{"expiry":1670024171.935458,"host":"vA9oKLb+VzFjdrV+bccuN8QaVNSXslt1MFtqqYkyfZI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1638488171.935465},{"expiry":1670024119.436192,"host":"7QT/HAN40NvtLf/i7IKTHV6PBeq7825X4YD7PSA5F3s=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1638488119.436195}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7be8e5c1-f995-4b4d-95ab-696234609c74.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):	5132
Entropy (8bit):	4.977245542376917
Encrypted:	false
SSDEEP:	96:nTXbueRqm9paAKIvjxk0JCKL8lkz1fKbOTQVuwn:nTXbu9m9p9r4KekzBA
MD5:	F0263F1B03F44B0311C59CE183FA4A82
SHA1:	723B68D7557A8779A8430B4418640785FBA9BD17
SHA-256:	A4C04D39BFC90ED8BA3F6C2890AC66D7D4625CE0972B32EB4FAF372DD69E43C3
SHA-512:	61E39B737FDC7DC608A7C1EBB9A8EBAA462FA0AFEE00877F4D36C9449D4103BF4C3499CE3F34D3D7B7046F4225855C70A17F775DF8A5F2C2368EE1C4FAE7649
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13282961712527985","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\91766259-d4c1-47b0-9a71-f628aca0b38f.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):	2648
Entropy (8bit):	4.906310108162665
Encrypted:	false
SSDEEP:	48:YALteBdpNntw3qTCXDHz5s4TGsfIRLsRrr4qsLyKsAUAMHOq2vPsjxbG:2lNnOaTCXDHzFThIkr4RbGOq2vKxS
MD5:	52BC91D0904D8C3EA9E8136C0A189351
SHA1:	7840A3F1D363E4A1EC842B49ACE805973A7FFC8A
SHA-256:	54959B5A680E7FFC87E7262E9D72B362595C4FC0F18D56C6ED5FAD6F2C60195F
SHA-512:	FD107D7AA5BA84E614486AE16DB578C0AD8B714B8C89B37C0BBACC71E0113A4D9E37B28A38D910C60A4A7DF7D7EC39CBDEE03179835228EF3E2BA4E7C89E4713
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://www.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://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13285553714178472","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://r

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9d173c99-2d33-4abf-bd56-0181d3bb9e4c.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):	5211
Entropy (8bit):	4.985875759457278
Encrypted:	false
SSDEEP:	96:nTXbUe0L7k9paAKIvExk0JCKL8lkz1fKbOTQVuwn:nTXbUY9p9m4KekzBA
MD5:	63CE1075EEC2F5798598F21E38B6356F
SHA1:	32AA5A9128435E82F44F7765685704F38F0A18B0
SHA-256:	9D5ECC31641A687A6196FA4B4CC0C1BF4A1CA1200979F9F95CEA0A11EFEE90BD
SHA-512:	85C116E2013CBD646AB62FF03523572F0017FCAA7586B845F0BDC56B60524CCE5AEDCC1F54286DE07E474DC68F3110E95E9DF8B759624D0B852BCFB8C193B3I4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9d173c99-2d33-4abf-bd56-0181d3bb9e4c.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13282961712527985","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"daily_received_length":["0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUscllJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkIjEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

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):	38
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlXNQxlX:qTCT
MD5:	51A2CBB807F5085530DEC18E45CB8569
SHA1:	7AD88CD3DE5844C7FC269C4500228A630016AB5B
SHA-256:	1C43A1BDA1E458863C46DFAE7FB43BFB3E27802169F37320399B1DD799A819AC
SHA-512:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985DF
Malicious:	false
Reputation:	low
Preview:	.f.5................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):	375
Entropy (8bit):	5.215126988120863
Encrypted:	false
SSDEEP:	6:mNJVGq2PN723iKKdK25+Xqx8chI+IFUtMJX5NZmwKJyjzkwON723iKKdK25+Xqx7:i7GvVa5KkTXfchI3FUtMnN/KoP5Oa5KN
MD5:	6BC19C0C60BFFFCA059141D47FA92CDA
SHA1:	4D0730A027E46B800084E73719AEBAD84A72B016
SHA-256:	255BA1E9CEFC083A4C1A86196FFD914F30EF1A18E65F8EC5C134B4384B1DABEB
SHA-512:	523C32811A2CBE19DE26B0102682DC8C0DE5E088785873B7D70C2628EA7D411B439EF598B5BF389A2B61A8C4E55280266C4A81E77F9D58F8950637FC31A14CCI
Malicious:	false
Reputation:	low
Preview:	2021/12/02-15:35:29.850 f24 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/12/02-15:35:29.852 f24 Recovering log #3.2021/12/02-15:35:29.853 f24 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\AvailabilityDB\LOG.oldbc (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	375
Entropy (8bit):	5.215126988120863
Encrypted:	false
SSDEEP:	6:mNJVGq2PN723iKKdK25+Xqx8chI+IFUtMJX5NZmwKJyjzkwON723iKKdK25+Xqx7:i7GvVa5KkTXfchI3FUtMnN/KoP5Oa5KN
MD5:	6BC19C0C60BFFFCA059141D47FA92CDA
SHA1:	4D0730A027E46B800084E73719AEBAD84A72B016
SHA-256:	255BA1E9CEFC083A4C1A86196FFD914F30EF1A18E65F8EC5C134B4384B1DABEB
SHA-512:	523C32811A2CBE19DE26B0102682DC8C0DE5E088785873B7D70C2628EA7D411B439EF598B5BF389A2B61A8C4E55280266C4A81E77F9D58F8950637FC31A14CCI
Malicious:	false
Reputation:	low
Preview:	2021/12/02-15:35:29.850 f24 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/12/02-15:35:29.852 f24 Recovering log #3.2021/12/02-15:35:29.853 f24 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\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	855
Entropy (8bit):	5.482841411092195
Encrypted:	false
SSDEEP:	24:eQ7b3Rblp03C73ZLu3Xfl6T2dYTcrUNR8:eQ33RbTuCy3Xfl6ydIc5
MD5:	60A57DF2481872C00DDE3142ACB20880
SHA1:	6CC49D81F2FF1FD48BE617F3A55BBD4FA0571404
SHA-256:	E131710DB1A37A831E20712663549931O9CA18B27110C2E07B16F5342C78861F
SHA-512:	0DD83A6C5086E7274C0CE39D5F302E8CF3C8759A191F1A8004F32CA5E254DAF0EEB689021C90C29EF5B792441E3C90A7831DAF5199874175D8D26A8EF6E04E3
Malicious:	false
Reputation:	low
Preview:	.....T....com..http..pentontraining.....www*.....com.....http.....pentontraining.....www.....2.....a.....c.....e.....g.. .....h.....i.....m.....n.....o.....p.....r.....t.....w.....:o..... .....B.....b..... .....*.http://pentontraining.com/2$.....:.....k..... .....*.http://www.pentontraining.com/2$.....:..... .....J'.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy)	
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):	2825
Entropy (8bit):	4.86435102445835
Encrypted:	false
SSDEEP:	48:YALtdpBeMsNMHK5sJDysACs37sHWsd5/sSYMHCKs/MHCzsSOMHwsSJtFsX3RLs9D:HQxGKWDS1i/5vYGmGqOGKJ03QshS
MD5:	95488A82D5073BDAAFC1480073FF801F
SHA1:	E2E979B6D4A3EE16A815115C414D0A98E1DFA93F
SHA-256:	C091AE68AFCD5EC632B2C324B983D70F722463CB4D05A3CE8D52E07AA7E5A5D6
SHA-512:	D536466352320C5D394130A59B605617580050CDF325C4B3392D87D384C246E9D8C54FC16A247FF4B379F162536304E0D312D7781FFE245C643C5081B8BE08CD
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952675493","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":32613},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952813644","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952748754","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952634896","port":443,"protocol_str":"quic"}],"isolation":[],"server"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)	
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):	5146
Entropy (8bit):	4.978868955443446
Encrypted:	false
SSDEEP:	96:nTXbNegk9paAKIvjxk0JCKL8lkz1fKbOTQVuwn:nTXbNk9p9r4KekzBA

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)	
MD5:	7994B2468C5F611E4229765AEDB6E6D3
SHA1:	7BD7E5EF32818FF156211F9E3348647EE3BA9A63
SHA-256:	BC52D82535D884016E02C249EDEF54E90C4C3668A5FEBEA5B5C5BAC8DF98C8D5
SHA-512:	F59B7DC4CDFCE76BD710FE1B9AF550BC94DEBFE914D6593AE057E18D0D76F6D04190D13A942F2A354B5B60EA8E0A72A61EEC829262DD8B5332C35BCE0CABD 3AD
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13282961712527985","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences. (copy)	
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):	5146
Entropy (8bit):	4.978868955443446
Encrypted:	false
SSDEEP:	96:nTXbNegk9paAKIvjxk0JCKL8lkz1fKbOTQVuwn:nTXbNk9p9r4KekzBA
MD5:	7994B2468C5F611E4229765AEDB6E6D3
SHA1:	7BD7E5EF32818FF156211F9E3348647EE3BA9A63
SHA-256:	BC52D82535D884016E02C249EDEF54E90C4C3668A5FEBEA5B5C5BAC8DF98C8D5
SHA-512:	F59B7DC4CDFCE76BD710FE1B9AF550BC94DEBFE914D6593AE057E18D0D76F6D04190D13A942F2A354B5B60EA8E0A72A61EEC829262DD8B5332C35BCE0CABD 3AD
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13282961712527985","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\PreferencesMP (copy)	
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):	5211
Entropy (8bit):	4.985875759457278
Encrypted:	false
SSDEEP:	96:nTXbUe0L7k9paAKIvExk0JCKL8lkz1fKbOTQVuwn:nTXbUY9p9m4KekzBA
MD5:	63CE1075EEC2F5798598F21E38B6356F
SHA1:	32AA5A9128435E82F44F7765685704F38F0A18B0
SHA-256:	9D5ECC31641A687A6196FA4B4CC0C1BF4A1CA1200979F9F95CEA0A11EFEE90BD
SHA-512:	85C116E2013CBD646AB62FF03523572F0017FCAA7586B845F0BDC56B60524CCE5AEDCC1F54286DE07E474DC68F3110E95E9DF8B759624D0B852BCFB8C193B3I 4
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13282961712527985","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\PreferencesT. (copy)	
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):	5289
Entropy (8bit):	4.992838745235726
Encrypted:	false
SSDEEP:	96:nTXb7e0Lrk9paAKIvGxk0JCKL8lkz1fpbOTchVuwn:nTXb7Y9p9s4KekzBpH
MD5:	CC8395B57F88330B415504283174037C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\PreferencesT. (copy)	
SHA1:	952FB11A813D22D366944A3F91A109A062BDCFDC
SHA-256:	EC66C38B0AEF63561E0F44B701AC5B8DF4614F6D6E2BBC5E3A1F326720DFA3B5
SHA-512:	6D526F38B1FA82627DE455F9997E1520AB1B6859C2CBC679F0E966746F66D312026C4DFE868B39B2D3E56023CACC2162D20A815150244EF56D61E4AC124180A9
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13282961712527985","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences. (copy)	
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):	17092
Entropy (8bit):	5.582916751026906
Encrypted:	false
SSDEEP:	384:ZottFLlBYXm1kXqKf/pUZNCgVLH2HfDQrUt6Bd+44f:iLl0m1kXqKf/pUZNCgVLH2HfsrUE1A
MD5:	45DBD6F94FF0C444BC595B9D8390F522
SHA1:	799FB07AB4643CA8931D33D96DD44A92F407E90E
SHA-256:	92C9F08BB9BD9CE6B7EE332440FE509A5E8098D9FF8E117EC5DAC6DEE741A929
SHA-512:	17DE2B4789E4A3854C6F485956583F08EA06301FE3D64F668542000D1F2F3B7EF245D08C3B826A5DBAC4E988F89A70EEADB42D83A1E35ECD850D1840C9C0843
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13282961711991619","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\Secure Preferences.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.5770945037337425
Encrypted:	false
SSDEEP:	384:ZottULlBYXm1kXqKf/pUZNCgVLH2HfDQrU9By+44g:tLl0m1kXqKf/pUZNCgVLH2HfsrUu1H
MD5:	1203C3FD17A8DEB9B30CF93ED477073D
SHA1:	130AEB29FAB5303816534F720E133CB684DFFD59
SHA-256:	4EC4B68412A796A291D33671BBD0F53EE2A94A5B8EF247A4C09998F72868547E
SHA-512:	0BFD363F3A08B25A4ADDDD1A6EC94A0FFFC95F12ECE208AF083B094774F52DF5ACC53A65DDF2C8303DB0D521DF8B231DCD4B23D611EA1A7A9437BA62BA5F5AD0
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13282961711991619","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\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\85f5594e-647a-4a6e-959b-9af5c4100a0b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.95629898779197
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5kjxZsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdSZsBdLJlyH7E4f3K33y
MD5:	D5BB2F0F1694209F0C6AE5BA44DAC338

