ID: 344965
Cookbook: browseurl.jbs
Time: 15:02:08
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

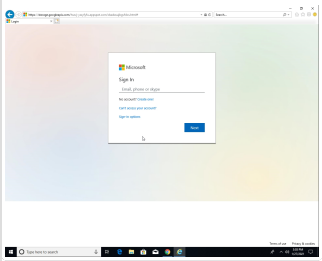
Analysis Report https://quip.com/R1lpAz7okW3E

Overview

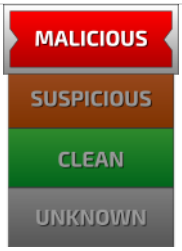
General Information

Sample URL:	http://https://quip.com/R1lpAz7okW3E
Analysis ID:	344965

Most interesting Screenshot:



Detection



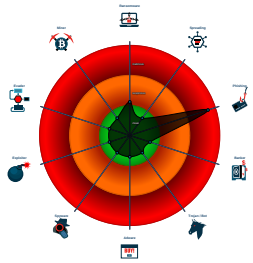
HTMLPhisher

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Phishing site detected (based on fav…
- Yara detected HtmlPhish_10
- Yara detected HtmlPhish_20
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- Invalid T&C link found
- Monitors certain registry keys / valu…

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 6724 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --force-renderer-accessibility 'https://quip.com/R1lpAz7okW3E' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6976 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1508,11710123193784369909,9829296053474170828,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1820 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- dllhost.exe (PID: 6448 cmdline: C:\Windows\system32\DllHost.exe /Processid:{49F171DD-B51A-40D3-9A6C-52D674CC729D} MD5: 2528137C6745C4EADD87817A1909677E)
  - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- iexplore.exe (PID: 8172 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4876 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:8172 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

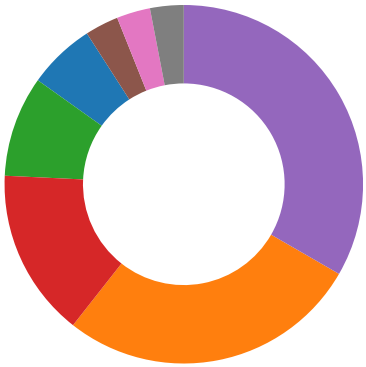
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\dsadasujbgvfdcs[1].html	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Phishing
- Compliance
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- HIPS / PFW / Operating System Protection Evasion

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish_10

Yara detected HtmlPhish_20

Phishing site detected (based on logo template match)

Compliance:

Uses new MSVCR Dlls

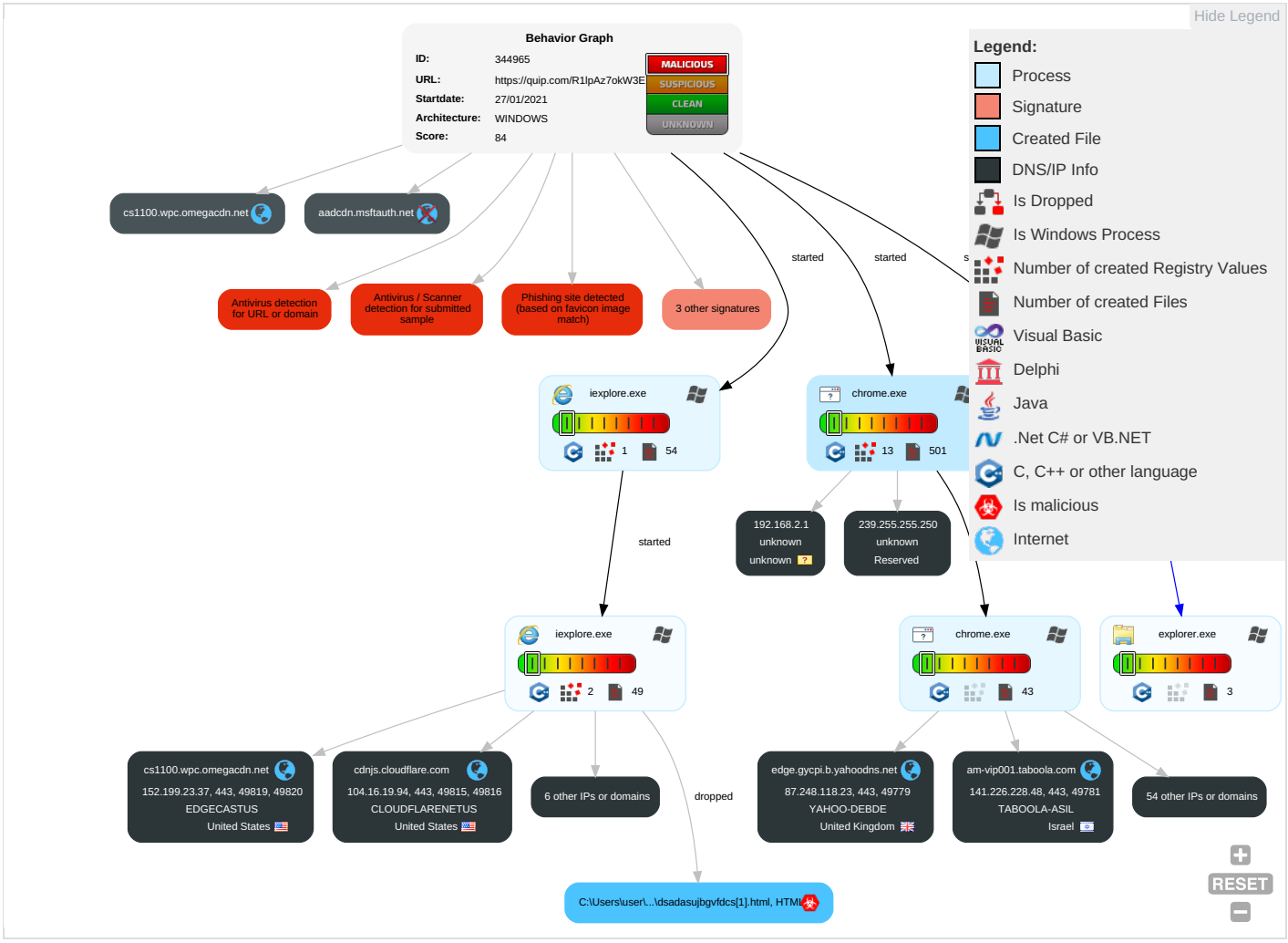
Uses secure TLS version for HTTPS connections

Binary contains paths to debug symbols

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	Im
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mo Sy Pa
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	De Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	De De Da
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Ca Bill Fra