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\85f5594e-647a-4a6e-959b-9af5c4100a0b.tmp	
SHA1:	41B2CDE10C8937FC9607E608AF65EDF709033350
SHA-256:	20FC2ED4DA8AC625B83B6B84C1B88B534BC35B18DC8BD7521C66FFDABAB53738
SHA-512:	A713918E0F88AE62AFAC2A6202107CF547B962900BCB779C7C5C2C8A228C140AAC5191A50BDAF5718EAAE91446DB21648CF2A7B967B9029AF16F13E923FD6EE2
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544897343531","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):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E889858
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State* (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.95629898779197
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5kjxZsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdSZsBdLJlyH7E4f3K33y
MD5:	D5BB2F0F1694209F0C6AE5BA44DAC338
SHA1:	41B2CDE10C8937FC9607E608AF65EDF709033350
SHA-256:	20FC2ED4DA8AC625B83B6B84C1B88B534BC35B18DC8BD7521C66FFDABAB53738
SHA-512:	A713918E0F88AE62AFAC2A6202107CF547B962900BCB779C7C5C2C8A228C140AAC5191A50BDAF5718EAAE91446DB21648CF2A7B967B9029AF16F13E923FD6EE2
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544897343531","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\8b448f7d-2fa2-4737-ac01-0d0214e45f49.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.958114650763609
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV59YIEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdXXEsBdLJlyH7E4f3K33y
MD5:	F08847672DDD58749FE32FEFD1DBBAE9
SHA1:	C4C1750B297311628D53B0D3DD473F3EDD6019E9
SHA-256:	4165A9C7A2CA81E34A969C02FC75FFA899F49A5B04899EBA10E341C44839CC90
SHA-512:	541C4ADF3A92398F61F1E90C9995FD9CCB668FF51F578968C6CCD73AB81AB24668D969A9F98A1B529F631022EF4A3D224D76B4EDCB656ADADB27A7E40653950
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\8b448f7d-2fa2-4737-ac01-0d0214e45f49.tmp	
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544901990438","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):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898I58
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	436
Entropy (8bit):	5.190530202190765
Encrypted:	false
SSDEEP:	12:iJxpvVa5KkkGHArBFUtMJy/KJIT5Oa5KkkGHAryJ:idVa5KkkGgPgM5COa5KkkGga
MD5:	0BE0DC60B5F85D6415353ED948DC0C81
SHA1:	6454AA6A89F91C82A18522C3E8F677F95B49325C
SHA-256:	B3F5F45C7FF05541DE9EDE05AF1FF5A0809C4A7E6D69E710C980FAFAEB310BD7
SHA-512:	85D5628EC5695667B046A79772536DEAF80BE2409DCFEB1A05AB1388509157D7975E89FBA4D37125335F3ED9896016D94FAA107D09B0861B48C7A53905202A07
Malicious:	false
Reputation:	low
Preview:	2021/12/02-15:36:12.097 1864 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/12/02-15:36:12.105 1864 Recovering log #3.2021/12/02-15:36:12.109 1864 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\Local Storage\leveldb\LOG.oldg (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	436
Entropy (8bit):	5.190530202190765
Encrypted:	false
SSDEEP:	12:iJxpvVa5KkkGHArBFUtMJy/KJIT5Oa5KkkGHAryJ:idVa5KkkGgPgM5COa5KkkGga
MD5:	0BE0DC60B5F85D6415353ED948DC0C81
SHA1:	6454AA6A89F91C82A18522C3E8F677F95B49325C
SHA-256:	B3F5F45C7FF05541DE9EDE05AF1FF5A0809C4A7E6D69E710C980FAFAEB310BD7
SHA-512:	85D5628EC5695667B046A79772536DEAF80BE2409DCFEB1A05AB1388509157D7975E89FBA4D37125335F3ED9896016D94FAA107D09B0861B48C7A53905202A07
Malicious:	false
Reputation:	low
Preview:	2021/12/02-15:36:12.097 1864 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/12/02-15:36:12.105 1864 Recovering log #3.2021/12/02-15:36:12.109 1864 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\Network Persistent State. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Network Persistent State. (copy)	
Size (bytes):	325
Entropy (8bit):	4.958114650763609
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV59YIEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdXXEsBdLJlyH7E4f3K33y
MD5:	F08847672DDD58749FE32FEFD1DBBAE9
SHA1:	C4C1750B297311628D53B0D3DD473F3EDD6019E9
SHA-256:	4165A9C7A2CA81E34A969C02FC75FFA899F49A5B04899EBA10E341C44839CC90
SHA-512:	541C4ADF3A92398F61F1E90C9995FD9CCB668FF51F578968C6CCD73AB81AB24668D969A9F98A1B529F631022EF4A3D224D76B4EDCB656ADADB27A7E4065395A 0
Malicious:	false
Reputation:	low
Preview:	 {"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544901990438","port":443,"protocol_str":"quic"}],"isol ation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	438
Entropy (8bit):	5.149667443151634
Encrypted:	false
SSDEEP:	12:iJxYQ+vVa5KkkGHArqiuFUtMJX6g/KJCLQV5Oa5KkkGHArq2J:i6Va5KkkGgCgMZ6BOa5KkkGg7
MD5:	128564F810EB29C66DC84A0985788668
SHA1:	338A16B9F9FC5DDC2098AD9C08D769E0CA2C9B5B
SHA-256:	35B30BE00D5795C04F3428A31CDC779A7CCB2C2CE7A5A33FF20F74AB2ADCE55F
SHA-512:	63EAF1BEA4BCB956E30DD63AD6CC0C5708FA1EBC506CF67941440D7876F15F6C5B5BC651852475A8A225E50A9CEA51D96B84375B6B6573B367C285A16A7454
Malicious:	false
Reputation:	low
Preview:	 2021/12/02-15:36:12.098 15dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/12/02-15:36:12.106 15dc Recovering log #3.2021/12/02-15:36:12.111 15dc 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\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	438
Entropy (8bit):	5.149667443151634
Encrypted:	false
SSDEEP:	12:iJxYQ+vVa5KkkGHArqiuFUtMJX6g/KJCLQV5Oa5KkkGHArq2J:i6Va5KkkGgCgMZ6BOa5KkkGg7
MD5:	128564F810EB29C66DC84A0985788668
SHA1:	338A16B9F9FC5DDC2098AD9C08D769E0CA2C9B5B
SHA-256:	35B30BE00D5795C04F3428A31CDC779A7CCB2C2CE7A5A33FF20F74AB2ADCE55F
SHA-512:	63EAF1BEA4BCB956E30DD63AD6CC0C5708FA1EBC506CF67941440D7876F15F6C5B5BC651852475A8A225E50A9CEA51D96B84375B6B6573B367C285A16A7454
Malicious:	false
Reputation:	low
Preview:	 2021/12/02-15:36:12.098 15dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/12/02-15:36:12.106 15dc Recovering log #3.2021/12/02-15:36:12.111 15dc 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):	80
Entropy (8bit):	3.4921535629071894
Encrypted:	false
SSDEEP:	3:S8ltHlS+QUl1ASEGhTFljl:S85aEFljl
MD5:	69449520FD9C139C534E2970342C6BD8
SHA1:	230FE369A09DEF748F8CC23AD70FD19ED8D1B885
SHA-256:	3F2E9648DFDB2DDB8E9D607E8802FEF05AFA447E17733DD3FD6D933E7CA49277
SHA-512:	EA34C39AEA13B281A6067DE20AD0CDA84135E70C97DB3CDD59E25E6536B19F7781E5FC0CA4A11C3618D43FC3BD3FBC120DD5C1C47821A248B8AD351F9F4E6 67

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
Malicious:	false
Reputation:	low
Preview:	*...#.....version.1..namespace-..&f.....&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):	424
Entropy (8bit):	5.163146735976414
Encrypted:	false
SSDEEP:	12:i8YyvVa5KkkGHArAFUtMq/KiR5Oa5KkkGHArfJ:iWVa5KkkGgkgMrAOa5KkkGgV
MD5:	CCC14E53D3418EAE6B57350C2100FC43
SHA1:	804D5D5F8512164CFF7D0E67183EEFE5683267AD
SHA-256:	03220BCA5DC0C9CAD347E0908D04F026F6300CD7889A8E57F057C4BB683C59D6
SHA-512:	49AF9253E40035C131041B348635635F09200FA42D114E7B762365F55BEC669C7BF6A4BD0C5A14AB65275047C5AD86D0323902A3D5B1DD3AE629B32A84F477B3
Malicious:	false
Reputation:	low
Preview:	2021/12/02-15:36:28.144 16a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/12/02-15:36:28.145 16a4 Recovering log #3.2021/12/02-15:36:28.145 16a4 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\TransportSecurity (copy)	
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):	708
Entropy (8bit):	5.566682820886664
Encrypted:	false
SSDEEP:	12:YDbhUzQd+UAnIWBWYoIy9+UAnIO+YmYI34CM2vN+UAnIuvmeSrxEQ+UAnIYsQ:YWzNUVDsU3yI34CM2YUQvUrxeUesQ
MD5:	6CC79BB3B161A5E399018BC918FBDEED
SHA1:	CDD6C85A0956BDBD49C94512666E5A56BE1CF82A
SHA-256:	B76F63E17FD345F84F343E6DC9B6562A3212550F5DB40EA4854309F962FAD39D
SHA-512:	D24319CFD94982B4E91C62442F01ED46E38419835862E8CDD7B83C5864DC7375C792BAFE7DB2AA2287306059CA7FA48547DC18319E2EC7D3F01D1F490D938CF
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1670024171.049553,"host":"KGyVyOzcH38WQtFj4DzXbgPV6WlJ6jEXlGCy7bQqxP0=","mode":"force-https","sts_include_subdomains" :false,"sts_observed":1638488171.049561},{"expiry":1670024116.932907,"host":"dB37gun4g0pYnpLvPJ85IXXrTzlvNN7CKVwSG+Hf4es=","mode":"force-https","sts_i nclude_subdomains":false,"sts_observed":1638488116.932913},{"expiry":1670024171.935458,"host":"vA9oKLb+VzFjdrV+bccuN8QaVNSXslt1MFtqqYkyfZI=","mode":"f orce-https","sts_include_subdomains":false,"sts_observed":1638488171.935465},{"expiry":1670024119.436192,"host":"7QT/HAN40NvtLf/i7IKTHV6PBeq7825X4YD7P SA5F3s=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1638488119.436195}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a718ada4-dd26-4789-b16c-98d79475fd31.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):	17092
Entropy (8bit):	5.582916751026906
Encrypted:	false
SSDEEP:	384:ZottFLlBYXm1kXqKf/pUZNCgVLH2HfDQrUt6Bd+44f:iLl0m1kXqKf/pUZNCgVLH2HfsrUE1A
MD5:	45DBD6F94FF0C444BC595B9D8390F522
SHA1:	799FB07AB4643CA8931D33D96DD44A92F407E90E
SHA-256:	92C9F08BB9BD9CE6B7EE332440FE509A5E8098D9FF8E117EC5DAC6DEE741A929
SHA-512:	17DE2B4789E4A3854C6F485956583F08EA06301FE3D64F668542000D1F2F3B7EF245D08C3B826A5DBAC4E988F89A70EEADB42D83A1E35ECD850D1840C9C0843
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events": [],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13282961711991619","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVG ijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ac4acfe1-536b-4b76-a9ff-b2a5d0b7bba0.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):	2825
Entropy (8bit):	4.86435102445835
Encrypted:	false
SSDEEP:	48:YALtdpBeMsNMHK5sJDysACs37sHWsd5/sSYMHCKs/MHCzsSOMHwsSJtFsX3RLs9D:HQxGKWDS1i/5vYGmGqOGKJ03QshS
MD5:	95488A82D5073BDAAFC1480073FF801F
SHA1:	E2E979B6D4A3EE16A815115C414D0A98E1DFA93F
SHA-256:	C091AE68AFCD5EC632B2C324B983D70F722463CB4D05A3CE8D52E07AA7E5A5D6
SHA-512:	D536466352320C5D394130A59B605617580050CDF325C4B3392D87D384C246E9D8C54FC16A247FF4B379F162536304E0D312D7781FFE245C643C5081B8BE08CD
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952675493","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":32613},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952813644","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952748754","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952634896","port":443,"protocol_str":"quic"}],"isolation":[],"server"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b27b8324-fb75-414a-a45b-ebf70f2e2e0e.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):	5289
Entropy (8bit):	4.992964671656898
Encrypted:	false
SSDEEP:	96:nTXb7e0Lrk9paAKIvFxk0JCKL8lkz1fpbOTcUVuwn:nTXb7Y9p9J4KekzBpi
MD5:	17EE12F7E3C89574A4D45930353E1739
SHA1:	DBE3DE46926F2C9394582DEE8BDDCE6A98E4A7A0
SHA-256:	95EB6D769B1E668035084BD69309628E135F3A967F804F1BB2FEE67ED7D1C754
SHA-512:	2BC00ECD455CD5A21E47185068D79540390CB1EB881DD3AE6D3451363685F86B9BD184C19C886D484EF6A1FFAFFF46828E94236A3B3F4635A89EE1AFB49E88E
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13282961712527985","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c70fecca-6ddc-4258-bfad-5d23137a0d29.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):	19182
Entropy (8bit):	5.569936755334637
Encrypted:	false
SSDEEP:	384:ZottFLlBYXm1kXqKf/pUZNCgVLH2HfDQrUNHGn6B7j+44T:iLl0m1kXqKf/pUZNCgVLH2HfsrUxGwja
MD5:	217BA7A3378F86DD8662E198361E77B9
SHA1:	9707F2666C3677B2B65A1E54FC945EDCE2667213
SHA-256:	AF8B20ECD2848E5E6A9BDC39429891CD697941ABC7CFB11C4137CF688E230E67
SHA-512:	28ADFF31BB0B7450721DA8693A0B666E298988D175B9A0133DB4D0AD3AF29D9A34CFD6FEE6588C31A90537FF00E485CA3A3266C5EA1B2056D4880B7850F8499
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13282961711991619","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\d063a90b-21fd-4294-998b-ee77345facbf.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d063a90b-21fd-4294-998b-ee77345facbf.tmp	
Size (bytes):	5289
Entropy (8bit):	4.992838745235726
Encrypted:	false
SSDEEP:	96:nTXb7e0Lrk9paAKIvGxk0JCKL8lkz1fpbOTchVuwn:nTXb7Y9p9s4KekzBpH
MD5:	CC8395B57F88330B415504283174037C
SHA1:	952FB11A813D22D366944A3F91A109A062BDCFDC
SHA-256:	EC66C38B0AEF63561E0F44B701AC5B8DF4614F6D6E2BBC5E3A1F326720DFA3B5
SHA-512:	6D526F38B1FA82627DE455F9997E1520AB1B6859C2CBC679F0E966746F66D312026C4DFE868B39B2D3E56023CACC2162D20A815150244EF56D61E4AC124180A9
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13282961712527985","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d7dbd7a6-f8c0-4c35-a9a3-db0fce8eefe5.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	low
Preview:	.

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENTl (copy)	
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\dce54595-8243-41eb-9ec6-acf65b4ab1ca.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):	19181
Entropy (8bit):	5.569866768372386
Encrypted:	false
SSDEEP:	384:ZottFLlBYXm1kXqKf/pUZNCgVLH2HfDQrUNHGu6Bm+44g:iLl0m1kXqKf/pUZNCgVLH2HfsrUxGS1H
MD5:	0478ECC8F19043F92D3C8679D9DEDBFF
SHA1:	DC4855186F6A84CBF9794E76E77FF181F7AD19EB
SHA-256:	B06C006CD99EE4DA7675FC3E9CA0DFD56786D19B6D8BCD4AE5AB7343C43E689D
SHA-512:	C6B4AD6EE2D3B82770EC2F7329CECD54D3CD59C3DE986447D5B7C256407CFDEDAC1996459BF393A03DF065F2E90363ABA15EB9F8C3AB4049CA9464C9F4CD9EE
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13282961711991619","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	344
Entropy (8bit):	5.212208547822107
Encrypted:	false
SSDEEP:	6:mNJ2E29+q2PN723iKKdKfrzAdIFUtMJ2EPJZmwKJ2EtgF39VkwON723iKKdKfrzS:isr9+vVa5Kk9FUtMsKJ/KsbF39V5Oa5A
MD5:	14B07670AAC99995CBF22BBA51CA3CE2
SHA1:	F33012C139F3DF3C9CD6FD586EC4B7DF5EE935E6
SHA-256:	DBBF460E98E231A5362305785220F8543632A8CEEE5892AE7CBC12CDD808CF79
SHA-512:	1D724C09DFD0952E12C8299D5A55F6E23B11B803A4AD88ED4B86CFE3C3639560438247FA8DD7286216155E1EFCEFD731BF0D1B27918D9ECE99D156E0ACB3F3C
Malicious:	false
Reputation:	low
Preview:	2021/12/02-15:35:30.707 184c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/12/02-15:35:30.708 184c Recovering log #3.2021/12/02-15:35:30.709 184c 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\Default\shared_proto_db\metadata\LOG.old* (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	344
Entropy (8bit):	5.212208547822107
Encrypted:	false
SSDEEP:	6:mNJ2E29+q2PN723iKKdKfrzAdIFUtMJ2EPJZmwKJ2EtgF39VkwON723iKKdKfrzS:isr9+vVa5Kk9FUtMsKJ/KsbF39V5Oa5A
MD5:	14B07670AAC99995CBF22BBA51CA3CE2
SHA1:	F33012C139F3DF3C9CD6FD586EC4B7DF5EE935E6
SHA-256:	DBBF460E98E231A5362305785220F8543632A8CEEE5892AE7CBC12CDD808CF79
SHA-512:	1D724C09DFD0952E12C8299D5A55F6E23B11B803A4AD88ED4B86CFE3C3639560438247FA8DD7286216155E1EFCEFD731BF0D1B27918D9ECE99D156E0ACB3F3C
Malicious:	false
Reputation:	low
Preview:	2021/12/02-15:35:30.707 184c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/12/02-15:35:30.708 184c Recovering log #3.2021/12/02-15:35:30.709 184c 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:tblolIrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy)	
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):	399236
Entropy (8bit):	6.047649888295861
Encrypted:	false
SSDEEP:	6144:6MWT5jsSyAiP5i3aRG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinX:6MHSmc3aRGNPUZ+w7wJHyEtAW+
MD5:	6591F42E222F5B0D62E9C3F979B08E6E
SHA1:	6363218ED149EFDD75DA74E4B277BE2A9B922441
SHA-256:	E267CE4C0884CEE320BEA0E8F5C2A88736656ACF700701136D2F84820A28C460
SHA-512:	8474F4186495D6F8084A007438AA7F849C504EFCB1BE9F25BDC5D85C36EAA700B82330F643F221C9660C8C424802836646BEEF8912572D7CB39FC4443902E7B1
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":1.638488114000646e+12,"network":1.638455715e+12,"ticks":167985729.0,"uncertainty":3993797.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local StateMP (copy)	
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):	399236
Entropy (8bit):	6.047649770453321
Encrypted:	false
SSDEEP:	6144:3MWT5jsSyAiP5i3aRG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinX:3MHSmc3aRGNPUZ+w7wJHyEtAW+
MD5:	A521579CA194321980ACFF683CE483D8
SHA1:	0FE120D45CE2DF507F53E903D11EF1B9314984CC