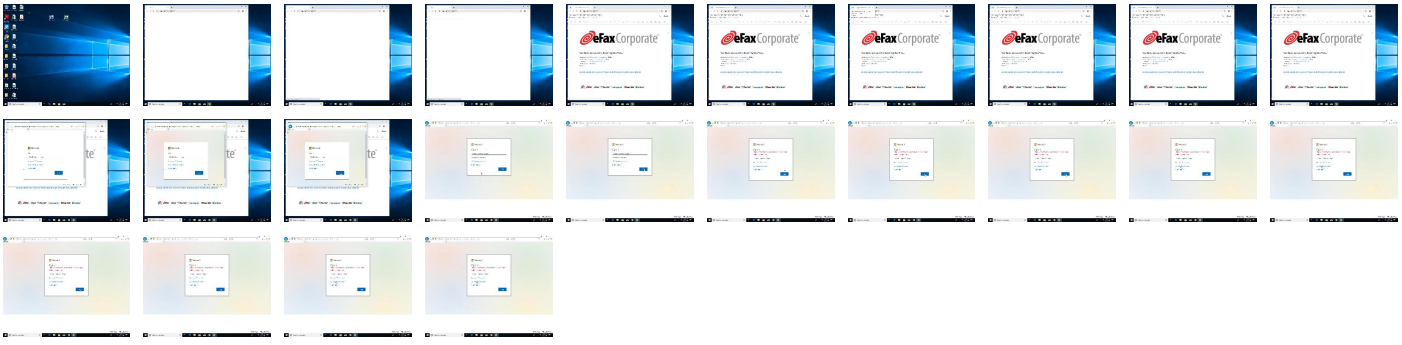
Behavior Graph

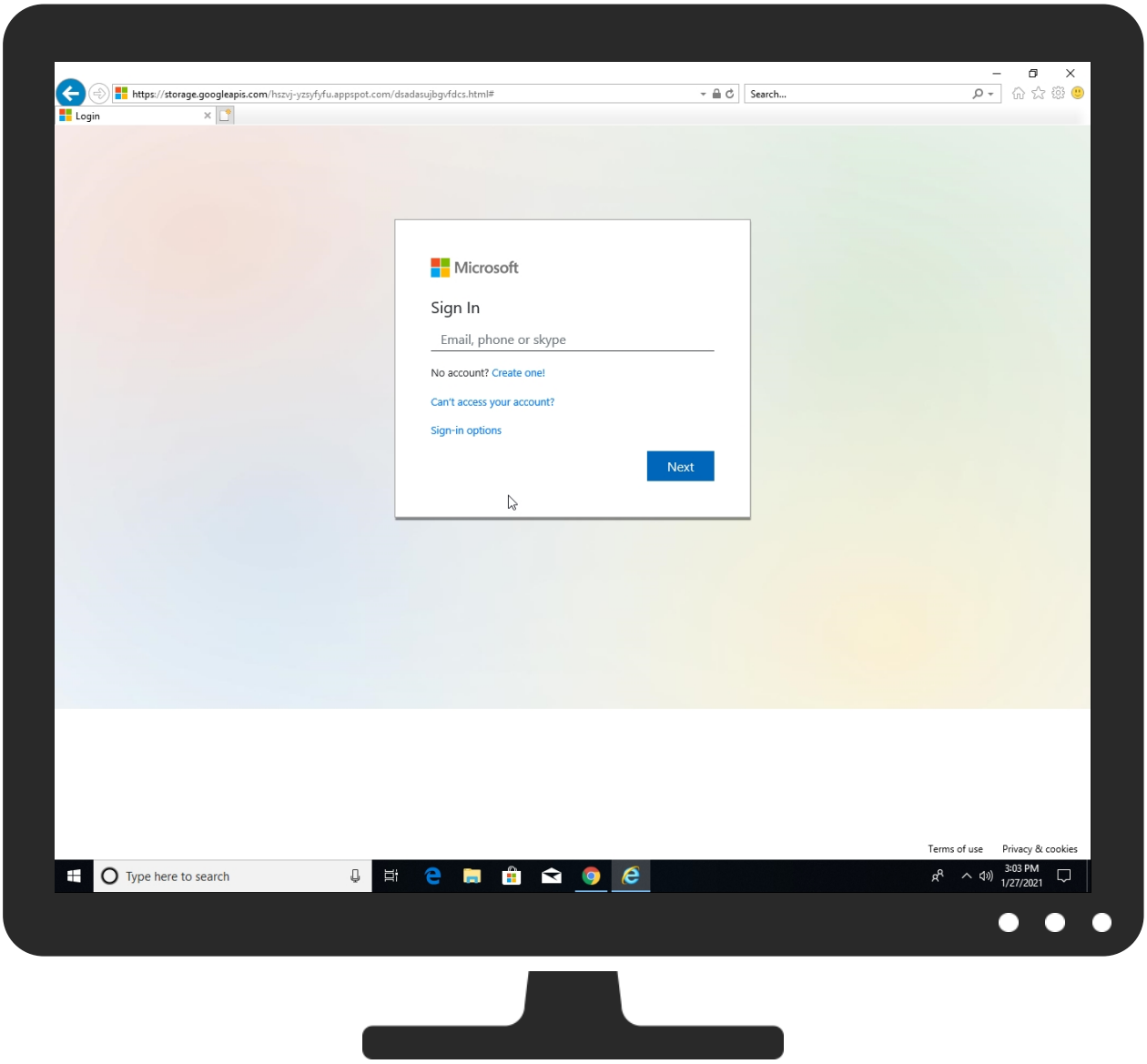


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://quip.com/R1lpAz7okW3E	0%	Avira URL Cloud	safe	
http://https://quip.com/R1lpAz7okW3E	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
http://https://storage.googleapis.com/hszvj-yzsyfyfu.appspot.com/dsadasujbgvfdcs.html#	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://storage.googleapis.com/hszvj-yzsyfyfu.appspot.com/dsadasujbgvfdcs.html#	100%	UrlScan	phishing brand: microsoft	Browse
http://https://apis.googl	0%	Avira URL Cloud	safe	
http://https://quip-cdn.com/LAf64rubV-Hr3Ux_DVJKkwtl	0%	Avira URL Cloud	safe	
http://https://payments.goo	0%	Avira URL Cloud	safe	
http://https://fonts.googeapis.com;	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://https://www.amazon.	0%	Avira URL Cloud	safe	
http://https://www.amazon.co.br	0%	Avira URL Cloud	safe	
http://ocsp.sca1b.amazontrust.com06	0%	URL Reputation	safe	
http://ocsp.sca1b.amazontrust.com06	0%	URL Reputation	safe	
http://ocsp.sca1b.amazontrust.com06	0%	URL Reputation	safe	
http://https://quip-cdn.com/LAf64rubV-Hr3Ux_DVJKkw0	0%	Avira URL Cloud	safe	
http://https://checkout.stripe.	0%	Avira URL Cloud	safe	
http://https://quip-cdn.com/LAf64rubV-Hr3Ux_DVJKkw1	0%	Avira URL Cloud	safe	
http://ocsp.rootca1.amazontrust.com0:	0%	Avira URL Cloud	safe	
http://https://quip-cdn.com/LAf64rubV-Hr3Ux_DVJKkwt)	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://https://quip-cdn.com/X0n7F3PI0Kx27nCksjb_Dg-win-gz	0%	Avira URL Cloud	safe	
http://https://feedback.gogleusercontent.com	0%	Avira URL Cloud	safe	
http://crl.rootg2.amazontrust.com/rootg2.crl0	0%	URL Reputation	safe	
http://crl.rootg2.amazontrust.com/rootg2.crl0	0%	URL Reputation	safe	
http://crl.rootg2.amazontrust.com/rootg2.crl0	0%	URL Reputation	safe	
http://https://chromium-i18n.appspot.com/ssl-aggregate-address/idator7	0%	Avira URL Cloud	safe	
http://https://quip-marketing.com	0%	Avira URL Cloud	safe	
http://https://storage.gRoot	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://storage.google	0%	URL Reputation	safe	
http://https://storage.google	0%	URL Reputation	safe	
http://https://storage.google	0%	URL Reputation	safe	
http://https://simage2.pubmatic	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://https://ups.analytics.ya	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://https://m.addthisedge.com	0%	Avira URL Cloud	safe	
http://https://www.youtube.com;	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://crl.rootca1.ama	0%	Avira URL Cloud	safe	
http://https://quip-cdn.com	0%	Avira URL Cloud	safe	
http://https://angouts.google.	0%	Avira URL Cloud	safe	
http://https://bidswitch.net/	0%	Avira URL Cloud	safe	
http://https://tag.demandbase.com4	0%	Avira URL Cloud	safe	
http://https://company-target.com/	0%	Avira URL Cloud	safe	
http://chrome.googl	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cs1100.wpc.omegacdn.net	152.199.23.37	true	false		unknown
segments.company-target.com	99.86.154.45	true	false		unknown
alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com	52.57.142.16	true	false		high
adserver-vpc-alb-2-1264451658.eu-west-1.elb.amazonaws.com	54.74.23.153	true	false		high
idsync.rlcdn.com	34.120.207.148	true	false		high
s3.amazonaws.com	52.216.9.237	true	false		high
quip.com	44.238.32.151	true	false		high
pagead.l.doubleclick.net	172.217.23.66	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
quip-cdn.com	99.86.154.85	true	false		unknown
listenweb3.quip.com	52.39.66.75	true	false		high
id.rlcdn.com	34.120.207.148	true	false		high
am-vip001.taboola.com	141.226.228.48	true	false		high
match.prod.bidr.io	52.49.193.31	true	false		unknown
pagead46.l.doubleclick.net	172.217.20.226	true	false		high
nydc1.outbrain.org	64.202.112.159	true	false		unknown
us-u.openx.net	34.98.64.218	true	false		high
stats.l.doubleclick.net	108.177.15.157	true	false		high
prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud	3.124.119.192	true	false		unknown
pug22000nf.pubmatic.com	185.64.189.110	true	false		high
dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com	3.125.223.182	true	false		high
pop-tln1-alpha.mix.linkedin.com	185.63.144.5	true	false		high
www.google.co.uk	172.217.22.227	true	false		unknown
api.company-target.com	99.86.154.35	true	false		unknown
ib.anycast.adnxs.com	185.33.221.15	true	false		high
prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud	3.126.56.137	true	false		unknown
scripts.demandbase.com	143.204.11.42	true	false		high
edge.gycpi.b.yahoodns.net	87.248.118.23	true	false		unknown
googlehosted.l.googleusercontent.com	172.217.22.225	true	false		high
adserver-vpc-alb-0-1578609942.eu-west-1.elb.amazonaws.com	54.170.19.229	true	false		high
d.adroll.mgr.consensu.org	unknown	unknown	false		unknown
ka-f.fontawesome.com	unknown	unknown	false		high
d.adroll.com	unknown	unknown	false		high
ups.analytics.yahoo.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
ads.yahoo.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
cm.g.doubleclick.net	unknown	unknown	false		high
pixel.advertising.com	unknown	unknown	false		high
sync.outbrain.com	unknown	unknown	false		high
sync.taboola.com	unknown	unknown	false		high
x.bidswitch.net	unknown	unknown	false		unknown
kit.fontawesome.com	unknown	unknown	false		high
www.linkedin.com	unknown	unknown	false		high
pixel.rubiconproject.com	unknown	unknown	false		high
maxcdn.bootstrapcdn.com	unknown	unknown	false		high
aadcdn.msftauth.net	unknown	unknown	false		unknown
s.adroll.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
px.ads.linkedin.com	unknown	unknown	false		high
simage2.pubmatic.com	unknown	unknown	false		high
dsum-sec.casalemedia.com	unknown	unknown	false		high
googleads.g.doubleclick.net	unknown	unknown	false		high
snap.licdn.com	unknown	unknown	false		high
ib.adnxs.com	unknown	unknown	false		high
eb2.3lift.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	chrome.exe, 00000000.00000002.928607718.000001FD5E201000.00000002.00000001.sdmp, chrome.exe, 00000000.00000002.933117795.000001FD61350000.00000004.00000001.sdmp	false		high
http://https://scripts.demandbase.com/841642b6.min.js	chrome.exe, 00000000.00000002.927159784.000001FD5DDF0000.00000004.00000001.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	chrome.exe, 00000000.00000002.933117795.000001FD61350000.00000004.00000001.sdmp	false		high
http://https://quip.com/csp-report	chrome.exe, 00000000.00000002.933923413.000001FD617D8000.00000004.00000001.sdmp	false		high
http://https://search.yahoo.com/search?ei=&fr=crmas&p=	chrome.exe, 00000000.00000002.933117795.000001FD61350000.00000004.00000001.sdmp	false		high
http://https://casalemedia.com/	chrome.exe, 00000000.00000002.934420011.000001FD61AF9000.00000004.00000001.sdmp	false		high
http://https://quip.com/R1lpAz7okW3EYou	chrome.exe, 00000000.00000002.927108307.000001FD5DDB1000.00000002.00000001.sdmp	false		high
http://https://apis.googl	chrome.exe, 00000000.00000002.933257550.000001FD61481000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000003.00000000.698282230.000000000B976000.00000002.00000001.sdmp	false		high
http://https://checkout.stripe.com	chrome.exe, 00000000.00000002.927750990.000001FD5DEE7000.00000004.00000001.sdmp	false		high
http://https://quip-cdn.com/LAf64rubV-Hr3Ux_DVJKkwtl	chrome.exe, 00000000.00000002.933923413.000001FD617D8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://fontawesome.com	free-v4-shims.min[1].css.11.dr	false		high
http://https://bugs.chromium.org/p/chromium/issues/entry?template=Safety	chrome.exe, 00000000.00000002.918209570.000001FD5A380000.00000002.00000001.sdmp	false		high
http://https://quip.com/	chrome.exe, 00000000.00000002.926679663.000001FD5DAC0000.00000004.00000001.sdmp, chrome.exe, 00000000.00000002.934002982.000001FD6185C000.00000004.00000001.sdmp, chrome.exe, 00000000.00000002.934420011.000001FD61AF9000.00000004.00000001.sdmp, c9226d7c7cc7ba4b_0.0.dr	false		high
http://https://payments.goo	chrome.exe, 00000000.00000002.934838262.000001FD62554000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.cookielaw.org/consent/4a3b4a16-9af0-4726-976d-39737fb16905.js	chrome.exe, 00000000.00000002.927750990.000001FD5DEE7000.00000004.00000001.sdmp	false		high
http://https://fonts.googeapis.com;	chrome.exe, 00000000.00000002.933257550.000001FD61481000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.amazon.it	chrome.exe, 00000000.00000002.917919008.000001FD5A23E000.00000004.00000020.sdmp	false		high
http://www.galapagosdesign.com/DPlease	chrome.exe, 00000000.00000002.929140697.000001FD5E716000.00000002.00000001.sdmp, explorer.exe, 00000003.00000000.698282230.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://apis.googl.com	chrome.exe, 00000000.00000002.933257550.000001FD61481000.00000004.00000001.sdmp	false		high
http://www.zhongyicts.com.cn	chrome.exe, 00000000.00000002.929772524.000001FD5EAB0000.00000002.00000001.sdmp, explorer.exe, 00000003.00000000.698282230.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.amazon.	chrome.exe, 00000000.00000002.917919008.000001FD5A23E000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://quip.com/t	d978b0efc727804e_0.0.dr	false		high
http://https://quip.com/-/blob/MIMAAAvS41x/pekwCRQ_M07RxR0fa7T8lw?s=R1lpAz7okW3E	chrome.exe, 00000000.00000002.934018519.000001FD6186A000.00000004.00000001.sdmp	false		high
http://https://www.amazon.co.br	chrome.exe, 00000000.00000002.917919008.000001FD5A23E000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://quip.com/R1lpAz7okW3E7okW3Er	chrome.exe, 00000000.00000003.728822473.000001FD61730000.00000004.00000001.sdmp	false		high
http://ocsp.sca1b.amazontrust.com06	chrome.exe, 00000000.00000002.927159784.000001FD5DDF0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://duckduckgo.com/?q=	chrome.exe, 00000000.00000002.933117795.000001FD61350000.00000004.00000001.sdmp	false		high
http://https://quip.com/R1lpAz7okW3EentState	chrome.exe, 00000000.00000002.917905875.000001FD5A236000.00000004.00000020.sdmp	false		high
http://https://quip-cdn.com/LAf64rubV-Hr3Ux_DVJKkw0	chrome.exe, 00000000.00000002.934626745.000001FD62400000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://checkout.stripe.	chrome.exe, 00000000.00000002.933117795.000001FD61350000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://quip-cdn.com/LAf64rubV-Hr3Ux_DVJKkw1	chrome.exe, 00000000.00000002.934041316.000001FD6188D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://search.yahoo.com/search?ei=&fr=crmas&p=searchTerms	chrome.exe, 00000000.00000002.933117795.000001FD61350000.00000004.00000001.sdmp	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.ico	chrome.exe, 00000000.00000002.933117795.000001FD61350000.00000004.00000001.sdmp	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	chrome.exe, 00000000.00000002.928607718.000001FD5E201000.00000002.00000001.sdmp	false		high
http://https://quip.com/R1lpAz7okW3EQZQz6	chrome.exe, 00000000.00000002.934258371.000001FD61A02000.00000004.00000001.sdmp	false		high
http://https://quip.com/R1lpAz7okW3E=P	chrome.exe, 00000000.00000002.934626745.000001FD62400000.00000004.00000001.sdmp	false		high
http://ocsp.rootca1.amazontrust.com0:	chrome.exe, 00000000.00000002.927159784.000001FD5DDF0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://quip.com/R1lpAz7okW3Eome	chrome.exe, 00000000.00000002.934626745.000001FD62400000.00000004.00000001.sdmp	false		high
http://https://quip-cdn.com/LAf64rubV-Hr3Ux_DVJKkwt)	chrome.exe, 00000000.00000002.934041316.000001FD6188D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/favicon.ico	chrome.exe, 00000000.00000002.933117795.000001FD61350000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	chrome.exe, 00000000.00000002.929140697.000001FD5E716000.00000002.00000001.sdmp, explorer.exe, 00000003.00000000.698282230.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://quip-cdn.com/X0n7F3PI0Kx27nCksjb_Dg-win-gz	chrome.exe, 00000000.00000002.927159784.000001FD5DDF0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://feedback.gogleusercontent.com	chrome.exe, 00000000.00000002.933257550.000001FD61481000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.rootg2.amazontrust.com/rootg2.crl0	chrome.exe, 00000000.00000002.928381970.000001FD5E127000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://chromium-i18n.appspot.com/ssl-aggregate-address/idator7	chrome.exe, 00000000.00000002.933923413.000001FD617D8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://geolocation.onetrust.com	chrome.exe, 00000000.00000002.927750990.000001FD5DEE7000.00000004.00000001.sdmp	false		high
http://https://demdex.com	chrome.exe, 00000000.00000002.927750990.000001FD5DEE7000.00000004.00000001.sdmp	false		high
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap.min[1].css.11.dr	false		high
http://https://3lift.com/	chrome.exe, 00000000.00000002.933923413.000001FD617D8000.00000004.00000001.sdmp	false		high
http://https://quip-marketing.com	chrome.exe, 00000000.00000002.927750990.000001FD5DEE7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://taboola.com/	chrome.exe, 00000000.00000002.933923413.000001FD617D8000.00000004.00000001.sdmp	false		high
http://https://feedback.googleusercontent.com	chrome.exe, 00000000.00000002.934371060.000001FD61A92000.00000004.00000001.sdmp, chrome.exe, 00000000.00000002.926679663.000001FD5DAC0000.00000004.00000001.sdmp	false		high
http://https://adroll.com/	chrome.exe, 00000000.00000002.934018519.000001FD6186A000.00000004.00000001.sdmp	false		high
http://https://quip.com/R1lpAz7okW3EiiwYo	chrome.exe, 00000000.00000002.934258371.000001FD61A02000.00000004.00000001.sdmp	false		high
http://https://storage.gRoot	{70FA3506-60A8-11EB-90EB-ECF4BBEA1588}.dat.10.dr	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/bThe	chrome.exe, 00000000.00000002.929140697.000001FD5E716000.00000002.00000001.sdmp, explorer.exe, 00000003.00000000.698282230.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://storage.google	{70FA3506-60A8-11EB-90EB-ECF4BBEA1588}.dat.10.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://doubleclick.net/	chrome.exe, 00000000.00000002.934341022.000001FD61A76000.00000004.00000001.sdmp	false		high
http://https://adnxs.com/	chrome.exe, 00000000.00000002.933923413.000001FD617D8000.00000004.00000001.sdmp	false		high
http://https://px.ads.linkedin.com/	chrome.exe, 00000000.00000002.927750990.000001FD5DEE7000.00000004.00000001.sdmp	false		high
http://www.unicode.org/copyright.html	chrome.exe, 00000000.00000002.921646704.000001FD5C4F7000.00000002.00000001.sdmp	false		high
http://https://quip.com/283875	chrome.exe, 00000000.00000002.934923660.000001FD62629000.00000004.00000001.sdmp	false		high
http://https://simage2.pubmatic	chrome.exe, 00000000.00000002.933257550.000001FD61481000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://openx.net/	chrome.exe, 00000000.00000002.933923413.000001FD617D8000.00000004.00000001.sdmp	false		high
http://https://analytics.twitter.com	chrome.exe, 00000000.00000002.927750990.000001FD5DEE7000.00000004.00000001.sdmp	false		high
http://https://googleads.g.doubleclick.net/	chrome.exe, 00000000.00000002.927750990.000001FD5DEE7000.00000004.00000001.sdmp	false		high
http://https://www.ecosia.org/search?q=&addon=opensearch	chrome.exe, 00000000.00000002.933117795.000001FD61350000.00000004.00000001.sdmp	false		high
http://https://rubiconproject.com/	chrome.exe, 00000000.00000002.934341022.000001FD61A76000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ups.analytics.yahoo.com/ups/55980/sync?uid=MzM1NzAyYThhMTNkMzU5MjkyOTgzNTQ1NmE5MzhkNTc&_orig	chrome.exe, 00000000.00000003.727807957.000001FD616AA000.00000004.00000001.sdmp	false		high
http://https://autocomplete.demandbase.com	chrome.exe, 00000000.00000002.927750990.000001FD5DEE7000.00000004.00000001.sdmp	false		high
http://https://www-onepick-opensocial.googleusercontent.com	chrome.exe, 00000000.00000002.922309416.000001FD5C940000.00000004.00000001.sdmp	false		high
http://https://fontawesome.com/license/free	free-v4-shims.min[1].css.11.dr	false		high
http://www.typography.netD	chrome.exe, 00000000.00000002.929140697.000001FD5E716000.00000002.00000001.sdmp, explorer.exe, 00000003.00000000.698282230.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ups.analytics.ya	chrome.exe, 00000000.00000002.933257550.000001FD61481000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://fontfabrik.com	chrome.exe, 00000000.00000002.929639146.000001FD5E9D2000.00000002.00000001.sdmp, explorer.exe, 00000003.00000000.701388573.000000000BC32000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://m.addthis.com	chrome.exe, 00000000.00000002.927750990.000001FD5DEE7000.00000004.00000001.sdmp	false		high
http://https://m.addthisedge.com	chrome.exe, 00000000.00000002.927750990.000001FD5DEE7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com;	chrome.exe, 00000000.00000002.922309416.000001FD5C940000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://safebrowsing.googleusercontent.com/safebrowsing/clientreport/chrome-certs	chrome.exe, 00000000.00000002.928218204.000001FD5E0A4000.00000004.00000001.sdmp	false		high
http://www.%s.comPA	explorer.exe, 00000003.00000000.670728920.0000000002B50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	chrome.exe, 00000000.00000002.929639146.000001FD5E9D2000.00000002.00000001.sdmp, explorer.exe, 00000003.00000000.701388573.000000000BC32000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	chrome.exe, 00000000.00000002.929140697.000001FD5E716000.00000002.00000001.sdmp, explorer.exe, 00000003.00000000.698282230.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://quip.com/R1lpAz7okW3El-ntp.html	chrome.exe, 00000000.00000003.728822473.000001FD61730000.00000004.00000001.sdmp	false		high
http://crl.rootca1.ama	chrome.exe, 00000000.00000002.934018519.000001FD6186A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://scripts.demandbase.com	chrome.exe, 00000000.00000002.927750990.000001FD5DEE7000.00000004.00000001.sdmp, chrome.exe, 00000000.00000002.927159784.000001FD5DDF0000.00000004.00000001.sdmp	false		high
http://https://quip-cdn.com	chrome.exe, 00000000.00000002.927750990.000001FD5DEE7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://angouts.google.	chrome.exe, 00000000.00000003.728340528.000001FD626C3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://bidswitch.net/	chrome.exe, 00000000.00000002.933923413.000001FD617D8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://tag.demandbase.com4	chrome.exe, 00000000.00000002.922309416.000001FD5C940000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://company-target.com/	chrome.exe, 00000000.00000002.934341022.000001FD61A76000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://org62.my.salesforce.com	chrome.exe, 00000000.00000002.927750990.000001FD5DEE7000.00000004.00000001.sdmp	false		high
http://https://quip.com/R1lpAz7okW3Ex	chrome.exe, 00000000.00000002.934838262.000001FD62554000.00000004.00000001.sdmp	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	chrome.exe, 00000000.00000002.928607718.000001FD5E201000.00000002.00000001.sdmp	false		high
http://https://fast.wistia.com	chrome.exe, 00000000.00000002.927750990.000001FD5DEE7000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.htmlN	chrome.exe, 00000000.00000002.929140697.000001FD5E716000.00000002.00000001.sdmp, explorer.exe, 00000003.00000000.698282230.000000000B976000.00000002.00000001.sdmp	false		high
http://https://connect.facebook.net	chrome.exe, 00000000.00000002.927750990.000001FD5DEE7000.00000004.00000001.sdmp	false		high
http://chrome.googl	chrome.exe, 00000000.00000003.727068130.000001FD6273A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	chrome.exe, 00000000.00000002.929140697.000001FD5E716000.00000002.00000001.sdmp, explorer.exe, 00000003.00000000.698282230.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://quip.com/R1lpAz7okW3E	chrome.exe, 00000000.00000002.917802089.000001FD5A1F0000.00000004.00000020.sdmp, Current Session.0.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
99.86.154.35	unknown	United States		16509	AMAZON-02US	false
108.177.15.157	unknown	United States		15169	GOOGLEUS	false
3.125.223.182	unknown	United States		16509	AMAZON-02US	false
185.33.221.15	unknown	Netherlands		29990	ASN-APPNEXUS	false
52.216.9.237	unknown	United States		16509	AMAZON-02US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
99.86.154.85	unknown	United States		16509	AMAZON-02US	false
52.57.142.16	unknown	United States		16509	AMAZON-02US	false
44.238.32.151	unknown	United States		16509	AMAZON-02US	false
185.63.144.5	unknown	United States		14413	LINKEDINUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.217.23.66	unknown	United States		15169	GOOGLEUS	false
3.126.56.137	unknown	United States		16509	AMAZON-02US	false
152.199.23.37	unknown	United States		15133	EDGECASTUS	false
172.217.22.227	unknown	United States		15169	GOOGLEUS	false
172.217.22.225	unknown	United States		15169	GOOGLEUS	false
185.64.189.110	unknown	United Kingdom		62713	AS-PUBMATICUS	false
64.202.112.159	unknown	United States		22075	AS-OUTBRAINUS	false
3.124.119.192	unknown	United States		16509	AMAZON-02US	false
52.39.66.75	unknown	United States		16509	AMAZON-02US	false
143.204.11.42	unknown	United States		16509	AMAZON-02US	false
141.226.228.48	unknown	Israel		200478	TABOOLA-ASIL	false
172.217.20.226	unknown	United States		15169	GOOGLEUS	false
99.86.154.45	unknown	United States		16509	AMAZON-02US	false
34.120.207.148	unknown	United States		15169	GOOGLEUS	false
87.248.118.23	unknown	United Kingdom		203220	YAHOO-DEBDE	false
54.74.23.153	unknown	United States		16509	AMAZON-02US	false
34.98.64.218	unknown	United States		15169	GOOGLEUS	false
54.170.19.229	unknown	United States		16509	AMAZON-02US	false
52.49.193.31	unknown	United States		16509	AMAZON-02US	false
104.16.19.94	unknown	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344965
Start date:	27.01.2021
Start time:	15:02:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://quip.com/R1lpAz7okW3E
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:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.phis.win@43/286@40/31
EGA 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 • Browsing link: https://storage .googleapis.com/hszvj-yzsyfyfu .appspot.com/dsadasujbgvfdcs.html#
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 13.88.21.125, 172.217.23.78, 172.217.20.237, 216.58.207.174, 173.194.187.106, 142.250.185.206, 216.58.207.136, 172.217.23.35, 172.217.23.68, 23.210.249.242, 23.210.248.216, 192.124.249.41, 192.124.249.23, 192.124.249.24, 192.124.249.22, 192.124.249.36, 13.107.42.14, 72.247.178.42, 72.247.178.8, 72.247.178.11, 23.210.249.164, 69.173.144.165, 69.173.144.139, 69.173.144.138, 216.58.207.131, 216.58.207.138, 216.58.207.170, 172.217.20.234, 172.217.23.10, 172.217.23.42, 172.217.23.74, 172.217.22.202, 51.104.144.132, 104.108.39.131, 95.101.22.216, 95.101.22.224, 216.58.207.144, 216.58.207.176, 172.217.20.240, 172.217.23.16, 172.217.23.80, 172.217.22.208, 172.217.22.240, 209.197.3.24, 209.197.3.15, 104.18.22.52, 104.18.23.52, 172.64.203.28, 172.64.202.28, 72.247.178.35, 52.155.217.156, 20.54.26.129, 172.217.23.67, 152.199.19.161, 173.194.164.103, 173.194.182.198, 173.194.187.6, 51.104.139.180, 173.194.188.38, 173.194.151.103 • Excluded domains from analysis (whitelisted): ssl.gstatic.com, cds.s5x3j6q5.hwcdn.net, arc.msn.com.nsatc.net, storage.googleapis.com, ka-f.fontawesome.com.cdn.cloudflare.net, clientservices.googleapis.com, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, l-0005.l-msedge.net, clients2.google.com, audownload.windowsupdate.nsatc.net, update.googleapis.com, www.google.com, watson.telemetry.microsoft.com, www.gstatic.com, r1---sn-4g5e6ney.gvt1.com, ocsp.godaddy.com.akadns.net, au-bg-shim.trafficmanager.net, www.google-analytics.com, fonts.googleapis.com, r1---sn-4g5e6nss.gvt1.com, ajax.googleapis.com, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, aadcdnoriginneu.azureedge.net, www.googleapis.com, ris.api.iris.microsoft.com, r1---sn-4g5e6ne6.gvt1.com, wildcard.adroll.com.edgekey.net, blobcollector.events.data.trafficmanager.net, dsum-sec.casalemedia.com.edgekey.net, clients.l.google.com, r1.sn-4g5e6ney.gvt1.com, r1---sn-4g5ednse.gvt1.com, e4007.g.akamaiedge.net, cs9.wpc.v0cdn.net, au.download.windowsupdate.com.edgesuite.net, r1---sn-4g5e6ns6.gvt1.com, pixel.rubiconproject.net.akadns.net, r1.sn-4g5e6nss.gvt1.com, r5---sn-4g5e6nsr.gvt1.com, a1449.dscg2.akamai.net, arc.msn.com, e9706.dscg.akamaiedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, iecvlist.microsoft.com, e8037.g.akamaiedge.net, go.microsoft.com, redirector.gvt1.com, www.googletagmanager.com, r1.sn-4g5e6ne6.gvt1.com, safebrowsing.googleapis.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, r1.sn-4g5ednse.gvt1.com, www-linkedin-com.l-0005.l-msedge.net, kit.fontawesome.com.cdn.cloudflare.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, accounts.google.com, www-google-analytics.l.google.com, ie9comview.vo.msecnd.net, www-googletagmanager.l.google.com, r1.sn-4g5e6ns6.gvt1.com, ctldl.windowsupdate.com, a767.dscg3.akamai.net, aadcdnoriginneu.ec.azureedge.net, wildcard.licdn.com.edgekey.net,

	go.microsoft.com.edgekey.net, cds.j3z9t3p6.hwcdn.net, r5.sn-4g5e6nsr.gvt1.com, ocsp.godaddy.com, skypedataprdcolwus15.cloudapp.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtQueryVolumeInformationFile calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found. • VT rate limit hit for: https://quip.com/R1lpAz7okW3E

Simulations

Behavior and APIs

Time	Type	Description
15:03:05	API Interceptor	1x Sleep call for process: dllhost.exe modified
15:03:07	API Interceptor	3x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1731
Entropy (8bit):	7.308660761132808
Encrypted:	false
SSDEEP:	48:panitqb2NIYEyeDnita8lnitq1+Zvl3oXS9As5RmEWqu5H99:pWi2Nye2z1+boavLJpu5

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771	
MD5:	5BC0D504EB02FB705D0358F62F22A6A6
SHA1:	89C856F3354CCB3B6543C1797F2A252E496DA0EC
SHA-256:	A19E067FFE72E062BD7DA7D09407C9C8D2D4E43A516059943A7F63B36A456905
SHA-512:	F62D3EFA7205E1B2F33C534F6C3A6AD705506B001B68724010ED4EFCC12C208ED55787F24DDDAC8A90446013AB4838CE2DEC66D108E10C6072A71B5AE259D46
Malicious:	false
Reputation:	low
Preview:	0.....0.....+.....0.....0...0.....0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.100...U...'Go Daddy Root Validation Authority - G2..20210126173125Z0d0b0:0...+.....#o..K.....#....+...:....g(.....An .....20210126173125Z....20210128053125Z0...*.H.....l.:....m.l.....t..OTx.....d.ak?....w.M..%6...;m|^.....U..''.jc.....p...qus.'.U....,..SC..Vk.O..._.....5.....'....O."....W..r..X.t,B....l.....Jy...e.3.....h>a....q....{.....x?e..t?A/;.P.(.?.....<./..A...6%.h3.oK..j.%.5.....*..4.....0...0...0..g.....f..p.t0...*.H.....0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.110/..U...(Go Daddy Root Certificate Authority - G20...200909070000Z..2109090700000Z0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.100...U...'Go Daddy Root Validation Authority - G20..''0...*.H.....0.....'....^Y.u..U.qU..."......-]XG(qk#.+....J...G.3

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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EB2C4AB8B68FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1697
Entropy (8bit):	7.295266314140904
Encrypted:	false
SSDEEP:	48:snitqJbkJ8LuVnitqsXA49e5REMeZ6+23wQ:UJ8sw49eEMeZ6+Y
MD5:	0DCE087B10635554C57BD35851FB7514
SHA1:	CDE8C57241796215FB64F5148101E6942A659447
SHA-256:	A3957F0BEE87993D3F3C78C1D969C59EDFB9ED6C2769244F45F74470A901EEBA
SHA-512:	327F29C6EE2D8333934419ECBE3C8E7B35AF066E91D1FC716D620BB7DB23AA009E65ED22739D1D1E9124F93A632C24291268791CD042E7131FBB59584CDB77D
Malicious:	false
Reputation:	low
Preview:	0.....0.....+.....0.....0...0.....0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.100...U...'Go Daddy Root Validation Authority - G1..20210126204909Z0f0d0<0...+..... .....]..J^.y_..F<.....L.q.a.=...j.....202101262049092....20210128084909Z0...*.H.....*.d.x.../8...K.7.....S..~r..m.,..+b...g]..-....'.&.....K..u.R)..\.l.O....w...c..l.aImf..x/.a.<?"..[..$Q).*C=9B.j....4t.M....-%..u]..G.....)....S.-..r.A..9&.....pap9.X...#.I..#...qE..G.D.T.....S...FPu.bu"(ot.L....bn. .e.I..3..8..../,.g...b0..^0..Z0..B.....1g...r.0...*.H.....0c1.0...U....US1!0...U....The Go Daddy Group, Inc.110/..U...(Go Daddy Class 2 Certification Authority0...161213070000Z..211213070000Z0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.100...U...'Go Daddy Root Validation Authority - G10..''0...*.H.....0.....}...@.H.....j.b.2.c...'eSA...6""2.hf.m.m9....._N."gV..{.J"{..0f.W$.X

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	900
Entropy (8bit):	3.772812252079064
Encrypted:	false
SSDEEP:	24:aGwyPV13MhmyFqbNcsFwyPV13MhmyFqbNcz:FwkV1XyF3sFwkV1XyF3z
MD5:	8AFBACC9C21BDECEF28012182BE947D3

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771	
SHA1:	8FBEDF14C42C8FACBF6530482CB429DEB4ACFDA9
SHA-256:	4852E0D7D25E2E7459C1901B121A13B16BA87989A9EAFE6ABC30F0D7EDE33CC1
SHA-512:	01053B5ABCDA876B7781017511ED72D742121768016CAB1D6B5E5E9838312AB63A60465495884754CDDEBC535BD97CF35DBF4DFBBC9B8FB0B6F513D1C24341(
Malicious:	false
Reputation:	low
Preview:	p..... .....+.#....(..... .....T .....V.....h.t.t.p.:././.o.c.s.p...g.o.d.a.d.d.y...c.o.m././.M.E.I.w.Q.D.A.%.2.B.M.D.w.w.O.j.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.Q.d.I.2.%.2.B.O.B.k.u.X.H.9.3.f.o.R.U.j.4.a.7.I.A.r.4.r.G.w.Q.U.O.p.q.F.B.x.B.n.K.L.b.v.9.r.0.F.Q.W.4.g.w.Z.T.a.D.9.4.C.A.Q.c.%.3.D...".8.9.c.8.5.6.f.3.3.5.4.c.c.b.3.b.6.5.4.3.c.1.7.9.7.f.2.a.2.5.2.e.4.9.6.d.a.0.e.c."...p..... .....+.#....(.....T .....6.....6... .....T .....V.....h.t.t.p.:././.o.c.s.p...g.o.d.a.d.d.y...c.o.m././.M.E.I.w.Q.D.A.%.2.B.M.D.w.w.O.j.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.Q.d.I.2.%.2.B.O.B.k.u.X.H.9.3.f.o.R.U.j.4.a.7.I.A.r.4.r.G.w.Q.U.O.p.q.F.B.x.B.n.K.L.b.v.9.r.0.F.Q.W.4.g.w.Z.T.a.D.9.4.C.A.Q.c.%.3.D...".8.9.c.8.5.6.f.3.3.5.4.c.c.b.3.b.6.5.4.3.c.1.7.9.7.f.2.a.2.5.2.e.4.9.6.d.a.0.e.c."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.090852246460565
Encrypted:	false
SSDEEP:	6:kKwPbqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:IW3kPlE99SNxAhUeo+aKt
MD5:	E5C3C4DB3B14B761E72FB57E89E81460
SHA1:	DF9596BBB6C530A8FC82AE2DCC419EADC85F469C
SHA-256:	2FDA94C20AEB9AE7952660F044D34F351D801E11555004EAC282C5059B15D99D
SHA-512:	4EA35FED8D6EFF82B461E16F9CE418126F1DFF78551550E202565BFA4C40C3FD2C70B893CA6E0F1E3638CD55D3C274E33BCA5E9193B77F9BC81AEAD89BD8247
Malicious:	false
Reputation:	low
Preview:	p..... .....G....(..... .....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.e.b.b.a.e.1.d.7.e.a.d.6.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EB2C4AB8B68FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	916
Entropy (8bit):	3.8133430888995448
Encrypted:	false
SSDEEP:	12:PPrQEFDsFrvgxE0P6GANMStX0+ttn+rQEFDsFrvgxE0P6GANMStX0+tw:nV4xaVSGAmStkCtn+V4xaVSGAmStkCw
MD5:	155FE7513ADD27A9F2FF8A6943545F22
SHA1:	EFF1BA709794F84D79602151169E952B7B0A7870
SHA-256:	238ADE481DFFB0E8CB17B35CDA5A3952B5CAC2B7C701810F6D7F9590B97D78AD
SHA-512:	50EA139DB7A8727B1C4172ACD4F6BFFFD765942357221102B6556BF887D2DA977D507A4A948F0E1379A78081D2EF28002A0AAED7A33E59D4CC3AA312375C7B6
Malicious:	false
Reputation:	low
Preview:	p..... .....#....(..... .....$.....V.....h.t.t.p.:././.o.c.s.p...g.o.d.a.d.d.y...c.o.m././.M.E.Q.w.Q.j.B.A.M.D.4.w.P.D.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.k.I.I.n.K.B.A.z.X.k.F.0.Q.h.0.p.e.l.3.l.f.H.J.9.G.P.A.Q.U.0.s.S.w.0.p.H.U.T.B.F.x.s.2.H.L.P.a.H.%.2.B.3.a.h.q.1.O.M.C.A.x.v.n.F.Q.%.3.D.%.3.D...".c.d.e.8.c.5.7.2.4.1.7.9.6.2.1.5.f.b.6.4.f.5.1.4.8.1.0.1.e.6.9.4.2.a.6.5.9.4.4.7."...p..... .....#....(.....$.....=qR.....=qR... .....$.....V.....h.t.t.p.:././.o.c.s.p...g.o.d.a.d.d.y...c.o.m././.M.E.Q.w.Q.j.B.A.M.D.4.w.P.D.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.k.I.I.n.K.B.A.z.X.k.F.0.Q.h.0.p.e.l.3.l.f.H.J.9.G.P.A.Q.U.0.s.S.w.0.p.H.U.T.B.F.x.s.2.H.L.P.a.H.%.2.B.3.a.h.q.1.O.M.C.A.x.v.n.F.Q.%.3.D.%.3.D...".c.d.e.8.c.5.7.2.4.1.7.9.6.2.1.5.f.b.6.4.f.5.1.4.8.1.0.1.e.6.9.4.2.a.6.5.9.4.4.7."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\11674e03-c374-4c45-a4d9-f693e8e7912a.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):	163630
Entropy (8bit):	6.081588549485293
Encrypted:	false
SSDEEP:	3072:rJ72w0rBlQ96umxmsP6tttYVj4UnSFcbXafIB0u1GOJmA3iuRM:tq1lAumJe8UYaqfIlUOoSiuRM
MD5:	B975BF3507236E4EDCA27D978F2E2B70
SHA1:	33AAD439369CA9C7321BEA126A72870173A62292
SHA-256:	A1737594AF3369C2E823BDC2F71180C0F43DE772C1B4BEC51363F19593FE0932
SHA-512:	B444AD8207648D633EED8EEADEDB977D017B25D4C4D8F77AC31F5C39A6FD514C7875726C4DBEE58AC7D5CA03335999E204302FA4C81569EAC3D93D1F0D2685F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\11674e03-c374-4c45-a4d9-f693e8e7912a.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.611756184321173e+12,"network":1.611756186e+12,"ticks":309758658.0,"uncertainty":4550305.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBljSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\1255963f-2254-4a9d-8bc7-2add57153ef5.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7514941856159383
Encrypted:	false
SSDEEP:	384:rhRcWiG4/dkEjm9NKrPv+23VegpHkRGBYrDASwxtkggjr7GmHMjw62mNOEIuNH1p:tiWa1hiw1ZUeTRuSAMvHmqKo2qpT
MD5:	9A86F9F1E53F2AB10C1A93D985E72AF2
SHA1:	CF9E99999D371C649B80826ADCE5F71A7ACED603
SHA-256:	6A0097C39205DB8494CF3A52EDCE2D9CFE7541BD1A10C7644033DB2E7E7FEBAC
SHA-512:	3572A78A69CB287302F155CD3317AB8B351A0D5FCE03010AD66BBC1CC42ACF03096C6B4F009C8037BC6D6B75FDC19BFC27E8AB707540E99A7522E9ACEDE913E5
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n..../8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\33ae8e23-e997-4137-b804-c883e19a3e6b.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):	155432
Entropy (8bit):	6.0522981675921335
Encrypted:	false
SSDEEP:	3072:62w0rBlQ96umxmsP6tttYVj4UnSFcbXafIB0u1GOJmA3iuRM:P1lAumJe8UYaqfIlUOoSiuRM
MD5:	B087A211FAC0391B121E5AE76FE6EB6D
SHA1:	157DCC7F34544F2DA407A25213A728A973CFD287
SHA-256:	DF17D98C6F33F969E2140D75D6F2E7CF305D260ECE3D581AF1F2FD0959BE90FA
SHA-512:	5594AD9F8CF5F8B09E340EE12BB72CF8B24B1AC46875106426CF4DE1EBFBA2A02FA8507EBBA97B4E2839E4DD1B8CF7CD520CED3C2D32A919C7BBD14ECB911661
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.611756184321173e+12,"network":1.611756186e+12,"ticks":309758658.0,"uncertainty":4550305.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBljSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715645491"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\36e83c7e-e7d4-4839-b9b4-9e5e81631ec6.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):	155158
Entropy (8bit):	6.051653588588145
Encrypted:	false
SSDEEP:	3072:q2w0rBlQ96umxmsP6tttYVj4UnSFcbXafIB0u1GOJmA3iuRM:f1lAumJe8UYaqfIlUOoSiuRM
MD5:	C9EBB814F7AB2176ACE2BB58CC51EC29
SHA1:	485DA886D02FAE1DD228C828E647E9D226BF91A8
SHA-256:	52D5B69249D342DABBC48D9477B4F7EAB45FBA2B7AFFB5CED176EAB5E25B3D8A
SHA-512:	B9711928439E296727B604E4968EE958589610B1B19E463001C63CFAB0DDFB519AEE4C87AA7F160605F784F40D02D745A0357A5E488AB28743AA08D500AD5961
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\36e83c7e-e7d4-4839-b9b4-9e5e81631ec6.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.611756184321173e+12,"network":1.611756186e+12,"ticks":309758658.0,"uncertainty":4550305.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715645491"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\387f2232-a35f-4b00-8f1b-a7330026c2b9.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7520348917522353
Encrypted:	false
SSDEEP:	384:1hRcWiG4/dAHEKVXJm9NKrPv+23VegpHkRGBYrDASwxtkggjr7GmHztjw62mNOEw:7iGWa1hiw4ZUeTRuSAMvHmqKo2qpM
MD5:	1E8152332B7797142651D31DCC1FCD6B
SHA1:	18C921B562916186ACCF604082355A5282091106
SHA-256:	C822AD5D5FF5EB5301CAC8C55F68D19F017F79B16494659D6CCC5E97379A104D
SHA-512:	6673F511DBFD90DA3A487C421A57A55BDE451E56547402A00308016A2406ADD5E970DCA7CD37EFBDE0E5916ED6A4561BD295221D6677E9A30B77C9955CFC8D5
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..../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\86b62e7c-bc19-4288-864c-3d8d1f5097b8.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.751772579170583
Encrypted:	false
SSDEEP:	384:FhRcWiG4/dAHEKVXJm9NKrPv+23VegpHkRGBYrDASwxtkggjr7GmHMjw62mNOEIX:riGWa1hiw1ZUeTRuSAMvHmqKo2qpP4
MD5:	692F2DE18602E677E40B2BE4BA0B5D00
SHA1:	1B8189073CD32870CE40DE33A6002259530B829D
SHA-256:	704342C6E659D75E488BB34B22C3F408C3EEA79A60D5535BA05D92E8B93B5740
SHA-512:	FC14809B1406141B28071E73BFA4A648F06CBDE16F78DAD590CC3705EBC55C7A3D4B621EF19B9F3729C8EC3802A067FDFE4A9F4497C9556530FA2ED5509712E
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..../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\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXwgs0oRL6twgs0oRL6twgs0oRLn:+taRL+taRL+taRLn
MD5:	E6C1693D9F0F6B6E878D098FBFD4C92A
SHA1:	D9D2708143B4A3BA5D14DFED59DCB6B88DF172D9
SHA-256:	E9DA6B8F6549D084D8740EB4C25755989B057EBF4F36B5E526F34DFFAB7500CF
SHA-512:	19B28BFE66708B294AB033C2F87D219E1C29D4F9363AC92E89B9406F6E2ACB13AD5DF73DD7E163D1ADEC0AF89C42DA112AE153EB23378EC29302F91192B7C59
Malicious:	false
Reputation:	low
Preview:	sdPC.....UO..E.D.Q.o....sdPC.....UO..E.D.Q.o....sdPC.....UO..E.D.Q.o....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2459ddf2-9847-4e8d-9cd3-115af6041cdf.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):	5437
Entropy (8bit):	5.180337187503269
Encrypted:	false
SSDEEP:	96:nkL8ZX+rvIVqHk0JCKL88kYj31bOElVuHn:nkLeOrvIYP4KzkYTe
MD5:	49E95670B9B1E68E71BF15873373B389
SHA1:	96EF845EEB14126D3BF2D0980C6E331418617025
SHA-256:	14824A7B46D7E3D93A30553569BD6DB198FC9EFAEA7CD1534ECE859F0986B656
SHA-512:	1CFC6C1D7B3A32C4D23B2ED4DF6CC1251DE20DD6F39130B6004026725735BF4BC7CCC61A27A1F967D90B211D4F7E9A88FBFD98D75B1BB5EE9637C0B07B773 7
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13256229780894561","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"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","2042016"],"daily_rece

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2eb5cf83-edbd-4677-9d1b-6509f92c7f74.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):	22746
Entropy (8bit):	5.549862933644964
Encrypted:	false
SSDEEP:	384:Dut3LlufXf1kXqKf/pUZNCgVLH2HfDIrUIHG0HG9nZk0Epj4u:ILlYf1kXqKf/pUZNCgVLH2HfUrU8G4G2
MD5:	AF6B9A5F339C24EA9AE833B73AF185C4
SHA1:	53BE7A4F1CC85B135F249987C0F76C92576E32F0
SHA-256:	EB05DD71342A7273903AD889BCD105E6C86A5822FBFA3EBD864BAF98B8A6638E
SHA-512:	3FB7DCF64DBE69C9D0691FFA5EDF260773EBDEC18646EC16E014D4BB1F2DDECF539C87DAC78465D3032C30B00339C8ACA807EF4FA9BBB60384AF6B6E1A137 D3F
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":"13256229780659829","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\433e9023-3b1c-4fba-88c8-b8bd23dd665e.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):	4291
Entropy (8bit):	4.852165518610062
Encrypted:	false
SSDEEP:	96:JzMKxDHGXCtDj6V4eaSCLN8iJtZk8+1Vznwa4FEVGRBcG4G/ehM:JzMKxDHGXCtDj6V4eaSCL+iJtZk8+1VC
MD5:	51626DD7D02B371EA86685313DEF658A
SHA1:	C6AC19EDBF2688B7F5C52A7E0925061267E0EA3F
SHA-256:	9868B799B925C9392F333FC393EA73B3F94FBBF4687AD9C22B7526EC174994AD
SHA-512:	FB7D79BDD976706E39C943BBEABFA36DF2545C18ECD75693C5100B8189925B72BC861FF03CE4922E6C1CAC0913941206ED1947A0EAADF489F8FD328DB713A6 6
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13258821784068470","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13258821785219928","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://www.googletagmana

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6106f48b-a90d-43bf-be50-905eb2270ba7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6106f48b-a90d-43bf-be50-905eb2270ba7.tmp

File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2714
Entropy (8bit):	5.59575783573714
Encrypted:	false
SSDEEP:	48:YIUooN5U9GCaeUopieUo76UUh7U9iUo4mUoTKUeiaqUoDpU92BsmU9eqPeUekUeC:PUogU9daeUopieUoeUUpU9iUovUoTKUF
MD5:	15DAEBCDF490EEAABECA3A7E1C7D003A
SHA1:	AF46B2806D632FE319E1020EC504C8E5701F50A9
SHA-256:	63F9C20B40BF510BC5AC5B241372A4E5BC2350426F28ED6CB90A08134867066D
SHA-512:	18C41E1742BBD64124DFD7ABD3898B4D787C287A58989CD6E8B4271C0FFA01693A9ADE44A3881377E39EB654DE6C6A38271C28E3FC6726FF9091D9530F76A36
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1614348248.24103,"host":"Dg14flaciUHGX6Lc+OnYmaNiAA/ADiwumtIyPrC3d6U=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1611756248.241034},{"expiry":1627308279.106947,"host":"HS0xQK8RrrSZ/KdSgKIC7bLU+xijlimr9JuWvTPbfkE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1611756279.106951},{"expiry":1622642586.021525,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1611756186.021529},{"expiry":1643292185.221761,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1611756185.221768},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1643292279.386712,"host":"Y1cbV6ziZu1KjdKdxBzKmgzsZCYqaDEHWONjJAo942Q=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6b3e909c-0693-4093-b6f1-1adcac6f9773.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):	21283
Entropy (8bit):	5.552965376572306
Encrypted:	false
SSDEEP:	384:Dut3LlufXf1kXqKf/pUZNCgVLH2HfDIrUrHGcnZk0Apj4f:ILlYf1kXqKf/pUZNCgVLH2HfUrU7Gcnl
MD5:	69BAAC395B8F94C1768B34947765C625
SHA1:	0AD744765FF169909509C8343D318449B683AE62
SHA-256:	FF8FBC0601246EEDA4BE70FE822D8AAC1AF080BA374D363C5225F84EFC7F2AEB
SHA-512:	5415F2BBD5D51DE36E619D4374E14506A0E9503B30AD12EE3561EF5DD7300876B621EDCBA92449C22A15F2DF2BCC32DED1ADB401BEE570C780D18D1B3586969
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":"13256229780659829","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\9c4e306c-f3b9-4e55-9625-fd0925c1662c.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):	15427
Entropy (8bit):	5.601074750751302
Encrypted:	false
SSDEEP:	384:DutyLlufXf1kXqKf/pUZNCgVLH2HfDIrUp80Npj4v:fLlYf1kXqKf/pUZNCgVLH2HfUrUp8up4
MD5:	CB970383E7E128FECE8043D0601ADDA4
SHA1:	87340C289C6EFF41A9DBDD1B143972D61D08EB28
SHA-256:	0C2F058D3F986A63DE8D20EE55763B9A61A535B8DB9079F71BD704EFB97A3018
SHA-512:	5738C046E515C1AB6552C8FBF9B8F5BE78326574EB3C6AEBABEFE93F37E73DDB9B06DF3E705D391F357DD63A60DBF002B064F4D2FB90091132837B75C038E66A
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":"13256229780659829","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.222426249564994
Encrypted:	false
SSDEEP:	6:mZo0Oq2Pwkn23iKKdK9RXXTZIFUtpkdYZZmwPkPkwOwkn23iKKdK9RXX5LJ:kOvYf5Kk7XT2FUtpUYZ/P25Jf5Kk7XVJ
MD5:	708E8579C97D5D599B30523A726514EA
SHA1:	A2BA2567CDE2A3AECC377037DC292E8D7DEEADCE
SHA-256:	7000743DE33C6C2D9D1921D35FF0E8D127D04D40C4C3DBB641DE95D572BB6F6F
SHA-512:	70DA47DE6DE2916E7FDD239A020288620A32E0471C9AEBAF4D587AFF6E40D144D39BF69E82CD022CD10652D47DBB3804CF0B8D8F66A3BD4F61685CBF767FEF A
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:03:15.667 1ae4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/ 01/27-15:03:15.668 1ae4 Recovering log #3.2021/01/27-15:03:15.669 1ae4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrik eDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.185903564257753
Encrypted:	false
SSDEEP:	6:mZX5q2Pwkn23iKKdKyDZIFUtpkdZZmwPkRkkwOwkn23iKKdKyJLJ:evYf5Kk02FUtpc/PYk5Jf5KkWJ
MD5:	83B26E05E79920E6B1D51447A8AA4C9B
SHA1:	1D2121DBD4985FBF145A35B082E52757EC8A5352
SHA-256:	FD7A87B773FC6AEC16439A3B299181B922F54FC304DACBE1B10E96CCB0D5ECB1
SHA-512:	238E39F85EC73778468D3494AF8655CDFD5DACB722D23C14DF18E078DA492FF5178A49A3A9CB5A16F562A5C8695D30695783C84DEB0D79AC597F27F61A11473
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:03:15.662 1ae4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/01/27-15 :03:15.663 1ae4 Recovering log #3.2021/01/27-15:03:15.664 1ae4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatab ase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0526a56c7251902d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	201
Entropy (8bit):	5.575858843048221
Encrypted:	false
SSDEEP:	6:mqYQiiGEqCfrgRmCtgs7kHN6ch9/ZK6t:six5fURmIuN/
MD5:	CF746339950E390A17FF5AB6465DA785
SHA1:	C3B4759EC51751DE572A6DC5A71B97B5C5271B01
SHA-256:	BD6F752018DEBFE6646E1F1D50F8008111FAD9AAA2627A97BA033D6C591F2089
SHA-512:	FABAF5268A0B21E994DAE0C6CF01F927450D5134B432AD5985C1E9D55AC5584520E9E13C58118A854B2626DEA3FCDE930473F63DEBF53CCDFF1FDBEC760B74 E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....E...W..g...._keyhttps://quip-cdn.com/8537vty5Chq4BaEBxXH7sA-gz .https://quip.com/J.c.x./.....b..!A.@....U.dN\...}..P5.._<..Q.A..Eo.....e46K.....A.. Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0c0c9f7a3d839981_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.584337194516423
Encrypted:	false
SSDEEP:	6:m1YGLSmXZCLRr7xgrHgZGhcjumUiXLkAcK6t:eXMGh3mUi7c
MD5:	525FAF506853B5A0AA8248ED60BD9F15
SHA1:	C3803D85AFBFC415D45AE80933C827FAB757DFEF