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local StateMP (copy)	
SHA-256:	AE332F703AACEB22FCCD3A7E954DF7F3B9CC1EDFFC2B46D6C0C15215980435D7
SHA-512:	69D8D45A073359B43E1F1315CF80EED05CEF47A07A6E6756D1EA98851973759F22F30833DE00AED2754B786FF4604734884604DFD7E58A6021D1190A05BCD5BF
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":1.638488114000646e+12,"network":1.638455715e+12,"ticks":167985729.0,"uncertainty":3993797.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488002404"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local StateIt (copy)	
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):	399236
Entropy (8bit):	6.047650034452815
Encrypted:	false
SSDEEP:	6144:RMWT5jsSyAiP5i3aRG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinX:RMHSmc3aRGNPUZ+w7wJHyEtAW+
MD5:	0AAFA6632417A589799B2A812B153203
SHA1:	EC2350C78D67589D6064226F2A83DB9B8896096C
SHA-256:	3460D5B263ADFC46F2069D7BBDBE7CD9A09414642B4EE52860B783237AC57316
SHA-512:	86B334CC3065063B978D99F0E7E4B2EFC70FD10AF6AB576E7FE1C3C62C5788FFA20ED216E8C4A8749BAF689E83AE0C0931BFC1F1485A93E292B8FA995D97C634
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":1.638488114000646e+12,"network":1.638455715e+12,"ticks":167985729.0,"uncertainty":3993797.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488002404"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info CacheMP (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7481346932167363
Encrypted:	false
SSDEEP:	384:H3tyK0PNUAv2pNar/vOG3luQdHYtGRorzQO8xdIkQnrvWmDgzgqaWJOoE6Nb1KD4:XeZZKoxJgengqUIPXG+KYG65/
MD5:	C1276BA2F9F2432BD620AEE38F9CF7A3
SHA1:	4C20C2E9D83A74C367D2F0155FE7EEAE95B30D3A
SHA-256:	189A1C54A2F724B635F9F7233FDD5F7141CF2B8E2E97181727AA52FB9BC16F85
SHA-512:	B6726A145B29C36CA500C176285D4EAC4B2BD488B74EEC7ABA530E991370542B6F5602F96A731653A31FF5210374E735BE49DBD557F88BEFAD654F0A55AD9C8
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....L8.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\Module Info CacheN (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.748889407168919
Encrypted:	false
SSDEEP:	384:h3tyK0PNQXAuVn52pNar/vOG3luQdHYtGRorzQO8xdIkQnrvWmDgzgqaWJOoE6N7:RGeZZKoxJgengqUIPXG+KYG65H
MD5:	410B05D976D84787EC2431B4BA961B14
SHA1:	9016F65A9AAFFE12FC15F3C9FE0AF98E3837388A
SHA-256:	8EBE7392F594473A78BBCA67B8617DA3386C1F3D9DB6CFF4647FD5D7A95600B6

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info CacheN (copy)	
SHA-512:	46521524CF3E97A9E5C4BA3CFAE1952EB4B1E94C1B9FED2831A0F21A3FDC226C4967FC15D71A984491E716CC58A005A7D02C492C7CEB670CCE68C8C2396EC 9
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....L8.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\Subresource Filter\Indexed Rules\27\scoped_dir5448_3896177\Ruleset Data	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	142128
Entropy (8bit):	4.846664953094921
Encrypted:	false
SSDEEP:	3072:kYotddpTo2daWZy+CSzpjNTSha0NyruDcG4JCNDKR:kYoR+QNyYuDIL
MD5:	580DB025FA9444FBD3D00A0B7F4AEEE6
SHA1:	26BA225F9E58BA440E455B151AFA62E6DA71D052
SHA-256:	4DF7686CE689C87AE5AC45DE42E602ADB0AC316EE7C9F55717DEAD2509058ECC
SHA-512:	5940A7BA74606EC99BC366B42C47F32A89B11A6D1DF164C34BDE87241BE971BE81BC2762A6EACB5F58264573D1EDE7D233097D4A4CE6CBC033FA8B6507BE9D 9E
Malicious:	false
Reputation:	low
Preview:	.....$T..... ...X...l...h...d...0.....X...T...P...L...H.....@...<.....4...0...,.....\|...`...D..... ..... /.....ozama.....8/.....g.bat..... P/.....onwod.....h...h/.....ennab.....P..../.....nozam.....d..../.....geips...../.....rekoj...../.....lgoog.....@..../.....uotpo...../.....lreko.....H.../.....lR..... ...@R..$R...R...Q...Q..HR...Q..@R..<R..8R..4R...Q..,R..(R..$R.. R...R..TQ...R...R..0Q...R...Q...R...P...Q...Q...P...Q...Q...Q...Q...Q...P...Q..xP...Q...Q...Q..PP...Q...Q...Q... Q...Q...Q...Q...Q...Q...Q...Q...Q...P...O..\|Q..xQ..tQ..pQ..lQ..hQ..dQ..`Q..\Q...O..TQ...O..hO..HQ..DQ..@Q..@O..8Q..4Q..0Q..,Q..(Q..$Q.. Q...Q...Q...Q...Q...Q...Q. ..Q...P...P...N...P...N...P...P...P...P...P...P...P...P...N..lN..PN...P...P...P...P...P...P...N...P...P...P...P...M...P...M...P...P...P..|P..xP..tP..pP..lP..hP..dP..`P..\P..XP..TP..PP..xM..HP..

C:\Users\user\AppData\Local\Google\Chrome\User Data\d0b1314a-7b35-4c07-96da-d01457987cda.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):	399236
Entropy (8bit):	6.047649888295861
Encrypted:	false
SSDEEP:	6144:6MWT5jsSyAiP5i3aRG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinX:6MHSmc3aRGNPUZ+w7wJHyEtAW+
MD5:	6591F42E222F5B0D62E9C3F979B08E6E
SHA1:	6363218ED149EFDD75DA74E4B277BE2A9B922441
SHA-256:	E267CE4C0884CEE320BEA0E8F5C2A88736656ACF700701136D2F84820A28C460
SHA-512:	8474F4186495D6F8084A007438AA7F849C504EFCB1BE9F25BDC5D85C36EAA700B82330F643F221C9660C8C424802836646BEEF8912572D7CB39FC4443902E7B1
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"use r":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time": {"network_time_mapping":{"local":1.638488114000646e+12,"network":1.638455715e+12,"ticks":167985729.0,"uncertainty":3993797.0}},"os_crypt":{"encrypted_key":"RF BBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OU Dn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfi V1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_man ager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\01891a2b-1f5e-4cf8-89e8-eb6975905796.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21

C:\Users\user\AppData\Local\Temp\01891a2b-1f5e-4cf8-89e8-eb6975905796.tmp	
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\5448_1362032334\LICENSE	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1558
Entropy (8bit):	5.11458514637545
Encrypted:	false
SSDEEP:	48:OBOCrYJ4rYJVwUCLHDy43HV713XEyMmZ3teTHn:LCrYJ4rYJVwUCHZ3Z13XtdUTH
MD5:	EE002CB9E51BB8DFA89640A406A1090A
SHA1:	49EE3AD535947D8821FFDEB67FFC9BC37D1EBBB2
SHA-256:	3DBD2C90050B652D63656481C3E5871C52261575292DB77D4EA63419F187A55B
SHA-512:	D1FDCC436B8CA8C68D4DC7077F84F803A535BF2CE31D9EB5D0C466B62D6567B2C59974995060403ED757E92245DB07E70C6BDDBF1C3519FED300CC5B9BF91 C
Malicious:	false
Reputation:	low
Preview:	// Copyright 2015 The Chromium Authors. All rights reserved..//.// Redistribution and use in source and binary forms, with or without.// modification, are permitted provided that the following conditions are.// met:.//.// * Redistributions of source code must retain the above copyright.// notice, this list of conditions and the following disclaimer..// * Redistributions in binary form must reproduce the above.// copyright notice, this list of conditions and the following disclaimer.// in the documentation and/or other materials provided with the.// distribution..// * Neither the name of Google Inc. nor the names of its.// contributors may be used to endorse or promote products derived from.// this software without specific prior written permission..//.// THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS.// "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT.// LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR.// A PARTICULAR

C:\Users\user\AppData\Local\Temp\5448_1362032334_metadata\verified_contents.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):	1511
Entropy (8bit):	5.979291691594053
Encrypted:	false
SSDEEP:	24:pZRj/flTU3YO15a/KC+VjoYB7aoXmN+YAuA4wkr50+eToXvkocE272Cg9xZByxLE:p/hUIeoCCK7akmN+tuN5DeTkvrD2749N
MD5:	F967BFDDD97F602EDB5726B566780C67
SHA1:	EA8896D8E67E860C11DE3CFA8EBA0D4C462F7A9E
SHA-256:	D346723C1ADC48DDCC16C8E5E3CB6851D2471920FD58B5E29E4B6FA7651E9592
SHA-512:	7D7B1F840A8EE6E37096E5F13EF53C7DA78F736EB57686AF65422A40FFDDE2ECFF255998AADB740FC88F2C7AD9630A6ED8EBD0BC91DA566EDFD01D26B663E BA
Malicious:	false
Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiO lt7InBhdGgiOiJMSUNFTlNFIiwicm9vdF9oYXNoIjoiUGIwc2tBVUxaUzFqWldTQnctV0hIRkltRlhVcExiZDlUcVkwR2ZHSHBWcyJ9LHsicGF0aCI6ImNybC1zZXQiLCJ yb290X2hhc2giOiIzNEhva2RjVGhxX3huM0laMkE0TDlaYU1GWFRYbE94aDktdDFoTWZ6eDlvIn0seyJwYXRoIjoibWFuaWZlc3QuanNvbiIsInJvb3RfaGFzaCI6ImVEV WMzMjdqaF9EeFFqb0R5MXp5U1lhdER2Q2hseHlpMEVTbl9nY05qdXcifV0sImZvcm1hdCI6InRyZWVoYXNoIiwiaGFzaF9ibG9ja19zaXplIjo0MDk2fV0sIml0ZW1faWQ iOiJoZm5rcGltbGhoZ2llYWRkZ2ZlbWpob2ZtZmJsbW5pYiIsIml0ZW1fdmVyc2lvbiI6IjcwMTEiLCJwcm90b2NvbF92ZXJzaW9uIjoxfQ","signatures":[{"header":{"kid": "publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"ZYPYgIj-Y_KQ8rLb1au0dBFYxLkVPJTS17qTCkWXYNmFVxp0WyVBXZ7panyY9PwTAKwr7OARXI78lHp XH6DJM00u5NRSYWYuIOvPqFj8ekBwnkHc0Bq9XaZKUuo23sc_eWeAH0z-6mFaItYZ4rH91WM81d9XH0rhJ5hhtInEWveG9UP_hRKFBfyFSTr8tRyUaSbXuwM VQ6ls4j4DYQIGpVVMKZ82ufwfBMSeBZjS2AsxbfYb3eeMLBayzFnlrrIovB-

C:\Users\user\AppData\Local\Temp\5448_1362032334\crl-set	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	22506
Entropy (8bit):	7.823318814032266
Encrypted:	false
SSDEEP:	384:z26XPKKMeWUUxWVPpDzbm80WDzyloBG396550S8yzFP0trxasG9S3y/LaPJBr:zfG0ZVBDv2Wnylo6960S8It0r4sG/uP
MD5:	11C2E9F65FED549046B8A7FB0282C042
SHA1:	AC84C44C794A79AF427EF13ED8CCC3F9A99ECF15
SHA-256:	933B054D63E4542F84C8903CE627FADBD5991ED65AB7D0FE3FB2F19A6A8AE9BD
SHA-512:	720C317737792547ACDBAD2770904BF8754A6AD2CEB2A16220A71B63B60EA5857CEB7964E300E17CB17A5BE1F078934E3D2DDAF0049C2DD32B4560BFD11AF06 3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\5448_1362032334\crl-set	
Preview:	".{"Version":0,"ContentType":"CRLSet","Sequence":7011,"DeltaFrom":0,"NumParents":191,"BlockedSPKIs":["Jdoa1Yu/z7In2HI7GFfUwY57qnQXtPnv+TZrXoafizk=","li5LVLuYp+5dX+uWM/mR08MwDpUU2t57DU+CjHlPjoc=","yP3cdcsb27WMB7TqhHKH9iZIndZrwQomrdm1dbOgo40=","BN3pqpp59hSYaCMl+ghwJ2cH+5ypU4QSC0aJMmhJT8k=","tbqN1/iVZMKInT1kU8hJmMd4JJGbZOoINapimGWRvlA=","wO0gU0a7veButWD1zuAqNjTiR0p+ds+PvvVjuxF90OM=","eBpM8ukkUvPuAdDDgaQhTzkEFlw5CtvWH80RJE4Jstw=","/NdsyiNH5c1bOTR/Uc9DZUtpor/JBzZwpr5H2HAebg4=","lo26afv/Fb83YgiUMa3lp+rUt+rxvnACaBC8V9HGT24=","fNKVt1VEgIq9lAlGbwg3xarcAuM7YVDGZE3goJZZ8jw=","9Sk9R+041MMbLULe47WzrOl8omyirANl42Iu6AITH7s=","nFmjzK6kaZhCsGjPxSz5RdtRmGlXyDLNsYynOEn7ue4=","OUz/WJ5okxLPwHHuC8Gf5MYGIWzlQ0Kd5tti5C27O8E=","NuqWEoyJg5+2IfitDh7gucIgb2Kre02ixnZYk8m3ztI=","pqyh7JgJzFtIlf+dKcXr5lGWC5Gx8ZzIm1Xvh4GKlQk=","MO/kE4JHbDOA8C9+I+ZrovhnsFnuHqaHlrRBuFtdElY=","r1kVGOLmxg67/AkHr6pJvEBR1F5/IUq/7nUS7gD2Ye0=","6EnHF2yT32X2S2FpgjZuVmMReBK2+ivAyPqK6u5Bgcw=","0x7DkoW3pTGdAVfbQg7YfHQ+Mzu8d/h3H3BGT0NqYEk=","h7/Yr