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0c0c9f7a3d839981_0	
SHA-256:	F5900096D818321FD8EA690D76B5C84FAEADF8BE8994FD288D9BF8119B9AB4C1
SHA-512:	399FDB00B229DA35B5FE7742C527D206C319C6428E7DD5A3C41237B6FFDB076D0A25EC84DC61F2EC781C16D2E86A57B9321C5A225355C9B1268CF1BA2556AE8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L...Z..H...._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-WBS6NX .https://quip.com/.h.x./.....v.....9.....w+... Al.(ho..[..m].A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3267e7daf16fbf9a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	209
Entropy (8bit):	5.4338238453699566
Encrypted:	false
SSDEEP:	6:mebvY+PW/ULMdaNogfWgovvScxqd0hZhQK6t:8rU5mvv++vI
MD5:	64656A06608E6BEB3C8E0E8EBE61EA2E
SHA1:	2FC3AE8E1BD871F778894CB6EC9057AEA4A471F8
SHA-256:	05D8AA1F182A3292BF130E83817A650FE24A5298C8B6DE9382DDD142FB83DCF3
SHA-512:	0E0A252CE450795E4DE43B4385BB80645A6E24BA9F5409B4EC8F2C6675CADDE371146809F1E9C5D08C614456D28F0BB817E234AB0BC990A1A3EE5CEABE3D9BF9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M...u../...._keyhttps://snap.licdn.com/li.lms-analytics/insight.min.js .https://quip.com/~...x./.....?...`?.....U!v@..zW..=..q.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\44a148030134590f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	201
Entropy (8bit):	5.410265745957952
Encrypted:	false
SSDEEP:	3:m+lt1AntLA8RzYzYlIL+RXHTLZuFvDthK51ov/l/lHCeClJbnWuAA/EUmFMvpK5M:mWAnnYMlXzFQg51ovtg5lWPAM/FOK6t
MD5:	BEF495D09CBAFEDF7FD4D6705CF8E687
SHA1:	801BEF7A556CEE4A8D820B6B172BC174CDAF08D6
SHA-256:	CD1D892273A05C776A82840990795C320F16A80ADF76C05A0FE9EB8D24884E44
SHA-512:	CBFE891212B0AACE6A58B64EBEE459564F8A4C7166941B4F8DC73F8F76A67E644BB94E8947B24389AFBF3F2D45A30EA8B14450FC8A5715260156899E6AE09821
Malicious:	false
Reputation:	low
Preview:	0\r..m.....E.....B...._keyhttps://scripts.demandbase.com/841642b6.min.js .https://quip.com/tG..x./.....d....5....(..G1e1<.v..d.].w.\..A..Eo.....V.mh.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b38fff78a48142d9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	200
Entropy (8bit):	5.296384675365347
Encrypted:	false
SSDEEP:	6:m/AEYGL+MIwJJOgxgaymbhVDOm4qIhK6t:EAsIwvP7fmmK7
MD5:	028F6041A15A3EE868B6788C95A89393
SHA1:	28787CFCF99CB5A5279B4625B6C834A7B8C0820E
SHA-256:	B6CC884D1BC9D0EFE9586E83F38249375784DC3393435ADE0C7F97756CD91763
SHA-512:	AF7481A416E3C12E6A5ECC4FB61963EE08C250620887F40EE7C26803DBF47D14130EC17C7B5A7C8807AEA069E14F49683D04B185B4A86D235CECD0564B4869B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....D...I.t...._keyhttps://www.google-analytics.com/analytics.js .https://quip.com/.gh.x./.....h.....b.....l../l..a...0w.A..Eo.....o.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c9226d7c7cc7ba4b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c9226d7c7cc7ba4b_0	
Size (bytes):	211
Entropy (8bit):	5.583913304938311
Encrypted:	false
SSDEEP:	3:m+lfKVll/6v8RzYQiWLyTGN/nViBwKWXc/tV7hKGBdHl/lHCPf/lfrIs+PLWKaCU:md/XYQisQBwCZg8gPCs+P7aYEK6t
MD5:	87D0DE228F8B0D168CEB9EACDEECE89A
SHA1:	89C905729670E64EFF1F58C6FF4B76ABCEB9C670
SHA-256:	A7DA31410598B2E30F4D0C82F637FC2F653CAAEEA11AB935D6E13423E1AE91A3
SHA-512:	720782851DB386C4FCF705FDB738A2B145F7A40AC8374F32C4CDC892B97449032AA9343FD2036CC26E226789AEF4F4FB8C4E005C86166E62FB7D2875D5CEF05
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O..../?;...._keyhttps://quip-cdn.com/xhZBtVClR2EcdOOOPl8eYg-ancillary-gz .https://quip.com/<.d.x./.....T.....b...m..s.....r.A..Eo.....P.GO.... .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d978b0efc727804e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	190
Entropy (8bit):	5.33475214841895
Encrypted:	false
SSDEEP:	3:m+lD1ztla8RzY4rKUKbbXRthKBm/KHl/lHCutbC/JamfNXy/zK5maDvl/lllpK5M:mE5nY4rkvXrgBm/ug5f74IvRK6t
MD5:	F47C5CBC9A00E3F92DC8F5B64B9380A9
SHA1:	64F4D41B87FA6FA134E14415D19DCC2FF2334EF1
SHA-256:	45E2A31582208DB76B2409068F4C81C1ABB86F5D7F169F1AD57C08D377D2E3E7
SHA-512:	E062E875237CFBA53805966529F7E1F76CC894153C385760B4893B80EC37CAE8EE38DEFE0B1E8691C69A79CAC23959830C8DD0CDC1D936C9437DFD81AD6935
Malicious:	false
Reputation:	low
Preview:	0\r..m.....:.....RV...._keyhttps://s.adroll.com/j/roundtrip.js .https://quip.com/t...x./.....HU..2.....$j..E...c.....A..Eo.....1.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ec99ea3009e95d65_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	253
Entropy (8bit):	5.897155150155169
Encrypted:	false
SSDEEP:	6:mQ0Y4rgdsPDYQvnafjh/gSWurgNLo/gDhZrV2ATljqnK6t:87LBnwjqSdUN1/lqp
MD5:	4817D9A9BB5D92FE97DB9563D8E68598
SHA1:	6D03C782DE089CFDBCC609BE826C7E6B29999293
SHA-256:	7A4DD8D30DF52548CB7C3C122DEC7EEC2B069A94AD5A604BE590568257ED1020
SHA-512:	E1EDFF9FD43A2BB8E4319C1E7D3E6172027FA3A3F9572EDBC53620A7B23AD93DB629B07E38DC9A4A45DAADD2B25EF79B651546C27515C37914D663DDFCE09 94
Malicious:	false
Reputation:	low
Preview:	0\r..m.....y....._keyhttps://s.adroll.com/pixel/VNM53VCKEFACRMFQE65VV4/IB7LZPOS3RCN3J2MSNRBFC/X27ESS35BFE4LKRZIE373P.js .https://quip.com/..*.x ./.....q.J...=.N-;.%.....p.m".9.A..Eo.....@.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.022736434583451
Encrypted:	false
SSDEEP:	6:9tAtGW7sN57XDtigG+SHlymKcTxzPawAfyDn6l:95hV5irlnZXUyGl
MD5:	96A8F310F5461CB436A6122AF3698278
SHA1:	149808929FCBB85F3517362B963A0357CFF4F99B
SHA-256:	CA9F7C041FB1D45E6ED92863FA7BE47EAA628F54D52089FF4A9277EE46FDCDC8
SHA-512:	575D7596143B3CF1CEC3DABF04AE0CD48C8FA54B90A201CD90E9192056C24C642B4A0F6D0E36AF40B0055EFF752B1F57C4D4C95560DAD328A4F6F221FD9AAD C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Preview:	......X3oy retne.....e]..0.....x./.....Y4..H.D...x./.....N.'..x....x./.....o...g2...x./.....-.Qrl.&...t.x./.....K..||m".@Xe.x./.....=z...@Xe.x./.....B..x.. .@Xe.x./.....^}.Np....4&../.....-..0..x..4&../...../...3...&../.....I....uW....&../.....Q.i....&../.....6,2.+.g...&../.....D....3...&../.....4T/f.C3....&../.....x./.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	4.253231191930472
Encrypted:	false
SSDEEP:	192:zuDMwrNxATTFYZpMwsmWYN+RPV7I9soEnjmiSbRtZ:l6xAvSjsmW/1d6soEjxSb9
MD5:	ED91B758FAC2110B7ACE85EF8D190249
SHA1:	E9E41902F783B992613581ADB92B0C7FC02AD855
SHA-256:	2B250D943EA4DAD19069888467B41069044848E9230CD5F26920507CC97647E7
SHA-512:	A940A0D86520AB4602B587506059C7A13E33D9D179830D6369FF6899AAA3AC5BAE3DC45D911DFF59C755CA718D7ED5649BF7D69CD9A88ACE2E313721285B68(D
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9736028666896172
Encrypted:	false
SSDEEP:	24:9e9H6pf1H1oNiqLbJLbXaFpEO5bNmISHn06UwX8:9bfvoNiq5LLOpEO5J/Kn7UQ8
MD5:	D73B75268A3A60D0B2C2762D91C3DF07
SHA1:	6A95C37EFD0B144CA6AAD5D8E7A166A305006407
SHA-256:	ACF698FF0D59F5B7DA82E0624BE1C6204D5EED5B905C0B182860B247784AE0B0
SHA-512:	7DB58BA559E4577B3E6A438D25E2CCDFB96C99535F648BA92AF618EBF35E0CBC04E9B42A6C2C8875F6A7B262618E7F9E056206CD7B9AB877D02FA2D7E7C2DA 06
Malicious:	false
Reputation:	low
Preview:	.....).S..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1925
Entropy (8bit):	3.6105245329908877
Encrypted:	false
SSDEEP:	24:34SkruZVNloJSdyfEl+OZbofZaVW2awEluOZV3Oh1pRMlJlh:342ZdDdGM+OZbhuluOZNSmrh
MD5:	1C59A2B605B9E800D0ACF9FD250D820D
SHA1:	614AC26A1EEA384110DDEFE4D60089EB5B168132
SHA-256:	E147E8984FDF7D68B22DC6E87B2A2B34845B9BB47F04F1608F97A2B8A0A561C9
SHA-512:	9D3148D2557F5431F63D20AEA10E7EFA668877C7335A31F04AFF1351B7F8E160EB2296FA5CBCD1FA621C200E1DA2D7914D0DB420FCE1184BFF216FB8293AD52
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...856ac389_42f7_4696_b718_8a6fe81731ce.....A.....5..0.....&... {730C75E3-B87A-4292-818B-DC8F984D08AE}.....https://quip.com/R1lpAz7okW3E.....Q.u.i.p..... h.....`.....:.....:...@.....X.....X.....B.....h.t.t.p.s.:././.q.u.i.p...c.o.m./.R.1.l.p.A.z.7.o.k.W.3.E.....F..... ..o".objectId".MIMAAAvS41x".secretPath0".navigationKey".~{.....8.....0.....8..... .....https://quip.c om.....https://quip.com/R1lpAz7okW3E.....|.x./.....V.].x./.....V.].x./.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	57
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlXNQxlXNQxlX:qTCTCT
MD5:	41C7D1373DE8E7BD508C548A70910E51
SHA1:	F919499049571C75C7EB73FDAAA5198E6DD641B6
SHA-256:	99C59CBE7DB56D56A286485635E4467004641C6275E708887DD35728EB05109A
SHA-512:	C30CB4EA2478FD816B4A160626B08CB63D2B9DC50EAB694607D44D05117E6AF8DD707BF4E14CF001CF69007A654ADE55149A61ED07F9DE6A9A2EDCB51AFA0 73
Malicious:	false
Reputation:	low
Preview:	.f.5.....f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.225945638537733
Encrypted:	false
SSDEEP:	6:msFBq2Pwkn23iKKdK8aPrqIFUtpkZmwPMUzkwOwkn23iKKdK8amLJ:/FBvYf5KkL3FUtpk/Pl5Jf5KkQJ
MD5:	DC46A4B43F479B19BBCE5DA4BC7DDA84
SHA1:	28A77F3B8EA522390881764E16791A80799D6C99
SHA-256:	83D0A7FF5F9C9F48CD8448991923578C022C5EE7C48E91B952842201CD713F94
SHA-512:	BC372D5C54139AEC77011004FDA7A09C49569E9DAC32D36E0EC775C6E2F8204A0B864F97F10570C02300B9D2CAD0C1B8ABD34E0F78E7FD7EB4A438B42C66EF 8
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:03:15.999 1b64 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/01/27-1 5:03:16.002 1b64 Recovering log #3.2021/01/27-15:03:16.003 1b64 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log

Reputation:	low
Preview:	.f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f. 5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5.. ....f.5................f.5................f.5...............

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.169487097380187
Encrypted:	false
SSDEEP:	6:mel4SQyq2Pwkn23iKKdK8NIFUtpDZG1ZmwPD3ImSQRkwOwkn23iKKdK8+eLJ:p4SVvYf5KkpFUtpdG1/PUJI5Jf5KkqJ
MD5:	F19DBA6E0AEE9C8DC8EBC8CFE6C5147D
SHA1:	A093C4AE635B0986BC7E652496D592FFD4D7F6A4
SHA-256:	D6E4E8ACC32DF7A196BF0F8032C202F48E554440AE3C3D7546B10A69EFA65561
SHA-512:	16A87113BE225441CD1DC7588E278CD38ADB57867EAF1B87007D7DCD40817A1D1300FA295A921CB08477956A286A647104490ABC1485D3E5D2A45BAF075C943
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:03:03.739 1b70 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/01/27-15:03:03.740 1b70 Recovering log #3.2021/01/27-15:03:03.741 1b70 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_1_metadata\computed_hashes.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17938
Entropy (8bit):	6.061511031838911
Encrypted:	false
SSDEEP:	384:ahlZ97TC4hNLFkQF/4H/vo3c93yaM5ZAVGnLMeP3rrBsuzfccHyfXRH0MVEPT:ahlvS2Fk5ooNM5Zg+YePRgpXRHLVA
MD5:	58E0F46E53B12F255C9DCFD2FC198362
SHA1:	24E3904DED013ED70FFC033CFA4855FBB6C41C19
SHA-256:	F82EEF4F80D86F5DEF0F40F91FFB6453E1706CA5FD8A7172EDB19C4B17E2F330
SHA-512:	1AC83CDFF124E4C0281FBBFC0A919AA177F1524AB85434D82E5A87DDDF7CAC26A761C5E6249566626054C62D6B0F46A51AAC1F6E64C260F50832AE1D5F0A49 C
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["vyABSKu1ssLnoQtj8Nqw6CjEthL33alh0QYBLzRg9+E=","DGWrOFQ2mF53Fk3FM5jLCV5sKg1DgRTF750mXhpKaoM=","f8vmSL13lL5/sEk/UBo2z9BTE1au+kMnftvxebWlLfQ=","g6BagkGM3fYVfhX6pe9v+WIhrxb6KJyr1H8KEdf3iQc=","6GdjKPovCi9TAL74Kj/R6GzGC1RVsWCb0lMtrG41ElU=","vttVT0ok78296FZBpoJgEIMmZmATBpKLrC5wr6RiPIg=","5dwwmOMAg6GXh2x6hn99MsZgiXJCxgTnwFdiMmcl2/0=","lQFxytI8i5cYLqNLbSnc45XXd/jEIuKwO1nAvNh5/WE=","qETF6aAOXwVcduPggf/FGrY8l2ALwdIswKxFJWG2JpQ=","+fjs95t/ESSgtcK9SzZOIcY/aemUr2I/yYI07esfjbk=","H+r4m51qI4G0z8YtAibc3/AGYvPK9qT14BbGvmM4/y4=","Qz4vtomAqVrAeKIcJ/zbVi5yDpFiY+F7tP/FTdoAKwU=","k110zqa69JMO5T4RH/nBdkCVX9I/98Gd7K2dnRuyFyg=","+QrRx4Pz8wbz4ef9ch1Q2aAQDZbv0r64NMyj9z0qaaE=","6q/tcYekY7TN66ZdPx4ALLcteRLQJqFy0wgcIqL6fFU=","djipPPtOAFsToDpKDbadLJLGQiCzTkN2qsRbzvKijBo=","uHEm1DVxHADroGNWHjmdfpdNUgtHXDQ0zfTmdqtJgYo=","1C2E0Gz2nqKFG3ghcQEVyiTYI4rTYNnrpsHQY9J7BfI=","swYZ8T85/4tzx26dfC0RKxMiHwnjqJoxtn0Mb8NdcjI=","AuXwavx8SOtkgFhnRlnM4roIw243Ryh2ktL0QZRDLoE=","oG0S5XUkjBtAHts9X+uQt5MTsf

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_2_metadata\computed_hashes.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17938
Entropy (8bit):	6.061511031838911
Encrypted:	false
SSDEEP:	384:ahlZ97TC4hNLFkQF/4H/vo3c93yaM5ZAVGnLMeP3rrBsuzfccHyfXRH0MVEPT:ahlvS2Fk5ooNM5Zg+YePRgpXRHLVA
MD5:	58E0F46E53B12F255C9DCFD2FC198362
SHA1:	24E3904DED013ED70FFC033CFA4855FBB6C41C19
SHA-256:	F82EEF4F80D86F5DEF0F40F91FFB6453E1706CA5FD8A7172EDB19C4B17E2F330
SHA-512:	1AC83CDFF124E4C0281FBBFC0A919AA177F1524AB85434D82E5A87DDDF7CAC26A761C5E6249566626054C62D6B0F46A51AAC1F6E64C260F50832AE1D5F0A49 C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_2_metadata\computed_hashes.json	
Preview:	{"file_hashes":[{"block_hashes":["vyABSKu1ssLnoQtj8Nqw6CjEthL33alh0QYBLzRg9+E=","DGWrOFQ2mF53Fk3FM5jLCV5sKg1DgRTF750mXhpKaoM=","f8vmSL13lL5/sEk/UBo2z9BTE1au+kMnftvxebWlLfQ=","g6BagkGM3fYVfhX6pe9v+WIhrxb6KJyr1H8KEdf3iQc=","6GdjKPovCi9TAL74Kj/R6GzGC1RVsWCb0lMtrG41ElU=","vttVT0ok78296FZBpoJgEIMmZmATBpKLrC5wr6RiPIg=","5dwwmOMAg6GXh2x6hn99MsZgiXJCxgTnwFdiMmcl2/0=","lQFxytI8i5cYLqNLbSnc45XXd/jEIuKwO1nAvNh5/WE=","qETF6aAOXwVcduPggf/FGrY8l2ALwdIswKxFJWG2JpQ=","+fjs95t/ESSgtcK9SzZOIcY/aemUr2I/yYl07esfjbk=","H+r4m51qI4G0z8YtAibc3/AGYvPK9qT14BbGvmM4/y4=","Qz4vtomAqVrAeKIcJ/zbVi5yDpFiY+F7tP/FTdoAKwU=","k110zqa69JMO5T4RH/nBdkCVX9I/98Gd7K2dnRuyFyg=","+QrRx4Pz8wbz4ef9ch1Q2aAQDZbv0r64NMyj9z0qaaE=","6q/tcYekY7TN66ZdPx4ALLcteRLQJqFy0wgcIqL6fFU=","djipPPtOAFsToDpKDbadLJLGQiCzTkN2qsRbzvKijBo=","uHEm1DVxHADroGNWHjmdfpdNUgtHXDQ0zfTmdqtJgYo=","1C2E0Gz2nqKFG3ghcQEVyiTYI4rTYNnrpsHQY9J7BfI=","swYZ8T85/4tzx26dfC0RKxMiHwnjqJoxtn0Mb8NdcjI=","AuXwavx8SOtkgFhnRlnM4rolw243Ryh2ktL0QZRDLoE=","oG0S5XUkjBtAHts9X+uQt5MTsf

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.412217718747323
Encrypted:	false
SSDEEP:	24:LLitYxh0GY/l1rWR1PmCx9fZjsBX+T6Uw5F/MIgC1FXdEzubo4gznoB8c4V:tBmw6fUiF/MIvrmzubjmvcw
MD5:	6B213DB35ADD79A2A1269A153F29A7FB
SHA1:	D2CD7E921347E21BBA982B5CCE985ABB6F382FD9
SHA-256:	C318D17F2B153EBC27A20406128AB253BBF9E5C1F32FEC644B2B578AA8D26E9A
SHA-512:	DF90A4AEEA0BE997E17FA6723F6DD75EEAFB7490C87EAE60C43DCC7CAB4AB1D0EDC8674315E345A015DAD06F0A91E959AC63B71B79F9969CCC24DEDCF5091815
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16972
Entropy (8bit):	0.8122964515215189
Encrypted:	false
SSDEEP:	24:/jJ9lnwBQZSWyLjtVxh0GY/l1rWR1PmCx9fZjsBX+T6UwA3n:Bnq0vCBmw6fUf3n
MD5:	5548103663588342113DCBEBE2B01FE6
SHA1:	5042D9662617E782B998D2EEC4DFDDCE0920394D
SHA-256:	0D3220914FD8217158866F01809ABEABB9C35C5ED8A4464187399AED044C047C
SHA-512:	1E442744B423EC13C8469DC35F235208D1B51C67232B49C109507CE3ADDB7AE6C9DA1DC53EB38D1CF930EE46EB81163EDD50CEBDB65B52BF62034C0467DA0C4
Malicious:	false

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
Reputation:	low
Preview:	.f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.228435614433346
Encrypted:	false
SSDEEP:	6:mfTumq2Pwkn23iKKdK25+Xqx8chI+IFUtpioQZmwPidYzkwOwkn23iKKdK25+Xqp:ST5vYf5KkTXfchI3FUtpiT/PiWz5Jf5G
MD5:	D05FBF786C3594F9F6A48A2082B031D4
SHA1:	1D149A216849C14F2AAB141571D9E586A6451738
SHA-256:	4B9F13EBD15BF4229A6BD551964EE8A49ECE7181654D14103F787EE81E276F24
SHA-512:	C95D01B902DB611799E9F6C4311FB60B60151C78787FA6A01CCE62A73736B13D7F6CACD0A350CC637505815023D765D585CB302F67FDE867E947C78FB4F460B
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:03:15.606 1ae4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/01/27-15:03:15.607 1ae4 Recovering log #3.2021/01/27-15:03:15.608 1ae4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.152533434272296
Encrypted:	false
SSDEEP:	6:mfVumq2Pwkn23iKKdK25+XuoIFUtpie8ZZmwPie8zkwOwkn23iKKdK25+XuxWLJ:SnvYf5KkTXYFUtpieQ/PieY5Jf5KkTXp
MD5:	A7411E475E79592A24D0D84548782C25
SHA1:	2647B4E4248E0A9A8CCBCAE03566C15036148899
SHA-256:	3EE8E43776AA9DB0FB94B073BB93405CD8B6A3B1E219DB521FA421F33B2615B9
SHA-512:	AE0003AEFDFB6CFADFB11B58AD100759F15FC30858E5B507B48BEDA43993F4525BDBB5D1E052F71E10C508879ACE5D76D5B15702DC9E516C0550A136B38F4E0
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:03:15.600 1ae4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/01/27-15:03:15.601 1ae4 Recovering log #3.2021/01/27-15:03:15.601 1ae4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Entropy (8bit):	5.214058342603387
Encrypted:	false
SSDEEP:	6:mA2Vq2Pwkn23iKKdKWT5g1IdqIFUtpH0gZmwPrKV0IkwOwkn23iKKdKWT5g1l3Ud:x2VvYf5Kkg5gSRFUtpH0g/PrO0I5Jf5N
MD5:	5E934D60D1155F74E6241F1549C6047F
SHA1:	8652CF13850AA653D391FF689429B08220FDC0B3
SHA-256:	98DD315BE8578A9C5BF63246FF6223CFBAC9AE35F2AAB06CEAF36F022BF89A63
SHA-512:	C7F7122D9CE17A112917EBA831BD2C7B170C6F4714E65C91ECFAB8A589DF16A56ACD4B6A1363B1EA7C72F047C314EED6C5626C520CF091FF6E2B6E41B741958
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:03:15.567 1604 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/01/27-15:03:15.570 1604 Recovering log #3.2021/01/27-15:03:15.571 1604 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.23706762340105336
Encrypted:	false
SSDEEP:	12:TL+A/Dfhy6XNvd2ZEPnDUpDbxrzb/HibzVQMBkkpCFsOwrYRsN1SUkLWh9Ko:TLxZaxT/H8zVNnCFsOwVxkLWh5
MD5:	DBBDA01ECF5F17E278DAEE38D468C21B
SHA1:	E288DAC0DEBAC5C984422E3367460F1F9E9394B1
SHA-256:	81121C4E69FF0C7C3057C30F5FA23B170DC84B85EAB433A61BB1F71F7AF41E9F
SHA-512:	422A0111571B13E0A3AC091DCF15FCF2DB9116CDD2762A2A19604A059C9A6D8400DDC672F850371F688C7568D7F7A112BE4CCB39EF8C362335092B1152423194
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	860
Entropy (8bit):	5.483485444769726
Encrypted:	false
SSDEEP:	24:p81prcq2X6wn1cEQZQ4/2Y78BJgskfa9yBGNhYljcMhLcS2Rc:e7vdu1cTQ7UCYljcMhLcS2Rc
MD5:	726D160C25502EE034A0122FF694E7F0
SHA1:	F1DAD7D3642F0CB43EDC3F7AC40A1702883191AC
SHA-256:	3B631ACF2C9FB4912A0E6401CF988B570FB7207112F7066ED2DBFC2706652898
SHA-512:	0C1129703546A95A6C20CAF1CD37F73E7F2AAC926D20B5246FF8AFD203441F917B44BE15B68D57AFE8204DBD3F9F3AEF63797DEB69609721B84A4782DB3F3C7
Malicious:	false
Reputation:	low
Preview:	....."R....com..doc..files..have..https..incoming..quip..r1lpaz7okw3e..receive..some..you*~.....com.....doc.....files.....have.....https.....incoming.....quip.....r1lpaz7okw3e.....receive.....some.....you..2.....1.....3.....7.....a.....c.....d.....e.....f.....g.....h.....i.....k.....l.....m.....n.....o.....p.....q.....r.....s.....t.....u.....v.....w.....y.....z...:e.....B..... .....*.https://quip.com/R1lpAz7okW3E22You have receive some incoming doc files... - Quip:.....:.....:.....:.....:.....:.....:.....:.....J.....#.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	42076
Entropy (8bit):	0.11649233793077282
Encrypted:	false
SSDEEP:	12:R0EqDRIHfopqLBj/YZAt3lKE4nMWQASjG9LSBQZ8fOM:WqLBY6t3of1NSTfl
MD5:	386A0A1567A7B25A013A43C8E4DAE762
SHA1:	3D8F300538EBF1BF332E6056376A7D33CF5AA197
SHA-256:	DE32C37B0F87B8D005DC935F4135F353803E6B14972A3FB24F0C691BB3F437B2
SHA-512:	1CF8AB9C870E5217718E42893BC7D87CD816FCA2FA113B611DE02C9563D84BB48C0100C50A5B9DD5006C7422D593813B1C1D6148F62295178145E557C16BD905
Malicious:	false

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_quip.com_0.indexeddb.leveldb\000001.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//Uv:1qIFUv
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_quip.com_0.indexeddb.leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1045
Entropy (8bit):	3.7016118986071485
Encrypted:	false
SSDEEP:	12:6XRMDj0yFpXNNRj8l2UhdsillvvW3hOajcyOTHMewsvH/chYtB8FQ9flXVlsn:rnNf7o2Adn/+FjcyFeG2F1Xs
MD5:	10449FFCB253788415B2941651E862C9
SHA1:	8EDF489AEF999BE2B7E7454DE34FFB1CC33C7973
SHA-256:	00FC93C113DFF6B02FF101B4680EDC723D1FACF69CF9D230CB70B505FD8A849C
SHA-512:	19706169FD3E0CE15A287F77BDB41D86AEF34B1F6100004ECC3DF6F0C3B9FBB92FB95A6329692184CD88B9A2EA2BB8A874953EF127B27AAF74F04E88FA0B2DC 4
Malicious:	false
Reputation:	low
Preview:	. .....2....(.o".....o..9d.....9.....h.t.t.p.s._.q.u.i.p...c.o.m._.0.@.1..m.e.t.r.i.c.s.....Of.jV.....2..... ....2.....|..}.....2..&.b.u.f.f.e.r.e.d.-.m.e.t.r.i.c.-.l.o.g.....2.....2.....2.....2.....2.....2.....,.....b.u.f.f.e.r.e.d.-.m.e.t.r.i.c.-.l.o.g .....2.....2.....2.....2.....2.....2.....2.....2.....2.....2.....2.....2.....2.....2.....2.....2.....2.. .....2.....2.....2.....0...,.....b.u.f.f.e.r.e.d.-.m.e.t.r.i.c.-.l.o.g..... .....2.....2.....2.....2.....2.....2.....2.....2.....2.....2..... .....2.....2.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_quip.com_0.indexeddb.leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	168
Entropy (8bit):	5.3533261784089134
Encrypted:	false
SSDEEP:	3:tUKX9Y4LhMKKqFkPt+kiE2J5iKKKc64E/x14kUg6Vw/IrscWIV//Uv:mSCq2Pwkn23iKKdKETg6OVIFUv
MD5:	12F5150077536B767FE493B4155EE116
SHA1:	84FC59AAA660D5E0EB073638B301A0D3E905F158
SHA-256:	0D06ABBBD254C783D6449F988AD97F4C20DC751B182E524B15F047D588C2C0D1
SHA-512:	1F614D2FAD31EA4F841FAA6D5163DB16FB8D7DB491E9354A2890A2261B136F03174CB3EFFF97B92E108765EC03817B3ACDF7DBD718834555898903081ECF9107
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:03:07.136 1b50 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_quip.com_0.indexeddb.leveldb /MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_quip.com_0.indexeddb.leveldb\MANIFEST-000001	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_quip.com_0.indexeddb.leveldb\MANIFEST-000001	
Size (bytes):	23
Entropy (8bit):	4.142914673354254
Encrypted:	false
SSDEEP:	3:Fdb+4Ll:Zl
MD5:	3FD11FF447C1EE23538DC4D9724427A3
SHA1:	1335E6F71CC4E3CF7025233523B4760F8893E9C9
SHA-256:	720A78803B84CBCC8EB204D5CF8EA6EE2F693BE0AB2124DDF2B81455DE02A3ED
SHA-512:	10A3BD3813014EB6F8C2993182E1FA382D745372F8921519E1D25F70D76F08640E84CB8D0B554CCD329A6B4E6DE6872328650FEFA91F98C3C0CFC204899EE824
Malicious:	false
Reputation:	low
Preview:	.....idb_cmp1.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	14497
Entropy (8bit):	5.556335903097668
Encrypted:	false
SSDEEP:	384:wCL69VmuHZJvaAYKuPPogNh3M3gY/4327/vcJhH12dxKDM9VUD6/K4uJToeXo1px:f+gY/4mGC3
MD5:	AE43EF4BF6319E12E83106F543F470AF
SHA1:	B28F51E92326E719E20116A5706BE3F2651ABEC2
SHA-256:	DCD56B54AC07CACAB7FE8A71871A3201695AC0D0A67D5FB7C58C6FBFE0644D0B
SHA-512:	5BE29F75F92BC66EC97E001A23C3E6DEFFC8985C3389698D889F659B77F094510CCBDF9FB8CF46293B98CBCD7BB4DDC47D7EEECF2005598256B34CEFADF074B
Malicious:	false
Reputation:	low
Preview:	....-.*.....C.....META:https://quip.com.....N.&_https://quip.com..activity-recent-ids..[{"id":"MIMAAAvS41x"}].-_https://quip.com..activity-recent-thread-ids3.[{"id":"MIMAAAvS41x","secretPath":"R1lpAz7okW3E"}]./_https://quip.com..folder-prefs-expanded/groups..true.l_https://quip.com..server-options-add_remove_alerts_for_cdc_report_alerts..true.@_https://quip.com..server-options-canned_thread_metadata_by_name..."{\"default_slide_layouts_titles\": {\"canned_thread_id\": \"LAfAAAUyuy2\", \"canned_thread_secret_path\": \"87LaAqoqquhS\"}, \"default_slide_layouts_text\": {\"canned_thread_id\": \"JMVAAA0xVOm\", \"canned_thread_secret_path\": \"ixM9ACeC9KUb\"}, \"default_slide_layouts_data\": {\"canned_thread_id\": \"fHLAAAhoNpU\", \"canned_thread_secret_path\": \"LDAjARItrHhE\"}, \"default_slide_layouts_media\": {\"canned_thread_id\": \"SRIAAAK0b1p\", \"canned_thread_secret_path\": \"KVfqAQAjkgyZ\"}, \"default_slide_layouts_diagrams\": {\"canned_thread_id\": \"cLRAAAKWPCD\", \"canned

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.177952367930593
Encrypted:	false
SSDEEP:	6:mTwe3cM+q2Pwkn23iKKdK8a2jMGIFUtp8hEJZmwP8hEcMVkwOwkn23iKKdK8a2jz:MweMM+vYf5Kk8EFUtp88/P83MV5Jf5KV
MD5:	A069B747F502E761E8BFE604CB40DE14
SHA1:	90DDF59032512836E60C270E6217B6B4D53505C6
SHA-256:	98F9927055714DE450FD2C3415F15998BEB8FC55015EAA84687AC8553AA17330
SHA-512:	935CD327F607BFC633226F1F993249D95F6A82FBE0F37BAAF55551439A5EC33CD2B81E22A552A83F9CA1340678D2BE610185401656C8D8A18998FF19971BFBC2
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:03:00.688 1b6c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/01/27-15:03:00.690 1b6c Recovering log #3.2021/01/27-15:03:00.690 1b6c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.240817412323139
Encrypted:	false
SSDEEP:	6:mTk0Vq2Pwkn23iKKdKgXz4rRIFUtp8xRSgZmwP8FIkwOwkn23iKKdKgXz4q8LJ:Mk0VvYf5KkgXiuFUtp8x0g/P8FI5Jf5j
MD5:	A2082243B4C1AA0C43C83868B89D02AF
SHA1:	88209416813BAAB33DE9FA36D292017AF4498D69
SHA-256:	A586576224A2BAE69D8105D3997FC108B725DFE448123A7026C9087CD4A9A24A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
SHA-512:	C33E558FEE05EFE88204959BC4C32E74367464D78B6987B6C349D258DDB18739A405699AC2D4CBC28686C6D40CD3F4AC16AEFACF0BA8477427ADEE448333FE5
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:03:00.982 1b54 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/01/27-15:03:00.983 1b54 Recovering log #3.2021/01/27-15:03:00.984 1b54 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\QuotaManager	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	77824
Entropy (8bit):	0.4764387219116521
Encrypted:	false
SSDEEP:	96:vCIG+6bDdsDaBJvtHIm50I4sX/CIG+6bDdsDaBJvtHIm50I4p:a96EJTv4sXK96EJTv4p
MD5:	E476EBDF36AD6609E3D64A6619C71D0E
SHA1:	74DE642B26884AE0F227175174D7343D71844080
SHA-256:	B528A8D0DFB72963052B2F97438F2AB28FC0C0E38D39CA6687081142FB4213DF
SHA-512:	815B84B0EFBC33FD1508F709F91A0B5092FC75A62CC026A04F770103A9B91A71DBE305CB68213F76D09532E0B8B7F55C33B67F8270A07AC7DF8534DE370D0ED
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g....*.W.L.[....."..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\QuotaManager-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	25672
Entropy (8bit):	0.6530030104586435
Encrypted:	false
SSDEEP:	48:YRMLTQqzLbCIG+6bDdsDaKgJgKtHIm50I9a+U55:64TQsCIG+6bDdsDaBJvtHIm50I4d
MD5:	7F7EB054A6663CEE635C838F82AC0F34
SHA1:	114369B749A354556ACD124480B440E83B00F574
SHA-256:	256C014530ED48721059EB070F0FA6E7DD4295DADE5893D4CC9DFA8D562912E7
SHA-512:	00F06D746542605ED3A7DFD21750ACA50950C05BB09D4280094BE018D33EEEC74555623CE1C03E9FE9D688552EE9B24957D33B72DC1CAB10C6ECEB1FB39A1F7
Malicious:	false
Reputation:	low
Preview:	.....b.r..... ..... .c.....R... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	4.4858720341971905
Encrypted:	false
SSDEEP:	6:5lAEXlai93l2O7d4RgRptOLxMAmgn+TSlkTSlkTSlkT:5lXXXlldlRpyxB8TSlkTSlkTSlkT
MD5:	2101CE294EC2D5C10896DD2D8FF72AF3
SHA1:	BBA41A822D74DE3F50EAEB92F47074781AA48D1A
SHA-256:	03A707182C6B4D7A0DDD4185B1252AE2AF934669605F7527F180A75C8EDE677F
SHA-512:	9601D5F88C779F636113011E9E24AEB2A2535C09AB50C9D0F583776E0C4EE23FE472785A2838A8C2FCCD4432C9C341A460A8280FF3F820AFA2B1934C6B6EC181
Malicious:	false
Reputation:	low
Preview:	..&f....._.....next-map-id.1.@namespace-856ac389_42f7_4696_b718_8a6fe81731ce-https://quip.com/.0..A. .....map-0-quotaTestKey2B.l.....2B.l.....2B.l.....2B.l.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.081833025982015
Encrypted:	false
SSDEEP:	6:mT37Flyq2Pwkn23iKKdKrQMxIFUtp8sh1ZmwP8+wlRkwOwkn23iKKdKrQMFLJ:M3ivYf5KkCFUtp8g1/P8+c5Jf5KktJ
MD5:	F9250CF9E34287BA6487FB354F0EF46C
SHA1:	83E8C116B66484F6B9C02004CFF129ACF7B21CCC
SHA-256:	D57D4197753B84ADAEE40FB3DD8E4DD89FB607E9EAB7CFFB850ACB2F50AE3BF0
SHA-512:	41400F61AC73F1925D2FE971FE9C61AEB0360593FA25924C1F7801516E3652860549F1290978A6EA493A2784A5F4378BDC61ACE33444A955A2AB373015830E13
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:03:00.861 1ae0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/01/27-15:03:00.862 1ae0 Recovering log #3.2021/01/27-15:03:00.863 1ae0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.135857582919184
Encrypted:	false
SSDEEP:	6:mT/qM+q2Pwkn23iKKdK7Uh2ghZIFUtp8YYZZmwP8rpMVkwOwkn23iKKdK7Uh2gnd:M/3+vYf5KkIhHh2FUtp8XZ/P8riV5Jfl
MD5:	3615D3942598A438ECA593D15FEFF787
SHA1:	898AFFC81CAC5FABF6B0A3FA6DB4AA2E04727A61
SHA-256:	69CD24844B25F5787451A031A85EECFC70F104BA8F9136E2F82A4378EBF151A1
SHA-512:	A6E32C417386C1F550F942D204E7E0175D604A78940BCC54DAA7772840CD2CA0DDC38137C3516C6BF3806355A03A58F9D39271D0EF471596905C6AA6AEC5BB5
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:03:00.656 1b1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/01/27-15:03:00.661 1b1c Recovering log #3.2021/01/27-15:03:00.664 1b1c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.179963682653365
Encrypted:	false
SSDEEP:	6:mTIClyq2Pwkn23iKKdKusNpV/2jMGIFUtp8a1ZmwP8MRkwOwkn23iKKdKusNpV/s:MIjvYf5KkFFUtp8a1/P8c5Jf5KkOJ
MD5:	254EEB14DAC54DCF182AFCD9A5CA3FFC
SHA1:	45CB2B8EF660F281881D861432788E70FC7D7F0E
SHA-256:	E6974039E5E46F9877A42B0DA880989C1CBC3F807564BC45D660B7E42C287EDE
SHA-512:	4635DD779E3A94F791151E5FD0CA8C924598CE060D597C57D90C102F666BA441CADE254A47889E0AAF22BBC175CF6AC5C4676581D4D64555F63DF22BDF7664C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:03:00.881 1ae0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/01/27-15:03:00.882 1ae0 Recovering log #3.2021/01/27-15:03:00.882 1ae0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.205894583997941
Encrypted:	false
SSDEEP:	12:Z6VvYf5KkmiuFUtppHJG1/PpgI5Jf5Kkm2J:Z65Yf5KkSgnp4gSJf5Kkr
MD5:	86704E34D4881AC583C79E167AEEC52D
SHA1:	B4E348B9A9BE6EDB8B9FA8D11128D2B9B48FB127
SHA-256:	F2A8B5F26DCBDE0061CE36AA2ED32E5FCAC5A98E80C42414CD6F23F517B9255D
SHA-512:	20E84FEF2A95AFD147DB17E0A64B76B0683003ADC55CE0381B8524AA8B6F955CC9ADBBAD96F02F868C4965521A58A4A9F9A50FB532076581BDB33015535415F8
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:03:01.031 1b70 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/01/27-15:03:01.032 1b70 Recovering log #3.2021/01/27-15:03:01.033 1b70 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.2123297775977795
Encrypted:	false
SSDEEP:	6:mau3yq2Pwkn23iKKdKusNpZQMxIFUtpl11ZmwPDLwlRkwOwkn23iKKdKusNpZQMT:9uivYf5KkMFUtpl11/PYz5Jf5KkTJ
MD5:	AB6C2C11FE5726CDB092416750EB9458
SHA1:	13FE3548B811B341577D1F05A1D80FA5B7A33F2F
SHA-256:	E5660DC537E36D3A62526609E2CF10011D7674917BCF2BE344848B49464F2F23
SHA-512:	79AA7AE2E01DE3E0E51A1028659E56E02CA02A4011BC4F1AEADC3541F32462194C8FC3CE357D08604BCE7478AD243E2710F69238C25DADC9535E9A246625F66
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:03:17.766 1ae0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/01/27-15:03:17.767 1ae0 Recovering log #3.2021/01/27-15:03:17.768 1ae0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\f469bfe5-6d75-4b2d-9d3a-f268f27734d6.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\f469bfe5-6d75-4b2d-9d3a-f268f27734d6.tmp	
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F8
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","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\19e27815-a9e0-44e0-8228-91cae7f33fb5.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):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2F7ED
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","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):	592
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E8E:8N
MD5:	B505641E5E90B7CF4BC869DD1B4BE451
SHA1:	0EC7B13DC043E054AB48B8F45FE49EF1209C01AA
SHA-256:	2755F85F14CF33404CEEBF053D0CB79DC3B98D643A51075737E6A5BE154FE1D9
SHA-512:	610AF095630C93B0586F4D9CA84FA75454C472C557D4FDBC0D5C1851F9AABF8653079A7ADE4659ABADDEDC2E02E58AD13C7244CD004B0AA5A462307F293F833
Malicious:	false
Reputation:	low
Preview:	.'..(.....'..(.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.199450686192778
Encrypted:	false
SSDEEP:	12:UVvYf5KkkGHArBFUtp1g/PKnI5Jf5KkkGHAryJ:WYf5KkkGgPgpSJf5KkkGga
MD5:	8CCDEF54EB5B358D423B9A8650B335C4
SHA1:	87D4E2DF292C38FB390210EE5B6CEF057BB09EFB
SHA-256:	2697EA0C1EDB9A24BD4293B754BD26B9B4B9B6445188346028423BD20D2F7E87
SHA-512:	69C969E544158588125CC54F6A388A250570101937C98D7E97E30843EAB7B5B3657E0647D357DA28C5BDB80657AFC1B7D3680A3DF1E1167F30736D4203460A5C
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Reputation:	low
Preview:	2021/01/27-15:03:16.002 1b54 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/01/27-15:03:16.003 1b54 Recovering log #3.2021/01/27-15:03:16.004 1b54 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.18188599327492
Encrypted:	false
SSDEEP:	12:FOvYf5KkkGHArqiuFUtpl1/P/5Jf5KkkGHArq2J:iYf5KkkGgCgjJf5KkkGg7
MD5:	CE8DDD14F44AE8EE55F1F1FA1663AB37
SHA1:	78D233C392E2325557EF24CD3675A34E255E566B
SHA-256:	DB65D924FC745CCD6D04391C75FC7BF93B28B412D97EB408DD90AE1CC511600A
SHA-512:	E352A67C485F9A001C9706AE7F245964CBDE68CB7DBBA6123A5C30CEC89844D1030D1EFBCF3CF7A07D5605E5C84A0FE586CDE1028F332C0CBAC724E90501B96F
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:03:16.047 1ae0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/01/27-15:03:16.049 1ae0 Recovering log #3.2021/01/27-15:03:16.050 1ae0 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):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljl:5ljl
MD5:	E9C694B34731BF91073CF432768A9C44
SHA1:	861F5A99AD9EF017106CA6826EFE42413CDA1A0E
SHA-256:	01C766E2C0228436212045FA98D970A0AD1F1F73ABAA6A26E97C6639A4950D85
SHA-512:	2A359571C4326559459C881CBA4FF4FA9F312F6A7C2955B120B907430B700EA6FD42A48FBB3CC9F0CA2950D114DF036D1BB3B0618D137A36EBAAA17092FE5F0
Malicious:	false
Reputation:	low
Preview:	..&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):	418
Entropy (8bit):	5.211474397747561
Encrypted:	false
SSDEEP:	12:1ZvovYf5KkkGHArAFUtpF1/PF+5Jf5KkkGHArfJ:uYf5KkkGgkgYJf5KkkGgV
MD5:	6916FD2AEB98F85B58327C1B1FC8F0C0
SHA1:	1B630BB51F86CAA467CC8469C8C81031BF9BE0FC
SHA-256:	1475522DA0DE1B7A7A7B58AE200FF8689C07975D55D0CE0C4C5DE0547B850AC1
SHA-512:	43925D092510FFFA038082369ABB81ED71D1F407DCA11EF8776655175CAB29B65D8ABAFAC8846776EDE6E97737C5334AED74F495B77344C69E57EDB1F87F57E5
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:03:31.360 1b78 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/01/27-15:03:31.362 1b78 Recovering log #3.2021/01/27-15:03:31.363 1b78 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF21 24
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.2160350768548875
Encrypted:	false
SSDEEP:	6:mTY/Oq2Pwkn23iKKdKpIFUtp8mHkZmwP86kwOwkn23iKKdKa/WLJ:MaOvYf5KkmFUtp83/P865Jf5KkaUJ
MD5:	C1816C42ECC1E809735AFF861E80E58D
SHA1:	623752F96B65152BD4A9CA0CE3B1A335A42581FE
SHA-256:	ED5E961AC39212FD1666E35DBF841AB35B316EE3806D5AC1F4A97A8E405C2EF6
SHA-512:	812B3735232A92400B4A0EDBDA5228BB2E076AD89572077AC225B72F85441C167ADDDD7D975E6C81D9938AA5A76B917BBE381E0D6E13E3F60A8121B37E8B273 D
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:03:00.661 1b14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/01/27-15:03:00.666 1b14 Recovering log #3.2021/01/27-15:03:00.672 1b14 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.249942739397614
Encrypted:	false
SSDEEP:	6:mklyq2Pwkn23iKKdKks8Y5JKKhdIFUtpc1ZmwPkRkwOwkn23iKKdKks8Y5JKKTLJ:zIvYf5KkkOrsFUtpc1/Pk5Jf5KkkOrzJ
MD5:	A0D8F43F5FEF4826CC58645E5F39B9E7
SHA1:	C4D16ACC78F230237969A02AEC30678419657C36
SHA-256:	0B91D94CE5EEAD843D3ACE4CD7DC570314EC999AFAAB6F6BAEB6CF38D58FF1BA
SHA-512:	634ED15AA410131D97450EF2EC06417C65E490F65F4E8775A7897210607210CE264333054A0B8E005BAE15FE37AF699D42C52F2182B23F7E23377ABBDB56B0A9
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:03:17.068 1ae0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/01/27-15:03:17.069 1ae0 Recovering log #3.2021/01/27-15:03:17.070 1ae0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12
Entropy (8bit):	3.188721875540867
Encrypted:	false
SSDEEP:	3:Zh2Q9:Z99
MD5:	EBE692244C462149776081961C253325
SHA1:	92CB34CF6F3E8FEEC3D7F0644D3460BFE9D0AA4B
SHA-256:	8ED6749AF092F4ED4F65933CB61E4B06BA0AC291E93355E193FFA885B79034DD
SHA-512:	6E149BD320E4030B5BE89822A0A1CFBDB8BB4F40E3E81F17D405E7AE1F37EA9BCF5379E68BA1001C45C5251D2FC8936AD89A281AF03564CDB446DA7BC30F2A 9A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Preview:	....}D.y....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\69b737ad-04dd-4fa8-9f95-3977523a16f6.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 13 icons, 8x8, 32 bits/pixel, 10x10, 32 bits/pixel
Category:	dropped
Size (bytes):	175509
Entropy (8bit):	5.489440694064333
Encrypted:	false
SSDEEP:	1536:rKbsLAR2A4VBQV1111111111111Nr366R6faFR+up0y0y2im1OsFcgYzQNL9X:rKbsLAR2fe/FZntrslfX
MD5:	33EABC19FDF40F3D36B6870EF5861957
SHA1:	CF3EF59C3940B58C314E9F6A1616751553F2D9A2
SHA-256:	647D07F37554672865902B2CEE80864B5A5283C372C7263BB1497D5582054E57
SHA-512:	47CFEDB1FDBC9BC09905C70F69A5114C64A8FC791BCA480D24972275276F00CEB230C579B4217337F9C69ECB2AB3221A3B549F06E8074D76BCE2F31773FB69F
Malicious:	false
Reputation:	low
Preview:	..... .H..... ..... .p..... .h...n..... ....n...((.... .h.....00.... ..%..~H..@@.... .(B..&n..``.... .....N..... .(....D..... .w`...M..(..... .....+.O-8&]P>/^Q?-^&:?I.1;<....qye.f.%.....X...E.....I...k}....{.m.t.CP.....E...\.....=H..,A..,J..;P.....nn p}nnp}.....~~~.....!...!---2---2.. .....(..... .....!...7.#.:3,";3,!<.&'/.....NPLYt.F.K.%.....L..C.....1...`...KOPVutz}..A.BxX.....P.. .Q.....1...x...tqpyxuux...0D..DP.....G.....uojuppnw....t|..9F..-=..+:..5:..rr.....llkrkkmw.....ggitllkv.....hhgssss~.....YY\eYY[e..... ....nnnzXXXa.....RRR\.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\Chrome Web Store Payments.ico.md5	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16
Entropy (8bit):	4.0
Encrypted:	false
SSDEEP:	3:SeFcn:Sec
MD5:	61B979ECA159ECAC9C7F8F1D6FD43E9D
SHA1:	0373696351FC2172E811DA8393DEC84036FA34A0
SHA-256:	AB05E0A6FF7E8FFF89F924B279D93AFC72ACCE817C4D250C60BB8059CC534303
SHA-512:	C95825DA33CBDDFA627D9FF9A5B8371BC5F4E643A09573B6E1E839A83B619F53D878C344030B9701DCBC24D4CECCC016CF4D298D10EE8C37D1B5FEC1A5168 B6
Malicious:	false
Reputation:	low
Preview:	F.....r...(R..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a426348c-f4bc-41c6-b874-0b6409b929dd.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):	21284
Entropy (8bit):	5.553045050889991
Encrypted:	false
SSDEEP:	384:Dut3LlufXf1kXqKf/pUZNCgVLH2HfDIrUrHGHnZk0Wpj4y:ILlYf1kXqKf/pUZNCgVLH2HfUrU7GHnu
MD5:	6207DBCAF45C5C98DD293FC2AEA3BA9A
SHA1:	CADA8984C78431BFD2A64ACFC3117FE1A593F038
SHA-256:	BE8DAFCE7151EE13341B379FFBB60FE7BD128A2232EF02DB13D898740A959B61
SHA-512:	39460FFA1162B628AE9E8FD521C84FB2F28AA1B4D72A3C274450F9E8E1ED1EEE1AAFAF8F953B217C825A5AF89AC86FB22892F5574D072DD84430F8676245964E
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":"13256229780659829","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/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a8993d7a-06c0-4dd2-85b5-7fe30282e7fa.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a8993d7a-06c0-4dd2-85b5-7fe30282e7fa.tmp	
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b40cede3-bf3a-44b7-b8c0-23eecc68383d.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):	4800
Entropy (8bit):	4.952208727791652
Encrypted:	false
SSDEEP:	48:YcskKSChkSixqAT4qTlYGlQuoTw00Frf4MqM8c1Nfct/9BhUJo3KhmeSnpSkJJb+:nkL5mpIVqHk0JCKL8SkJ1VbOElVuHn
MD5:	A806E34DCB9DA0496B23FB466AF42338
SHA1:	17E4CF732230B8B03C1F142AB4337737B6FDC44C
SHA-256:	80C0C972F9457A8600D6819B3CC61258B43A804C1A9B28B70805C3958F8FBFB1
SHA-512:	26E77B590A74AFE22010E4E26CE409BC1C91B52EA2C1638F2BD5B9A98C5338FC925E139CED9444F70E28BFEB9471FF98D6553EF0849825D9DA12480DF5CA743
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13256229780894561","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"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","2042016"],"daily_rece