C:\Users\user\AppData\Local\Temp\5448_1362032334\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):	3.8278192192699882
Encrypted:	false
SSDEEP:	3:SqHUdDE21irNU/E4cdEUy84zDT:Sq0y21irGMRi7zP
MD5:	A4C8FDA8592FD17EA1AD4BF082FC78AC
SHA1:	5CBF926543FF1927852408565B29A99621D5636C
SHA-256:	325E20F06B443EFA27537DE6F33775AF4416E970F8DBB9A8955076539BE3D920
SHA-512:	56539780A9ED829A516CA2E6245FC5E362FA249F9BC36B873D478CF88DF55DEFAF2E4946396FFA142786E8050E0B04CB0CD84223E1CA786A3D976CD8D7113E3
Malicious:	false
Reputation:	low
Preview:	1.f67b18faaf8d7cf1555edc37a1f3a2aae390664c38381e8385858c4ad6e840f6

C:\Users\user\AppData\Local\Temp\5448_1362032334\manifest.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	191
Entropy (8bit):	4.814344044116775
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFJ3cX3uKFgS1sEeSWU4pv/8F/FxLj2RF2fcTZTotL:F6VlMhS1tWfB0NpK4aotL
MD5:	942B31C383F74A19CD5E77646ACD62BB
SHA1:	6ADC927CA24F0D68E5B902476E8C446F2AA15C27
SHA-256:	78351CDF6EE387F0F1423A03CB5CF24986AD0EF0A1971CA2D044A7FE070D8EEC
SHA-512:	BB3670ECE7C9C8EE6D547E79929FACC05157A2AB509F641083DFB5CA73E91D05B97726D1BA96AE4E8167334657422FD9903857E33D94D9FA93A0E900B9484FE
Malicious:	false
Reputation:	low
Preview:	{. "manifest_version": 2,. "name": "crl-set-7065225719339459948.data",. "version": "7011",. "imageName": "image.squash",. "squash": true,. "fsType": "squashfs",. "isRemovable": false.}

C:\Users\user\AppData\Local\Temp\5448_1734265358\Filtering Rules	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	91283
Entropy (8bit):	5.445591581715125
Encrypted:	false
SSDEEP:	1536:FOONphT5b05W9w2ZH3HhahaHVFzIFSXkRrw8p1:HNNb0mwY3hpHVZIsX0d1
MD5:	492D833A4DACDC2843C7E1835DE22679
SHA1:	50461C265B3FF063690DFD7B5FDF742BA06DE36D
SHA-256:	081284C6EB49939EA138A836CD347C212E130266A4E0FAF3A5DF7C01F9F27E21
SHA-512:	9D82234FE1662226B348762028F7C2C9F0D36ACA06F758938ECE4F6D025FFCAA2FEC5D7A01E75B2156F914A7095E67EE3277B82DBF71445229121E4BBE779D13
Malicious:	false
Reputation:	low
Preview:	.....o0.8.@.R.-728x90.....o0.8.@.R.adtdp.com^.....o*...epaper.timesgroup.com*...nbcsports.com*...windalert.com*...kowb1290.com*...k2radio.com*...vimeo.com*..koel.com*...uefa.com0.8.@.R#googletagservices.com/tag/js/gpt.js.....o0.8.@.R./ad-inserter/.9.....o*...adcore.com.au..*...adcore.ch..0.8.@.R./adcore_.....o0.8.@.Ruwoaptee.com^.....o0.8.@.R._468_60..8.....o0.8.@.R)bancodevenezuela.com/imagenes/publicidad/.....o0.8.@.R..adbutler-.....o0.8.@.R.adrecover.com^.>....o*...google.com0.8.@.R!developers.google.com/google-ads/.-.....o*...vk.com0.8.@.R.vk.me/css/al/ads.css.+.....o0.8.@.R.mysmth.net/nForum/*/ADAgent_.....o0.8.@.R.indoleads.com^.%.....0.8.@.R.discordapp.com/banners/.D.....o*...daum.net0.8.@.R)daumcdn.net/adfit/static/ad-native.min.js.'.....o0.8.@.R.looker.com/api/internal/."......o0.8.@.R.broadstreetads.com^.....o0.8.@.R./banner.cgi?.....o*...thefreedictionary.com*...downloads.codefi.re*...windows7themes.net*...smallseotools.com*..

C:\Users\user\AppData\Local\Temp\5448_1734265358\LICENSE.txt	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\5448_1734265358\LICENSE.txt	
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	24623
Entropy (8bit):	4.588307081140814
Encrypted:	false
SSDEEP:	384:mva5sf5dXrCN7tnBxpxkepTqzazijFgZk231Py9zD6WApYbm0:mvagXreRnTqzazWgj0v6XqD
MD5:	D33AAA5246E1CE0A94FA15BA0C407AE2
SHA1:	11D197ACB61361657D638154A9416DC3249EC9FB
SHA-256:	1D4FF95CE9C6E21FE4A4FF3B41E7A0DF88638DD449D909A7B46974D3DFAB7311
SHA-512:	98B1B12FF0991FD7A5612141F83F69B86BC5A89DD62FC472EE5971817B7BBB612A034C746C2D81AE58FDF6873129256A89AA8BB7456022246DC4515BAAE2454B
Malicious:	false
Reputation:	low
Preview:	EasyList Repository Licences.... Unless otherwise noted, the contents of the EasyList repository.. (https://github.com/easylist) is dual licensed under the GNU General.. Public License version 3 of the License, or (at your option) any later.. version, and Creative Commons Attribution-ShareAlike 3.0 Unported, or.. (at your option) any later version. You may use and/or modify the files.. as permitted by either licence; if required, "The EasyList authors.. (https://easylist.to/)" should be attributed as the source of the.. material. All relevant licence files are included in the repository..... Please be aware that files hosted externally and referenced in the.. repository, including but not limited to subscriptions other than.. EasyList, EasyPrivacy, EasyList Germany and EasyList Italy, may be.. available under other conditions; permission must be granted by the.. respective copyright holders to authorise the use of their material.....Creative Commons Attribut

C:\Users\user\AppData\Local\Temp\5448_1734265358_metadata\verified_contents.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):	1529
Entropy (8bit):	5.987722096297769
Encrypted:	false
SSDEEP:	24:pZRj/flTHYXKl0kYbKNzjeT3qzkaoXqyCUV0szeMXmx0eoXECqG3l0+3pGX8fpaj:p/h4X8ybKNOTqkak1CSyxtkJl00AXN
MD5:	531658FD4A53DCAA6706C4E299F7F321
SHA1:	30E6E2BBF0C17CDED7D479A14E96468B94B647C3
SHA-256:	99CFEEE3A649590AB00880AFF978CB3E9BE65302AE2CD60B134387D606F1C79A
SHA-512:	727967425E95B297071B293CE9E18A4F9D4851819E93EFE1D8670DED887270ADCC9BECA280687E1DCD3AA6EDCFDDBE61A7074B92CEC95656CB2BC5DD995F9F5
Malicious:	false
Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJGaWx0ZXJpbmcgUnVsZXMiLCJyb290X2hhc2giOiJGb0toZEFTUTJiTGp4Mm9lODhqNnBVTTR4VF9aVDYwVWRvNGFvMEdQRW1rIn0seyJwYXRoIjoiTElDRU5TRS50eHQiLCJyb290X2hhc2giOiIyaWswNmk0TFlCdVNHNWphRGFIS253NE9pdnVSRzZsQ0JKMVk0TGtzRFJJJln0seyJwYXRoIjoibWFuaWZlc3QuanNvbiIsInJvb3RfaGFzaCI6IlhZRXVyY2cyNUN3eVpKSmpVbDk4LWlfaEUtbkMwRTVEYnU0Yl81Zm5FMWsifV0sImZvcm1hdCI6InRyZWVoYXNoIiwiaGFzaF9ibG9ja19zaXplIjo0MDk2fV0sIml0ZW1faWQiOiJnY21qa21nZGxnbmtrY29jbW9laW1pbmFpam1tam5paSIsIml0ZW1fdmVyc2lvbiI6IjAuMzIuMCIsInByb3RvY29sX3ZlcnNpb24iOjF9","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"yR3CR9-1WdhFXwIas-furfbkFjIT_vSCGmIc0g-d4snFbxb2ANfYiEM-CW7ZAilSpXLZEiYUxhrhtU6C-NbLrEfhyRxanHjYONy4YkWjp_VmS8dnZ1PAxC5KhmIOQoHRA4G4979n-OrSkHNubBTVntbKAdPl9YK0Wb6QBLBX_IFcvew8SKs2bhxb2SEf9PNAbM36eMVRZhTf6R7MfjxR-heObZwJJTnsgiqhOlldNjehhH2Pl

C:\Users\user\AppData\Local\Temp\5448_1734265358\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):	3.9462477267061056
Encrypted:	false
SSDEEP:	3:SxEQdYTVAUTVzDD4XScWGcY2R+Ql:SxEIYxAobaSnOQl
MD5:	665E5819FD3845C8CF669B0FC7C35244
SHA1:	C807724385F53E2B2410E269CAEEA719ABB03F76
SHA-256:	317A5B0177F17156279688F1FEF1D2568AAEB975239BB48702C76E2C4EFCC050
SHA-512:	19820AC3AC8FE1615AC15804EC7F735F932A957C2CCE690145240D74686DCEF87A91B2F918291525E386EBD1FE50BD31E4A1DC9E1EE0DFDB6D690523B97FA0I3
Malicious:	false
Reputation:	low
Preview:	1.dbbba5869c1d8946e5e23215c0404619fe82793d60eb89489b345ef55023e077

C:\Users\user\AppData\Local\Temp\5448_1734265358\manifest.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	115
Entropy (8bit):	4.545910352797257

C:\Users\user\AppData\Local\Temp\5448_1734265358\manifest.json	
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFHXG7LGMdv5HcDKhtUJKS17vC:F6VlMZWuMt5SKPS1rC
MD5:	B0E35F2BE526F795B810BE0E88B72358
SHA1:	0C7CB5B9E7AF8DE8ABB306CFB722994820656A1A
SHA-256:	5D812EADC836E42C32649263525F7CFA2FE113E9C2D04E436EEE1BFF97E71359
SHA-512:	6C35C45F3524824DD5B2D9A571B36687E3CEE375723F5467FCE2BB9F743D88D16D9F07015772AD8736725EA5F6C3366F1671505FCA18B0CE3EB6EC21B0FC41A
Malicious:	false
Reputation:	low
Preview:	{. "manifest_version": 2,. "name": "Subresource Filtering Rules",. "ruleset_format": 1,. "version": "9.32.0".}.

C:\Users\user\AppData\Local\Temp\623d69bb-9823-47d5-9baf-fa51bf7cf1c3.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n. <Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v....;.._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./ ?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U .KHF(n3.\"...,g.c...6)..(.E...U...#.i.a.:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F ....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...l.o...,....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\6a22cc1d-88b2-458d-b67a-681ab171e66c.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:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C 88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n. <Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L]....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..& ..l.6r[yU...%..f.....N..V.....<+.....l.}.{...z...)y.n..'..).....,b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,.. .W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6.. @?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\967463ec-2e22-4511-baa1-ebcf544b72fc.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false

C:\Users\user\AppData\Local\Temp\967463ec-2e22-4511-baa1-ebcf544b72fc.tmp	
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\scoped_dir5448_1078465076\623d69bb-9823-47d5-9baf-fa51bf7cf1c3.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n. <Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v....;.._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./ ?'.....L..fH&..._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U .KHF(n3.\"...,g.c...6)..(.E...U...#.i.a.:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....I-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F ....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...l.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\scoped_dir5448_1078465076\CRX_INSTALL_locales\am\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17307
Entropy (8bit):	5.461848619761356
Encrypted:	false
SSDEEP:	384:arfbEVrFvMP4rMhuDopC3vUuFBYZV6uml:aHEVrFvMP4KuFvr6D6uml
MD5:	26330929DF0ED4E86F06C00C03F07CE3
SHA1:	478F3B7E7A7E007BEE182B89C2EF6FFE6045E92C
SHA-256:	621B5139ED199022BB6529AF18ED4DC312AE9F3E90ECAF3B2C9E1D12114F5B22
SHA-512:	0BE6183A1BF12575C0F99960705D4249E79CDB8528C55FF132BE99A111F09494231AD6A36CD61B090A3B34C6971D68A29373BA346888E852C52E05DC14380682
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "....".. },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "1282768764603190 75": {.. "message": "..... ...".. },.. "142844886969078126731": {.. "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_dir5448_1078465076\CRX_INSTALL_locales\ar\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16809
Entropy (8bit):	5.458147730761559
Encrypted:	false
SSDEEP:	192:0lprKC78JmUjk8RkeryFOYPATxLZ8fsbE3/IFV6c8TEKdl:Jrp8JjA8RkerK0lc3wFV6uml
MD5:	44325A88063573A4C77F6EF943B0FC3E
SHA1:	78908D766F3E7A0E4545E7BD823C8ED47C7164EB
SHA-256:	67A439A08804EF4BEF261BDBADD8F0FEFD51729167D01EDCA99DD4AF57D6108B
SHA-512:	889C02BC986794C58C76022E78F57F867DD1D5217687F12D679A33A2DB9E5A18F3A37CF94D8FE4585E747C78E4662EAB93361FF7D945990774C7CFCACCFB79D
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "....".. },.. "1213957982723875920": {.. "message": ".. .. ..".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "...".. },.. "1636686747687494376": {.. "message": "....".. },.. "1802762746589457177": {.. "message": "..... .....".. },.. "1850397500312020388": {.. "message": "... .... Chromecast .. $START_LINK$..... Google HomeEND_LINK. $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {..

C:\Users\user\AppData\Local\Temp\scoped_dir5448_1078465076\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\scoped_dir5448_1078465076\CRX_INSTALL_locales\bg\messages.json	
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	18086
Entropy (8bit):	5.408731329060678
Encrypted:	false
SSDEEP:	192:4jjpr342SIwPIasR9VhMkACVmrv8evj+3eXivOMbb2vVzCkwRV6V6c8TEKdl:4ZrYo+rxT+qOV6V6uml
MD5:	6911CE87E8C47223F33BEF9488272E40
SHA1:	980398F076BB7D451B18D7FDE2DE09041B1F55AD
SHA-256:	273DEF0F67F0FA080802B85EF6F334DE50A19408F46BDF41F0F099B1F5501EEA
SHA-512:	CDB69405BB553E46DCF02F71B1A394307D0051E7FA662DFFEBA7888F30DD933F13C7FD6E32F1D7AEAEE8746316873B6E1D92029724ABDC75E49DCC092172EA2
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "......".. },.. "1213957982723875920": {.. "message": "... .. ..-..... ....?".. },.. "12827687 6460319075": {.. "message": "..... .. ..".. },.. "1428448869078126731": {.. "message": "..... .. ..".. },.. "1522140683318860351": {.. "message": "..... .. .., ...".. },.. "150904064710828958": {.. "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_dir5448_1078465076\CRX_INSTALL_locales\bn\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19695
Entropy (8bit):	5.315564774032776
Encrypted:	false
SSDEEP:	384:PrUCrcTIOeswIW/Vre/sZn8TFfzheV6uml:lPswIWtoK8xfG6uml
MD5:	F9DDF525C07251282A3BFFCEE9A09ABB
SHA1:	A343A078E804AF400A8F3E1891E3390DA754A5CD
SHA-256:	C69C6C90F7EB8F10685CD815AF1F6F1B87CF30C4E8D95DF1D577DE1105AAD227
SHA-512:	EBD339C37162984672513019D470B92DF8B743DD69D4430361EF12D42FD1C208DBDE818A7BFE20BE8A7D63CD6E02B3F4344DEA1C4AEDB8719D789981A49DA4C
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".... ...".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128 276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... ....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "150904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": "......".. },.. "18027627 46589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "$START_LINK$ Google

C:\Users\user\AppData\Local\Temp\scoped_dir5448_1078465076\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15518
Entropy (8bit):	5.242542310885
Encrypted:	false
SSDEEP:	384:drGUBKxMF2ayv8FrIccUVFmwf+7d9VKS3V6uml:dCUBKxMFBy0FE3UzmQ+zkSl6uml
MD5:	A90CF7930E7C3BEC61EE252DEFAD574A
SHA1:	F630CA01114A7BDD39607CB84B8280CCE218A5C6
SHA-256:	A533740E17559E2ADF40B4555C60F21EEC84E92C09CDBC19EED033A0B4DD2474
SHA-512:	598F991B344FA6724617D6CE57BB0D6D64EF86B4F5317BF6AD5EDF43E6B0A385094E7885F7A8FA2B107405B31C3D9F76E92315BC1D9BB52ACD4ECAD342917DE1
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Es congela".. },.. "1213957982723875920": {.. "message": "Quina de les opcions.seg.ents descriu millor la vostra xarxa?".. },.. "128276876460319075": {.. "message": "Detecci. de dispositius".. },.. "1428448869078126731": {.. "message": "Flu.desa del v.deo".. },.. "1522140683318860351": {.. "message": "S'ha produ.t un error en la connexi.. Torneu-ho a provar.".. },.. "150904064710828958": {.. "message": "Correcta".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volum".. },.. "1850397500312020388": {.. "message": "Pots veure el Chromecast a l'$START_LINK$aplicaci. Google.HomeEND_LINK?$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "

C:\Users\user\AppData\Local\Temp\scoped_dir5448_1078465076\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15552

C:\Users\user\AppData\Local\Temp\scoped_dir5448_1078465076\CRX_INSTALL_locales\cs\messages.json	
Entropy (8bit):	5.406413558584244
Encrypted:	false
SSDEEP:	192:eVdprJrG5efiTk93ebrxZR1fdc8VDCwT9fTV6c8TEKdl:2rMqiQerxQ88W7V6uml
MD5:	17E753EE877FDED25886D5F7925CA652
SHA1:	8E4EC969777CC0CEB7C12D0C1B9D87EBBB9C4678
SHA-256:	C562FCCFCE374D446BFAC30AC9B18FF17E7A3EF101C919FF857104917F300382
SHA-512:	33D61F6327FC81D7A45AA2CC97922DC527F5F43E54AA1A1638DA6EE407024A2F10CFD82CC5C3C581C2E7B216276987CB26C3FA95198572E139ACF29CC5B7AD B
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Video zamrz.".. },.. "1213957982723875920": {.. "message": "Kter. popis nejl.pe vystihuje va.i s..?".. },.. "128276876460319075": {.. "message": "Zji..ov.n. za..zen.".. },.. "1428448869078126731": {.. "message": "Plynulost videa".. },.. "1522140683318860351": {.. "message": "P.ipojen. se nezda.ilo. Zkuste to pros.m znovu.".. },.. "1550904064710828958": {.. "message": "Plynul.".. },.. "1636686747687494376": {.. "m essage": "Perfektn.".. },.. "1802762746589457177": {.. "message": "Hlasitost".. },.. "1850397500312020388": {.. "message": "Vid.te sv.j Chromecast v.$ST ART_LINK$aplikaci Google Home END_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. " END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir5448_1078465076\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15340
Entropy (8bit):	5.2479291792849105
Encrypted:	false
SSDEEP:	192:+Upr8XnI1MY2kPuir8j7Rd3kbTWc4QtV6c8TEKdl:FrJ1H9br8h6eZCV6uml
MD5:	F08A313C78454109B629B37521959B33
SHA1:	3D585D52EC8B4399F66D4BE88CED10F4A034FCCC
SHA-256:	23BF7E5EDF70291CA6D8F4A64788C5B86379EECB628E3DFA7DD83344612F7564
SHA-512:	9F2868AEBBF7F6167A7EA120FE65E752F9A65D1DC51072AA2413B2FDE374DA2D169D455A4788E341717F694179E6F1FA80413C080D9CD8CB397C3E84668CBFE
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Fryser".. },.. "1213957982723875920": {.. "message": "Hvilket af f.lgende udsagn beskriver bedst dit netv.rk?".. },.. "128276876460319075": {.. "message": "Enhedsregistrering".. },.. "1428448869078126731": {.. "message": "Videostabilitet".. },.. "152214068331 8860351": {.. "message": "Forbindelsen blev afbrudt. Pr.v igen.".. },.. "1550904064710828958": {.. "message": "Problemfri".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lydstyrke".. },.. "1850397500312020388": {.. "message": "Kan du se din Chromecast i $ START_LINK$ Google Home-appenEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "STAR

C:\Users\user\AppData\Local\Temp\scoped_dir5448_1078465076\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15555
Entropy (8bit):	5.258022363187752
Encrypted:	false
SSDEEP:	192:AJprM71A4qyJSwlk5KR5rtXsmvL0xhVw921YV6c8TEKdl:2re3jJS5A5rt8msA2KV6uml
MD5:	980FB419ED6ED94AD75686AFFB4E4C2E
SHA1:	871BFBCA6BCBA9197811883A93C50C0716562D57
SHA-256:	585C7814AFD2453232BC940252D4AE821D6E6CBCFD74A793F78E5DB8BA5342F1
SHA-512:	1681FA9C3BA882250A5005FB807D759EB8A634F1AA011725B1C865C0028BE7AB7BC16DC821A7F5BBFBA84C91E7D663ADE715284798E7E84E8FFF2D254488882
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "H.ngenbleiben".. },.. "1213957982723875920": {.. "message": "Welche dieser Aussagen beschreibt dein Netzwerk am besten?".. },.. "128276876460319075": {.. "message": "Ger.teerkennung".. },.. "1428448869078126731": {.. "message": "Videowiedergabequalit.t".. },.. "1522140683318860351": {.. "message": "Fehler beim Herstellen der Verbindung. Bitte versuche es noch einmal.".. },.. "1550904064710828958": {.. "message": "St.rungsfrei".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lautst.rke".. },.. "18503975003 12020388": {.. "message": "Siehst du deinen Chromecast in der $START_LINK$Google Home AppEND_LINK? $START_SPAN$*END_SPAN",.. "placeholde rs": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.

C:\Users\user\AppData\Local\Temp\scoped_dir5448_1078465076\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17941
Entropy (8bit):	5.465343004010711
Encrypted:	false
SSDEEP:	384:S0rDuhLh41cZrP3TzDBknbpgo6djlV6uml:S0fuBh46ZD3TzDinbpgoUK6uml

C:\Users\user\AppData\Local\Temp\scoped_dir5448_1078465076\CRX_INSTALL_locales\el\messages.json	
MD5:	40EB778339005A24FF9DA775D56E02B7
SHA1:	B00561CC7020F7FE717B5F692884253C689A7C61
SHA-256:	F56BF7C171AA20038EE30B754478B69A98F3014C89362779B0A8788C7B9BEEE1
SHA-512:	8BED281A33EC1E4E88A9F9D62BB13FE0266C0FAF8856D1DC2A843D26DD3CE5E7D1400FD3325ABD783B0364EC4FB1188AD941D56AEB9073BC365BE0D12DE6C013
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "......".. },.. "1213957982723875920": {.. "message": ".... ... .;".. },.. "1282768 76460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": "......".. },.. "1802762746589457177": {.. "message": "..... ....".. },.. "1850397500312020388": {.. "message": "..... .. .. Chromecast .... $START_LINK$..... Google HomeEND_LINK; $START_SPAN $*$END_SPAN$",.. "placeholders": {.. "END_LINK": {.. "content

C:\Users\user\AppData\Local\Temp\scoped_dir5448_1078465076\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	14897
Entropy (8bit):	5.197356586852831
Encrypted:	false
SSDEEP:	96:2MKUOp5N7GTNMRuv6M0bIt3FXGkW6/5NkkQ9NJKJhnH3t9F410sUA+ISN6cGDSyR:VKzprogudTGkWqrKcJhdIR+V6c8TEKdl
MD5:	8351AF4EA9BDD9C09019BC85D25B0016
SHA1:	F6EC1FFD291C8632758E01C9EE837B1AD18D4DCF
SHA-256:	F41C82D8A4F0E9B645656D630C882BE94A0FB7F8CEC0FE864B57298F0312B212
SHA-512:	75672B57F21F38F97341AD76A199AD764E9FBAB2384D701BF6EB06CEFDE6C4F20F047F9051A4E30D99621E5C1FBBDB9E38E8D2B47470806704B38DA130A146C
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Freezes".. },.. "1213957982723875920": {.. "message": "Which of the following best describes your network?".. },.. "128276876460319075": {.. "message": "Device Discovery".. },.. "1428448869078126731": {.. "message": "Video Smoothness".. },.. "1522140683318860 351": {.. "message": "Connection failed. Please try again.".. },.. "1550904064710828958": {.. "message": "Smooth".. },.. "1636686747687494376": {.. "message": "Perfect".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Are you able to see your Chrom ecast in the $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "START

C:\Users\user\AppData\Local\Temp\scoped_dir5448_1078465076\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15560
Entropy (8bit):	5.236752363299121
Encrypted:	false
SSDEEP:	192:NAgprfy1pTCukFr+1DIyDRoanvV6c8TEKdl:KMrq6FrmvV6uml
MD5:	8A70C18BB1090AA4D500DE9E8E4A00EF
SHA1:	8AFC097FA956C1317DB0835348B2DA19F0789669
SHA-256:	FF173D1CEF665B1234E02F11070ABD2B65230318150734579A03C7F31B4AE3F4
SHA-512:	140BAF40A4ABE9B8AF0855B0EBB7DFDF17869EDFC4EE1037C5EA7FDD8EDEBD4850E055B6A4D7B8782657618BCE1517813779BA01BA993CC838BB43E0BE71EEEE
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Congelaci.n de im.genes".. },.. "1213957982723875920": {.. "message": ".Cu.l de las siguientes respuestas descr ibe mejor tu red?".. },.. "128276876460319075": {.. "message": "Detecci.n de dispositivo".. },.. "1428448869078126731": {.. "message": "Fluidez del v.deo".. },.. "1522140683318860351": {.. "message": "Error en la conexi.n. Vuelve a intentarlo.".. },.. "1550904064710828958": {.. "message": "V.deo fluido".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volumen".. },.. "1850397500312020388": {.. "message": ".Puedes ver tu Chromecast en la $START_LINK$aplicaci.n Google.HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir5448_1078465076\CRX_INSTALL_locales\et\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15139
Entropy (8bit):	5.228213017029721
Encrypted:	false
SSDEEP:	96:Z48bxhWYp5Ny5M63niwAKD4rrJSJ2RkPXh9P5NFP2+NBMU01jewUEVez3QOiSevy:ikxprot3lYkf/rHBc0KsUV6c8TEKdl
MD5:	A62F12BCBA6D2C579212CA2FF90F8266
SHA1:	F7E964A2D9BBDA364252BCE5CFBA3FD34FDD825E
SHA-256:	3EB3EB0B3B4A8E5A477D1B3C3A3891CCC7DC6B8879ECE243A7BD7C478068273D

C:\Users\user\AppData\Local\Temp\scoped_dir5448_1078465076\CRX_INSTALL_locales\et\messages.json	
SHA-512:	E300201245C00ADEC8F39D586875F8FA4607AB203572BF3CE353C1CA7CDCA05B8786810CA0CEE27E4EA54A5EFD53690F1EA7AA4148CFF472A66BB1120272356
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Hangub".. },.. "1213957982723875920": {.. "message": "Milline j.rgmistest v.idetest kirjeldab k.ige paremini teie v.rku?".. },.. "128276876460319075": {.. "message": "Seadme tuvastamine".. },.. "1428448869078126731": {.. "message": "Video sujuvus".. },.. "1522140683318860351": {.. "message": ".hendamine eba.nnestus. Proovige uuesti.".. },.. "1550904064710828958": {.. "message": ".htlane".. },.. "1636686747687494376": {.. "message": "T.iuslik".. },.. "1802762746589457177": {.. "message": "Helitugevus".. },.. "1850397500312020388": {.. "message": "Kas n.ete oma Chromecasti $START_LINK$rakenduses Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir5448_1078465076\CRX_INSTALL_locales\fa\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17004
Entropy (8bit):	5.485874780010479
Encrypted:	false
SSDEEP:	192:rngaIprIX/t9wkjTJrs3hqaXxRQdiIMDnD+LhfHdoltV6c8TEKdl:4rin5rU1X7Qd0M9CtV6uml
MD5:	852BD3CFF960F1BC3A2AAB3CB3874EF9
SHA1:	C9F6F3C776542889FE3B67971D65ACFE048A3A0A
SHA-256:	D87597B6C10364501B98AA42524843F109009CCEF022D8E0170440D7F144F4C6
SHA-512:	2A7AE4D70E33E53EE31831CE2E61DD8DF103C4170EC483BDA14B8788E5DD536EEE84DBA340CACBDF16889C7E6465B48D82C4714E746E8A7B372D12CBDF37195
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".... ... .".. },.. "1213957982723875920": {.. "message": ".... .. ..".. },.. "1282768460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "....".. },.. "1802762746589457177": {.. "message": "..... ...".. },.. "1850397500312020388": {.. "message": ".... ..... Chromecast ... . $START_LINK$ ..... Google HomeEND_LINK ..... $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir5448_1078465076\CRX_INSTALL_locales\fi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15268
Entropy (8bit):	5.268402902466895
Encrypted:	false
SSDEEP:	192:efMprYXiYUNpj5Coik1tXxrUhvUzSPWV6c8TEKdl:eIrjbjosdrU5WV6uml
MD5:	3902581B6170D0CEA9B1ECF6CC82D669
SHA1:	C8208AC2B1DD6D4F8BDAAE01C8BD71FFFA5A732B
SHA-256:	D2A8180225A83A423BB6E17343DFA8F636D517154944002ED9240411B8C0C5E1
SHA-512:	612FDD8A3C5051F0A4F1E11E50B5D124B337C77D62D987D35C2AF9E08AFC6AFCEBAEE8D40FDFBCD1E1889F39758B96FAECBF6C6D1CF146C741A526195205021
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Pys.htyy".. },.. "1213957982723875920": {.. "message": "Mik. seuraavista kuvaa parhaiten verkkoasi?".. },.. "128276876460319075": {.. "message": "Laitteiden tunnistaminen".. },.. "1428448869078126731": {.. "message": "Videon tasaisuus".. },.. "1522140683318860351": {.. "message": "Yhteys ep.onnistui. Yrit. uudelleen.".. },.. "1550904064710828958": {.. "message": "Tasainen".. },.. "1636686747687494376": {.. "message": "T.ydellinen".. },.. "1802762746589457177": {.. "message": "..nenvoimakkuus".. },.. "1850397500312020388": {.. "message": "N.etk. Chromecastisi $START_LINK$Google Home .sovelluksessaEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },..