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c93ce266-9fd4-4a3e-84f6-5974e441cc77.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):	5411
Entropy (8bit):	5.178037790993984
Encrypted:	false
SSDEEP:	96:nkLLZX+rvIVqHk0JCKL88kYjmbOElVuHn:nkLlOrvIYP4KzkYv
MD5:	C3C5913183B28732328CF8606BE12C87
SHA1:	EE4CDFE4A0BA631A7F9156423D82C567680A461E
SHA-256:	96965E7EA9F40457F2E80DF006B0B6E1499E6673004A1F18C9FAA5DC1DDAF8DD
SHA-512:	95C394894530D2D1D08E1934A2DE16B446612614763EDFCE4062921936D71BED12690DC374A32F7682167B6DE1FE43B37BD899ECD4DC4A9E9EE828839B5FFF8
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13256229780894561","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"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","2042016"],"daily_rece

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ce1007bc-5a58-479b-b0c5-dd714bea1ce1.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):	3473
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhIGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIIyGzRDYLiEHYDBKSUpCQHrSP

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ce1007bc-5a58-479b-b0c5-dd714bea1ce1.tmp	
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607497410","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":27387},"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607318875","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":23359},"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248

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:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.4235638930393675
Encrypted:	false
SSDEEP:	3:tUKX9YXFUadTyZmwv3R9YARuEARl7V8sR9YARuEARl7WGv:mgZmwP4b7Vv4b7tv
MD5:	8DCB98D658CA6FCCB6DCA36BB0D109CA
SHA1:	E432B2B065028E9ED71D975D663DC963C58F5C51
SHA-256:	9CF4AF555A6BF985D2C385BCC4EBB8EFF57B5C5542D0428ABFE0E90A408BBE04
SHA-512:	76673BC37EA82E988218B9D4237105DA87FAFC3A90F8F0473D7CDD27AB82BB9D61AB22C662F98C8A3F1E08A242A0A54D878F0B33C2EA1B089B025A9FC52E5433
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:03:15.354 1ae4 Recovering log #3.2021/01/27-15:03:15.414 1ae4 Delete type=0 #3.2021/01/27-15:03:15.414 1ae4 Delete type=3 #2.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e6e8ce12-40a4-40ec-a85a-fba026de4eda.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):	2714
Entropy (8bit):	5.596519752521911
Encrypted:	false
SSDEEP:	48:YIUooN5U9GCaeUopieUo76UUh7U9iUoLmUoNKUeiaqUoDpU92BsmU9eqPeUekUeC:PUogU9daeUopieUoeUUpU9iUoCUoNKUF
MD5:	C19F9A01FA6CCCA2FAEB08B863A753E0
SHA1:	93F77E9F9A86F236E6004F96A9B7DC3F49BFA534
SHA-256:	9EAB0C455782EF8A293929236EEB5EC1C863A027CAD0CF4C57275E2727D4CE01
SHA-512:	DA803C9059DB4CE109BAC548FE888813087BDB585D7825E62983E7D28674357213E91CA96246BB2ADBBD876CE2AEDBE4F012E7369530B1518E2142402C96281
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1614348248.24103,"host":"Dg14fIaciUHGX6Lc+OnYmaNiAA/ADiwumtIyPrC3d6U=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1611756248.241034},{"expiry":1627308279.106947,"host":"HS0xQK8RrrSZ/KdSgKIC7bLU+xijlimr9JuWvTPbfkE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1611756279.106951},{"expiry":1622642586.021525,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1611756186.021529},{"expiry":1643292185.221761,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1611756185.221768},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1643292279.386712,"host":"Y1cbV6ziZu1KjdKdxBzKmgzsZCYqaDEHWONjJAo942Q=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e8cb0cf6-a6f7-499e-b5cd-7ee73e17288f.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):	5410
Entropy (8bit):	5.179268123834522
Encrypted:	false
SSDEEP:	96:nkLLZX+rvIVqHk0JCKL8SkJ1VbOElVuHn:nkLlOrvIYP4KNkJQ
MD5:	C463F3040A86F26C1101D4347FD676E6
SHA1:	C972D97B1D310BE624991E89BA92F65D7452C03F
SHA-256:	C8EC73D99BFAE2AA1BDD415E09680D257348C6435F6A6D8B607D2089E5EFD18F
SHA-512:	0A07468A3C227C13490DEDC7F1D357E4CD140EB3AED8F6EAD5601B32F61CCA87811FC489FA29C412A710D110048AE534802D9C57FA524287F6CE4BA4FCB3E72
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13256229780894561","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"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","2042016"],"daily_rece

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.167513820747632
Encrypted:	false
SSDEEP:	6:mXnlyq2Pwkn23iKKdKfrzAdIFUtpqXFY1ZmwPqXFORkwOwkn23iKKdKfrzILJ:aIvYf5Kk9FUtpqXO1/PqXg5Jf5Kk2J
MD5:	E686FB9065E8168D6CE4A2FEFD086BF5
SHA1:	3282532A06F3A2970445B8603C4CC3154F9ED9EC
SHA-256:	46F575CB9B8E95A00F06CF6E47FF79B8AF32480DEFC0CBD62A16C48693AF8FE7
SHA-512:	C4F783493858080ACE0BD4A7A1917A0663E1365BA9FBBD3C1ADAA64F17726C3A08E658501292A918F39AD7BBE6448DDE4F917154A21934AD5583AE6DDB50FB88
Malicious:	false
Reputation:	low
Preview:	2021/01/27-15:03:15.681 1ae0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/01/27-15:03:15.682 1ae0 Recovering log #3.2021/01/27-15:03:15.682 1ae0 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

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Safe Browsing Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	24576
Entropy (8bit):	0.5152012911247779
Encrypted:	false
SSDEEP:	24:TLiuWoKI6UwcQPx5fPqLLJLbXaFpEO5bNmISHn06Uwd:TZWoSU1uPqpLLOpEO5J/Kn7U
MD5:	CDDBE1AAD7512CC5AF36C321EE9B33F0
SHA1:	C4A648BA4C74057EC582F323848E65F4A3A65538
SHA-256:	B4C3106D5B0A0D2ADFAD5E1CDA37B872E76ABF883481F6F301D39847BD00E154
SHA-512:	192DD9A94199FF7A4739D04AEB504CA4CBA1273159B264574EC702C698D0B0469D2C5FEEC96FFDDEB6330D45571A2B39939108A8FB862740F75987FC5A49C90
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g..g..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Safe Browsing Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5152
Entropy (8bit):	0.5015737532619124
Encrypted:	false
SSDEEP:	6:r+/l/lGMFPg9bNFlEuWkOl5qKZwkvAngLusiOImWtz0vlWmW8QeZams/l+:r+t/lGyqLiuWkOl0KONFxOUwamst+
MD5:	60A1C72A26A03C0DD2CD6DAC001A0B65
SHA1:	618019E479B1A2310E134BA9F7A0CBF76A31E492
SHA-256:	E25A8F271E62673D0AD13C65DEDC7C36AD8DFF7FFB33B30C0E523930B767B85B
SHA-512:	127FBEA8E1017A5BEB7EEBF4E8314A692D08EEB339C2110F39A270E4257F745A4B17DB4B49560CD95C8DC02988C20BB2B42A2C42A203B7C677BE7405C08F4F1E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Safe Browsing Cookies-journal	
Preview:	..........t..... .... .c.....v.r. ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Safe Browsing\CertCsdDownloadWhitelist.store_new	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	75
Entropy (8bit):	5.655224690380502
Encrypted:	false
SSDEEP:	3:owj17daBkHmV+JenEXCCQ7CwZBLvwgn:owj17sSGcJTSCWpDwg
MD5:	DDD66452695D680592EAD653ABD596BB
SHA1:	366ECD5C29D696548515DA8C4341D7B26782D341
SHA-256:	B705449B5C67CB8EF616932F585746CFF790043DBED3631E5C5DF637F6AC875B
SHA-512:	FD5375F33ED0191C9DCC5D5239621FE04E4D228242027EF3DBD010AE8F089AFB72B1C9FCAB5E7F1C1D5E767B375D005C5201B8BA2FF22104B6F95E9E5A6B052 7
Malicious:	false
Reputation:	low
Preview:	.....A .:.....".0010.....r..B". ..B.....o.$'.A.d..L....xR.U

C:\Users\user\AppData\Local\Google\Chrome\User Data\Safe Browsing\ChromeExtMalware.store_new	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	977854
Entropy (8bit):	4.0015345999571625
Encrypted:	false
SSDEEP:	24576:6+XaSGIbczb6KGbDd+L6ThXZQsU0iqFOJHhyywAomKXtFWNHovzG0H/NeT1KUgJK:6+j/bczI3d+LAhpQD0iqghcVmStFWNHf
MD5:	288BD7A7A0016424491BFC75A82CE5BF
SHA1:	C18C76BFD446BF6803FB47710FEF25B98D3FCCD0
SHA-256:	A19C01ACECE288859B6022AD6A489EF3A977B85416EB4601B20235344B0D572E
SHA-512:	E5263C74786F750AFA9E32150A1730D65DE564F464BA8663D4FEE96990988BBE54820E8A6CC9B210E6FEAD6D3B26DEB3E97021384A55E9E0C8B01F16DB3B58A 6
Malicious:	false
Reputation:	low
Preview:	.....; .*..;....;. ...;aaaadbolalgmogecpogmlebfkpigmpdjaaaaiognmpgbjoffachmpnnppfnokcbeaaaakngccdmgikgidoadpaopippmdfihaaaggnhhcicpemabkcpekihlocinhaalaaai inppadbheljngocoegdcncpaejiiaaalhkjlldhojjcmmiaoopcglbdlfjcpaaamfohdgeiomgdngemljnheihdmgkecaaamnkbkbppehfhhkmiodoniifhfpkkaaaanfaliloicindpienfhcnpnd cibpcgaaankgpdiealiomopmnjblmeimiejfdaaabajgbpmnnmnmhdfmjmnbkbjpibhmefdaabchfpoaokbenfoikepjpdidacbiekfaabchjflcbccncldaekpjpcienceijonaabefojcgchjbojm keidhaceaaojjjodaabgniekficofjmfoejkgpncpaimldcmaabllpaogiigffnofgfhaecokpnhflghaaboihdfgkjdneohdofabaponaaibbdeaacdffaeghaialcklmicpdlpnikjholcaacfcn ecbpnccnonpbdgpbljaghhclaaaacgihcbcjhegjcfgkobdigjngohmjmfaacgmmndomhckgeglaphhdeegmonpbfjaacjmcdmclhpdpjagjcmclecpgjodlmgaackamlchlgmalkmcp hbhhcjebbpnfdfaacoogimceghmcjhdknjbikmcmgkkbjaaacpkpemoapjccepeaiijomchejhlinpaadcaglikmoilfnonemffapkjhdloomeaadjhlpjcoakeaehahddpgehekineoegaadjjecd jlokenchpmeonkndpbnfhbnbaadkehkkkcijmdmihoaecockheacjhkhaaebnekdkiappbkmbjglidgcokafcgjaaaefcbjhnd

C:\Users\user\AppData\Local\Google\Chrome\User Data\Safe Browsing\ChromeUrlClientIncident.store_new	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	725
Entropy (8bit):	7.718505783723005
Encrypted:	false
SSDEEP:	12:3jMpctaC1+pzj4aA3x5DhA54pGZNaZH2mxy/8IzoHSvTnSjZKlcYqD35:4gEP4aqrDhA54pGKZWR8TSvb84cl
MD5:	BADC5A64420378F5A99A6E9FAA720497
SHA1:	706BDE71B7DCE3207C5506989B004E1D3877B320
SHA-256:	B135AB47E1D01744ECED28629F0631479551BD1DB31D59FB16D3851361C627DD
SHA-512:	FD20CAA029E62326A13B79A441A445ABD254DD5F43466FC5DE4DE066D2B4A218EDB3FB4FCE47B6902B50932D8EFBA0ED42E6BE5DD84C14CAA5E10BC355CE(616
Malicious:	false
Reputation:	low
Preview:	..... .*.....3))...o._.....m.../J.....;.Pv....<.xW...i>!4.<!.(".M.#*.C#ZCW$..k&.n.*`..+.....r70..+0>.12...7.0.8i..:e=q:m.c=|..>f..?...C...F.O.H...H.4.ILWaI.)!KB3.O3..P.{.Sc..S. ..W.+W..WYTV.ZC.IZ...[...[.sY\.fN\.++_3{._.)a_...`9..`{..a80.b...c.m>d39Adh..g.t,h.-\iI..k..o_..pe>Ns...u.2.v.=.yoU.z.b.z...z..$}.4.}B4_...w.....,...1'..iV.....AO.z.6..{..[....9...;..e..... .b.K.v[I.../..eM...m.....I.&...=.;....@S.....w..D.v...X..|.....9....=...Yk.....n.A...a..<..;.c..r;.9..."....o..q.....-...0,..&.Y.....W..3...Ft.sP...N.0Nh..b}..(.K$...Dr..9X.....>.Q.....8... .}u.h.W.y[P..~[.1.5...Y.....PO.....N.:....."..0010.....r.B". -...R.>.}..)..L.I._.Vr....*...k

C:\Users\user\AppData\Local\Google\Chrome\User Data\Safe Browsing\IpMalware.store_new	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	5.897362907230098
Encrypted:	false
SSDEEP:	3:owj1aWxAhZ9yjIlf8voy9+M79YXNDf9oNFG:owj15x6Z9ycf+Tk06VoNFG
MD5:	FFE3372DD80A0ABDE9DD0FE6EFCC8097
SHA1:	7CD49876E6088DEC8567106AD5767D1DC0CD8091
SHA-256:	01A9C564A29FE1778F5657E0F5D50BFF3A406881777BA57CBE42EB00563C6317
SHA-512:	34BD35F34A70898F9C3BD70142D30A89678A22DF756E77AB13E81246709B6337EF588D795F90B47C0CC53F2DD7D050C508DB8418330B145C005AACFDAC645B1
Malicious:	false
Reputation:	low
Preview:	.....` .*.....<.4N..E..:.....".0010.....Y.t}B". .p.....\H...J#..).o.....(`....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Safe Browsing\UrlBilling.store_new	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	32830
Entropy (8bit):	**7.994644445164613**
Encrypted:	**true**
SSDEEP:	768:7wel3kLAiiIZW41V+k5dMTE2BaFmBrfl8CzYa1BC:cgJ3oV+koI2Z5N8Cdq
MD5:	41B0C7B1D904F5DB0B6182E76FE3E2BD
SHA1:	877A72A8C3403C8601976020BBD59266244E9D53
SHA-256:	78FDCE59FA3063036DD0AE23E3337B326A6C40D7D08CA338F46929977196D0DC
SHA-512:	9C96425640B26E393DD944688E11A7F145F67A826B98F14B0A989E0F1A9EE4AE85ADB792DF0848065E0B32A8CF85872601411BA82B5CD5978107E740CF5D3BD2
Malicious:	false
Reputation:	low
Preview:	..... .*.....v...J.)..%...(....`X.Bur.D$b.J:..O..S...V..._%Z.eP..h.,.sY..zP1...3...8.....}.....%....c.....]&..~....._.....<.....PA.#%e.,.I.1...8...H.0.M...Y1..\.m.`...e...g...mS..y....c>.....3...../.....gp..6.....t.....@.....c[..r...1L...U...E. ...$...%/^.&^..)x..:|..=...AA..E=..J...O...O.R.Q...X.r.a...e...m...t...t.E.....(...i6.....t.....q.....s....9.....ow.....#...%.*.1...3i..7...9.r.>w].Aj..O.;.X...rw.....~..rE.,...I..q...8.....@@..6...I...:.....A.....%L.....03R.>...V...`y..d.\.h.S.i...{.;...o.....[.....F.....9.....]....6..~...n..N...M.....W..[V..~.....o....{...D. ...#...2.>.3_w.7L1.;G..D.4.K.Z.N.T.P+..T..\...f.V.j...v._...k2.....{...q.....n....x.....xE...j.....AN.....;.....{....d..... .!6..+...0..1...B...F5..LI..N. .Zeq.]...e.h.gW..m.[...3...r..$0...!.....[k..*Y...z...n.....r?....._...x..4...3.....b.(D..L...T..b.5.bJM.q

Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 164

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:03:04.390201092 CET	49741	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:04.392211914 CET	49742	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:04.560935020 CET	49744	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:04.588988066 CET	443	49741	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:04.589092016 CET	49741	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:04.589366913 CET	49741	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:04.591460943 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:04.591568947 CET	49742	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:04.591792107 CET	49742	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:04.758800030 CET	443	49744	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:04.758955002 CET	49744	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:04.759381056 CET	49744	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:04.788018942 CET	443	49741	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:04.788952112 CET	443	49741	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:04.788970947 CET	443	49741	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:04.788983107 CET	443	49741	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:04.788994074 CET	443	49741	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:04.789067984 CET	49741	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:04.791003942 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:04.791870117 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:04.791896105 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:04.791908026 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:04.791924953 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:04.791980982 CET	49742	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:04.792006016 CET	49742	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:04.858118057 CET	49742	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:04.859414101 CET	49741	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:04.859561920 CET	49741	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:04.859702110 CET	49742	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:04.860223055 CET	49742	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:04.959876060 CET	443	49744	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:04.960582972 CET	443	49744	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:04.960613966 CET	443	49744	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:04.960638046 CET	443	49744	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:04.960659981 CET	443	49744	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:04.960690975 CET	49744	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:04.960727930 CET	49744	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:04.962481976 CET	49744	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:05.057909966 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.057940006 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.058130980 CET	49742	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:05.058279991 CET	443	49741	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.058295965 CET	443	49741	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.058346033 CET	49742	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:05.058383942 CET	49741	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:05.058429003 CET	49741	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:05.059297085 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.099613905 CET	49742	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:05.102989912 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.157290936 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.157314062 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.157427073 CET	49742	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:05.157589912 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.157608032 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.157674074 CET	49742	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:05.157700062 CET	49742	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:05.160120010 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.160569906 CET	443	49744	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.160582066 CET	443	49744	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.160656929 CET	49744	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:05.199628115 CET	49742	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:05.257731915 CET	443	49742	44.238.32.151	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:03:05.295691013 CET	49747	443	192.168.2.4	99.86.154.85
Jan 27, 2021 15:03:05.295979977 CET	49748	443	192.168.2.4	99.86.154.85
Jan 27, 2021 15:03:05.296230078 CET	49749	443	192.168.2.4	99.86.154.85
Jan 27, 2021 15:03:05.339396954 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.339431047 CET	443	49747	99.86.154.85	192.168.2.4
Jan 27, 2021 15:03:05.339549065 CET	49747	443	192.168.2.4	99.86.154.85
Jan 27, 2021 15:03:05.340004921 CET	49747	443	192.168.2.4	99.86.154.85
Jan 27, 2021 15:03:05.340873957 CET	443	49748	99.86.154.85	192.168.2.4
Jan 27, 2021 15:03:05.340894938 CET	443	49749	99.86.154.85	192.168.2.4
Jan 27, 2021 15:03:05.340964079 CET	49748	443	192.168.2.4	99.86.154.85
Jan 27, 2021 15:03:05.341005087 CET	49749	443	192.168.2.4	99.86.154.85
Jan 27, 2021 15:03:05.341223955 CET	49748	443	192.168.2.4	99.86.154.85
Jan 27, 2021 15:03:05.341315031 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.341350079 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.341377020 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.341388941 CET	49742	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:05.341454983 CET	49742	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:05.341511965 CET	49749	443	192.168.2.4	99.86.154.85
Jan 27, 2021 15:03:05.343945026 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.345968962 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.346050024 CET	49742	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:05.348535061 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.348575115 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.348629951 CET	49742	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:05.356678963 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.363476038 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.363518953 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.363549948 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.363571882 CET	49742	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:05.363617897 CET	49742	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:05.366106987 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.368551970 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.368637085 CET	49742	443	192.168.2.4	44.238.32.151
Jan 27, 2021 15:03:05.368740082 CET	443	49742	44.238.32.151	192.168.2.4
Jan 27, 2021 15:03:05.385097027 CET	443	49747	99.86.154.85	192.168.2.4
Jan 27, 2021 15:03:05.387994051 CET	443	49748	99.86.154.85	192.168.2.4
Jan 27, 2021 15:03:05.388073921 CET	443	49747	99.86.154.85	192.168.2.4
Jan 27, 2021 15:03:05.388112068 CET	443	49747	99.86.154.85	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:02:51.759309053 CET	49910	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:02:51.807482004 CET	53	49910	8.8.8.8	192.168.2.4
Jan 27, 2021 15:02:52.558501005 CET	55854	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:02:52.608607054 CET	53	55854	8.8.8.8	192.168.2.4
Jan 27, 2021 15:02:53.352268934 CET	64549	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:02:53.401554108 CET	53	64549	8.8.8.8	192.168.2.4
Jan 27, 2021 15:02:55.382153988 CET	63153	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:02:55.441312075 CET	53	63153	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:00.393712044 CET	52991	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:00.441607952 CET	53	52991	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:01.457494020 CET	53700	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:01.571070910 CET	53	53700	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:04.004549980 CET	56534	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:04.060867071 CET	53	56534	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:04.314944029 CET	56627	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:04.317116022 CET	56621	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:04.317470074 CET	63116	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:04.382841110 CET	53	56627	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:04.384790897 CET	53	63116	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:04.386076927 CET	53	56621	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:04.878576994 CET	64078	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:04.948534966 CET	53	64078	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:03:05.077353954 CET	64801	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:05.142286062 CET	53	64801	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:05.232079983 CET	61721	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:05.292988062 CET	53	61721	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:05.330586910 CET	61522	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:05.382030010 CET	53	61522	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:05.660799026 CET	52337	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:05.663925886 CET	55046	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:05.709013939 CET	53	52337	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:05.720199108 CET	53	55046	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:06.308454990 CET	49612	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:06.377595901 CET	53	49612	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:06.407831907 CET	49285	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:06.464085102 CET	53	49285	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:07.210529089 CET	50601	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:07.272370100 CET	53	50601	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:07.713485956 CET	60875	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:07.715549946 CET	56448	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:07.765651941 CET	53	60875	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:07.784496069 CET	53	56448	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:08.017549038 CET	59172	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:08.023480892 CET	62420	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:08.027479887 CET	60579	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:08.079540014 CET	53	59172	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:08.083401918 CET	53	62420	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:08.087954044 CET	53	60579	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:08.237914085 CET	50183	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:08.255374908 CET	61531	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:08.273950100 CET	49228	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:08.287091970 CET	53	50183	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:08.317133904 CET	53	61531	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:08.339361906 CET	53	49228	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:08.620125055 CET	60542	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:08.620654106 CET	60689	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:08.621226072 CET	64206	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:08.681869030 CET	53	60689	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:08.682693958 CET	53	64206	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:08.686980963 CET	53	60542	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:08.699606895 CET	50904	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:08.699959993 CET	57525	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:08.750848055 CET	53	57525	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:08.760138988 CET	53	50904	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:08.789218903 CET	53814	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:08.836925983 CET	53	53814	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:08.946974039 CET	53418	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:09.006879091 CET	53	53418	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:09.374979973 CET	62833	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:09.434494019 CET	53	62833	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:09.437829018 CET	59260	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:09.441962004 CET	49944	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:09.444886923 CET	63300	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:09.488627911 CET	53	59260	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:09.499766111 CET	53	49944	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:09.502976894 CET	53	63300	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:09.503663063 CET	61449	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:09.507529974 CET	51275	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:09.515090942 CET	63492	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:09.551395893 CET	53	61449	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:09.554145098 CET	58945	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:09.555378914 CET	53	51275	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:09.558029890 CET	60779	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:09.566368103 CET	53	63492	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:09.568805933 CET	64014	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:09.607739925 CET	53	60779	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:03:09.615612030 CET	53	58945	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:09.621542931 CET	53	64014	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:09.918526888 CET	57091	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:09.919281006 CET	55904	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:09.919872999 CET	52109	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:09.966464996 CET	53	57091	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:09.967405081 CET	53	52109	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:09.980231047 CET	53	55904	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:10.091106892 CET	54450	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:10.151464939 CET	49374	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:10.155116081 CET	53	54450	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:10.213429928 CET	53	49374	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:10.348792076 CET	50436	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:10.410037994 CET	53	50436	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:10.411251068 CET	50437	443	192.168.2.4	172.217.20.226
Jan 27, 2021 15:03:10.423413992 CET	62605	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:10.467628002 CET	443	50437	172.217.20.226	192.168.2.4
Jan 27, 2021 15:03:10.467693090 CET	443	50437	172.217.20.226	192.168.2.4
Jan 27, 2021 15:03:10.471343994 CET	53	62605	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:10.662791967 CET	50437	443	192.168.2.4	172.217.20.226
Jan 27, 2021 15:03:10.663661957 CET	50437	443	192.168.2.4	172.217.20.226
Jan 27, 2021 15:03:10.667505026 CET	443	50437	172.217.20.226	192.168.2.4
Jan 27, 2021 15:03:10.667538881 CET	443	50437	172.217.20.226	192.168.2.4
Jan 27, 2021 15:03:10.670243025 CET	50437	443	192.168.2.4	172.217.20.226
Jan 27, 2021 15:03:10.733419895 CET	443	50437	172.217.20.226	192.168.2.4
Jan 27, 2021 15:03:10.734174013 CET	443	50437	172.217.20.226	192.168.2.4
Jan 27, 2021 15:03:10.735255957 CET	50437	443	192.168.2.4	172.217.20.226
Jan 27, 2021 15:03:10.753978968 CET	443	50437	172.217.20.226	192.168.2.4
Jan 27, 2021 15:03:10.753998995 CET	443	50437	172.217.20.226	192.168.2.4
Jan 27, 2021 15:03:10.783139944 CET	50437	443	192.168.2.4	172.217.20.226
Jan 27, 2021 15:03:13.180402040 CET	56131	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:13.206209898 CET	50437	443	192.168.2.4	172.217.20.226
Jan 27, 2021 15:03:13.249242067 CET	53	56131	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:13.276129007 CET	443	50437	172.217.20.226	192.168.2.4
Jan 27, 2021 15:03:15.654130936 CET	54432	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:15.707011938 CET	53	54432	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:16.181094885 CET	57227	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:16.248859882 CET	53	57227	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:17.540823936 CET	58383	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:17.605176926 CET	53	58383	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:18.157474041 CET	63136	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:18.208373070 CET	53	63136	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:21.482125044 CET	50911	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:21.534570932 CET	53	50911	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:24.044301033 CET	63409	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:24.094760895 CET	59185	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:24.103508949 CET	53	63409	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:24.144681931 CET	53	59185	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:24.833144903 CET	64236	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:24.894644022 CET	53	64236	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:35.067605972 CET	56157	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:35.128263950 CET	53	56157	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:36.021617889 CET	55601	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:36.084503889 CET	53	55601	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:36.329488993 CET	52984	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:36.394345045 CET	53	52984	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:36.859855890 CET	51141	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:36.861304998 CET	53610	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:36.896714926 CET	61247	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:36.903567076 CET	65165	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:36.912028074 CET	53	53610	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:36.924258947 CET	53	51141	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:36.944664001 CET	53	61247	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:36.962522984 CET	53	65165	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:03:36.973546982 CET	52076	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:36.985450029 CET	54903	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:36.998724937 CET	55045	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:37.023475885 CET	53	52076	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:37.046499968 CET	53	54903	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:37.050127983 CET	53	55045	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:37.448251009 CET	54464	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:37.501313925 CET	53	54464	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:37.906884909 CET	50970	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:37.973927021 CET	53	50970	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:41.582851887 CET	55261	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:41.642606020 CET	53	55261	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:52.170304060 CET	59809	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:52.229203939 CET	53	59809	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:52.642278910 CET	51278	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:52.702111959 CET	53	51278	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:52.901321888 CET	51932	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:52.962558031 CET	53	51932	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:53.538372993 CET	59494	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:53.596666098 CET	53	59494	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:53.616142988 CET	55915	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:53.680829048 CET	53	55915	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:54.080451012 CET	49779	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:54.141844988 CET	53	49779	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:54.949311018 CET	49458	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:55.005522966 CET	53	49458	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:55.565639973 CET	57164	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:55.626991987 CET	53	57164	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:56.343528986 CET	49840	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:56.402710915 CET	53	49840	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:57.147094965 CET	57174	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:57.205435991 CET	53	57174	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:58.094310999 CET	58531	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:58.153172970 CET	53	58531	8.8.8.8	192.168.2.4
Jan 27, 2021 15:03:58.614368916 CET	49608	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:03:58.662389040 CET	53	49608	8.8.8.8	192.168.2.4
Jan 27, 2021 15:04:00.429253101 CET	55682	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:04:00.494437933 CET	53	55682	8.8.8.8	192.168.2.4
Jan 27, 2021 15:04:01.626298904 CET	62436	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:04:01.688885927 CET	53	62436	8.8.8.8	192.168.2.4
Jan 27, 2021 15:04:03.324793100 CET	64730	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:04:03.391758919 CET	53	64730	8.8.8.8	192.168.2.4
Jan 27, 2021 15:04:05.023678064 CET	60624	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:04:05.071849108 CET	53	60624	8.8.8.8	192.168.2.4
Jan 27, 2021 15:04:05.132636070 CET	62600	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:04:05.180856943 CET	53	62600	8.8.8.8	192.168.2.4
Jan 27, 2021 15:04:05.325201035 CET	53200	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:04:05.390167952 CET	53	53200	8.8.8.8	192.168.2.4
Jan 27, 2021 15:04:05.517909050 CET	61034	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:04:05.576405048 CET	53	61034	8.8.8.8	192.168.2.4
Jan 27, 2021 15:04:05.771049976 CET	57687	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:04:05.819300890 CET	53	57687	8.8.8.8	192.168.2.4
Jan 27, 2021 15:04:06.014624119 CET	60624	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:04:06.062644958 CET	53	60624	8.8.8.8	192.168.2.4
Jan 27, 2021 15:04:06.777550936 CET	57687	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:04:06.826247931 CET	53	57687	8.8.8.8	192.168.2.4
Jan 27, 2021 15:04:07.028669119 CET	60624	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:04:07.085213900 CET	53	60624	8.8.8.8	192.168.2.4
Jan 27, 2021 15:04:07.780416965 CET	57687	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:04:07.828530073 CET	53	57687	8.8.8.8	192.168.2.4
Jan 27, 2021 15:04:09.040493965 CET	60624	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:04:09.099241018 CET	53	60624	8.8.8.8	192.168.2.4
Jan 27, 2021 15:04:09.790620089 CET	57687	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:04:09.849271059 CET	53	57687	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:04:13.056488037 CET	60624	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:04:13.118274927 CET	53	60624	8.8.8.8	192.168.2.4
Jan 27, 2021 15:04:13.806617022 CET	57687	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:04:13.863511086 CET	53	57687	8.8.8.8	192.168.2.4
Jan 27, 2021 15:04:23.470562935 CET	57975	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:04:23.529488087 CET	53	57975	8.8.8.8	192.168.2.4
Jan 27, 2021 15:04:32.717922926 CET	55137	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:04:32.787343979 CET	53	55137	8.8.8.8	192.168.2.4
Jan 27, 2021 15:04:32.937354088 CET	59216	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:04:33.006581068 CET	53	59216	8.8.8.8	192.168.2.4
Jan 27, 2021 15:04:36.979837894 CET	63495	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:04:37.047208071 CET	53	63495	8.8.8.8	192.168.2.4
Jan 27, 2021 15:04:37.208517075 CET	64371	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:04:37.268817902 CET	53	64371	8.8.8.8	192.168.2.4
Jan 27, 2021 15:04:39.187407017 CET	54037	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:04:39.240674973 CET	53	54037	8.8.8.8	192.168.2.4
Jan 27, 2021 15:04:40.928057909 CET	53481	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:04:40.943185091 CET	58313	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:04:40.997206926 CET	53	53481	8.8.8.8	192.168.2.4
Jan 27, 2021 15:04:41.015516996 CET	53	58313	8.8.8.8	192.168.2.4
Jan 27, 2021 15:04:41.123346090 CET	58950	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:04:41.182816982 CET	53	58950	8.8.8.8	192.168.2.4
Jan 27, 2021 15:04:41.248152971 CET	55011	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:04:41.313021898 CET	53	55011	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 15:03:04.314944029 CET	192.168.2.4	8.8.8.8	0xb00d	Standard query (0)	quip.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:05.232079983 CET	192.168.2.4	8.8.8.8	0xe78	Standard query (0)	quip-cdn.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:06.407831907 CET	192.168.2.4	8.8.8.8	0xf80a	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:07.210529089 CET	192.168.2.4	8.8.8.8	0x777a	Standard query (0)	listenweb3.quip.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:07.715549946 CET	192.168.2.4	8.8.8.8	0x43d5	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.017549038 CET	192.168.2.4	8.8.8.8	0x393f	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.023480892 CET	192.168.2.4	8.8.8.8	0xe106	Standard query (0)	s.adroll.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.027479887 CET	192.168.2.4	8.8.8.8	0x78b1	Standard query (0)	scripts.demandbase.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.237914085 CET	192.168.2.4	8.8.8.8	0x7c5c	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.255374908 CET	192.168.2.4	8.8.8.8	0xee21	Standard query (0)	d.adroll.mgr.consensu.org	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.620125055 CET	192.168.2.4	8.8.8.8	0x9c76	Standard query (0)	api.company-target.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.620654106 CET	192.168.2.4	8.8.8.8	0x44f2	Standard query (0)	match.prod.bidr.io	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.621226072 CET	192.168.2.4	8.8.8.8	0x8f8d	Standard query (0)	id.rlcdn.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.699606895 CET	192.168.2.4	8.8.8.8	0x7da	Standard query (0)	d.adroll.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.699959993 CET	192.168.2.4	8.8.8.8	0xd031	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.374979973 CET	192.168.2.4	8.8.8.8	0x3c30	Standard query (0)	segments.company-target.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.437829018 CET	192.168.2.4	8.8.8.8	0x3c1e	Standard query (0)	pixel.advertising.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.441962004 CET	192.168.2.4	8.8.8.8	0xe823	Standard query (0)	dsum-sec.casalemedia.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.444886923 CET	192.168.2.4	8.8.8.8	0x8d6c	Standard query (0)	pixel.rubiconproject.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.503663063 CET	192.168.2.4	8.8.8.8	0x4d82	Standard query (0)	sync.outbrain.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 15:03:09.507529974 CET	192.168.2.4	8.8.8.8	0x7763	Standard query (0)	simage2.pubmatic.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.515090942 CET	192.168.2.4	8.8.8.8	0xf8a4	Standard query (0)	ads.yahoo.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.554145098 CET	192.168.2.4	8.8.8.8	0xacb0	Standard query (0)	sync.taboola.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.558029890 CET	192.168.2.4	8.8.8.8	0x806a	Standard query (0)	eb2.3lift.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.568805933 CET	192.168.2.4	8.8.8.8	0xac91	Standard query (0)	x.bidswitch.net	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.918526888 CET	192.168.2.4	8.8.8.8	0x5f16	Standard query (0)	ib.adnxs.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.919281006 CET	192.168.2.4	8.8.8.8	0x1477	Standard query (0)	idsync.rlcdn.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.919872999 CET	192.168.2.4	8.8.8.8	0x6f00	Standard query (0)	us-u.openx.net	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:10.091106892 CET	192.168.2.4	8.8.8.8	0x35ee	Standard query (0)	cm.g.doubleclick.net	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:10.151464939 CET	192.168.2.4	8.8.8.8	0x53e0	Standard query (0)	ups.analytics.yahoo.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:10.348792076 CET	192.168.2.4	8.8.8.8	0x1b34	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:16.181094885 CET	192.168.2.4	8.8.8.8	0x4edd	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:36.861304998 CET	192.168.2.4	8.8.8.8	0xe27d	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:36.896714926 CET	192.168.2.4	8.8.8.8	0x76c2	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:36.973546982 CET	192.168.2.4	8.8.8.8	0xba70	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:36.985450029 CET	192.168.2.4	8.8.8.8	0x8972	Standard query (0)	s3.amazonaws.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:36.998724937 CET	192.168.2.4	8.8.8.8	0xe346	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:37.448251009 CET	192.168.2.4	8.8.8.8	0xd91	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:37.906884909 CET	192.168.2.4	8.8.8.8	0x27f3	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:52.642278910 CET	192.168.2.4	8.8.8.8	0xc7ba	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 15:03:04.382841110 CET	8.8.8.8	192.168.2.4	0xb00d	No error (0)	quip.com		44.238.32.151	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:04.382841110 CET	8.8.8.8	192.168.2.4	0xb00d	No error (0)	quip.com		52.39.66.75	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:04.382841110 CET	8.8.8.8	192.168.2.4	0xb00d	No error (0)	quip.com		54.191.147.46	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:05.292988062 CET	8.8.8.8	192.168.2.4	0xe78	No error (0)	quip-cdn.com		99.86.154.85	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:05.292988062 CET	8.8.8.8	192.168.2.4	0xe78	No error (0)	quip-cdn.com		99.86.154.9	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:05.292988062 CET	8.8.8.8	192.168.2.4	0xe78	No error (0)	quip-cdn.com		99.86.154.21	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:05.292988062 CET	8.8.8.8	192.168.2.4	0xe78	No error (0)	quip-cdn.com		99.86.154.50	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:06.464085102 CET	8.8.8.8	192.168.2.4	0xf80a	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:06.464085102 CET	8.8.8.8	192.168.2.4	0xf80a	No error (0)	stats.l.doubleclick.net		108.177.15.157	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:06.464085102 CET	8.8.8.8	192.168.2.4	0xf80a	No error (0)	stats.l.doubleclick.net		108.177.15.154	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 15:03:06.464085102 CET	8.8.8.8	192.168.2.4	0xf80a	No error (0)	stats.l.doubleclick.net		108.177.15.155	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:06.464085102 CET	8.8.8.8	192.168.2.4	0xf80a	No error (0)	stats.l.doubleclick.net		108.177.15.156	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:07.272370100 CET	8.8.8.8	192.168.2.4	0x777a	No error (0)	listenweb3.quip.com		52.39.66.75	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:07.272370100 CET	8.8.8.8	192.168.2.4	0x777a	No error (0)	listenweb3.quip.com		54.191.147.46	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:07.272370100 CET	8.8.8.8	192.168.2.4	0x777a	No error (0)	listenweb3.quip.com		44.238.32.151	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:07.784496069 CET	8.8.8.8	192.168.2.4	0x43d5	No error (0)	www.google.co.uk		172.217.22.227	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.079540014 CET	8.8.8.8	192.168.2.4	0x393f	No error (0)	snap.licdn.com	wildcard.licdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:08.083401918 CET	8.8.8.8	192.168.2.4	0xe106	No error (0)	s.adroll.com	wildcard.adroll.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:08.087954044 CET	8.8.8.8	192.168.2.4	0x78b1	No error (0)	scripts.demandbase.com		143.204.11.42	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.087954044 CET	8.8.8.8	192.168.2.4	0x78b1	No error (0)	scripts.demandbase.com		143.204.11.23	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.087954044 CET	8.8.8.8	192.168.2.4	0x78b1	No error (0)	scripts.demandbase.com		143.204.11.7	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.087954044 CET	8.8.8.8	192.168.2.4	0x78b1	No error (0)	scripts.demandbase.com		143.204.11.81	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.287091970 CET	8.8.8.8	192.168.2.4	0x7c5c	No error (0)	px.ads.linkedin.com	mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:08.287091970 CET	8.8.8.8	192.168.2.4	0x7c5c	No error (0)	mix.linkedin.com	pop-tln1-alpha.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:08.287091970 CET	8.8.8.8	192.168.2.4	0x7c5c	No error (0)	pop-tln1-alpha.mix.linkedin.com		185.63.144.5	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.317133904 CET	8.8.8.8	192.168.2.4	0xee21	No error (0)	d.adroll.mgr.consensu.org	d.adroll.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:08.317133904 CET	8.8.8.8	192.168.2.4	0xee21	No error (0)	d.adroll.com	adserver-vpc-alb-0-1578609942.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:08.317133904 CET	8.8.8.8	192.168.2.4	0xee21	No error (0)	adserver-vpc-alb-0-1578609942.eu-west-1.elb.amazonaws.com		54.170.19.229	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.317133904 CET	8.8.8.8	192.168.2.4	0xee21	No error (0)	adserver-vpc-alb-0-1578609942.eu-west-1.elb.amazonaws.com		63.35.200.21	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.681869030 CET	8.8.8.8	192.168.2.4	0x44f2	No error (0)	match.prod.bidr.io		52.49.193.31	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.681869030 CET	8.8.8.8	192.168.2.4	0x44f2	No error (0)	match.prod.bidr.io		54.72.203.0	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.681869030 CET	8.8.8.8	192.168.2.4	0x44f2	No error (0)	match.prod.bidr.io		52.31.242.159	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.681869030 CET	8.8.8.8	192.168.2.4	0x44f2	No error (0)	match.prod.bidr.io		52.214.70.9	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.681869030 CET	8.8.8.8	192.168.2.4	0x44f2	No error (0)	match.prod.bidr.io		54.228.192.197	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 15:03:08.681869030 CET	8.8.8.8	192.168.2.4	0x44f2	No error (0)	match.prod.bidr.io		52.215.8.160	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.682693958 CET	8.8.8.8	192.168.2.4	0x8f8d	No error (0)	id.rlcdn.com		34.120.207.148	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.686980963 CET	8.8.8.8	192.168.2.4	0x9c76	No error (0)	api.company-target.com		99.86.154.35	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.686980963 CET	8.8.8.8	192.168.2.4	0x9c76	No error (0)	api.company-target.com		99.86.154.83	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.686980963 CET	8.8.8.8	192.168.2.4	0x9c76	No error (0)	api.company-target.com		99.86.154.15	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.686980963 CET	8.8.8.8	192.168.2.4	0x9c76	No error (0)	api.company-target.com		99.86.154.58	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.750848055 CET	8.8.8.8	192.168.2.4	0xd031	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:08.760138988 CET	8.8.8.8	192.168.2.4	0x7da	No error (0)	d.adroll.com	adserver-vpc-alb-2-1264451658.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:08.760138988 CET	8.8.8.8	192.168.2.4	0x7da	No error (0)	adserver-vpc-alb-2-1264451658.eu-west-1.elb.amazonaws.com		54.74.23.153	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:08.760138988 CET	8.8.8.8	192.168.2.4	0x7da	No error (0)	adserver-vpc-alb-2-1264451658.eu-west-1.elb.amazonaws.com		63.35.114.199	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.434494019 CET	8.8.8.8	192.168.2.4	0x3c30	No error (0)	segments.company-target.com		99.86.154.45	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.434494019 CET	8.8.8.8	192.168.2.4	0x3c30	No error (0)	segments.company-target.com		99.86.154.17	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.434494019 CET	8.8.8.8	192.168.2.4	0x3c30	No error (0)	segments.company-target.com		99.86.154.99	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.434494019 CET	8.8.8.8	192.168.2.4	0x3c30	No error (0)	segments.company-target.com		99.86.154.70	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.488627911 CET	8.8.8.8	192.168.2.4	0x3c1e	No error (0)	pixel.advertising.com	prod.ups-adcom.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:09.488627911 CET	8.8.8.8	192.168.2.4	0x3c1e	No error (0)	prod.ups-adcom.aolp-ds-prd.aws.oath.cloud	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:09.488627911 CET	8.8.8.8	192.168.2.4	0x3c1e	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		3.124.119.192	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.488627911 CET	8.8.8.8	192.168.2.4	0x3c1e	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		35.156.106.231	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.488627911 CET	8.8.8.8	192.168.2.4	0x3c1e	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		52.28.239.147	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.488627911 CET	8.8.8.8	192.168.2.4	0x3c1e	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		52.28.254.214	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.488627911 CET	8.8.8.8	192.168.2.4	0x3c1e	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		3.126.63.176	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.488627911 CET	8.8.8.8	192.168.2.4	0x3c1e	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.197.47.23	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 15:03:09.488627911 CET	8.8.8.8	192.168.2.4	0x3c1e	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		35.156.153.71	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.488627911 CET	8.8.8.8	192.168.2.4	0x3c1e	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		52.57.10.248	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.499766111 CET	8.8.8.8	192.168.2.4	0xe823	No error (0)	dsum-sec.casalemedia.com	dsum-sec.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:09.502976894 CET	8.8.8.8	192.168.2.4	0x8d6c	No error (0)	pixel.rubiconproject.com	pixel.rubiconproject.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:09.551395893 CET	8.8.8.8	192.168.2.4	0x4d82	No error (0)	sync.outbrain.com	alldcs.outbrain.org		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:09.551395893 CET	8.8.8.8	192.168.2.4	0x4d82	No error (0)	alldcs.outbrain.org	nydc1.outbrain.org		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:09.551395893 CET	8.8.8.8	192.168.2.4	0x4d82	No error (0)	nydc1.outbrain.org		64.202.112.159	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.555378914 CET	8.8.8.8	192.168.2.4	0x7763	No error (0)	simage2.pubmatic.com	pug22000nfc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:09.555378914 CET	8.8.8.8	192.168.2.4	0x7763	No error (0)	pug22000nfc.pubmatic.com	pug22000nf.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:09.555378914 CET	8.8.8.8	192.168.2.4	0x7763	No error (0)	pug22000nf.pubmatic.com		185.64.189.110	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.566368103 CET	8.8.8.8	192.168.2.4	0xf8a4	No error (0)	ads.yahoo.com	edge.gycpi.b.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:09.566368103 CET	8.8.8.8	192.168.2.4	0xf8a4	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.23	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.566368103 CET	8.8.8.8	192.168.2.4	0xf8a4	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.22	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.607739925 CET	8.8.8.8	192.168.2.4	0x806a	No error (0)	eb2.3lift.com	eu-eb2.3lift.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:09.607739925 CET	8.8.8.8	192.168.2.4	0x806a	No error (0)	eu-eb2.3lift.com	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:09.607739925 CET	8.8.8.8	192.168.2.4	0x806a	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		3.125.223.182	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.607739925 CET	8.8.8.8	192.168.2.4	0x806a	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		52.57.56.160	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.607739925 CET	8.8.8.8	192.168.2.4	0x806a	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		18.185.170.181	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.607739925 CET	8.8.8.8	192.168.2.4	0x806a	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		52.57.49.235	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 15:03:09.607739925 CET	8.8.8.8	192.168.2.4	0x806a	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		18.158.74.203	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.607739925 CET	8.8.8.8	192.168.2.4	0x806a	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		18.195.223.167	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.607739925 CET	8.8.8.8	192.168.2.4	0x806a	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		18.185.82.201	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.607739925 CET	8.8.8.8	192.168.2.4	0x806a	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		35.156.37.164	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.615612030 CET	8.8.8.8	192.168.2.4	0xacb0	No error (0)	sync.taboola.com	am-sync.taboola.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:09.615612030 CET	8.8.8.8	192.168.2.4	0xacb0	No error (0)	am-sync.taboola.com	am-vip001.taboola.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:09.615612030 CET	8.8.8.8	192.168.2.4	0xacb0	No error (0)	am-vip001.taboola.com		141.226.228.48	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.621542931 CET	8.8.8.8	192.168.2.4	0xac91	No error (0)	x.bidswitch.net	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:09.621542931 CET	8.8.8.8	192.168.2.4	0xac91	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		52.57.142.16	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.621542931 CET	8.8.8.8	192.168.2.4	0xac91	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		35.157.221.90	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.621542931 CET	8.8.8.8	192.168.2.4	0xac91	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		3.126.158.103	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.621542931 CET	8.8.8.8	192.168.2.4	0xac91	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		35.156.158.150	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.621542931 CET	8.8.8.8	192.168.2.4	0xac91	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		52.58.146.86	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.621542931 CET	8.8.8.8	192.168.2.4	0xac91	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		18.194.69.213	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.621542931 CET	8.8.8.8	192.168.2.4	0xac91	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		3.120.52.76	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.621542931 CET	8.8.8.8	192.168.2.4	0xac91	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		35.158.172.137	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 15:03:09.966464996 CET	8.8.8.8	192.168.2.4	0x5f16	No error (0)	ib.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:09.966464996 CET	8.8.8.8	192.168.2.4	0x5f16	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:09.966464996 CET	8.8.8.8	192.168.2.4	0x5f16	No error (0)	ib.anycast .adnxs.com		185.33.221.15	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.966464996 CET	8.8.8.8	192.168.2.4	0x5f16	No error (0)	ib.anycast .adnxs.com		185.33.221.91	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.966464996 CET	8.8.8.8	192.168.2.4	0x5f16	No error (0)	ib.anycast .adnxs.com		185.33.220.240	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.966464996 CET	8.8.8.8	192.168.2.4	0x5f16	No error (0)	ib.anycast .adnxs.com		185.33.221.52	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.966464996 CET	8.8.8.8	192.168.2.4	0x5f16	No error (0)	ib.anycast .adnxs.com		185.33.221.90	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.966464996 CET	8.8.8.8	192.168.2.4	0x5f16	No error (0)	ib.anycast .adnxs.com		185.33.221.87	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.966464996 CET	8.8.8.8	192.168.2.4	0x5f16	No error (0)	ib.anycast .adnxs.com		185.33.220.145	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.966464996 CET	8.8.8.8	192.168.2.4	0x5f16	No error (0)	ib.anycast .adnxs.com		185.33.221.53	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.967405081 CET	8.8.8.8	192.168.2.4	0x6f00	No error (0)	us-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.967405081 CET	8.8.8.8	192.168.2.4	0x6f00	No error (0)	us-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:09.980231047 CET	8.8.8.8	192.168.2.4	0x1477	No error (0)	idsync.rlcdn.com		34.120.207.148	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:10.155116081 CET	8.8.8.8	192.168.2.4	0x35ee	No error (0)	cm.g.doubleclick.net	pagead.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:10.155116081 CET	8.8.8.8	192.168.2.4	0x35ee	No error (0)	pagead.l.doubleclick.net		172.217.23.66	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:10.213429928 CET	8.8.8.8	192.168.2.4	0x53e0	No error (0)	ups.analytics.yahoo.com	prod.ups-ats.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:10.213429928 CET	8.8.8.8	192.168.2.4	0x53e0	No error (0)	prod.ups-ats.aolp-ds-prd.aws.oath.cloud	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:10.213429928 CET	8.8.8.8	192.168.2.4	0x53e0	No error (0)	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		3.126.56.137	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:10.213429928 CET	8.8.8.8	192.168.2.4	0x53e0	No error (0)	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		18.156.0.31	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:10.410037994 CET	8.8.8.8	192.168.2.4	0x1b34	No error (0)	googleads.g.doubleclick.net	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:10.410037994 CET	8.8.8.8	192.168.2.4	0x1b34	No error (0)	pagead46.l.doubleclick.net		172.217.20.226	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:16.248859882 CET	8.8.8.8	192.168.2.4	0x4edd	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:16.248859882 CET	8.8.8.8	192.168.2.4	0x4edd	No error (0)	googlehosted.l.googleusercontent.com		172.217.22.225	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:36.912028074 CET	8.8.8.8	192.168.2.4	0xe27d	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:36.944664001 CET	8.8.8.8	192.168.2.4	0x76c2	No error (0)	maxcdn.bootstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 15:03:37.023475885 CET	8.8.8.8	192.168.2.4	0xba70	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:37.046499968 CET	8.8.8.8	192.168.2.4	0x8972	No error (0)	s3.amazonaws.com		52.216.9.237	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:37.050127983 CET	8.8.8.8	192.168.2.4	0xe346	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:37.050127983 CET	8.8.8.8	192.168.2.4	0xe346	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:37.501313925 CET	8.8.8.8	192.168.2.4	0xd91	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:37.973927021 CET	8.8.8.8	192.168.2.4	0x27f3	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:37.973927021 CET	8.8.8.8	192.168.2.4	0x27f3	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Jan 27, 2021 15:03:52.702111959 CET	8.8.8.8	192.168.2.4	0xc7ba	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:03:52.702111959 CET	8.8.8.8	192.168.2.4	0xc7ba	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 15:03:04.788994074 CET	44.238.32.151	443	192.168.2.4	49741	CN=quip.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Thu Apr 30 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sun May 30 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 15:03:04.791924953 CET	44.238.32.151	443	192.168.2.4	49742	CN=quip.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Thu Apr 30 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sun May 30 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 27, 2021 15:03:04.960659981 CET	44.238.32.151	443	192.168.2.4	49744	CN=quip.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Thu Apr 30 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sun May 30 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 15:03:07.679637909 CET	52.39.66.75	443	192.168.2.4	49755	CN=quip.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Thu Apr 30 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sun May 30 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-5-13-18-51-45-43-27-21,29-23-24,0	74ad8ec6876e2e3366bfd566581ca7e8
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 27, 2021 15:03:08.396365881 CET	185.63.144.5	443	192.168.2.4	49763	CN=px.ads.linkedin.com, O=LinkedIn Corporation, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jan 06 01:00:00 CET 2021 Wed Sep 23 02:00:00 CEST 2020	Tue Jul 06 01:59:59 CEST 2021 Mon Sep 23 01:59:59 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
Jan 27, 2021 15:03:08.449645996 CET	54.170.19.229	443	192.168.2.4	49764	CN=adroll.mgr.consensu.org CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Thu Oct 08 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sun Nov 07 13:00:00 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 27, 2021 15:03:08.810899973 CET	52.49.193.31	443	192.168.2.4	49766	CN=*.match.prod.bidr.io CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Thu Mar 26 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Apr 26 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 27, 2021 15:03:08.893743038 CET	54.74.23.153	443	192.168.2.4	49770	CN=adroll.mgr.consensu.org CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Thu Oct 08 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sun Nov 07 13:00:00 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 15:03:09.572544098 CET	3.124.119.192	443	192.168.2.4	49774	CN=pixel.advertising.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=pixel.advertising.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Oct 04 02:00:00 CEST 2020 Sun Oct 04 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Wed Mar 31 14:00:00 CEST 2021 Wed Mar 31 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=pixel.advertising.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Oct 04 02:00:00 CEST 2020	Wed Mar 31 14:00:00 CEST 2021		
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jan 27, 2021 15:03:09.656075001 CET	185.64.189.110	443	192.168.2.4	49778	CN=*.pubmatic.com, OU=Enterprise SSL Pro Wildcard, OU=PubMatic, O="PubMatic, Inc.", STREET=305 Main St, L=Redwood City, ST=CA, OID.2.5.4.17=94063, C=US CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Feb 22 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Mon Feb 22 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
Jan 27, 2021 15:03:09.692554951 CET	3.125.223.182	443	192.168.2.4	49780	CN=*.3lift.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sat Jul 04 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Aug 05 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 15:03:09.706787109 CET	52.57.142.16	443	192.168.2.4	49782	CN=*.bidswitch.net CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Apr 23 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Thu May 05 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jan 27, 2021 15:03:09.718339920 CET	141.226.228.48	443	192.168.2.4	49781	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020 Wed Sep 23 02:00:00 CEST 2020	Mon Dec 27 00:59:59 CET 2021 Mon Sep 23 01:59:59 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
Jan 27, 2021 15:03:09.796659946 CET	64.202.112.159	443	192.168.2.4	49777	CN=*.outbrain.com, O=OUTBRAIN INC., L=New York, ST=New York, C=US CN=Thawte RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Thawte RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 29 01:00:00 CET 2019 Mon Nov 06 13:23:52 CET 2017	Tue Nov 23 13:00:00 CET 2021 Sat Nov 06 13:23:52 CET 2027	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Thawte RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:52 CET 2017	Sat Nov 06 13:23:52 CET 2027		
Jan 27, 2021 15:03:10.198044062 CET	185.33.221.15	443	192.168.2.4	49783	CN=*.adnxs.com, O="AppNexus, Inc.", L=New York, ST=New York, C=US CN=DigiCert ECC Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert ECC Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jan 23 01:00:00 CET 2019 Fri Mar 08 13:00:00 CET 2013	Mon Mar 08 13:00:00 CET 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert ECC Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jan 27, 2021 15:03:37.157644987 CET	104.16.19.94	443	192.168.2.4	49815	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 27, 2021 15:03:37.165674925 CET	104.16.19.94	443	192.168.2.4	49816	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 27, 2021 15:03:37.320074081 CET	52.216.9.237	443	192.168.2.4	49813	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Jan 27, 2021 15:03:37.321898937 CET	52.216.9.237	443	192.168.2.4	49814	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Jan 27, 2021 15:03:38.059457064 CET	152.199.23.37	443	192.168.2.4	49820	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