C:\Users\user\AppData\Local\Temp\scoped_dir5448_1078465076\CRX_INSTALL_locales\fil\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	12383
Entropy (8bit):	5.494089992951735
Encrypted:	false
SSDEEP:	192:xrQLrmhp68wl0fkKPJZrd4PyGnm3SRBiycLSK8eL+D75J4X:erP80sKPJZrKPy53jVLZqDA
MD5:	B698B5A4C95A37123FA3C738BFBB6523
SHA1:	2AA8FB8B5E08366A4E6A9AF95B31AB9871BEFD1C
SHA-256:	44A7157EBB87AC55EB1CCCA7DD31C8DE03C2141F7965E6D343758F589B5CE081
SHA-512:	9FCB2720C843ED66185CA97FF4D93C9A23B7579C77EA1D25A4BF5D3AB44D66A7E0B6FD8995705487859FB2461FEFD34B3D1032BFA966718982AEC771229EE37
Malicious:	false

C:\Users\user\AppData\Local\Temp\scoped_dir5448_1078465076\CRX_INSTALL_locales\fil\messages.json	
Reputation:	low
Preview:	{"1018984561488520517": {"message": "Hindi gumagalaw"}, "1213957982723875920": {"message": "Alin sa sumusunod ang pinakamahusay na naglalarawan sa iyong network?"}, "128276876460319075": {"message": "Pagtuklas ng Device"}, "1428448869078126731": {"message": "Pagka-smooth ng Video"}, "1522140683318860351": {"message": "Hindi nakakonekta. Pakisubukang muli."}, "1550904064710828958": {"message": "Smooth"}, "1636686747687494376": {"message": "Perpekto"}, "1802762746589457177": {"message": "Volume"}, "1850397500312020388": {"message": "Nakikita mo ba ang iyong Chromecast sa $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN", "placeholders": {"END_LINK": {"content": "$1"}, "END_SPAN": {"content": "$2"}, "START_LINK": {"content": "$3"}, "START_SPAN": {"content": "$4"}}}, "1850397500312020388_ph": {"message": "\ue000\ue000\ue000<span class=\"required-message\" ng-show=\"!top.sufficientFe

C:\Users\user\AppData\Local\Temp\scoped_dir5448_1078465076\CRX_INSTALL_locales\fr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	13082
Entropy (8bit):	5.506714680445029
Encrypted:	false
SSDEEP:	192:x7/ZQrr6x7U3kWXQ25Zri8EbeuGhZlsPj/LAP4wmHatiycLSK8eL+D75J4X:wrrKL25Zrikhk/LAP4w6VLZqDA
MD5:	29A947DEF8688A60267FA7CF5196F432
SHA1:	60F7A221077E13F29CD844C6F273A83C355F304D
SHA-256:	A13573E944CDAB491141F290C1C9772314A456E618E23D064D60E021EB5E92EC
SHA-512:	B62FDA4311406950E3D30622850D61166C9A0B4E43123511DF37E2D99D424EE9CE366081684A9B05C8064A460C81D256B3407E5405C33A5C354282C782884C9A
Malicious:	false
Reputation:	low
Preview:	{"1018984561488520517": {"message": "Se fige"}, "1213957982723875920": {"message": "Parmi les propositions suivantes, laquelle d\u00e9crit le mieux votre r\u00e9seau\u00a0?"}, "128276876460319075": {"message": "D\u00e9tection d'appareils"}, "1428448869078126731": {"message": "Fluidit\u00e9 de la vid\u00e9o"}, "1522140683318860351": {"message": "\u00c9chec de la connexion. Veuillez r\u00e9essayer."}, "1550904064710828958": {"message": "Fluide"}, "1636686747687494376": {"message": "Parfaite"}, "1802762746589457177": {"message": "Volume"}, "1850397500312020388": {"message": "Votre Chromecast est-il visible dans l'$START_LINK$ application Google\u00a0HomeEND_LINK\u00a0? $START_SPAN$*END_SPAN", "placeholders": {"END_LINK": {"content": "$1"}, "END_SPAN": {"content": "$2"}, "START_LINK": {"content": "$3"}, "START_SPAN": {"content": "$4"}}}, "1850397500312020388_ph": {"message": "\ue000\ue000<a href=\"https://support.google.com/chromecast/answer/2998456\" target=\"_blank\">\ue000

C:\Users\user\AppData\Local\Temp\scoped_dir5448_1078465076\CRX_INSTALL_locales\gu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22254
Entropy (8bit):	4.779170852082741
Encrypted:	false
SSDEEP:	384:DgtillrcJF8EgbOokOAZUgumAKtgYypgAW8V+aA9pk6yUISMUpAK8BP4yF4yJZCL:R252DjmZLG1VM0MLZqDA
MD5:	1F830A9EECC8B69B25D007873DF3255A
SHA1:	F50EF6F0D0E4DF50B64CBE58D50391820E90B188
SHA-256:	34AF1251F0AA10135883D8CB51F9AC1AD9D99F731CFB754529B7BA0D12357D04
SHA-512:	E315521DB19BA50EEF5F18893669E7AEE1D897C6B1DA0EB9E43FC0507486E18FCB0A7F07D995CAB1E713D6C161C042CBE9924AE0869A64D0D754CC9860CFD59
Malicious:	false
Reputation:	low
Preview:	{"1018984561488520517": {"message": "\u0ab8\u0acd\u0aa5\u0abf\u0ab0"}, "1213957982723875920": {"message": "\u0aa8\u0ac0\u0a9a\u0ac7\u0aa8\u0abe\u0aae\u0abe\u0a82\u0aa5\u0ac0 \u0a95\u0aaf\u0ac1\u0a82 \u0aa4\u0aae\u0abe\u0ab0\u0abe \u0aa8\u0ac7\u0a9f\u0ab5\u0ab0\u0acd\u0a95\u0aa8\u0ac1\u0a82 \u0ab6\u0acd\u0ab0\u0ac7\u0ab7\u0acd\u0aa0 \u0ab5\u0ab0\u0acd\u0aa3\u0aa8 \u0a95\u0ab0\u0ac7 \u0a9b\u0ac7?"}, "128276876460319075": {"message": "\u0a89\u0aaa\u0a95\u0ab0\u0aa3 \u0ab6\u0acb\u0aa7"}, "1428448869078126731": {"message": "\u0ab5\u0ac0\u0aa1\u0abf\u0aaf\u0acb\u0aa8\u0ac0 \u0ab8\u0ac1\u0a97\u0aae\u0aa4\u0abe"}, "1522140683318860351": {"message": "\u0a95\u0aa8\u0ac7\u0a95\u0acd\u0ab6\u0aa8 \u0aa8\u0abf\u0ab7\u0acd\u0aab\u0ab3 \u0aa5\u0aaf\u0ac1\u0a82. \u0a95\u0ac3\u0aaa\u0abe \u0a95\u0ab0\u0ac0\u0aa8\u0ac7 \u0aab\u0ab0\u0ac0\u0aa5\u0ac0 \u0aaa\u0acd\u0ab0\u0aaf\u0abe\u0ab8 \u0a95\u0ab0\u0acb."}, "1550904064710828958": {"message": "\u0ab8\u0ac1\u0a97\u0aae"}, "1636686747687494376": {"message"

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 15:35:14.002459049 CET	192.168.2.6	8.8.8.8	0xf0fd	Standard query (0)	pentontraining.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:14.031128883 CET	192.168.2.6	8.8.8.8	0x5222	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:14.047250986 CET	192.168.2.6	8.8.8.8	0xe53e	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:14.822489023 CET	192.168.2.6	8.8.8.8	0x3d75	Standard query (0)	www.pentontraining.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:16.016963959 CET	192.168.2.6	8.8.8.8	0xe898	Standard query (0)	02qyjs.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:16.483763933 CET	192.168.2.6	8.8.8.8	0x6b8c	Standard query (0)	crt.sectigo.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:17.241471052 CET	192.168.2.6	8.8.8.8	0xa53d	Standard query (0)	s4.cnzz.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:17.242260933 CET	192.168.2.6	8.8.8.8	0x1b0c	Standard query (0)	smtbb.cc	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:18.610851049 CET	192.168.2.6	8.8.8.8	0xe7e8	Standard query (0)	js.users.51.la	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:18.612379074 CET	192.168.2.6	8.8.8.8	0xedee	Standard query (0)	2021tupian.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:18.615051031 CET	192.168.2.6	8.8.8.8	0x6763	Standard query (0)	sc04.alicdn.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:18.615427971 CET	192.168.2.6	8.8.8.8	0x9cd5	Standard query (0)	cdn.wuxiqiangheng.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:18.646687031 CET	192.168.2.6	8.8.8.8	0x11ab	Standard query (0)	www.govzhajian.cn	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:18.970369101 CET	192.168.2.6	8.8.8.8	0x9039	Standard query (0)	c.cnzz.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:18.971805096 CET	192.168.2.6	8.8.8.8	0xff4f	Standard query (0)	z3.cnzz.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:19.231738091 CET	192.168.2.6	8.8.8.8	0x8b3e	Standard query (0)	www.govguangxi.cn	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:19.275918961 CET	192.168.2.6	8.8.8.8	0xc51c	Standard query (0)	fmlb.netlbtu.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:19.344444990 CET	192.168.2.6	8.8.8.8	0x4360	Standard query (0)	sycdn.comtucdncom.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:20.023683071 CET	192.168.2.6	8.8.8.8	0xd41a	Standard query (0)	ia.51.la	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:20.203028917 CET	192.168.2.6	8.8.8.8	0x9edd	Standard query (0)	cnzz.mmstat.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:20.284737110 CET	192.168.2.6	8.8.8.8	0xded0	Standard query (0)	www.cnzz.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:27.073836088 CET	192.168.2.6	8.8.8.8	0x1611	Standard query (0)	smtbb.cc	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:27.095310926 CET	192.168.2.6	8.8.8.8	0x20d3	Standard query (0)	2021tupian.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:27.123552084 CET	192.168.2.6	8.8.8.8	0xa251	Standard query (0)	sc04.alicdn.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:30.914988041 CET	192.168.2.6	8.8.8.8	0xefb9	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:39.245620012 CET	192.168.2.6	8.8.8.8	0xbe30	Standard query (0)	new.cnzz.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:40.517071009 CET	192.168.2.6	8.8.8.8	0x3b5e	Standard query (0)	uweb.umeng.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:43.140409946 CET	192.168.2.6	8.8.8.8	0x9407	Standard query (0)	at.alicdn.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:43.143290997 CET	192.168.2.6	8.8.8.8	0x8127	Standard query (0)	g.alicdn.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:43.146492004 CET	192.168.2.6	8.8.8.8	0x40c1	Standard query (0)	info.umeng.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:43.151273012 CET	192.168.2.6	8.8.8.8	0xc0f	Standard query (0)	s.umeng.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:45.907505035 CET	192.168.2.6	8.8.8.8	0xbee8	Standard query (0)	s5.cnzz.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 15:35:48.448211908 CET	192.168.2.6	8.8.8.8	0x4838	Standard query (0)	s13.cnzz.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:48.451191902 CET	192.168.2.6	8.8.8.8	0x487c	Standard query (0)	act.umeng.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:48.451638937 CET	192.168.2.6	8.8.8.8	0x74d3	Standard query (0)	w.cnzz.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:48.451940060 CET	192.168.2.6	8.8.8.8	0x322a	Standard query (0)	img.alicdn.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:48.452153921 CET	192.168.2.6	8.8.8.8	0x1d11	Standard query (0)	hm.baidu.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:48.452356100 CET	192.168.2.6	8.8.8.8	0xb7c5	Standard query (0)	d.alicdn.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:48.477165937 CET	192.168.2.6	8.8.8.8	0xbfc0	Standard query (0)	www.umeng.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:48.673517942 CET	192.168.2.6	8.8.8.8	0xd48a	Standard query (0)	node.www.umeng.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:48.676151037 CET	192.168.2.6	8.8.8.8	0xfd35	Standard query (0)	hzvs2.cnzz.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:49.765296936 CET	192.168.2.6	8.8.8.8	0xd412	Standard query (0)	icon.cnzz.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:53.457235098 CET	192.168.2.6	8.8.8.8	0x33e8	Standard query (0)	a.cnzz.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:53.457288980 CET	192.168.2.6	8.8.8.8	0x637	Standard query (0)	z13.cnzz.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:53.490297079 CET	192.168.2.6	8.8.8.8	0xe230	Standard query (0)	q3.cnzz.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:53.756900072 CET	192.168.2.6	8.8.8.8	0x276a	Standard query (0)	fragment.tmall.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:53.756949902 CET	192.168.2.6	8.8.8.8	0x79d5	Standard query (0)	passport.umeng.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:54.215214014 CET	192.168.2.6	8.8.8.8	0x54a0	Standard query (0)	log-api.aplus.emas-poc.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:54.488240004 CET	192.168.2.6	8.8.8.8	0x637	Standard query (0)	z13.cnzz.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:55.230537891 CET	192.168.2.6	8.8.8.8	0xa849	Standard query (0)	hqs2.cnzz.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:55.245471001 CET	192.168.2.6	8.8.8.8	0x55d7	Standard query (0)	z7.cnzz.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:56.412657022 CET	192.168.2.6	8.8.8.8	0x981a	Standard query (0)	gm.mmstat.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:56.723143101 CET	192.168.2.6	8.8.8.8	0x5f09	Standard query (0)	gxb.mmstat.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:59.621717930 CET	192.168.2.6	8.8.8.8	0x5f43	Standard query (0)	img.alicdn.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:59.651648998 CET	192.168.2.6	8.8.8.8	0xec09	Standard query (0)	icon.cnzz.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:36:07.830358982 CET	192.168.2.6	8.8.8.8	0x9135	Standard query (0)	pic.laoyaimg.com	A (IP address)	IN (0x0001)
Dec 2, 2021 15:36:19.893764019 CET	192.168.2.6	8.8.8.8	0xf42b	Standard query (0)	sycdn.comtucdncom.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 15:35:14.059101105 CET	8.8.8.8	192.168.2.6	0x5222	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:14.059101105 CET	8.8.8.8	192.168.2.6	0x5222	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:14.088155985 CET	8.8.8.8	192.168.2.6	0xe53e	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:14.174671888 CET	8.8.8.8	192.168.2.6	0xf0fd	No error (0)	pentontraining.com		154.81.191.203	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:14.988713026 CET	8.8.8.8	192.168.2.6	0x3d75	No error (0)	www.pentontraining.com		154.81.191.203	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:16.041599035 CET	8.8.8.8	192.168.2.6	0xe898	No error (0)	02qyjs.com		23.224.122.132	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 15:35:16.503504038 CET	8.8.8.8	192.168.2.6	0x6b8c	No error (0)	crt.sectigo.com		91.199.212.52	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:17.272294044 CET	8.8.8.8	192.168.2.6	0x1b0c	No error (0)	smtbb.cc		172.247.112.220	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:17.277843952 CET	8.8.8.8	192.168.2.6	0xa53d	No error (0)	s4.cnzz.com	c.cnzz.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:17.277843952 CET	8.8.8.8	192.168.2.6	0xa53d	No error (0)	c.cnzz.com	all.cnzz.com.danuoyi.tbcache.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:17.277843952 CET	8.8.8.8	192.168.2.6	0xa53d	No error (0)	all.cnzz.com.danuoyi.tbcache.com		58.215.157.250	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:18.632132053 CET	8.8.8.8	192.168.2.6	0xe7e8	No error (0)	js.users.51.la	js.users.51.la.c.cdnhwc1.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:18.632132053 CET	8.8.8.8	192.168.2.6	0xe7e8	No error (0)	js.users.51.la.c.cdnhwc1.com	hcdnd101.gslb.c.cdnhwc2.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:18.632132053 CET	8.8.8.8	192.168.2.6	0xe7e8	No error (0)	hcdnd101.gslb.c.cdnhwc2.com		120.52.95.243	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:18.632132053 CET	8.8.8.8	192.168.2.6	0xe7e8	No error (0)	hcdnd101.gslb.c.cdnhwc2.com		120.52.95.242	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:18.632132053 CET	8.8.8.8	192.168.2.6	0xe7e8	No error (0)	hcdnd101.gslb.c.cdnhwc2.com		218.12.76.151	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:18.632132053 CET	8.8.8.8	192.168.2.6	0xe7e8	No error (0)	hcdnd101.gslb.c.cdnhwc2.com		218.12.76.150	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:18.639909029 CET	8.8.8.8	192.168.2.6	0x6763	No error (0)	sc04.alicdn.com	sc04.alicdn.com.gds.alibabadns.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:18.639909029 CET	8.8.8.8	192.168.2.6	0x6763	No error (0)	sc04.alicdn.com.gds.alibabadns.com	static.wildcard.alicdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:18.643448114 CET	8.8.8.8	192.168.2.6	0xedee	No error (0)	2021tupian.com		23.224.122.133	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:18.668081999 CET	8.8.8.8	192.168.2.6	0x11ab	No error (0)	www.govzhajian.cn	daka.70qn.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:18.668081999 CET	8.8.8.8	192.168.2.6	0x11ab	No error (0)	daka.70qn.com		23.225.154.19	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:18.993382931 CET	8.8.8.8	192.168.2.6	0x9039	No error (0)	c.cnzz.com	all.cnzz.com.danuoyi.tbcache.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:18.993382931 CET	8.8.8.8	192.168.2.6	0x9039	No error (0)	all.cnzz.com.danuoyi.tbcache.com		218.94.207.228	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:19.113578081 CET	8.8.8.8	192.168.2.6	0x9cd5	No error (0)	cdn.wuxiqiangheng.com	cdn.wuxiqiangheng.com.cdn.dnsv1.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:19.113578081 CET	8.8.8.8	192.168.2.6	0x9cd5	No error (0)	cdn.wuxiqiangheng.com.cdn.dnsv1.com	cagnon2x.slt.sched.tdnsv8.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:19.113578081 CET	8.8.8.8	192.168.2.6	0x9cd5	No error (0)	cagnon2x.slt.sched.tdnsv8.com		61.176.194.20	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:19.113578081 CET	8.8.8.8	192.168.2.6	0x9cd5	No error (0)	cagnon2x.slt.sched.tdnsv8.com		59.83.204.154	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:19.113578081 CET	8.8.8.8	192.168.2.6	0x9cd5	No error (0)	cagnon2x.slt.sched.tdnsv8.com		59.83.204.153	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:19.113578081 CET	8.8.8.8	192.168.2.6	0x9cd5	No error (0)	cagnon2x.slt.sched.tdnsv8.com		110.52.193.33	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:19.113578081 CET	8.8.8.8	192.168.2.6	0x9cd5	No error (0)	cagnon2x.slt.sched.tdnsv8.com		116.177.248.23	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:19.251339912 CET	8.8.8.8	192.168.2.6	0x8b3e	No error (0)	www.govguangxi.cn	vip.70qn.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 15:35:19.251339912 CET	8.8.8.8	192.168.2.6	0x8b3e	No error (0)	vip.70qn.com		222.186.129.233	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:19.251339912 CET	8.8.8.8	192.168.2.6	0x8b3e	No error (0)	vip.70qn.com		222.186.150.152	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:19.251339912 CET	8.8.8.8	192.168.2.6	0x8b3e	No error (0)	vip.70qn.com		103.85.85.86	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:19.251339912 CET	8.8.8.8	192.168.2.6	0x8b3e	No error (0)	vip.70qn.com		202.189.8.69	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:19.298008919 CET	8.8.8.8	192.168.2.6	0xc51c	No error (0)	fmlb.netlbtu.com		172.67.25.30	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:19.298008919 CET	8.8.8.8	192.168.2.6	0xc51c	No error (0)	fmlb.netlbtu.com		104.22.45.113	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:19.298008919 CET	8.8.8.8	192.168.2.6	0xc51c	No error (0)	fmlb.netlbtu.com		104.22.44.113	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:19.298638105 CET	8.8.8.8	192.168.2.6	0xff4f	No error (0)	z3.cnzz.com	z.cnzz.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:19.298638105 CET	8.8.8.8	192.168.2.6	0xff4f	No error (0)	z.cnzz.com	z.gds.cnzz.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:19.298638105 CET	8.8.8.8	192.168.2.6	0xff4f	No error (0)	z.gds.cnzz.com		106.11.84.4	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:19.369136095 CET	8.8.8.8	192.168.2.6	0x4360	No error (0)	sycdn.comtucdncom.com		172.67.42.54	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:19.369136095 CET	8.8.8.8	192.168.2.6	0x4360	No error (0)	sycdn.comtucdncom.com		104.22.0.86	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:19.369136095 CET	8.8.8.8	192.168.2.6	0x4360	No error (0)	sycdn.comtucdncom.com		104.22.1.86	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:20.227638960 CET	8.8.8.8	192.168.2.6	0x9edd	No error (0)	cnzz.mmstat.com	gm.mmstat.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:20.227638960 CET	8.8.8.8	192.168.2.6	0x9edd	No error (0)	gm.mmstat.com	gm.gds.mmstat.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:20.227638960 CET	8.8.8.8	192.168.2.6	0x9edd	No error (0)	gm.gds.mmstat.com		47.246.136.160	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:20.345524073 CET	8.8.8.8	192.168.2.6	0xd41a	No error (0)	ia.51.la	d2cb5ad7002c4066.huaweisafedns.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:20.345524073 CET	8.8.8.8	192.168.2.6	0xd41a	No error (0)	d2cb5ad7002c4066.huaweisafedns.com		183.131.207.66	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:20.603097916 CET	8.8.8.8	192.168.2.6	0xded0	No error (0)	www.cnzz.com	default.wagbridge.umeng.alibabacorp.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:20.603097916 CET	8.8.8.8	192.168.2.6	0xded0	No error (0)	default.wagbridge.umeng.alibabacorp.com	default.wagbridge.umeng.alibabacorp.com.gds.alibabadns.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:20.603097916 CET	8.8.8.8	192.168.2.6	0xded0	No error (0)	default.wagbridge.umeng.alibabacorp.com.gds.alibabadns.com	default.cn.zb.wagbridge.umeng.alibabacorp.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:20.603097916 CET	8.8.8.8	192.168.2.6	0xded0	No error (0)	default.cn.zb.wagbridge.umeng.alibabacorp.com	default.cn.zb.wagbridge.umeng.alibabacorp.com.gds.alibabadns.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:20.603097916 CET	8.8.8.8	192.168.2.6	0xded0	No error (0)	default.cn.zb.wagbridge.umeng.alibabacorp.com.gds.alibabadns.com		59.82.29.248	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:27.098582983 CET	8.8.8.8	192.168.2.6	0x1611	No error (0)	smtbb.cc		172.247.112.220	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 15:35:27.114972115 CET	8.8.8.8	192.168.2.6	0x20d3	No error (0)	2021tupian.com		23.224.122.133	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:27.147664070 CET	8.8.8.8	192.168.2.6	0xa251	No error (0)	sc04.alicdn.com	sc04.alicdn.com.gds.alibabadns.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:27.147664070 CET	8.8.8.8	192.168.2.6	0xa251	No error (0)	sc04.alicdn.com.gds.alibabadns.com	static.wildcard.alicdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:30.934936047 CET	8.8.8.8	192.168.2.6	0xefb9	No error (0)	clients2.google usercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:30.934936047 CET	8.8.8.8	192.168.2.6	0xefb9	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:39.285384893 CET	8.8.8.8	192.168.2.6	0xbe30	No error (0)	new.cnzz.com	default.wagbridge.umeng.alibabacorp.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:39.285384893 CET	8.8.8.8	192.168.2.6	0xbe30	No error (0)	default.wagbridge.umeng.alibabacorp.com	default.wagbridge.umeng.alibabacorp.com.gds.alibabadns.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:39.285384893 CET	8.8.8.8	192.168.2.6	0xbe30	No error (0)	default.wagbridge.umeng.alibabacorp.com.gds.alibabadns.com	default.cn.zb.wagbridge.umeng.alibabacorp.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:39.285384893 CET	8.8.8.8	192.168.2.6	0xbe30	No error (0)	default.cn.zb.wagbridge.umeng.alibabacorp.com	default.cn.zb.wagbridge.umeng.alibabacorp.com.gds.alibabadns.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:39.285384893 CET	8.8.8.8	192.168.2.6	0xbe30	No error (0)	default.cn.zb.wagbridge.umeng.alibabacorp.com.gds.alibabadns.com		59.82.60.44	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:41.345628977 CET	8.8.8.8	192.168.2.6	0x3b5e	No error (0)	uweb.umeng.com	uweb.umeng.com.gds.alibabadns.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:41.345628977 CET	8.8.8.8	192.168.2.6	0x3b5e	No error (0)	uweb.umeng.com.gds.alibabadns.com	default.wagbridge.umeng.alibabacorp.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:41.345628977 CET	8.8.8.8	192.168.2.6	0x3b5e	No error (0)	default.wagbridge.umeng.alibabacorp.com	default.wagbridge.umeng.alibabacorp.com.gds.alibabadns.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:41.345628977 CET	8.8.8.8	192.168.2.6	0x3b5e	No error (0)	default.wagbridge.umeng.alibabacorp.com.gds.alibabadns.com	default.cn.zb.wagbridge.umeng.alibabacorp.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:41.345628977 CET	8.8.8.8	192.168.2.6	0x3b5e	No error (0)	default.cn.zb.wagbridge.umeng.alibabacorp.com	default.cn.zb.wagbridge.umeng.alibabacorp.com.gds.alibabadns.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:41.345628977 CET	8.8.8.8	192.168.2.6	0x3b5e	No error (0)	default.cn.zb.wagbridge.umeng.alibabacorp.com.gds.alibabadns.com		59.82.31.92	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:43.166393995 CET	8.8.8.8	192.168.2.6	0x8127	No error (0)	g.alicdn.com	g.alicdn.com.danuoyi.alicdn.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:43.166393995 CET	8.8.8.8	192.168.2.6	0x8127	No error (0)	g.alicdn.com.danuoyi.alicdn.com		79.133.177.252	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:43.166393995 CET	8.8.8.8	192.168.2.6	0x8127	No error (0)	g.alicdn.com.danuoyi.alicdn.com		79.133.177.251	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:43.190726995 CET	8.8.8.8	192.168.2.6	0xc0f	No error (0)	s.umeng.com	default.wagbridge.umeng.alibabacorp.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:43.190726995 CET	8.8.8.8	192.168.2.6	0xc0f	No error (0)	default.wagbridge.umeng.alibabacorp.com	default.wagbridge.umeng.alibabacorp.com.gds.alibabadns.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 15:35:43.190726995 CET	8.8.8.8	192.168.2.6	0xc0f	No error (0)	default.wagbridge.umeng.alibabacorp.com.gds.alibabadns.com	default.cn.zb.wagbridge.umeng.alibabacorp.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:43.190726995 CET	8.8.8.8	192.168.2.6	0xc0f	No error (0)	default.cn.zb.wagbridge.umeng.alibabacorp.com	default.cn.zb.wagbridge.umeng.alibabacorp.com.gds.alibabadns.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:43.190726995 CET	8.8.8.8	192.168.2.6	0xc0f	No error (0)	default.cn.zb.wagbridge.umeng.alibabacorp.com.gds.alibabadns.com		59.82.60.43	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:43.314990997 CET	8.8.8.8	192.168.2.6	0x40c1	No error (0)	info.umeng.com	et2-na61-na62.wagbridge.alibaba.tanx.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:43.314990997 CET	8.8.8.8	192.168.2.6	0x40c1	No error (0)	et2-na61-na62.wagbridge.alibaba.tanx.com	et2-na61-na62.wagbridge.alibaba.tanx.com.gds.alibabadns.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:43.314990997 CET	8.8.8.8	192.168.2.6	0x40c1	No error (0)	et2-na61-na62.wagbridge.alibaba.tanx.com.gds.alibabadns.com		203.119.214.125	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:44.161164045 CET	8.8.8.8	192.168.2.6	0x9407	No error (0)	at.alicdn.com	at.alicdn.com.danuoyi.alicdn.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:44.161164045 CET	8.8.8.8	192.168.2.6	0x9407	No error (0)	at.alicdn.com.danuoyi.alicdn.com		47.246.46.252	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:44.161164045 CET	8.8.8.8	192.168.2.6	0x9407	No error (0)	at.alicdn.com.danuoyi.alicdn.com		47.246.46.251	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:46.214560032 CET	8.8.8.8	192.168.2.6	0xbee8	No error (0)	s5.cnzz.com	c.cnzz.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:46.214560032 CET	8.8.8.8	192.168.2.6	0xbee8	No error (0)	c.cnzz.com	all.cnzz.com.danuoyi.tbcache.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:46.214560032 CET	8.8.8.8	192.168.2.6	0xbee8	No error (0)	all.cnzz.com.danuoyi.tbcache.com		218.94.207.228	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:48.471218109 CET	8.8.8.8	192.168.2.6	0x1d11	No error (0)	hm.baidu.com	hm.e.shifen.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:48.471218109 CET	8.8.8.8	192.168.2.6	0x1d11	No error (0)	hm.e.shifen.com		103.235.46.191	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:48.475131989 CET	8.8.8.8	192.168.2.6	0x322a	No error (0)	img.alicdn.com	img.alicdn.com.danuoyi.alicdn.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:48.475131989 CET	8.8.8.8	192.168.2.6	0x322a	No error (0)	img.alicdn.com.danuoyi.alicdn.com		47.246.49.251	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:48.475131989 CET	8.8.8.8	192.168.2.6	0x322a	No error (0)	img.alicdn.com.danuoyi.alicdn.com		47.246.49.252	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:48.475737095 CET	8.8.8.8	192.168.2.6	0x487c	No error (0)	act.umeng.com	na61-na62.wagbridge.alibaba.tanx.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:48.475737095 CET	8.8.8.8	192.168.2.6	0x487c	No error (0)	na61-na62.wagbridge.alibaba.tanx.com	na61-na62.wagbridge.alibaba.tanx.com.gds.alibabadns.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:48.475737095 CET	8.8.8.8	192.168.2.6	0x487c	No error (0)	na61-na62.wagbridge.alibaba.tanx.com.gds.alibabadns.com		203.119.169.41	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:48.484198093 CET	8.8.8.8	192.168.2.6	0xb7c5	No error (0)	d.alicdn.com	d.alicdn.com.w.cdngslb.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:48.484198093 CET	8.8.8.8	192.168.2.6	0xb7c5	No error (0)	d.alicdn.com.w.cdngslb.com		163.181.50.252	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 15:35:48.484198093 CET	8.8.8.8	192.168.2.6	0xb7c5	No error (0)	d.alicdn.com.w.cdngslb.com		163.181.50.251	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:48.494748116 CET	8.8.8.8	192.168.2.6	0x4838	No error (0)	s13.cnzz.com	c.cnzz.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:48.494748116 CET	8.8.8.8	192.168.2.6	0x4838	No error (0)	c.cnzz.com	all.cnzz.com.danuoyi.tbcache.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:48.494748116 CET	8.8.8.8	192.168.2.6	0x4838	No error (0)	all.cnzz.com.danuoyi.tbcache.com		218.94.207.228	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:48.497570038 CET	8.8.8.8	192.168.2.6	0x74d3	No error (0)	w.cnzz.com	c.cnzz.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:48.497570038 CET	8.8.8.8	192.168.2.6	0x74d3	No error (0)	c.cnzz.com	all.cnzz.com.danuoyi.tbcache.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:48.497570038 CET	8.8.8.8	192.168.2.6	0x74d3	No error (0)	all.cnzz.com.danuoyi.tbcache.com		218.94.207.228	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:48.516283035 CET	8.8.8.8	192.168.2.6	0xbfc0	No error (0)	www.umeng.com	default.wagbridge.umeng.alibabacorp.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:48.516283035 CET	8.8.8.8	192.168.2.6	0xbfc0	No error (0)	default.wagbridge.umeng.alibabacorp.com	default.wagbridge.umeng.alibabacorp.com.gds.alibabadns.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:48.516283035 CET	8.8.8.8	192.168.2.6	0xbfc0	No error (0)	default.wagbridge.umeng.alibabacorp.com.gds.alibabadns.com	default.cn.zb.wagbridge.umeng.alibabacorp.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:48.516283035 CET	8.8.8.8	192.168.2.6	0xbfc0	No error (0)	default.cn.zb.wagbridge.umeng.alibabacorp.com	default.cn.zb.wagbridge.umeng.alibabacorp.com.gds.alibabadns.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:48.516283035 CET	8.8.8.8	192.168.2.6	0xbfc0	No error (0)	default.cn.zb.wagbridge.umeng.alibabacorp.com.gds.alibabadns.com		59.82.31.209	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:49.112165928 CET	8.8.8.8	192.168.2.6	0xfd35	No error (0)	hzvs2.cnzz.com	z2.cnzz.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:49.112165928 CET	8.8.8.8	192.168.2.6	0xfd35	No error (0)	z2.cnzz.com	z.cnzz.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:49.112165928 CET	8.8.8.8	192.168.2.6	0xfd35	No error (0)	z.cnzz.com	z.gds.cnzz.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:49.112165928 CET	8.8.8.8	192.168.2.6	0xfd35	No error (0)	z.gds.cnzz.com		203.119.175.170	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:49.112207890 CET	8.8.8.8	192.168.2.6	0xd48a	No error (0)	node.www.umeng.com	node.www.umeng.com.gds.alibabadns.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:49.112207890 CET	8.8.8.8	192.168.2.6	0xd48a	No error (0)	node.www.umeng.com.gds.alibabadns.com	na61-na62.wagbridge.work.alibabacorp.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:49.112207890 CET	8.8.8.8	192.168.2.6	0xd48a	No error (0)	na61-na62.wagbridge.work.alibabacorp.com	na61-na62.wagbridge.work.alibabacorp.com.gds.alibabadns.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:49.112207890 CET	8.8.8.8	192.168.2.6	0xd48a	No error (0)	na61-na62.wagbridge.work.alibabacorp.com.gds.alibabadns.com		203.119.207.130	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:50.016346931 CET	8.8.8.8	192.168.2.6	0xd412	No error (0)	icon.cnzz.com	icon.cnzz.com.danuoyi.tbcache.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:50.016346931 CET	8.8.8.8	192.168.2.6	0xd412	No error (0)	icon.cnzz.com.danuoyi.tbcache.com		58.215.157.250	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 15:35:53.480067015 CET	8.8.8.8	192.168.2.6	0x33e8	No error (0)	a.cnzz.com	a.cnzz.com.gds.alibabadns.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:53.480067015 CET	8.8.8.8	192.168.2.6	0x33e8	No error (0)	a.cnzz.com.gds.alibabadns.com		203.119.216.77	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:53.791238070 CET	8.8.8.8	192.168.2.6	0x276a	No error (0)	fragment.tmall.com	fragment.tmall.com.danuoyi.alicdn.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:53.791238070 CET	8.8.8.8	192.168.2.6	0x276a	No error (0)	fragment.tmall.com.danuoyi.alicdn.com		47.246.2.234	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:53.791238070 CET	8.8.8.8	192.168.2.6	0x276a	No error (0)	fragment.tmall.com.danuoyi.alicdn.com		47.246.2.233	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:53.797473907 CET	8.8.8.8	192.168.2.6	0x79d5	No error (0)	passport.umeng.com	default.wagbridge.umeng.alibabacorp.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:53.797473907 CET	8.8.8.8	192.168.2.6	0x79d5	No error (0)	default.wagbridge.umeng.alibabacorp.com	default.wagbridge.umeng.alibabacorp.com.gds.alibabadns.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:53.797473907 CET	8.8.8.8	192.168.2.6	0x79d5	No error (0)	default.wagbridge.umeng.alibabacorp.com.gds.alibabadns.com	default.cn.zb.wagbridge.umeng.alibabacorp.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:53.797473907 CET	8.8.8.8	192.168.2.6	0x79d5	No error (0)	default.cn.zb.wagbridge.umeng.alibabacorp.com	default.cn.zb.wagbridge.umeng.alibabacorp.com.gds.alibabadns.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:53.797473907 CET	8.8.8.8	192.168.2.6	0x79d5	No error (0)	default.cn.zb.wagbridge.umeng.alibabacorp.com.gds.alibabadns.com		59.82.60.44	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:53.931869030 CET	8.8.8.8	192.168.2.6	0xe230	No error (0)	q3.cnzz.com	q.cnzz.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:53.931869030 CET	8.8.8.8	192.168.2.6	0xe230	No error (0)	q.cnzz.com	q.gds.cnzz.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:53.931869030 CET	8.8.8.8	192.168.2.6	0xe230	No error (0)	q.gds.cnzz.com		106.11.84.7	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:54.236393929 CET	8.8.8.8	192.168.2.6	0x54a0	No error (0)	log-api.aplus.emas-poc.com		101.132.251.31	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:54.744539022 CET	8.8.8.8	192.168.2.6	0x637	No error (0)	z13.cnzz.com	z.cnzz.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:54.744539022 CET	8.8.8.8	192.168.2.6	0x637	No error (0)	z.cnzz.com	z.gds.cnzz.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:54.744539022 CET	8.8.8.8	192.168.2.6	0x637	No error (0)	z.gds.cnzz.com		106.11.84.7	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:54.907155037 CET	8.8.8.8	192.168.2.6	0x637	No error (0)	z13.cnzz.com	z.cnzz.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:54.907155037 CET	8.8.8.8	192.168.2.6	0x637	No error (0)	z.cnzz.com	z.gds.cnzz.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:54.907155037 CET	8.8.8.8	192.168.2.6	0x637	No error (0)	z.gds.cnzz.com		106.11.84.7	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:55.269886017 CET	8.8.8.8	192.168.2.6	0x55d7	No error (0)	z7.cnzz.com	z.cnzz.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:55.269886017 CET	8.8.8.8	192.168.2.6	0x55d7	No error (0)	z.cnzz.com	z.gds.cnzz.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:55.269886017 CET	8.8.8.8	192.168.2.6	0x55d7	No error (0)	z.gds.cnzz.com		106.11.43.154	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 15:35:55.540112972 CET	8.8.8.8	192.168.2.6	0xa849	No error (0)	hqs2.cnzz.com	q3.cnzz.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:55.540112972 CET	8.8.8.8	192.168.2.6	0xa849	No error (0)	q3.cnzz.com	q.cnzz.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:55.540112972 CET	8.8.8.8	192.168.2.6	0xa849	No error (0)	q.cnzz.com	q.gds.cnzz.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:55.540112972 CET	8.8.8.8	192.168.2.6	0xa849	No error (0)	q.gds.cnzz.com		203.119.175.170	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:56.443427086 CET	8.8.8.8	192.168.2.6	0x981a	No error (0)	gm.mmstat.com	gm.gds.mmstat.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:56.443427086 CET	8.8.8.8	192.168.2.6	0x981a	No error (0)	gm.gds.mmstat.com		47.246.136.160	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:56.757107973 CET	8.8.8.8	192.168.2.6	0x5f09	No error (0)	gxb.mmstat.com	gxb.mmstat.com.gds.alibabadns.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:56.757107973 CET	8.8.8.8	192.168.2.6	0x5f09	No error (0)	gxb.mmstat.com.gds.alibabadns.com		47.246.136.160	A (IP address)	IN (0x0001)
Dec 2, 2021 15:35:59.675246000 CET	8.8.8.8	192.168.2.6	0xec09	No error (0)	icon.cnzz.com	icon.cnzz.com.danuoyi.tbcache.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:35:59.675246000 CET	8.8.8.8	192.168.2.6	0xec09	No error (0)	icon.cnzz.com.danuoyi.tbcache.com		58.215.157.250	A (IP address)	IN (0x0001)
Dec 2, 2021 15:36:00.045345068 CET	8.8.8.8	192.168.2.6	0x5f43	No error (0)	img.alicdn.com	img.alicdn.com.danuoyi.alicdn.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 15:36:00.045345068 CET	8.8.8.8	192.168.2.6	0x5f43	No error (0)	img.alicdn.com.danuoyi.alicdn.com		47.246.49.252	A (IP address)	IN (0x0001)
Dec 2, 2021 15:36:00.045345068 CET	8.8.8.8	192.168.2.6	0x5f43	No error (0)	img.alicdn.com.danuoyi.alicdn.com		47.246.49.251	A (IP address)	IN (0x0001)
Dec 2, 2021 15:36:07.851351023 CET	8.8.8.8	192.168.2.6	0x9135	No error (0)	pic.laoyaimg.com		213.159.203.19	A (IP address)	IN (0x0001)
Dec 2, 2021 15:36:07.851351023 CET	8.8.8.8	192.168.2.6	0x9135	No error (0)	pic.laoyaimg.com		83.217.10.236	A (IP address)	IN (0x0001)
Dec 2, 2021 15:36:07.851351023 CET	8.8.8.8	192.168.2.6	0x9135	No error (0)	pic.laoyaimg.com		37.220.37.246	A (IP address)	IN (0x0001)
Dec 2, 2021 15:36:07.851351023 CET	8.8.8.8	192.168.2.6	0x9135	No error (0)	pic.laoyaimg.com		37.220.37.250	A (IP address)	IN (0x0001)
Dec 2, 2021 15:36:07.851351023 CET	8.8.8.8	192.168.2.6	0x9135	No error (0)	pic.laoyaimg.com		37.220.37.248	A (IP address)	IN (0x0001)
Dec 2, 2021 15:36:07.851351023 CET	8.8.8.8	192.168.2.6	0x9135	No error (0)	pic.laoyaimg.com		192.74.252.144	A (IP address)	IN (0x0001)
Dec 2, 2021 15:36:07.851351023 CET	8.8.8.8	192.168.2.6	0x9135	No error (0)	pic.laoyaimg.com		185.134.120.95	A (IP address)	IN (0x0001)
Dec 2, 2021 15:36:07.851351023 CET	8.8.8.8	192.168.2.6	0x9135	No error (0)	pic.laoyaimg.com		37.220.37.249	A (IP address)	IN (0x0001)
Dec 2, 2021 15:36:07.851351023 CET	8.8.8.8	192.168.2.6	0x9135	No error (0)	pic.laoyaimg.com		137.175.32.1	A (IP address)	IN (0x0001)
Dec 2, 2021 15:36:07.851351023 CET	8.8.8.8	192.168.2.6	0x9135	No error (0)	pic.laoyaimg.com		185.134.120.93	A (IP address)	IN (0x0001)
Dec 2, 2021 15:36:07.851351023 CET	8.8.8.8	192.168.2.6	0x9135	No error (0)	pic.laoyaimg.com		37.220.37.247	A (IP address)	IN (0x0001)
Dec 2, 2021 15:36:07.851351023 CET	8.8.8.8	192.168.2.6	0x9135	No error (0)	pic.laoyaimg.com		83.217.10.198	A (IP address)	IN (0x0001)
Dec 2, 2021 15:36:19.916641951 CET	8.8.8.8	192.168.2.6	0xf42b	No error (0)	sycdn.comtucdncom.com		104.22.0.86	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 15:36:19.916641951 CET	8.8.8.8	192.168.2.6	0xf42b	No error (0)	sycdn.comt ucdncom.com		172.67.42.54	A (IP address)	IN (0x0001)
Dec 2, 2021 15:36:19.916641951 CET	8.8.8.8	192.168.2.6	0xf42b	No error (0)	sycdn.comt ucdncom.com		104.22.1.86	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- pentontraining.com
- www.pentontraining.com
- crt.sectigo.com
- fmlb.netlbtu.com
- new.cnzz.com

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5448 Parent PID: 4312

General

Start time:	15:35:10
Start date:	02/12/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "http://pentontraining.com
Imagebase:	0x7ff7c15e0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities — Show Windows behavior

Registry Activities — Show Windows behavior

Analysis Process: chrome.exe PID: 6160 Parent PID: 5448

General

Start time:	15:35:11
Start date:	02/12/2021
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=1624,18296224567106023194,6347225086560399399,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1932 /prefetch:8
Imagebase:	0x7ff7c15e0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly

Code Analysis