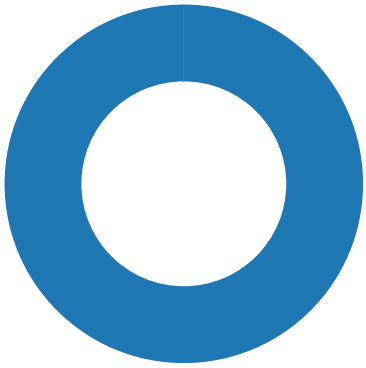
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 15:03:38.060065031 CET	152.199.23.37	443	192.168.2.4	49819	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jan 27, 2021 15:03:52.788377047 CET	152.199.23.37	443	192.168.2.4	49823	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

Code Manipulations

Statistics

Behavior

- chrome.exe
- chrome.exe
- dllhost.exe
- explorer.exe
- iexplore.exe
- iexplore.exe



Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 6724 Parent PID: 2440

General

Start time:	15:02:59
Start date:	27/01/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --force-renderer-accessibility 'https://quip.com/R1lpAz7okW3E'
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}	dr	unicode	0	1	success or wait	1	7FF609CBFC4B	RegSetValueExW

Analysis Process: chrome.exe PID: 6976 Parent PID: 6724

General

Start time:	15:03:01
Start date:	27/01/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1508,11710123193784369909,9829296053474170828,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1820 /prefetch:8
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

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

Analysis Process: dllhost.exe PID: 6448 Parent PID: 800

General

Start time:	15:03:04
Start date:	27/01/2021
Path:	C:\Windows\System32\dllhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\DllHost.exe /Processid:{49F171DD-B51A-40D3-9A6C-52D674CC729D}
Imagebase:	0x7ff714000000
File size:	20888 bytes
MD5 hash:	2528137C6745C4EADD87817A1909677E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: 3424 Parent PID: 6448

General

Start time:	15:03:06
Start date:	27/01/2021

Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 8172 Parent PID: 800

General

Start time:	15:03:33
Start date:	27/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff618280000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 4876 Parent PID: 8172

General

Start time:	15:03:34
Start date:	27/01/2021

Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:8172 CREDAT:17410 /prefetch:2
Imagebase:	0x1000000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis