ID: 345125
Cookbook: browseurl.jbs
Time: 18:22:08
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

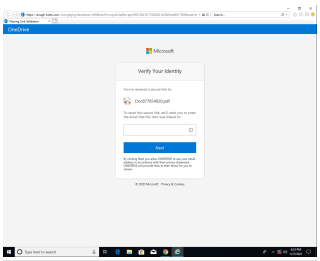
Analysis Report https://quip.com/OWCGAwI8CpAi

Overview

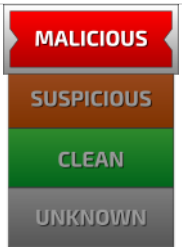
General Information

Sample URL:	http://https://quip.com/OWCGAwI8CpAi
Analysis ID:	345125

Most interesting Screenshot:



Detection



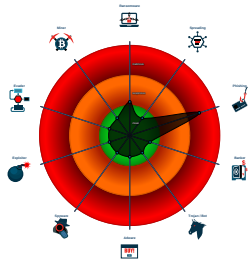
HTMLPhisher

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Yara detected HtmlPhish_10
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- Submit button contains javascript call
- Suspicious form URL found

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 6132 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --force-renderer-accessibility 'https://quip.com/OWCGAwI8CpAi' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 1488 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1540,11308364918695712584,1796156952568761714,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1796 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- dllhost.exe (PID: 6692 cmdline: C:\Windows\system32\DllHost.exe /Processid:{49F171DD-B51A-40D3-9A6C-52D674CC729D} MD5: 2528137C6745C4EADD87817A1909677E)
  - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- iexplore.exe (PID: 6348 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6356 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6348 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

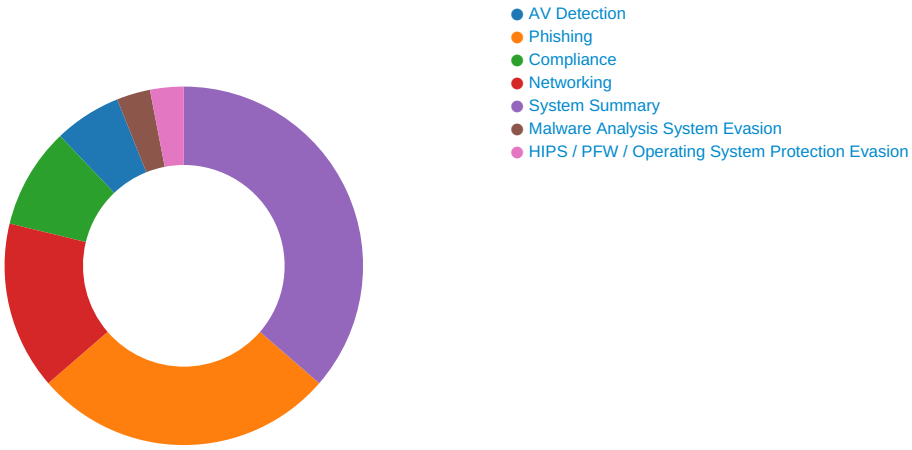
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing:

Yara detected HtmlPhish_10

Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

Compliance:

Creates a directory in C:\Program Files

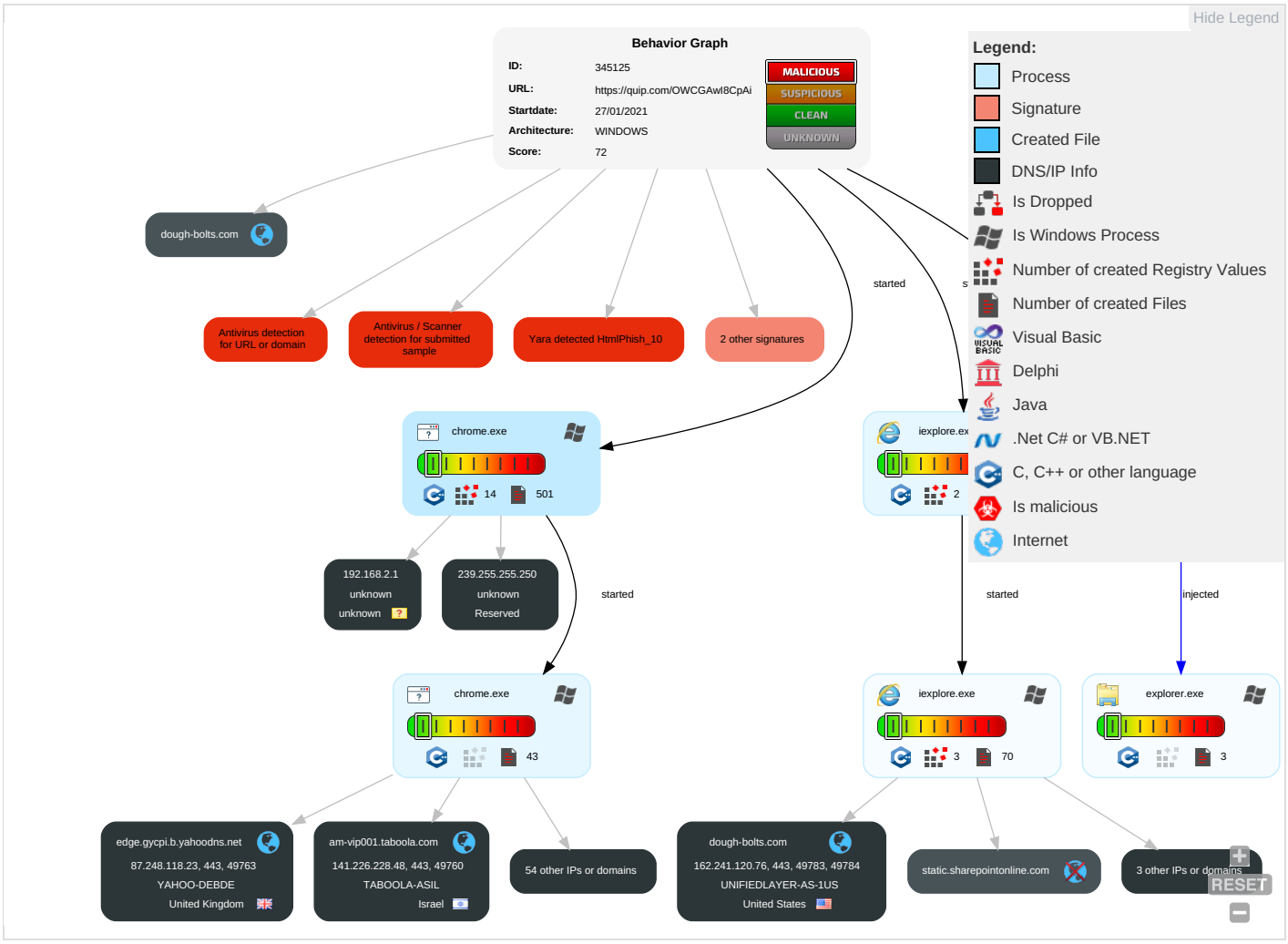
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impac
Valid Accounts	Scripting 1	Path Interception	Process Injection 2	Masquerading 3	OS Credential Dumping	Security Software Discovery 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	Modify Syster Partiti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	Process 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	Device Lockou
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1	Security Account Manager	File and Directory 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	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrie Billing Fraud

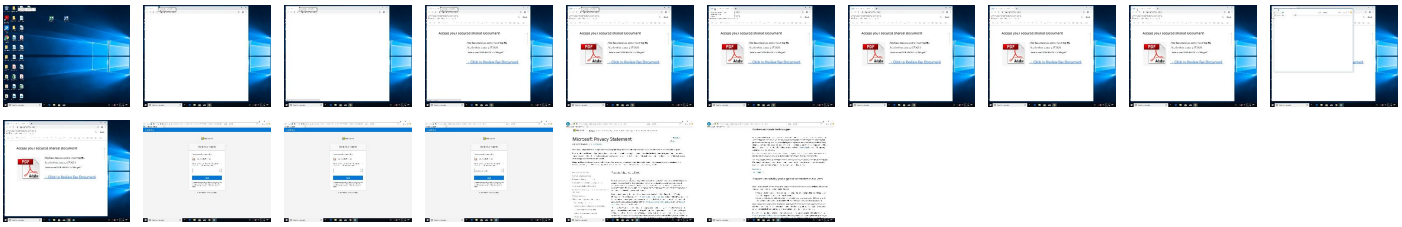
Behavior Graph

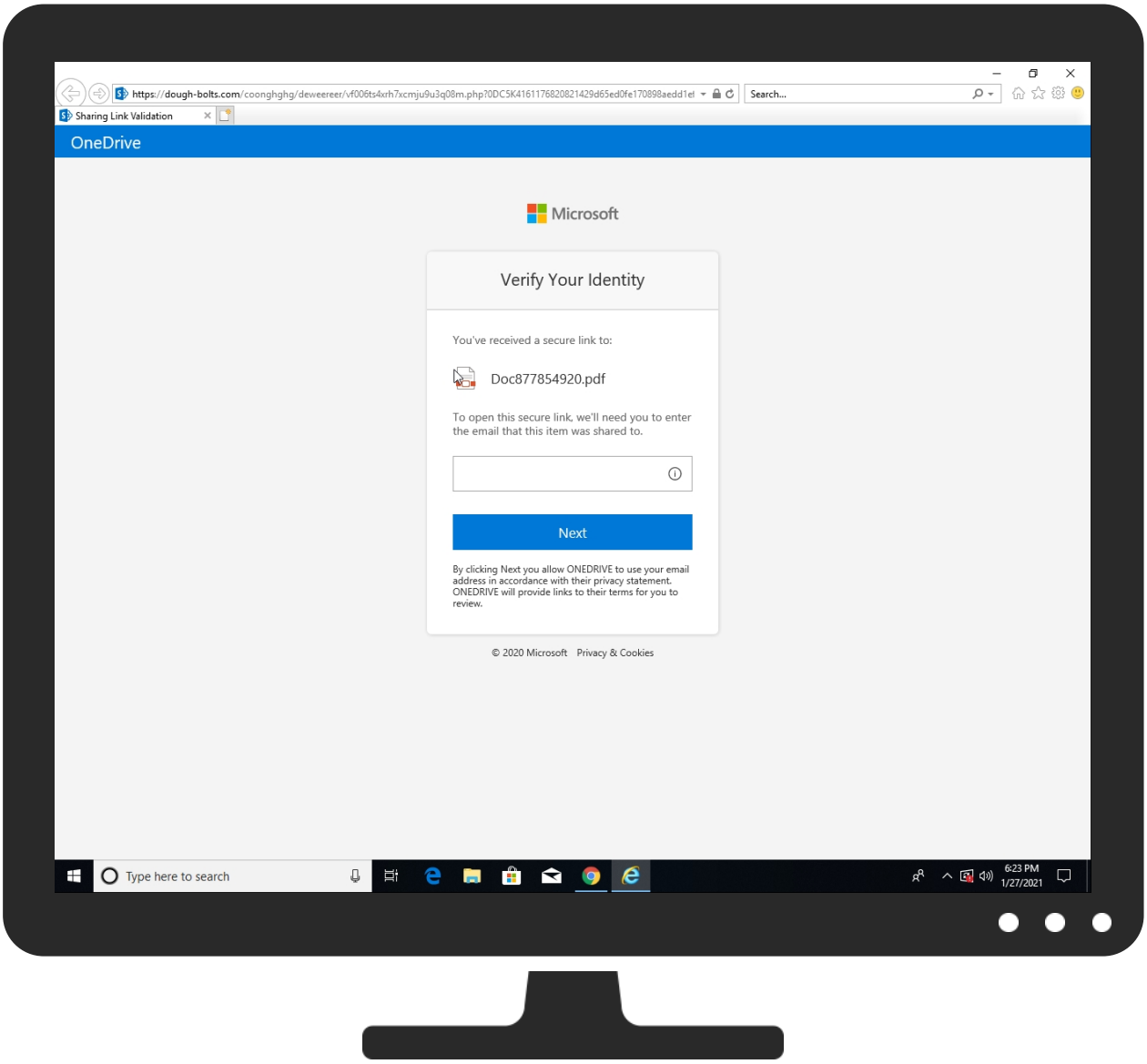


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://quip.com/OWCGAwI8CpAi	0%	Virustotal		Browse
http://https://quip.com/OWCGAwI8CpAi	0%	Avira URL Cloud	safe	
http://https://quip.com/OWCGAwI8CpAi	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
segments.company-target.com	0%	Virustotal		Browse
dough-bolts.com	4%	Virustotal		Browse
quip-cdn.com	0%	Virustotal		Browse
match.prod.bidr.io	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://dough-bolts.com/coonghghg/deweereer/vf006ts4xrh7xcmju9u3q08m.php?0DC5K4161176820821429d65ed0fe170898aedd1eff978e721429d65ed0fe170898aedd1eff978e721429d65ed0fe170898aedd1eff978e721429d65ed0fe170898aedd1eff978e721429d65ed0fe170898aedd1eff978e7&email=&error=	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
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://https://feedback.go	0%	Avira URL Cloud	safe	
http://https://quip.comC	0%	Avira URL Cloud	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://quip-cdn.com/LAf64rubV-Hr3Ux_DVJKkwble(origin)	0%	Avira URL Cloud	safe	
http://https://dough-bolts.com/coonghghg/deweereer/vf006ts4xrh7xcmju9u3q08m.php?0DC5K4161176820821429d65ed0	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://ocsp.rootca1.amazontrust.com0:	0%	Avira URL Cloud	safe	
http://https://quip-cdn.com/LAf64rubV-Hr3Ux_DVJKkwble	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://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://quip-marketing.com	0%	Avira URL Cloud	safe	
http://https://content.googleap	0%	Avira URL Cloud	safe	
http://https://content.googleapww.googl	0%	Avira URL Cloud	safe	
http://https://autocomplete.d	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://autocomplete.dmandbase.com	0%	Avira URL Cloud	safe	
http://https://quip-cdn.com/LAf64rubV-Hr3Ux_DVJKkwt)me=?ryW-	0%	Avira URL Cloud	safe	
http://https://quip-cdn.com/LAf64rubV-Hr3Ux_DVJKkwo	0%	Avira URL Cloud	safe	
http://https://www.gic.c	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://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.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://https://quip-cdn.com	0%	Avira URL Cloud	safe	
http://https://bidswitch.net/	0%	Avira URL Cloud	safe	
http://https://www.gsttic.com;	0%	Avira URL Cloud	safe	
http://https://company-target.com/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pug-lhr.pubmatic.com	185.64.190.80	true	false		high
segments.company-target.com	99.86.154.45	true	false	• 0%, Virustotal, Browse	unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
listenweb4.quip.com	52.39.66.75	true	false		high
dough-bolts.com	162.241.120.76	true	false	• 4%, Virustotal, Browse	unknown
idsync.rlcdn.com	34.120.207.148	true	false		high
quip.com	44.238.32.151	true	false		high
pagead.l.doubleclick.net	172.217.22.194	true	false		high
quip-cdn.com	99.86.154.21	true	false	• 0%, Virustotal, Browse	unknown
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	• 0%, Virustotal, Browse	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	35.156.106.231	true	false		unknown
alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com	18.195.193.185	true	false		high
dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com	18.185.170.181	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	185.33.221.13	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	143.204.11.81	true	false		high
adserver-vpc-alb-3-890571764.eu-west-1.elb.amazonaws.com	34.254.169.151	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
d.adroll.com	unknown	unknown	false		high
ups.analytics.yahoo.com	unknown	unknown	false		high
assets.onestore.ms	unknown	unknown	false		unknown
ajax.aspnetcdn.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
static.sharepointonline.com	unknown	unknown	false		unknown
clients2.googleusercontent.com	unknown	unknown	false		high
ads.yahoo.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
www.linkedin.com	unknown	unknown	false		high
pixel.rubiconproject.com	unknown	unknown	false		high
s.adroll.com	unknown	unknown	false		high
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
spoprod-a.akamaihd.net	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, 00000000.00000002.394051899.0000016F91121000.00000002.00000001.sdmp, chrome.exe, 00000000.00000003.255116238.0000016F93064000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/ac/?q=	chrome.exe, 00000000.00000003.255508066.0000016F90AEB000.00000004.00000001.sdmp, chrome.exe, 00000000.00000002.394051899.0000016F91121000.00000002.00000001.sdmp	false		high
http://https://search.yahoo.com/search?ei=&fr=crmas&p=	chrome.exe, 00000000.00000003.255116238.0000016F93064000.00000004.00000001.sdmp	false		high
http://https://ups.analytics.yahoo.com/ups/55980/sync?uid=MGM3MzhlYzI3NTk4YjY1MjA3MzI0MTY5OGFmMTI5ODE&_orig	chrome.exe, 00000000.00000002.397804456.0000016F93185000.00000004.00000001.sdmp, chrome.exe, 00000000.00000002.400356856.0000016F93511000.00000004.00000001.sdmp	false		high
http://https://casalemedia.com/	chrome.exe, 00000000.00000002.405346182.0000016F96014000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers	explorer.exe, 00000004.00000000.246639634.0000000008B46000.00000002.00000001.sdmp	false		high
http://https://quip.com/OWCGAwI8CpAilid	chrome.exe, 00000000.00000002.401218108.0000016F9370D000.00000004.00000001.sdmp	false		high
http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01	chrome.exe, 00000000.00000003.254076138.0000016F96407000.00000004.00000001.sdmp	false		high
http://https://checkout.stripe.com	chrome.exe, 00000000.00000003.255299453.0000016F930B2000.00000004.00000001.sdmp, chrome.exe, 00000000.00000003.255497916.0000016F937AB000.00000004.00000001.sdmp	false		high
http://https://s.adroll.com/pixel/VNM53VCKEFACRMFQE65VV4/IB7LZPOS3RCN3J2MSNRBFC/X27ESS35BFE4LKRZIE373P.js	chrome.exe, 00000000.00000002.393687658.0000016F9102C000.00000004.00000001.sdmp	false		high
http://https://quip.com/OWCGAwI8CpAitatushtmldOff_Saf	chrome.exe, 00000000.00000003.254880291.0000016F95E80000.00000004.00000001.sdmp	false		high
http://https://bugs.chromium.org/p/chromium/issues/entry?template=Safety	chrome.exe, 00000000.00000002.388455242.0000016F8F7B0000.00000002.00000001.sdmp	false		high
http://https://quip.com/	chrome.exe, 00000000.00000002.405312378.0000016F95FBE000.00000004.00000001.sdmp, chrome.exe, 00000000.00000002.405346182.0000016F96014000.00000004.00000001.sdmp, d978b0efc727804e_0.0.dr	false		high
http://https://cdn.cookielaw.org/consent/4a3b4a16-9af0-4726-976d-39737fb16905.js	chrome.exe, 00000000.00000002.392710488.0000016F90ADF000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	chrome.exe, 00000000.00000002.394766445.0000016F91630000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.246639634.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://feedback.go	chrome.exe, 00000000.00000002.405597163.0000016F961A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://quip.comC	chrome.exe, 00000000.00000002.401437473.0000016F93782000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://quip.com/OWCGAwI8CpAi..Z	chrome.exe, 00000000.00000003.254396676.0000016F935EF000.00000004.00000001.sdmp	false		high
http://www.zhongyicts.com.cn	chrome.exe, 00000000.00000002.401940138.0000016F93DBC000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.247334141.0000000008ED6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://quip-cdn.com/LAf64rubV-Hr3Ux_DVJKkwble(origin)	chrome.exe, 00000000.00000002.405372722.0000016F96056000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/google/closure-library/wiki/goog.module:-an-ES6-module-like-alternative-to-goog.p	chrome.exe, 00000000.00000003.272187825.0000016F964D2000.00000004.00000001.sdmp	false		high
http://https://dough-bolts.com/coonghghg/deweereer/vf006ts4xrh7xcmju9u3q08m.php?0DC5K4161176820821429d65ed0	{CCED0D34-610F-11EB-90E4-ECF4BB862DED}.dat.10.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.sca1b.amazontrust.com06	chrome.exe, 00000000.00000002.388575015.0000016F8F820000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://duckduckgo.com/?q=	chrome.exe, 00000000.00000003.255116238.0000016F93064000.00000004.00000001.sdmp	false		high
http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions	chrome.exe, 00000000.00000003.254076138.0000016F96407000.00000004.00000001.sdmp	false		high
http://https://search.yahoo.com/search?ei=&fr=crmas&p=searchTerms	chrome.exe, 00000000.00000003.255116238.0000016F93064000.00000004.00000001.sdmp	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.ico	chrome.exe, 00000000.00000003.255508066.0000016F90AEB000.00000004.00000001.sdmp	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	chrome.exe, 00000000.00000002.394051899.0000016F91121000.00000002.00000001.sdmp	false		high
http://https://quip.com/OWCGAwI8CpAiilter	chrome.exe, 00000000.00000002.397954189.0000016F932B3000.00000004.00000001.sdmp	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icot	chrome.exe, 00000000.00000003.255508066.0000016F90AEB000.00000004.00000001.sdmp	false		high
http://ocsp.rootca1.amazontrust.com0:	chrome.exe, 00000000.00000002.401437473.0000016F93782000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://quip.com/OWCGAwI8CpAiv	chrome.exe, 00000000.00000002.401301655.0000016F93737000.00000004.00000001.sdmp	false		high
http://https://duckduckgo.com/favicon.ico	chrome.exe, 00000000.00000003.255116238.0000016F93064000.00000004.00000001.sdmp	false		high
http://https://quip-cdn.com/LAf64rubV-Hr3Ux_DVJKkwble	chrome.exe, 00000000.00000002.405372722.0000016F96056000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://quip.com/OWCGAwI8CpAi#QQAACA2P7Po	chrome.exe, 00000000.00000003.254880291.0000016F95E80000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	chrome.exe, 00000000.00000002.394766445.0000016F91630000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.246639634.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.rootg2.amazontrust.com/rootg2.crl0	chrome.exe, 00000000.00000003.254396676.0000016F935EF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://geolocation.onetrust.com	chrome.exe, 00000000.00000003.255299453.0000016F930B2000.00000004.00000001.sdmp, chrome.exe, 00000000.00000003.255497916.0000016F937AB000.00000004.00000001.sdmp, chrome.exe, 00000000.00000002.401437473.0000016F93782000.00000004.00000001.sdmp	false		high
http://https://demdex.com	chrome.exe, 00000000.00000003.255299453.0000016F930B2000.00000004.00000001.sdmp, chrome.exe, 00000000.00000003.255497916.0000016F937AB000.00000004.00000001.sdmp	false		high
http://tools.ietf.org/html/rfc1950	chrome.exe, 00000000.00000003.254076138.0000016F96407000.00000004.00000001.sdmp	false		high
http://https://quip.com/OWCGAwI8CpAi69ccd1	chrome.exe, 00000000.00000003.254880291.0000016F95E80000.00000004.00000001.sdmp	false		high
http://https://quip.com/OWCGAwI8CpAi#QQAACAoBxV4;	chrome.exe, 00000000.00000002.405372722.0000016F96056000.00000004.00000001.sdmp	false		high
http://https://3lift.com/	chrome.exe, 00000000.00000002.405312378.0000016F95FBE000.00000004.00000001.sdmp	false		high
http://https://quip-marketing.com	chrome.exe, 00000000.00000003.255299453.0000016F930B2000.00000004.00000001.sdmp, chrome.exe, 00000000.00000003.255497916.0000016F937AB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://content.googleap	chrome.exe, 00000000.00000003.255243041.0000016F95ED1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://taboola.com/	chrome.exe, 00000000.00000002.405312378.0000016F95FBE000.00000004.00000001.sdmp	false		high
http://https://feedback.googleusercontent.com	chrome.exe, 00000000.00000003.254396676.0000016F935EF000.00000004.00000001.sdmp, chrome.exe, 00000000.00000002.405741778.0000016F962D8000.00000004.00000001.sdmp, chrome.exe, 00000000.00000002.405249322.0000016F95F2D000.00000004.00000001.sdmp, chrome.exe, 00000000.00000002.405394280.0000016F9608C000.00000004.00000001.sdmp	false		high
http://https://content.googleapww.googl	chrome.exe, 00000000.00000003.255243041.0000016F95ED1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://adroll.com/	chrome.exe, 00000000.00000002.405312378.0000016F95FBE000.00000004.00000001.sdmp	false		high
http://https://autocomplete.d	chrome.exe, 00000000.00000002.392710488.0000016F90ADF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/bThe	chrome.exe, 00000000.00000002.394766445.0000016F91630000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.246639634.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://autocomplete.dmandbase.com	chrome.exe, 00000000.00000002.392710488.0000016F90ADF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://doubleclick.net/	chrome.exe, 00000000.00000002.405346182.0000016F96014000.00000004.00000001.sdmp	false		high
http://https://quip-cdn.com/LAf64rubV-Hr3Ux_DVJKkwt)me=?ryW-	chrome.exe, 00000000.00000002.405372722.0000016F96056000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://quip.com/OWCGAwI8CpAiC	chrome.exe, 00000000.00000002.383108056.0000016F8D0D6000.00000004.00000020.sdmp	false		high
http://https://adnxs.com/	chrome.exe, 00000000.00000002.405312378.0000016F95FBE000.00000004.00000001.sdmp	false		high
http://https://px.ads.linkedin.com/	chrome.exe, 00000000.00000003.255299453.0000016F930B2000.00000004.00000001.sdmp, chrome.exe, 00000000.00000003.255497916.0000016F937AB000.00000004.00000001.sdmp	false		high
http://https://quip.com/OWCGAwI8CpAiA	Current Session.0.dr	false		high
http://www.unicode.org/copyright.html	chrome.exe, 00000000.00000002.385000845.0000016F8ED70000.00000002.00000001.sdmp	false		high
http://https://quip-cdn.com/LAf64rubV-Hr3Ux_DVJKkwo	chrome.exe, 00000000.00000002.405291145.0000016F95F8C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://quip.com/OWCGAwI8CpAiF	chrome.exe, 00000000.00000003.254396676.0000016F935EF000.00000004.00000001.sdmp	false		high
http://https://openx.net/	chrome.exe, 00000000.00000002.405312378.0000016F95FBE000.00000004.00000001.sdmp	false		high
http://https://analytics.twitter.com	chrome.exe, 00000000.00000003.255299453.0000016F930B2000.00000004.00000001.sdmp, chrome.exe, 00000000.00000003.255497916.0000016F937AB000.00000004.00000001.sdmp	false		high
http://https://googleads.g.doubleclick.net/	chrome.exe, 00000000.00000003.255299453.0000016F930B2000.00000004.00000001.sdmp, chrome.exe, 00000000.00000003.255497916.0000016F937AB000.00000004.00000001.sdmp	false		high
http://https://www.gic.c	chrome.exe, 00000000.00000002.405597163.0000016F961A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.ecosia.org/search?q=&addon=opensearch	chrome.exe, 00000000.00000002.388697394.0000016F8F8C0000.00000004.00000001.sdmp	false		high
http://https://quip.com/-/blob/QQAAAAnpLQ3/PB3ZFz0vmgmKAdDnt9w3MA?s=OWCGAwI8CpAi	chrome.exe, 00000000.00000002.405312378.0000016F95FBE000.00000004.00000001.sdmp	false		high
http://https://rubiconproject.com/	chrome.exe, 00000000.00000002.405346182.0000016F96014000.00000004.00000001.sdmp	false		high
http://https://quip.com/OWCGAwI8CpAi/	chrome.exe, 00000000.00000002.393552876.0000016F90F72000.00000004.00000001.sdmp	false		high
http://https://quip.com/OWCGAwI8CpAi2	chrome.exe, 00000000.00000002.405597163.0000016F961A1000.00000004.00000001.sdmp, History Provider Cache.0.dr	false		high
http://https://autocomplete.demandbase.com	chrome.exe, 00000000.00000003.255299453.0000016F930B2000.00000004.00000001.sdmp, chrome.exe, 00000000.00000003.255497916.0000016F937AB000.00000004.00000001.sdmp	false		high
http://https://quip.com/OWCGAwI8CpAi0	chrome.exe, 00000000.00000003.254880291.0000016F95E80000.00000004.00000001.sdmp	false		high
http://https://www-onepick-opensocial.googleusercontent.com	chrome.exe, 00000000.00000002.393028249.0000016F90D10000.00000004.00000001.sdmp	false		high
http://www.typography.netD	chrome.exe, 00000000.00000002.394766445.0000016F91630000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.246639634.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	chrome.exe, 00000000.00000002.401857259.0000016F93CDE000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.246639634.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://quip.com/OWCGAwI8CpAig	chrome.exe, 00000000.00000003.254880291.0000016F95E80000.00000004.00000001.sdmp	false		high
http://https://m.addthis.com	chrome.exe, 00000000.00000003.255299453.0000016F930B2000.00000004.00000001.sdmp, chrome.exe, 00000000.00000003.255497916.0000016F937AB000.00000004.00000001.sdmp	false		high
http://https://m.addthisedge.com	chrome.exe, 00000000.00000003.255299453.0000016F930B2000.00000004.00000001.sdmp, chrome.exe, 00000000.00000003.255497916.0000016F937AB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://quip.com/OWCGAwI8CpAid	chrome.exe, 00000000.00000003.254396676.0000016F935EF000.00000004.00000001.sdmp	false		high
http://https://www.youtube.com;	chrome.exe, 00000000.00000003.255299453.0000016F930B2000.00000004.00000001.sdmp, chrome.exe, 00000000.00000003.255497916.0000016F937AB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://safebrowsing.googleusercontent.com/safebrowsing/clientreport/chrome-certs	chrome.exe, 00000000.00000002.393687658.0000016F9102C000.00000004.00000001.sdmp	false		high
http://https://quip.com/OWCGAwI8CpAiwo	chrome.exe, 00000000.00000002.400828566.0000016F935EF000.00000004.00000001.sdmp	false		high
http://https://quip.com/OWCGAwI8CpAiK	chrome.exe, 00000000.00000002.401437473.0000016F93782000.00000004.00000001.sdmp	false		high
http://https://quip.com/OWCGAwI8CpAientState	chrome.exe, 00000000.00000002.383180690.0000016F8D0F9000.00000004.00000020.sdmp	false		high
http://https://quip.com/OWCGAwI8CpAiI	chrome.exe, 00000000.00000003.255116238.0000016F93064000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	chrome.exe, 00000000.00000002.401857259.0000016F93CDE000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.247117076.0000000008DFE000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	chrome.exe, 00000000.00000002.394766445.0000016F91630000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.246639634.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://quip.com/OWCGAwI8CpAiR	chrome.exe, 00000000.00000002.405158130.0000016F95E60000.00000004.00000001.sdmp	false		high
http://https://quip.com/OWCGAwI8CpAiP	chrome.exe, 00000000.00000002.401218108.0000016F9370D000.00000004.00000001.sdmp, chrome.exe, 00000000.00000003.255116238.0000016F93064000.00000004.00000001.sdmp	false		high
http://https://quip.com/OWCGAwI8CpAiT	chrome.exe, 00000000.00000003.254396676.0000016F935EF000.00000004.00000001.sdmp	false		high
http://https://scripts.demandbase.com	chrome.exe, 00000000.00000003.255299453.0000016F930B2000.00000004.00000001.sdmp, chrome.exe, 00000000.00000003.255497916.0000016F937AB000.00000004.00000001.sdmp, chrome.exe, 00000000.00000003.255116238.0000016F93064000.00000004.00000001.sdmp	false		high
http://https://quip-cdn.com	chrome.exe, 00000000.00000002.392710488.0000016F90ADF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://bidswitch.net/	chrome.exe, 00000000.00000002.405312378.0000016F95FBE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.gsttic.com;	chrome.exe, 00000000.00000003.255243041.0000016F95ED1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://company-target.com/	chrome.exe, 00000000.00000003.254396676.0000016F935EF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://quip.com/OWCGAwI8CpAiSyncService	chrome.exe, 00000000.00000002.393028249.0000016F90D10000.00000004.00000001.sdmp	false		high
http://https://quip.com/OWCGAwI8CpAi	Current Session.0.dr	false		high
http://https://org62.my.salesforce.com	chrome.exe, 00000000.00000003.255299453.0000016F930B2000.00000004.00000001.sdmp, chrome.exe, 00000000.00000003.255497916.0000016F937AB000.00000004.00000001.sdmp	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	chrome.exe, 00000000.00000002.394051899.0000016F91121000.00000002.00000001.sdmp	false		high
http://https://quip.com/OWCGAwI8CpAiome	chrome.exe, 00000000.00000002.401218108.0000016F9370D000.00000004.00000001.sdmp	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
185.33.221.13	unknown	Netherlands		29990	ASN-APPNEXUS	false
185.64.190.80	unknown	United Kingdom		62713	AS-PUBMATICUS	false
35.156.106.231	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
172.217.22.194	unknown	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
3.126.56.137	unknown	United States		16509	AMAZON-02US	false
172.217.22.227	unknown	United States		15169	GOOGLEUS	false
172.217.22.225	unknown	United States		15169	GOOGLEUS	false
34.254.169.151	unknown	United States		16509	AMAZON-02US	false
64.202.112.159	unknown	United States		22075	AS-OUTBRAINUS	false
52.39.66.75	unknown	United States		16509	AMAZON-02US	false
141.226.228.48	unknown	Israel		200478	TABOOLA-ASIL	false
18.185.170.181	unknown	United States		16509	AMAZON-02US	false
99.86.154.21	unknown	United States		16509	AMAZON-02US	false
143.204.11.81	unknown	United States		16509	AMAZON-02US	false
172.217.20.226	unknown	United States		15169	GOOGLEUS	false
99.86.154.45	unknown	United States		16509	AMAZON-02US	false
18.195.193.185	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
162.241.120.76	unknown	United States		46606	UNIFIEDLAYER-AS-1US	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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	345125
Start date:	27.01.2021
Start time:	18:22:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://quip.com/OWCGAwI8CpAi
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:	22
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:	mal72.phis.win@39/280@39/29
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://go.microsoft.com/fwlink/?linkid=845480
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, dllhost.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 172.217.23.35, 216.58.207.174, 172.217.20.237, 172.217.23.78, 173.194.187.70, 173.194.187.106, 216.58.207.136, 216.58.207.142, 23.210.249.242, 23.210.248.216, 172.217.23.68, 192.124.249.41, 192.124.249.24, 192.124.249.36, 192.124.249.23, 192.124.249.22, 13.107.42.14, 67.26.75.254, 67.27.158.126, 8.241.121.126, 8.248.143.254, 67.26.73.254, 23.210.249.164, 69.173.144.138, 69.173.144.165, 69.173.144.139, 216.58.207.131, 172.217.23.10, 172.217.23.42, 172.217.23.74, 172.217.22.202, 172.217.22.234, 216.58.207.138, 104.108.39.131, 23.210.248.85, 104.108.60.231, 95.101.22.119, 95.101.22.95, 51.104.139.180, 8.248.115.254, 67.27.159.126, 67.27.157.254, 67.27.159.254, 8.253.204.121, 51.103.5.159, 23.211.5.92, 95.101.22.125, 95.101.22.134, 152.199.19.160, 95.101.22.71, 95.101.22.133, 23.210.249.93, 104.108.38.107, 152.199.19.161, 172.217.23.67, 173.194.188.70, 173.194.164.103, 20.54.26.129, 173.194.182.198, 74.125.104.87, 51.104.144.132 • Excluded domains from analysis (whitelisted): ssl.gstatic.com, arc.msn.com.nsatc.net, assets.onestore.ms.edgekey.net, r1---sn-4g5e6nsk.gvt1.com, e13678.dscb.akamaiedge.net, clientservices.googleapis.com, i.s-microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, wns.notify.windows.com.akadns.net, a1945.g2.akamai.net, e11290.dspg.akamaiedge.net, r1---sn-4g5ednsl.gvt1.com, l-0005.l-msedge.net,

www.microsoft.com-c-3.edgekey.net, clients2.google.com, audownload.windowsupdate.nsatc.net, update.googleapis.com, www.google.com, statics-marketingsites-eus-ms-com.akamaized.net, 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, e10583.dspg.akamaiedge.net, fs.microsoft.com, r1---sn-4g5e6nss.gvt1.com, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, www.googleapis.com, assets.onestore.ms.akadns.net, c-s.cms.ms.akadns.net, ris.api.iris.microsoft.com, r1---sn-4g5ednle.gvt1.com, wildcard.adroll.com.edgekey.net, blobcollector.events.data.trafficmanager.net, dsum-sec.casalemedia.com.edgekey.net, r1.sn-4g5ednsl.gvt1.com, a1531.g2.akamai.net, spoprod-a.akamaihd.net.edgesuite.net, c.s-microsoft.com-c.edgekey.net, clients.l.google.com, e1780.dspg.akamaiedge.net, privacy.microsoft.com.edgekey.net, r1.sn-4g5e6ney.gvt1.com, par02p.wns.notify.trafficmanager.net, e4007.g.akamaiedge.net, cs9.wpc.v0cdn.net, pixel.rubiconproject.net.akadns.net, r1.sn-4g5e6nss.gvt1.com, i.s-microsoft.com, r5---sn-4g5e6nsr.gvt1.com, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, e9706.dscg.akamaiedge.net, iecvlist.microsoft.com, e8037.g.akamaiedge.net, go.microsoft.com, mscomajax.vo.msecnd.net, redirector.gvt1.com, r1.sn-4g5ednle.gvt1.com, www.googletagmanager.com, emea1.notify.windows.com.akadns.net, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, static.sharepointonline.com-c.edgekey.net, www-linkedin-com.l-0005.l-msedge.net, client.wns.windows.com, accounts.google.com, www-google-analytics.l.google.com, cs22.wpc.v0cdn.net, ie9comview.vo.msecnd.net, www-googletagmanager.l.google.com, r1.sn-4g5e6nsk.gvt1.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, c.s-microsoft.com, wildcard.licdn.com.edgekey.net, privacy.microsoft.com, go.microsoft.com.edgekey.net, e13678.dscg.akamaiedge.net, r5.sn-4g5e6nsr.gvt1.com, ocsp.godaddy.com, e13678.dspb.akamaiedge.net, www.microsoft.com

- 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.

Simulations

Behavior and APIs

Time	Type	Description
18:23:02	API Interceptor	1x Sleep call for process: dllhost.exe modified
18:23:04	API Interceptor	5x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\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
MD5:	5BC0D504EB02FB705D0358F62F22A6A6
SHA1:	89C856F3354CCB3B6543C1797F2A252E496DA0EC
SHA-256:	A19E067FFE72E062BD7DA7D09407C9C8D2D4E43A516059943A7F63B36A456905
SHA-512:	F62D3EFA7205E1B2F33C534F6C3A6AD705506B001B68724010ED4EFCC12C208ED55787F24DDDAC8A90446013AB4838CE2DEC66D108E10C6072A71B5AE259D46
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771	
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...2009090700000Z..210909070000Z0..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):	177402
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	3072:RN7MlanAQwElztTmN7MlanAQwElztTmN7MlanAQwElztTk:RNwl3JmNwl3JmNwl3Jk
MD5:	F1781C1859FB269F73BC46970907D4B5
SHA1:	A5706B51352CEB27A5CC0C197E0A9B26932818FA
SHA-256:	AFEFA441B14F7BE717729641DF6A358878C94E2BC5426952A949B6B40D166312
SHA-512:	73C5033B13F81B18E157279CC075210A13D0F4978F51524959B9937BC9BA17B3F27B7B178D72EDC19BD4385EB4BC68AF977FB4743857EEC709B8396EE08176F4
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'..Ir.....I.I6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;/..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....I.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a...,...E5X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xl@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/l\.cDB0.'.Y...r.[.....vM...o.=....zK..r..I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\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.....20210126204909Z....20210128084909Z0...*.H.....*.d.x.../8...K.7.....S..~r..m.,..+b...g]..-....'.&.....K..u.R)..\.l.O....w...c..l.aImf..x/.a.<?"..[..$Q).*C=9B.j....4t.M....-%..u]..G.....)....S.-..r.A..9&.....pap9.X...#.I..#...qE..G.D.T.....S...FPu.bu"(ot.L....bn. .e.I..3..8..../,.g...b0..^0..Z0..B.....1g...r.0...*.H.....0c1.0...U....US1!0...U....The Go Daddy Group, Inc.110/..U...(Go Daddy Class 2 Certification Authority0...1612130700002..211213070000Z0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.100...U...'Go Daddy Root Validation Authority - G10.."0...*.H.....0.....}...@.H.....j.b.2.c....'eSA...6""2.hf.m.m9....._N."gV..{.J"{..0f.W$.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):	3.7706365231679153
Encrypted:	false
SSDEEP:	24:FGwyPV13MhmyFqbNcDFwyPV13MhmyFqbNcz:AwkV1XyF3DFwkV1XyF3z
MD5:	4718AC249822462E422B7E6B4BB171DA
SHA1:	8E1E930634E3639FFE82C4FA5FB35DCE5173212C
SHA-256:	72155CED43C9573B3F82888BDA870F2A3EF52CB26C61F1FD4E97F90E216AE9F7
SHA-512:	9A75485CF2562FCB5A00A0728D77C5ED0893DB5BD3A3CBFC9033BBFC8F6649A31C91176D17763092EE88775AFBEAAF309950D383AB05B7D81030FDE408DF0D5
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771	
Preview:	p..... .....1.....(..... .....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.l.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..... .....1.....(.....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.l.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):	984
Entropy (8bit):	3.1068831788902576
Encrypted:	false
SSDEEP:	24:okPcUQUj+aKCkPcUQUj+aK2kPcUQUj+aKt:D1BK91BKZ1BKt
MD5:	206ED7633B92C852935D8390A950A5CB
SHA1:	5EE571806A0B0E00DE7DA599FE8720C5F738F46C
SHA-256:	F8BFCA18E85940FA55EE53D77A72BDAC29CC6F4E079CD291382727F8D754E9A7
SHA-512:	E5B64A166FC885A5E0A729C8F81A0E200CAC3B3568F795023AF6DB88D761BA7D44B5B8ABEB180F722BE7A54E8BF33B72CF1014C004BBBF383B4273AC374A72A 9
Malicious:	false
Reputation:	low
Preview:	p..... .....vO8.....(..... .....&.....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."...p..... .....S<f.....(..... .....&.....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. "...p..... .....W.....(..... .....&.....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):	3.8089762766724706
Encrypted:	false
SSDEEP:	24:44V4xaVSGAmStkCVbn+V4xaVSGAmStkCw:zVnMGBScVnMGBSU
MD5:	0D62ECFE166A81786E828E7ABC3FD046
SHA1:	E8C587466F9B75D34AB82BEC982C4D0CA73FFA71
SHA-256:	D1D152BD388D6CE18D65EBBFC04C052577873E17638D0C349AB96CCC698B4482
SHA-512:	FC9C04C1094CF465FA9E9E0071B01B1ADFC884EBFE32780396340C956692D1924A0DF745B02128B61845CF59A3533EB178ED6FB4194BD77422F0923CAFD90455
Malicious:	false
Reputation:	low
Preview:	p..... .....i.....(..... .....$.....V.....h.t.t.p.:././.o.c.s.p...g.o.d.a.d.d.y...c.o.m././.M.E.Q.w.Q.j.B.A.M.D.4.w.P.D.A.J.B.g.U.r.D.g.M .C.G.g.U.A.B.B.T.k.I.I.n.K.B.A.z.X.k.F.0.Q.h.0.p.e.I.3.l.f.H.J.9.G.P.A.Q.U.0.s.S.w.0.p.H.U.T.B.F.x.s.2.H.L.P.a.H.%.2.B.3.a.h.q.1.O.M.C.A.x.v.n.F.Q.%.3.D.%.3.D...".c.d.e.8 .c.5.7.2.4.1.7.9.6.2.1.5.f.b.6.4.f.5.1.4.8.1.0.1.e.6.9.4.2.a.6.5.9.4.4.7."...p..... .....i.....(.....$.....=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.I.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\342ed5ef-a2fc-4e76-b001-8d8bcafb43ed.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):	155016
Entropy (8bit):	6.051395431989984
Encrypted:	false
SSDEEP:	3072:DWZ9M5muYQcRjh2bN53qzK89AFcbXafIB0u1GOJmA3iuRi:C9MIuYT8afYaqfIlUOoSiuRi
MD5:	AB0F031EA1EF8DDE49F10B805E5EF27D
SHA1:	CE82E3E8737442B801F7D31CEC79CA647E8BB977
SHA-256:	D86957B100BA677E0D7E0E137D73A927217C8A070C57A00A3E0C02C066AEE009
SHA-512:	6441EF804BB73490AC339506EB6F5512AF4EB6DC3EDCCBB49876AB1753BD2ADBB6F390C3A0076346D42B9E711628DCDB5284A567E3E74B2112334440A988209
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\342ed5ef-a2fc-4e76-b001-8d8bcafb43ed.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.611800580172949e+12,"network":1.61176818e+12,"ticks":98173914.0,"uncertainty":2768664.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016201951"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Google\Chrome\User Data\52071df9-6c45-4818-8295-c13cec1da427.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):	163488
Entropy (8bit):	6.081592349772155
Encrypted:	false
SSDEEP:	3072:iC3WZ9M5muYQcRjh2bN53qzK89AFcbXafIB0u1GOJmA3iuRi:JG9MIuYT8afYaqfllUOoSiuRi
MD5:	F4CD1A23A6D8551FB7621BAB6DDCF568
SHA1:	BE76A5172EF8822380D96C53A3D666AB3F848EF7
SHA-256:	BE7FDC3013FD2BE79FE91E0317DE382B514E2178D19B034710EDEB6DD86BBC28
SHA-512:	98D781BD609F7328A6A22A11123BD980C23E128E123B51B7034172DEED8F83082362F8C3CEE999DAF5EE2764C9117A91738274937EC4DA5D82A20D51CE0E5C7
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.611800580172949e+12,"network":1.61176818e+12,"ticks":98173914.0,"uncertainty":2768664.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Google\Chrome\User Data\7d61d366-6692-43f4-8447-b508a8a15d6f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.751455018030905
Encrypted:	false
SSDEEP:	384:rTduakbhgYH6RNGrzvay3JSMNHolGtErPMesxBwc0vrHKmLof8eqCRO48SNj1OHP:va1RCsR1Mer8usEfXGuKs6uB4
MD5:	E4884D85C6C069B2716ADB25F574E665
SHA1:	93408300CED9E7C864F6BF95865585C806E05384
SHA-256:	9D9F70CE5831B7F79BA646C1D7231EFD7419A84AB7D07D97B43DC9FA5A04C48F
SHA-512:	DDD1E4D113F0FB273CFBBBAD0EAA50F90ABE5AAC3360C91548DB73E07E105185958F19AF066721AECFEE12E5DB0C603FF5EA113B44D0D5A6BD73D3A50794EA98
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\8084aeae-8429-43f3-a620-cc677bffb762.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7518461121736673
Encrypted:	false
SSDEEP:	384:1Tduakbh8rYWVTV6RNGrzvay3JSMNHolGtErPMesxBwc0vrHKmL/xf8eqCRO48Sz:IWa1RCsA1Mer8usEfXGuKs6uBF
MD5:	371FF1F35FD4E9A059D8A87EB357B4A2
SHA1:	ECB27D335FB3D3884ADF7BA0D85E9E4105BB6D3F
SHA-256:	413153A45FE24EBC4152091B8A0EEAF691B50C3A3A1DD1A1431CA916190AE289
SHA-512:	876C6092122C2822570D8F1FCCBE67AE56EB7DB646B26682B18A0CEA0D9EC9FF3FF0D47ACD7EEB4398337B357D40099B54E00BE79AB9EDF576987C035772621
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\8084aeae-8429-43f3-a620-cc677bffb762.tmp	
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.... ...g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....* ...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n..../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\8bd31d0d-1e76-4b4d-9e93-12884cb63548.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):	163488
Entropy (8bit):	6.081591508821402
Encrypted:	false
SSDEEP:	3072:NDQWZ9M5muYQcRjh2bN53qzK89AFcbXafIB0u1GOJmA3iuRi:tr9MIuYT8afYaqfIlUOoSiuRi
MD5:	5B6533E0AD3E3DB1C6E5FF7D8B5E2689
SHA1:	F6A6CE51B80D985BF1FA91D77F63B7C9F46B1B9A
SHA-256:	87188CDEC325681D5A5D15926A460390CCAC91E33781F059230C1AF83447C364
SHA-512:	3B7DA84203C7B235154BDA4EDF53000014B9694E24043B1146C88A521068CF904A67D72F6EC410DB22DD18286A9380AFE06F9D5F9C29B386A2E0B90AE7216D3C
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.611800580172949e+12,"network":1.61176818e+12,"ticks":98173914.0,"uncertainty":2768664.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016201951"},"plugins":{"metadata":{"adobe-flash-player":{"displa

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\134f162b-a9d1-4a25-930e-9a6b889c78f0.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):	21278
Entropy (8bit):	5.552506429954764
Encrypted:	false
SSDEEP:	384:KBzXtguLlnCw2Xmu1kXqKf/pUZNCgVLH2HfDurrUI2HGVunTlOFOA84Og:KROuLlnZcmu1kXqKf/pUZNCgVLH2HfaD
MD5:	ABBFF837AC72E1E806ADE6F43753B99F
SHA1:	D32682ED18D6B31BCAD2402EAD86DEC6B52D0815
SHA-256:	0645A037BF0877ABDA0844B1B005A6D1D825A46E1AC8CDBDA886D63FD5FDC43A
SHA-512:	12C433F3E841540AAF8BE8430F71802DA0F4D3FED04E6CA1E4CD0B8E104A164DDA324152DB55F3D1AA5AA516B2E01E8D0AAD3ED5C8BD984D15F16AFD81B92EB
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":"13256274178181292","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\17e52a83-3fa6-4817-beb1-ddc7f856c0cb.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):	5385
Entropy (8bit):	5.19111029870323
Encrypted:	false
SSDEEP:	96:nj7pCpFszKyYVt0ecVayk0JCKL8yrKk3fMFEDbOEQVuwn:nj7pCpA7Y/0ec94KdrKk3fhK
MD5:	336FF7BAA59E289DCA36C78ECB23BCE3
SHA1:	7BC6B39008E66967E9146741E192E8761317FA2B
SHA-256:	CF521B7590C74C4EBA823FA41DD03517CDDF46C74C4757E235CAA70C10D8ADA8
SHA-512:	466CC86427891B35A893B24E1A2DCC94E8D2CDF4D15D7811A87E527E728DE502CCD0402B7E7733179BE2928D784EBD4815C22B9F2F77624CDEC07CAD266EC8 1
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13256274178468160","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\38f445d3-869b-4cab-b7de-cf17796946e2.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):	17622
Entropy (8bit):	5.58984582891774
Encrypted:	false
SSDEEP:	384:KBzXtPuLlnCw2Xmu1kXqKf/pUZNCgVLH2HfDurrUm8HGrTFO9843:KRtuLlnZcmu1kXqKf/pUZNCgVLH2Hfaa
MD5:	5463D5677B08EF0725911D327DA1CC31
SHA1:	C23032A2FF9082D6039E657C6F3B5C81D052765B
SHA-256:	F2671D6B63AFF5105DA79EE96FA76B184A472A3378A58B38868BCF92C4D0C882
SHA-512:	ACA13CD8563450BC10675BF73D67E3D5B9F85F9129A774D4F41AE400FAA56625F0ED04B5C83EBE98167F7ADCF741CDD46AD0FAEFECD6F363042812ED0694D4 8
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":"13256274178181292","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\397cde4b-9cac-407f-b085-2446c5db82ac.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3fbd5d14-fcf8-4a8d-94ae-32b21da9794e.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):	4775

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3fbd5d14-fcf8-4a8d-94ae-32b21da9794e.tmp	
Entropy (8bit):	4.969300738586644
Encrypted:	false
SSDEEP:	96:nj7pCpFFzKypcVayk0JCKL8yqk3X1JrbOEQVuwn:nj7pCpb7pc94Kdqk3Xfi
MD5:	7689F2E1717C51EB787DB41A74FE975B
SHA1:	4DE292EE665C69916B1B83E42DB2034A5BC4FA7E
SHA-256:	AE3D0ECBF97C230BBB6BDB864D03F8B3BCC1695C11B3C31E7BBEC55D597DA603
SHA-512:	3F2CB59D8A673752A2687E05C7B28EAA09E8801126A52F004CD6D27AF1D8749CBCAA5D751F42DB50ADDF918CE677359DC51F1E1A36A504335F82AFAC7931A0I 7
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13256274178468160","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4c236923-159d-4571-afab-c94df53abe9e.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):	22737
Entropy (8bit):	5.549198944217199
Encrypted:	false
SSDEEP:	384:KBzXtguLlnCw2Xmu1kXqKf/pUZNCgVLH2HfDurrUzpHGMrHGvunTlOFOve84b:KROuLlnZcmu1kXqKf/pUZNCgVLH2Hfah
MD5:	891B264793A7DBEF2EABBA8953C773BB
SHA1:	C707160BA0E3D8C4DE9D07CECE26D38D4E352E86
SHA-256:	30DC56D3A4ED8B9ECD023B784F21D67FA850013255D083E3DD0B144C825AA105
SHA-512:	8B2D58F7E66E740BA5AB5D0C8077552CA9F64747EDF1FA89F9DFF1E79A8E5674B5A9DB66FCF20893037B3206FB14199C34AA1B6CBE43A7D5F6140FE797626C3
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":"13256274178181292","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/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQlDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\79321b5b-0327-43c0-b414-2a3116a7cd3d.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):	21277
Entropy (8bit):	5.552490926525343
Encrypted:	false
SSDEEP:	384:KBzXtguLlnCw2Xmu1kXqKf/pUZNCgVLH2HfDurrUI2HGqunTlOFOQ84e:KROuLlnZcmu1kXqKf/pUZNCgVLH2Hfar
MD5:	65E600EB4CF858322A6AA8C2F50B1345
SHA1:	7F677D792BA06E3E63A95CE2E962A7057BC152A4
SHA-256:	BE5B2CBC6F7F15F0111ED55DA8CB3E4F0AC72BDAC6F8690AEADF2C99E7C84F15
SHA-512:	56E7031B4A4D14EB26FDC6CF72AD34A4758CF6A8BACB91DDC8C6AFC1F17D6546A8F27D717E9C949CFBA2B5A3EB18987D870CF13E184E6A4E23ACC57F1E542 3E
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":"13256274178181292","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/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQlDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\814b6adb-ec34-4624-940e-e1a9053c6587.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):	2713
Entropy (8bit):	5.591645290738617

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\814b6adb-ec34-4624-940e-e1a9053c6587.tmp	
Encrypted:	false
SSDEEP:	48:YTjUoPz75U95eUoJieUow6UUhYU9ZUo2mUonseKUeYPqUoq3U9pBsmU9QqPeUer+:mUoPJU95eUoJieUo5UUCU9ZUoVUon3KG
MD5:	C00D3DAD8FF9763A46649DD3A2B3A713
SHA1:	67D64D1993BF105DF32994DBD0D85651C799C99E
SHA-256:	39FAA5D0AAB4B764BABB7605E8FE55420B0D0217A2082B00E49B13E85F84D33C
SHA-512:	9A55A2BF4489657B70860C08C1F44FB9FFD8FDA844EE1561A43C0149D0BF945323EABBAB390061111D866479D2B5E535EA4FFAE0933C4B903CF1A054CE00F4C
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1614392645.025859,"host":"Dg14fIaciUHGX6Lc+OnYmaNiAA/ADiwumtIyPrC3d6U=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1611800645.025863},{"expiry":1627352646.111733,"host":"HS0xQK8RrrSZ/KdSgKIC7bLU+xijlimr9JuWvTPbfkE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1611800646.111737},{"expiry":1622687045.120903,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1611800645.120907},{"expiry":1643336582.154742,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1611800582.154747},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1643336646.500605,"host":"Y1cbV6ziZu1KjdKdxBzKmgzsZCYqaDEHWONjJAo942Q=","mode":"force-https","sts_include_subdomains":false,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9de9dd0b-107e-4eee-b8df-0e0e3eb51129.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	4700
Entropy (8bit):	4.8791306180176885
Encrypted:	false
SSDEEP:	96:JTCXGDHzPmKSN20SCLiN8J18kZt+Vw9d+daZGCGPFE5GPBSG4GrZG+V+hH:JTCXGDHzPmn20SCLi+J18kZt+Vw9d+dA
MD5:	79CC2D24649E501198898E49BB59D7AD
SHA1:	EF0A472B21F8DEBA1D82C3C2CC9D190B93A69626
SHA-256:	29C53E9F91FE7433C411D71BC17824CD56A80520E6C326437FE4359D42E27A3A
SHA-512:	4EBD699E3922F5B6F6A0F3CE76B6FE311F29670581BF7A164AFB173AAA66B646AA7C3F7EC6673D573AF846C57DF0FDC6B6FD8216DD87406FD52C82F8AC07E3A5
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13258866180899991","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13258866180904670","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13258866181170535","port":443,"protocol_str":"quic"},{"advertis

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):	5.262936763806145
Encrypted:	false
SSDEEP:	6:m7mM+q2PWXp+N23iKKdK9RXXTZIFUtpcZZmwPcMMVkwOWXp+N23iKKdK9RXX5LJ:smM+va5Kk7XT2FUtpcZ/PcMMV5f5Kk73
MD5:	03895BE65685D5BF847EBDCD4DCBD898
SHA1:	41CAAEFA0FF999B82BBA3E65245D47F2803197DA
SHA-256:	6846F90B399A912C2EAF097DE769C4DF249B8878972411A0D84FBF09401269D2
SHA-512:	17EBABA7D476245D343DFA4D5A5734FC9516D768B9807513A6D4A7BE79FBEB9666343A24AF99FE5EF142545F805F596565002DEEC85E1B0DDDA1B6AA4443D67B
Malicious:	false
Reputation:	low
Preview:	2021/01/27-18:23:08.443 1bfc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/01/27-18:23:08.449 1bfc Recovering log #3.2021/01/27-18:23:08.449 1bfc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.25527033686879
Encrypted:	false
SSDEEP:	6:m7rM+q2PWXp+N23iKKdKyDZIFUtpczSZZmwPcm1MVkwOWXp+N23iKKdKyJLJ:srM+va5Kk02FUtpczm/Pcm1MV5f5KkWJ
MD5:	69FD503236D5E0C83AD6A56540CDC567

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
SHA1:	E6F7D5900E70D44A4BAB5558C87DBF8781CA95D4
SHA-256:	D3222266BE9DC753A6C1531EA3B19ADE64ED0A7FDD1A46256080CDE732046EC1
SHA-512:	978F6C35DB725303CA49F7CD902D884022E6BC3EC1BA07874391ADA44C2C117F8BCDDC660B0FFB6DA521F63C1AD2281F7206FFF7DDDF77E5BBC06A3013011 E
Malicious:	false
Reputation:	low
Preview:	2021/01/27-18:23:08.433 1bfc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/01/27-18 :23:08.435 1bfc Recovering log #3.2021/01/27-18:23:08.436 1bfc 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):	5.588248022131172
Encrypted:	false
SSDEEP:	6:mqYQiiGEqCfrgdJ+HgJ7kHN6chTBlhK6t:six5fUdMEuN9
MD5:	A8AB434F070FA6B294B4990DBEC2B817
SHA1:	C07A792F3A10DB600FDDDDDD892E94688C6621CA
SHA-256:	05820CE22592CFABC00E4A662AB749D45B0789C41C2E8096CC3BF3166B284431
SHA-512:	411A47E3D4E3C75DD7D8C07985CE07A58845815D915481593FD09EAF0A2BE2D78A7D95312479617FD696E1D58BFC46F115E8BB253A6D3362CC11BECFDBB669
Malicious:	false
Reputation:	low
Preview:	0\r..m.....E...W..g..._keyhttps://quip-cdn.com/8537vty5Chq4BaEBxXH7sA-gz .https://quip.com/.!.../.....n.....b..!A.@....U.dN\...}..P5._<..Q.A..Eo.....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):	5.5903233122944815
Encrypted:	false
SSDEEP:	6:m1YGLSmXZCLRr7xgfOzgIuhcjumUiXLkAtlIZK6t:eXnh3mUi7l1
MD5:	5A63B35CDABAB0DDF83053B5EAE97CA1
SHA1:	65553A8457A4DD00AB66AC47E04EF29D48417CC6
SHA-256:	7D7F585618CC6307E69BC5F47437991219304D164AFCFC9ED3D653EB2361D15A
SHA-512:	1847150C206286CC10A4C9FD3245D15B121539AE9F16EB3021058D47257173A6685ADCC07B36A1C72F8CFE317522F53B301CB719A99F9BFB7379E5D838F979C8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L...Z..H...._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-WBS6NX .https://quip.com/..../.....9.....w+... Al.(ho..[..m].A..Eo.....B.....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/ULMdaNogoogPahvScxqd0hZhvzQK6t:8rU55hv++vc
MD5:	71764AFA011C29A97ED798DD1C3032AE
SHA1:	B3772A629F614C86C244D9724F2A7244F7DD7E7D
SHA-256:	5BC0BAB0CB3916EA810E001C2664397B40A707F22B52D6EDE1029D33FBC9EF7A
SHA-512:	7B6FE041A7BCE1FFAA61D18956FB6DC1EB9868F43EEC320DD3CAD539345BE91ED7875E3A57B81FC0D81BD50C8EC6095EB2C759AC0F014A50024A94C8B2AC1 19
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M...u../...._keyhttps://snap.licdn.com/li.lms-analytics/insight.min.js .https://quip.com/R.../.....?...`?.....U!v@..zW..=..q.....A..Eo.....M.V.....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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\44a148030134590f_0	
File Type:	data
Category:	dropped
Size (bytes):	201
Entropy (8bit):	5.432928216415383
Encrypted:	false
SSDEEP:	3:m+lt1AntLA8RzYzYlIL+RXHTLZuFvDthKAo89Kt/lHCQqWnWuAA/EUmJ1lpK5kt:mWAnnYMlXzFQgD5tgsWPAM/3K6t
MD5:	DA299BF3C3B3B142C16941243713BE79
SHA1:	A7A54B33341B953DB5F5BEA2A2BFE33719F40544
SHA-256:	D9E049BBB42B5071307E578657701F89B91190FFD12A450BC4AB7CF31C844DB1
SHA-512:	3A4F90EA2AB62CDFF9805047EAE42E4EAD7A552341CDC3E48C63528CB93FC95378D682BA2081A22868FC3F81CAFA571E1F30A6C90709AE31D2786F0D1031F0E6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....E.....B...._keyhttps://scripts.demandbase.com/841642b6.min.js .https://quip.com/...../.....5.....d....5....(..G1e1<.v..d.].w.\..A..Eo.....v.....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):	5.330867660126546
Encrypted:	false
SSDEEP:	6:m/AEYGL+MIwJJOg90og93lgymbhVDOm4shK6t:EAsIwvP9Cifmmz7
MD5:	BF4A380DC64D3333CDD30485B85625A4
SHA1:	11542BA3D7729873C5CEA61AD6CC143941BEF340
SHA-256:	33938D2B230CDA06AD153E5883875A52C931E98D5D404D550BA7C8B41EEDCBDB
SHA-512:	E30C9166D06EC573E6A70CE928B810473785252B4FD700201BE663790EA56C544F241D5AC44123B95D4AAD0EED5EF8D297D07E8472E40580E172BE7D3ED4BC6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....D...I.t...._keyhttps://www.google-analytics.com/analytics.js .https://quip.com/v%.../.....b.....l../l..a...0w.A..Eo.....%h.....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
Size (bytes):	211
Entropy (8bit):	5.61765461052487
Encrypted:	false
SSDEEP:	6:md/XYQisQBwCZgnugVtKs+P7aYW/ZK6t:wU1wZlKs+PuFr
MD5:	3ECC43ACE7EDD0C8F9765ACAB37F6E07
SHA1:	E271F572CAF615461418CE1C93841BFADBFD8D22
SHA-256:	FA41AE2EADEEE0DCF3AA2B33AD35ADC9FBB32E5E6AAB6EF3E20D5C2981F329E6
SHA-512:	A857C6E41E2165ABA2B68C7BF588BEB800B30B800A274373DF68A3774B61C57ACD6BD20878C8715B6E627ADA6E3DA7A654A0DBF243E9FD0747ECB6468483646C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O..../?;...._keyhttps://quip-cdn.com/xhZBtVClR2EcdOOOPl8eYg-ancillary-gz .https://quip.com/.../.....T.....b...m..s.....r.A..Eo.....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):	5.327673317008707
Encrypted:	false
SSDEEP:	3:m+lD1ztla8RzY4rKUKbbXRthKt/lHCTpklE/JamfNXy/zK5mpEI/llpK5kt:mE5nY4rkvXrgtgT+Ef74pjhK6t
MD5:	0FAEE47DC867740C1CD1D60CAD532FAD
SHA1:	0B4AC881A56F80C218789EFA1CC72D8A6B7B4D7C
SHA-256:	3A7D11A454B396796C49B591705ED8DB63BABA540CEDCA2790BEA0738C7149B6
SHA-512:	85F9CAEDC43551C336CF1F0ECB23C2960AD22615A2F9386029E6D3599079BE74D0C27FC3AFD205D1615DF428B99525BDBACB71BAF23CCA9D1DB5296FE7698AD
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d978b0efc727804e_0	
Reputation:	low
Preview:	0\r..m.....:.....RV...._keyhttps://s.adroll.com/j/roundtrip.js .https://quip.com/...../.....HU..2.....$j..E...c.....A..Eo.....ay.....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):	5.8704559900675655
Encrypted:	false
SSDEEP:	6:mQ0Y4rgdsPDYQvnafjh/gSWurgdK9/gztnrV2ATl3onK6t:87LBnwjqSdUl9OxW
MD5:	6867889A81DFBBD5A7E1D1605F3D1C56
SHA1:	300CC8F5F7985104A77895D8691DCBA3AAA2908E
SHA-256:	9D70B472035642FA8E9C37BCB5231CE12357FC29A44AEF169769FD3296185B7A
SHA-512:	162389FA3F13A2B4E310A53E6B21A53F3B013DDA63712FA25D8DF82918ADA50B8060A56E123D27D01750C14FAD2392A4DDB008BAC4755E051A017D2C2B126C9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....y....._keyhttps://s.adroll.com/pixel/VNM53VCKEFACRMFQE65VV4/IB7LZPOS3RCN3J2MSNRBFC/X27ESS35BFE4LKRZIE373P.js .https://quip.com/..h.. /.....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):	5.015874158285975
Encrypted:	false
SSDEEP:	6:1tGW0pSiUHSHpKXD5aqj4im2oazQ3zbn3pHkQ+IRwH4:KffpKNaqj4im2Zzyz7V4h4
MD5:	2BE36AA2A49DEFE48CF01015F25EDA3C
SHA1:	AE9D04E0C19FC5EBB99BA3F9AD140E9F35B87EE4
SHA-256:	C318AD033482E2C3FAE038BB3E01571F1417D1A20C81AB1EF3DB2DB084097301
SHA-512:	E3F3B491225999BCDBCBC609EBE1E403FA05B7DA95B8501F3D60C69591609708B6F086D2C58C327019F8503EE2E0AD586DCB7E96D56EB72C0F2943C87919CCE C
Malicious:	false
Reputation:	low
Preview:	.....oy retne.....e]..0..@..../.....Y4..H.D.R.../.....N.'..x...../.....o...g2..../.....=z...../.....-.Qrl.&..../.....B..x...../.....K..||m".@.../.....^}.Np..@i kt../.....-..0..x@ikt../...../...3.KPu../.....KPu../.....&<..\.O$.KPu../.....p..(....KPu../.....q...._.KPu../.....+<P|...X.KPu../.....i..../.

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):	4.296920102420629
Encrypted:	false
SSDEEP:	192:zueNMad8YuUJKoo1rWOuyOjO4yx/Y8WRnvXX:p2ad8sFkrWOzHInvn
MD5:	14A4BAF62B6B565ADD9D75334197FF81
SHA1:	203FD70327F682E78CF888B63FE4F67D61863AF3
SHA-256:	9B7EAC92FCCD2EDBB4129ED8716C17BCD4EE2185B9F833704C720AA5A0AF8744
SHA-512:	DEB7EC0680C08475352B437551DE5E1DC42F7D81251D50A6A2B472797B355753FA552E301903353CD61C0B943AC4BB5D747603348C943DA80C66BEC02ACDAFF
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):	0.96806854789575

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Encrypted:	false
SSDEEP:	24:pcLgAZOZD/YxqLbJLbXaFpEO5bNmISHn06Uw08:p8NOZYxq5LLOpEO5J/Kn7UX8
MD5:	E86AD16ADA8D2B1661407E2C79D135B9
SHA1:	4D16AB091742C8E8D585E1D06031F91004F9C1D6
SHA-256:	81C9C41166767406C3DB97FC9A3957751A9D34636528703A6FBF92C69BA00A2E
SHA-512:	8C26D4EFA9D4EBB063282D124BEB0FA61B698AAF982ADC8E7B7BE101B852D43040A21E8B2AC7579F76A6A47DCAB52E1FC4FD9235B143319A51C0F0337F9C55C5
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1909
Entropy (8bit):	3.58824284816239
Encrypted:	false
SSDEEP:	24:34SheV85lyJTqPyql+lV/MKfZTqVHoZTqlW6swmlulV/A3pQJ1pRTqV2llJlh:346quSqP7+l2Equhqblul6pQJVqc/rh
MD5:	FEC77F5C7BDA947E72D2121BCEE4CFD8
SHA1:	EAF5A02A4F3EAE98F67EE8FD060B41B85516A374
SHA-256:	D342AAE6E15B861D15978D968EBF06604F21C036C9E2EE6930BDDCCEA626C3B7
SHA-512:	47A120A549D422E6909FE8671EF27C36559E5C03D7CD6179B842F553439BC531CA16660E128780AB5DA3F74750A3CCB482DF0947926BC638991BA3C2456F81C3
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...ccba7500_1361_4718_b325_0d598da4f064.....`l.....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....https://quip.com/OWCGAwI8CpAi.....Q.u.i.p.....h.....`...../.....0.....@.....X.....X.....B.....h.t.t.p.s.:././.q.u.i.p...c.o.m./.O.W.C.G.A.w.I.8.C.p.A.i.....F.....o".objectId".QQAAAAnpLQ3".secretPath0".navigationKey".~{.....8.....0.....8..... .....https://quip.com.....https://quip.com/OWCGAwI8CpAi...../...../...../.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	57
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlXNQxlXNQxlX:qTCTCT
MD5:	41C7D1373DE8E7BD508C548A70910E51
SHA1:	F919499049571C75C7EB73FDAAA5198E6DD641B6
SHA-256:	99C59CBE7DB56D56A286485635E4467004641C6275E708887DD35728EB05109A
SHA-512:	C30CB4EA2478FD816B4A160626B08CB63D2B9DC50EAB694607D44D05117E6AF8DD707BF4E14CF001CF69007A654ADE55149A61ED07F9DE6A9A2EDCB51AFA0773
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
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):	317
Entropy (8bit):	5.201117078689573
Encrypted:	false
SSDEEP:	6:m7p3+q2PWXp+N23iKKdK8aPrqIFUtpcdU2WZmwPcXNVkwOWXp+N23iKKdK8amLJ:sp3+va5KkL3FUtpcxW/Pc9V5f5KkQJ
MD5:	319C06160AFA4D69A37864747C1430F6
SHA1:	A5F93CAFCDACDFDC92964840F1E2ED909CB5FFA0
SHA-256:	16B12C853823138A6A0B68381C186D705F9C1FBD9DD63E36758B9C718219B7CE
SHA-512:	D1589BB02E9A96CC81E0DCB2428CDBB0D361611E32D8EEFF3E1DD106C609DA36FCF62FE6B5F05586BE42787C16152A4F1E6411399712A74B4070D5E65D1DD5 D
Malicious:	false
Reputation:	low
Preview:	2021/01/27-18:23:08.015 9ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/01/27-18 :23:08.018 9ec Recovering log #3.2021/01/27-18:23:08.019 9ec Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003. log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.143044828273374
Encrypted:	false
SSDEEP:	6:m7fq2PWXp+N23iKKdK8NIFUtpcbhZmwPcb7kwOWXp+N23iKKdK8+eLJ:sfva5KkpFUtpcd/Pcv5f5KkqJ
MD5:	5B0C1E2D7E1930E91A2197725AB16871
SHA1:	E98B3BF57E4F7090F3173C6D29EE9B69BEF69204
SHA-256:	82D0F20A7E32BED850912ECB9CB56FA6B4CD232A37C2CAA045C78ECC81AC996C
SHA-512:	D4F8891F23BCBC02AB4376029BA644140AF570791371B30FA64C2156CE3A272C123F7B83EFB7883E1DC591735B7899A8C7AA138F396E677D38346AE32B0707B0
Malicious:	false
Reputation:	low
Preview:	2021/01/27-18:23:00.441 100 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/01/27-18 :23:00.442 100 Recovering log #3.2021/01/27-18:23:00.442 100 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

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

Entropy (8bit):	6.061511031838911
Encrypted:	false
SSDEEP:	384:ahlZ97TC4hNLFkQF/4H/vo3c93yaM5ZAVGnLMeP3rrBsuzfccHyfXRH0MVEPT:ahlvS2Fk5ooNM5Zg+YePRgpXRHLVA
MD5:	58E0F46E53B12F255C9DCFD2FC198362
SHA1:	24E3904DED013ED70FFC033CFA4855FBB6C41C19
SHA-256:	F82EEF4F80D86F5DEF0F40F91FFB6453E1706CA5FD8A7172EDB19C4B17E2F330
SHA-512:	1AC83CDFF124E4C0281FBBFC0A919AA177F1524AB85434D82E5A87DDDF7CAC26A761C5E6249566626054C62D6B0F46A51AAC1F6E64C260F50832AE1D5F0A49I 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=","AuXwavx8SOtkgFhnRlnM4rolw243Ryh2ktL0QZRDLoE=","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:	1AC83CDFF124E4C0281FBBFC0A919AA177F1524AB85434D82E5A87DDDF7CAC26A761C5E6249566626054C62D6B0F46A51AAC1F6E64C260F50832AE1D5F0A49I 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=","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):	1.389250937717782
Encrypted:	false
SSDEEP:	24:LLwxh0GY/l1rWR1PmCx9fZjsBX+T6Uw3qQ3gC1FXdEzuDgznoB+qgcN:yBmw6fUCqQ3vrmzuDmFqgcN
MD5:	6CD06EEA661E8681AAA80D4231FACCCB
SHA1:	7AC1E4DE757AAF7C7D0A50102FC0B93A87550350
SHA-256:	4DE4630CFCEC9E54EB332374D6F91400914496E205A209FA21E4641E7A032396
SHA-512:	751E09BD51E62EEC0885FC14F2750E16A898A55BE378D54FD4590FAE0241EE32F2A1168264188F37788E28944EAF285F740E2CC8DCF10703E84343FD8B981F37
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):	0.7772312925259401
Encrypted:	false
SSDEEP:	24:uH6yLiXxh0GY/l1rWR1PmCx9fZjsBX+T6Uwiz3n:uH6dBmw6fUrz3n
MD5:	4C95A65B359480C8C47AE03D581DEF75
SHA1:	EC4CE9CCB588BA9BC7A18D44D4FB02109996E912
SHA-256:	937B860CAA1CEC5582BE188AE84F0233F52F9F7D987335946228212E49C0A5AA
SHA-512:	808C4A2112AB3C79418C038EDD5EAA17A44894C60DE34456FD746B8F4D04F0B5BDF2425FE0B060DFCAEE78EE8239F95C7B86BC48E16B7FD3BB99A687A9F304C
Malicious:	false
Reputation:	low
Preview:	.....u..... ....

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):	5.2562390194732025
Encrypted:	false
SSDEEP:	6:m7xIqM+q2PWXp+N23iKKdK25+Xqx8chI+IFUtpcqDGXZmwPcyMMVkwOWXp+N23ib:sx/M+va5KkTXfchI3FUtpcqaX/PcyMMs
MD5:	A657EE5245B7D84EB42D004326066E58
SHA1:	FB8E6E8FB056F490292F92D21091EA78DD46EDAB

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
SHA-256:	1806D8E76279EB94D577671D1F90F4AE5DAC640C0AB5321717CDBBF22C5776F3
SHA-512:	5D663E6A5F2C25D253059DA1618DB74F2ADCEA99B93C5FDD0834F67B8C522793A1A533BD5FD0973FADDAC80EFB40DCE2B1ACAFFAB65ECFA162EFC15DB53C99F2
Malicious:	false
Reputation:	low
Preview:	2021/01/27-18:23:08.329 1bfc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/01/27-18:23:08.331 1bfc Recovering log #3.2021/01/27-18:23:08.332 1bfc 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):	5.236171812327075
Encrypted:	false
SSDEEP:	6:m7b+SMM+q2PWXp+N23iKKdK25+XuoIFUtpcJGFZZmwPcTwMVkwOWXp+N23iKKdKl:sb+SMM+va5KkTXYFUtpcJm/PcTwMV5fR
MD5:	CE7D37E50873CBB0A6647A9145450142
SHA1:	78446002169FF1A0B69E42D0395FA82E8B2CA255
SHA-256:	F229A2BE40CC5E1BB26721E5C1EC47D27D1FEF725E43AB0C8C6FC5D2841C620A
SHA-512:	4682167A6E967F6CDC07013E2D1B621A94227FEAF2049CA6CEEDF7C8EF0D5B0AB2415BFE68AA8383DC9CDACD7183BD6996483C11970076E6AB01291F8C5E547
Malicious:	false
Reputation:	low
Preview:	2021/01/27-18:23:07.910 1bfc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/01/27-18:23:07.917 1bfc Recovering log #3.2021/01/27-18:23:07.918 1bfc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.241288917057461
Encrypted:	false
SSDEEP:	6:m7wq2PWXp+N23iKKdKWT5g1IdqIFUtpcxZmwPcp7kwOWXp+N23iKKdKWT5g1I3Ud:swva5Kkg5gSRFUtpcx/Pcp75f5Kkg5gZ
MD5:	22899EB9B25954E6C08A9F65D6242976
SHA1:	D73365E0C880DCF1AC7EB2B945B0553F289E1534
SHA-256:	7F607FD5C0B4BEE1A2A4FE0E6F51CC2F9D2FA02F8908174537C103CCB4AD3643
SHA-512:	E6AC7866E37B582BDB39AA3FB45407D1E1705A569F8B0687F6A9939D914D4D1EF2BF4E6F6ED2F652356A1D8CD97CB2C87A3C843B107E0ADFD28D4568195BC95
Malicious:	false
Reputation:	low
Preview:	2021/01/27-18:23:07.788 12b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/01/27-18:23:07.797 12b0 Recovering log #3.2021/01/27-18:23:07.799 12b0 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):	0.23134388468794498
Encrypted:	false
SSDEEP:	12:TL+A/VCZ6fhxq73ZEjae00dJ+Hi+ZQiLkkpCFsOwrYRsAXLxKxqF:TLxViYqGtiHB7nCFsOwVfqF
MD5:	E9FC10087E68AB22F0344544CDA55FDF
SHA1:	1209FAFB32D485354FAD4E3BE889D898DF7DED74
SHA-256:	28C4E1DAF778FC999791A83C43F5F7FEB3EAC6267B83BFE85EDDCEAFD9158FBB
SHA-512:	2658844EF89D80380239C1F7AF135926F27CC7B1BC2B63A52F6C07E0A6AC4D87A836C2D10AB6A2722C4FF903A89685CD7AD7BBD8C501C39AE1377E0BFB426F8A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
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):	748
Entropy (8bit):	5.53219177996347
Encrypted:	false
SSDEEP:	12:q/VUR5r1pcVMTDP5vU8pEnl5MZI73V5h79kjDJWKBk778B/xgskZBaS0UGdxqzph:okuMjpEMi73Dl9AgIY78BJgskfaSJmqv
MD5:	B4DAA8E27A42D5D70E25D56513E24B62
SHA1:	711FEC5E675BC4FF5B1A567EC171631A6254C075
SHA-256:	D9799061A2E9D4E4A9373269C6363F61977002C5ABE73DD08B4AA1C3DECBCA48
SHA-512:	952A985CD8BE4C3D607D72287BA8EE210690A27FDCE3C23E770A436A4A43CC25538DDEB410765DA4B26DDE0632E311D5A639B428AAAFA71F86CD3579782440 3
Malicious:	false
Reputation:	low
Preview:	....."K....access..com..document..https..owcgawi8cpai..quip..secured..shared..your*o.....access.....com.....document.....https.....owcgawi8cpai.....quip.....secured.. ....shared.....your..2.....8.....a.....c.....d.....e.....g.....h.....i.....m.....n.....o.....p.....q.....r.....s.....t.....u.....w.....y...:S..... .....B..... .....*.https://quip.com/OWCGAwI8CpAi2*Access your secured shared Document - 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):	0.11685039638865269
Encrypted:	false
SSDEEP:	6:O3xtTk7svg9bNFlWCj/l7/l3l6+04/fMt76Y4QZVRtRex99pG/6SqR4EZY4QZv8s:OE7svqLBj/j3l6z4nMWQA9L/BQZ8fOdn
MD5:	EAEA80610F73CC23978BEC5C441E93CE
SHA1:	7708A2D81C16114F21A1823D2A6E389D73EE31BD
SHA-256:	982D2E0FA055F9AA7ADD376E21A291D98A293200F1D5C3EA48D4A5137D260E0C
SHA-512:	D95E20B418A451A6B35EC28FB26C26EF38B3118C871205570AC7D5C13C916BC26A758FC08FC426A6963959EDD87F7F540E9F91055FD64AED2A786F3C3AA03A2
Malicious:	false
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_quip.com_0.indexeddb.leveldb\000003.log	
Size (bytes):	1045
Entropy (8bit):	3.7016118986071485
Encrypted:	false
SSDEEP:	12:6XRMDj0yFpXNNRj8l2Uhdsillvw3hOajcyOTHMewsvH/chYtB8FQ9flXVlsn:rnNf7o2Adn/+FjcyFeG2F1Xs
MD5:	10449FFCB253788415B2941651E862C9
SHA1:	8EDF489AEF999BE2B7E7454DE34FFB1CC33C7973
SHA-256:	00FC93C113DFF6B02FF101B4680EDC723D1FACF69CF9D230CB70B505FD8A849C
SHA-512:	19706169FD3E0CE15A287F77BDB41D86AEF34B1F6100004ECC3DF6F0C3B9FBB92FB95A6329692184CD88B9A2EA2BB8A874953EF127B27AAF74F04E88FA0B2D0 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..........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...........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...........

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):	167
Entropy (8bit):	5.32461487203481
Encrypted:	false
SSDEEP:	3:tUKaeEyUSQWKKqFkPWXp5cViE2J5iKKKc64E/x14kUg6Vw/IrscWIV//Uv:m7nyUOq2PWXp+N23iKKdKETg6OVIFUv
MD5:	8DDE27724C3428929D930E79E0E6476A
SHA1:	9E0FA7219B9267F48D7F148453AC8DF74AEAB267
SHA-256:	58D8481B01A24848F1C56ACC5EC0D06F4C346C2A168DAA78D796584EB4349174
SHA-512:	276BE5F8E97E2F1E477F71E418FE853674FFB3AB9D87F5B7C68D5C623D37684EDC03989ADB2FD80804079E53FDBE851E083CC96D61FCFDC3F92B35BDE92E41 B
Malicious:	false
Reputation:	low
Preview:	2021/01/27-18:23:03.270 100 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
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):	5.557210354026998
Encrypted:	false
SSDEEP:	384:GCL69VmuHZJvaAYKuPPogNh3M3gY/4327/vcJhH12dxKDM9VUD6/K4uJToeXo1pw:l+gY/4mGlx
MD5:	5C7C6363E92C8567FBC7BB9BFC9E11BA
SHA1:	26AFFB820557E4AFA1B0CE156AAD1BB594E9CA34
SHA-256:	E244D7F3802B7CF2A80D40E79F36BC709CC93E515EEC6C3A3E77DE1152C0BD81
SHA-512:	BB29C3EE6EED6E4BA0492E73D63B99907CDBE087479C1634C11E44280BDDDF5526170C040FA2A9A10F831D852027976BF30BFBECF799E83D6CF22D9F913603
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Reputation:	low
Preview:	.n,z.-.*.....C.....META:https://quip.com.....N.&_https://quip.com..activity-recent-ids..[{"id":"QQAAAAnpLQ3"}].-_https://quip.com..activity-recent-thread-ids3.[{" id":"QQAAAAnpLQ3","secretPath":"OWCGAwI8CpAi"}]./_https://quip.com..folder-prefs-expanded/groups..true.I_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\": \"ixM9ACe C9KUb\"}, \"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\": \"cLRA AAKWPCD\", \"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):	329
Entropy (8bit):	5.179499185181751
Encrypted:	false
SSDEEP:	6:m7f4bIq2PWXp+N23iKKdK8a2jMGIFUtpcf4HZmwPcf4lJkwOWXp+N23iKKdK8a23:sg0va5Kk8EFUtpcgH/Pcgf5f5Kk8bJ
MD5:	AF2D7CBF93CEEF38739D002B6C502C34
SHA1:	74EA069DF2659E69D60EE6A7F45E2BDC22C72E2B
SHA-256:	1407E6D88A332BD7DB7AE132B18BE3EA9ED5338FFFBE1D60A5AF78E5D9C95996
SHA-512:	1B328677E11ABD05DDF578BF59CBBF5B987C1B0B6E320F085FE479D8D352AAF7733F0D57F070E619993F69251435593CE43F69947E4DA3A4366AC4BEC6BF585A
Malicious:	false
Reputation:	low
Preview:	2021/01/27-18:22:58.257 2f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/01/27-18:22:58.259 2f0 Recovering log #3.2021/01/27-18:22:58.262 2f0 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):	331
Entropy (8bit):	5.216134635633482
Encrypted:	false
SSDEEP:	6:m7f4ulq2PWXp+N23iKKdKgXz4rRIFUtpcf4zhZmwPcf4z7kwOWXp+N23iKKdKgXS:sgulva5KkgXiuFUtpcgV/PcgH5f5Kkgi
MD5:	A241B5D87B1A60B4AEC9FA67B3B344BC
SHA1:	3311787548FF73F54AD9C768B87F6AB7F98B8601
SHA-256:	16EF809E9630910A53370AA39F53575259631F9B50F19C952EF42BD1061F8C36
SHA-512:	CE235C11F14F495EAD08F28942FD9390CEAEEFAB601A9F9D6D1D1AED33D888562FFFF95F74481917F22AA85FB0495AD853A912D992B527A72E474CB69A51A11
Malicious:	false
Reputation:	low
Preview:	2021/01/27-18:22:58.669 100 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/01/27-18:22:58.670 100 Recovering log #3.2021/01/27-18:22:58.670 100 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):	0.4769969847319502
Encrypted:	false
SSDEEP:	96:vCIG+6bDdsDaBJvtHIm50I4sX/CIG+6bDdsDaBJvtHIm50I45:a96EJTv4sXK96EJTv45
MD5:	AE4BFE86B1425A74F3F6802998DB8E1C
SHA1:	60DD61BAC02F3EC073857A489BDAB4F5E0079EB0
SHA-256:	C09C1328CB471ED67EBC278F38510ED1AFABFF9A1C6835E9848660C3D850177C
SHA-512:	87FF1BD87D02C7AEFCBBCDA02397FDC6BAFBB2AEAEDFB623304ED8B463DF081D58FE4B4EF118DF1D67A077F3F2B75B5043A983B70247540ED3BE46749A4EBE24
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):	0.6537298447748484
Encrypted:	false
SSDEEP:	48:KMjoqzLbCIG+6bDdsDaKgJgKtHIm50I9a+UX5:KqosCIG+6bDdsDaBJvtHIm50I4z
MD5:	EA230BC6C82826D9E349B46AA5B8A63E
SHA1:	30B988B7434B3770E82A2F2368C2820EEA77436D
SHA-256:	D16E6024856846E5C4A04AC4216C62C2049B7CF9D102671D2A2FD440ADB7D7FB
SHA-512:	9B1D6C8F930708D0F63864267C76BF1C3B87D1BD7F47A4E5A2122A089FFF4095F4C52469CD68EFC1CAE8FDD02F4BEDF4702302FA2F046177E5BCC709527DFFA A
Malicious:	false
Reputation:	low
Preview:	.....dYa..... ..... .c..... .....0V..... .....

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):	4.508697550925635
Encrypted:	false
SSDEEP:	6:5l2lai930E7ePewrgRptOLxMAmgn+TSlkTSlkTSlkT:5l2XlCewURpyxB8TSlkTSlkTSlkT
MD5:	FF86D4AF28E844E808B27B0E47F86B7F
SHA1:	39B88CB193CAFE1E0BA5326BC589353A0BB1BCBA
SHA-256:	0075BB741E35A0421A43D31FF81625528CAEE8609F3AB31815760F86CBE28306
SHA-512:	5BCDCD3D259105268607118876D14D735D852DA8879311400D9321DFFD70A5D1DBA07791C00F9A3DC79160E0AD83E72CEE6741A9B9CCF5D3F0A82B729F8DC1
Malicious:	false
Reputation:	low
Preview:	..&f.....w..._.....next-map-id.1.@namespace-ccba7500_1361_4718_b325_0d598da4f064-https://quip.com/.0..A. .....map-0-quotaTestKey2B.l.....2 B.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):	5.184214210972149
Encrypted:	false
SSDEEP:	6:m7f40Jn4q2PWXp+N23iKKdKrQMxIFUtpcf4NF3JZmwPcf4NF3DkwOWXp+N23iKKS:sgG4va5KkCFUtpcgNNJ/PcgNND5f5Kkf
MD5:	7A89391E814439494790B70863155195
SHA1:	4E80C02AFBFCC98CF733BC71A1058766C7B2420C
SHA-256:	45531DE463F839D59A29ADDB272D7E9EC174D754628832181 99EFD2F295E0A87
SHA-512:	54CA153DB14481AF9D434C6578673A1FEE3EDFAC128DAF63C18B1E9D22BA5EF0935B8A4A90E59F56008848E2F97852429019558FBC74808CF9B91D551397B39B
Malicious:	false
Reputation:	low
Preview:	2021/01/27-18:22:58.421 15f4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/01/27-1 8:22:58.422 15f4 Recovering log #3.2021/01/27-18:22:58.422 15f4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/0000 03.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	345
Entropy (8bit):	5.209782584659976
Encrypted:	false
SSDEEP:	6:m7f46mtN+q2PWXp+N23iKKdK7Uh2ghZIFUtpcf4m5ZmwPcf48CVkwOWXp+N23iKm:sg6yIva5KkIhHh2FUtpcga/PcgT5f5KF
MD5:	7E12D961525BE9D767BD093A0C8C551B
SHA1:	63394CFE3164E88CDE82D156E5B019974B878C86

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
SHA-256:	73EB4B129E9D384D924B1D38C430965E5744EF6BBBFD747D827D8AF1FA4AFC1B
SHA-512:	FECA4FCADA35B6F3A8D115B54CCA33D3CCDB5C40AB1379AA521227CDEEDEA8D9096DCC69675A731F78F0237BDFAA291161B0E5588B7ACEB928A3C5DAE6A7CA0B
Malicious:	false
Reputation:	low
Preview:	2021/01/27-18:22:58.162 988 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001 .2021/01/27-18:22:58.163 988 Recovering log #3.2021/01/27-18:22:58.164 988 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\2fd3e0cf-e507-483c-81b6-f3e988000ef0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
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):	5.274458274505184
Encrypted:	false
SSDEEP:	6:m7f4A34q2PWXp+N23iKKdKusNpV/2jMGIFUtpcf4VJZmwPcf4aF3DkwOWXp+N23e:sgS4va5KkFFUtpcgVJ/PcgYD5f5KkOJ
MD5:	67ACE4E604425DE1670A25006241C42C
SHA1:	F9D38872937AB5E17DFE5C334E29AE94D0351FD6
SHA-256:	C2D749B7B9F8A994F94828352C35CC18F39716753E2536EFF2E08B4FD7E751DE
SHA-512:	688FF778A0F3F2F2B536C2431B60DA78851EE20FFF22E0C3D4070A9BCDA3B13A36601CDFB4EDC45BEE93530871F395383F4D23C3EE1A2142D361A0942F92FC8
Malicious:	false
Reputation:	low
Preview:	2021/01/27-18:22:58.450 15f4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/01/27-18:22:58.451 15f4 Recovering log #3.2021/01/27-18:22:58.452 15f4 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):	5.323225242876995
Encrypted:	false
SSDEEP:	12:sgL4va5KkmiuFUtpcgm3J/PcgpD5f5Kkm2J:sAKa5KkSg+LqGVf5Kkr
MD5:	4BCF9E2CDAD28B603B3F67D785407B93
SHA1:	ED8C00958B4D71B0101E49B140A0EF591ED50B5F
SHA-256:	B806B66096B3D8F64FC5BA418FF954BD43843491287D67D42C958CB87BC7AC57
SHA-512:	E40A3CF5670E335E1FDA89068C63F044567E734D71E5F4EDB8ADB0C85B3E3C0F3ECC53EF04189DB2FFC08696110E732A457BD4FCC65C74D6648B0E65CC7C03B
Malicious:	false
Reputation:	low
Preview:	2021/01/27-18:22:58.736 15f4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/01/27-18:22:58.737 15f4 Recovering log #3.2021/01/27-18:22:58.738 15f4 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):	415
Entropy (8bit):	5.316722249454756
Encrypted:	false
SSDEEP:	6:m704+q2PWXp+N23iKKdKusNpZQMxIFUtpc0lJZmwPc06NVkwOWXp+N23iKKdKusx:sb+va5KkMFUtpcCJ/PcxV5f5KkTJ
MD5:	5E8E4E2B14228B4D2F368A782C0E7E4F
SHA1:	6B65EDFBED6418D54D12F6CFDF623F9ED7F65E64
SHA-256:	89553619E12D44D6316209C6DE3D8238184BB47190DA07AE315D9A4368467744
SHA-512:	871CEAFA0B6A5899A8DB8947EE232D266F3DCBF2A5DB8D147BA670BEEC38EE63833384C5F8536D8574F271B3C7DCFBF039E79C254E2C9B45CD5C309B9799EB5E
Malicious:	false
Reputation:	low
Preview:	2021/01/27-18:23:14.557 97c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/01/27-18:23:14.558 97c Recovering log #3.2021/01/27-18:23:14.559 97c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\8122d15e-f303-4746-8426-87f6586aafee.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\8122d15e-f303-4746-8426-87f6586aafee.tmp	
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	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):	427
Entropy (8bit):	5.191433640305679
Encrypted:	false
SSDEEP:	12:sn+va5KkkGHArBFUtpcr/Pc7V5f5KkkGHAryJ:sca5KkkGgPg+4zf5KkkGga
MD5:	B6A9171F25DC6129890B8911B05FA70B
SHA1:	0CB3C5DCA4356FBC6A72AE36F7E748068F521D08
SHA-256:	F8E521BAF47C5ECCC4B4F8B624023253BED1F5D9DCA4E50BE2D276647CA873EB
SHA-512:	B7B67E686A7A9027FB515A506808D8EA087C5532FB08EEC538D352946D74E72A61F87E1B15E408C442DF65724513D5E256BE8EB21B20FD8C23597EDA5A570FB
Malicious:	false
Reputation:	low
Preview:	2021/01/27-18:23:08.015 97c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/01/27-18:23:08.019 97c Recovering log #3.2021/01/27-18:23:08.020 97c 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):	429
Entropy (8bit):	5.212156395613632
Encrypted:	false
SSDEEP:	12:sP23+va5KkkGHArqiuFUtpc9W/PchV5f5KkkGHArq2J:sOMa5KkkGgCg+99hf5KkkGg7
MD5:	D31483F520B207567DDE0923170AA586
SHA1:	114DBAF4F440440A83E098945AFAD6C7CE70C35A
SHA-256:	EF38B20ED08B23BF646D496C3517FD33253E37EAFBD91CEE10387DC20D765DA9
SHA-512:	BC3C16961EA82AEBECD026D3A03ABC6196CFF3628459AD696840589FD6191572512827B548EE302F3E246C22D94B6E0EF20FEAD7872AD3F2E336D6AC16C5F3E
Malicious:	false
Reputation:	low
Preview:	2021/01/27-18:23:08.092 9ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/01/27-18:23:08.094 9ec Recovering log #3.2021/01/27-18:23:08.095 9ec 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):	415
Entropy (8bit):	5.194396193524865
Encrypted:	false
SSDEEP:	12:sxPU9+va5KkkGHArAFUtpcxREW/PcxZ9V5f5KkkGHArfJ:sxMKa5KkkGgkg+xi9x7f5KkkGgV
MD5:	22915B7EDD52171758F0A1093696AF97
SHA1:	04D766349DBDBC600053F8DA35890BC0DF928986
SHA-256:	CC91481D50B40D384CC53248CD1307D4D53D55E5ADD5B714B0C15969AADCFA38
SHA-512:	D6AEC0DF327F3F0DC89624F7280D0F96D40CC54B417BEA6A38F322367E50AAF24520E0338BE121E6DBB80457EDA48DAA5D99DC5E4AC258BEFE7617FC9FD432 82
Malicious:	false
Reputation:	low
Preview:	2021/01/27-18:23:23.363 9ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Session Storage/MANIFEST-000001.2021/01/27-18:23:23.364 9ec Recovering log #3.2021/01/27-18:23:23.371 9ec Reusing old log C:\Users\user\AppData\Lo cal\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF21 24
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	321
Entropy (8bit):	5.271815423156879
Encrypted:	false
SSDEEP:	6:m7f4Fm/+q2PWXp+N23iKKdKpIFUtpcf4fXZmwPcf4q4VkwOWXp+N23iKKdKa/WLJ:sgUGva5KkmFUtpcgfX/Pcgt5f5KkaUJ
MD5:	7424AFFBC67D400F7B920186D9EA6E68
SHA1:	5E3E1F4450248F23C55E357222EF72B495F8B9D9
SHA-256:	E7E9667D8AC19E773E71A02A067816C1F1CC39FCDC6C87A11E7FBB347883D6C8
SHA-512:	C10974303157B6B8EE72EAC604596E59399CEEB9044C6990016E92AC4EF30EF49F522E114807F859E7FEDB5E19CE70EEFB2AFA808DC589A64F0B35D490A8C8D 0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Malicious:	false
Reputation:	low
Preview:	2021/01/27-18:22:58.204 988 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/01/27-18:22:58.236 988 Recovering log #3.2021/01/27-18:22:58.243 988 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):	5.341312684519355
Encrypted:	false
SSDEEP:	12:sB+va5KkkOrsFUtpcj/Pc4V5f5KkkOrzJ:s2a5Kk+g+A6f5Kkn
MD5:	6830FF4529404C6E63F7E7A5CD8CF276
SHA1:	B3911DF6F3AA34391509AFBA6EDB04375266137B
SHA-256:	65BB00F22E641DE7DE7CE8FAFEA8D361E781928B6F722E69EAAA5B6BFCFB43CF
SHA-512:	F66FA0B45482A4ED754ED292D0B579453C270873EF5568B884F67B53E7D6144F96B9BDA4B9E42143C0AA5B24022E623E0A6DBFE476B8EC00C9B41FDF81000DB
Malicious:	false
Reputation:	low
Preview:	2021/01/27-18:23:09.580 15bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/01/27-18:23:09.582 15bc Recovering log #3.2021/01/27-18:23:09.583 15bc 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):	3.0220552088742005
Encrypted:	false
SSDEEP:	3:MApQ:s
MD5:	224E01E281CD38C405B522C7B276FD8A
SHA1:	0D917E3319A91B10CE4E9BC4D2A2C5BE64CFF6CB
SHA-256:	0327918BA4437C50545D6E6438A796E400C15C67EC57D30922E42A00951E85A7
SHA-512:	5A98AAB74818B68CFCA67F99B39D6D53B1800474AC44088CCDFE66960769EC128C4157C7069B0ED60061602E16A5B1AD91A2C1D6DAF0A2E24E17042589ACBE8
Malicious:	false
Reputation:	low
Preview:	....(..I.d.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\1468c75f-58fc-42d0-a2c0-5df3eaa768f0.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\Chrome Web Store Payments.ico.md5	
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:	C95825DA33CBDDFA627D9FF9A5B8371BC5F4E643A09573B6E1E839A83B619F53D878C344030B9701DCBC24D4CECCC016CF4D298D10EE8C37D1B5FEC1A5168B6
Malicious:	false
Reputation:	low
Preview:	F......r...(R..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b2529cfa-d554-496d-bd85-fc1e794239d9.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):	5.192812915162357
Encrypted:	false
SSDEEP:	96:nj7pCpFvzKyYVt0ecVayk0JCKL8yrKk3fMFENRbOEQVuwn:nj7pCpV7Y/0ec94KdrKk3fhN0
MD5:	4A88865754A3DBDC98FD56C12A011406
SHA1:	057BCCB0B163BF90CD16C6E114EB34B6EB8807F8
SHA-256:	BC7A075A5D10F26DFDEE124EA334920AC5696FE3776A12730622699B1BD930BD
SHA-512:	7265D0D2999550FB71E0D2B831E1763821C0D085CA65D8FE47E524E838463BD79B0FBBFD61DAABC5C2CA79113645EC5929953CEB597D2A73C8B486B98794F9A
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13256274178468160","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d7bbbe3d-52f1-4da2-a570-0962e9789276.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):	2713
Entropy (8bit):	5.594276645429931
Encrypted:	false
SSDEEP:	48:YTjUoPz75U95eUoJieUow6UUhYU9ZUogEmUozseKUeYPqUoq3U9pBsmU9QqPeUeq:mUoPJU95eUoJieUo5UUCU9ZUoUUoz3KG
MD5:	D580A0121199B4B15DA1358D28C9121D
SHA1:	A14437D4FCD5CC2A1625CFA19EABF849B06A34EC
SHA-256:	5AD01FC32476BD3B250BAE5B30C2B515392871EFCC8A677C3B8B73F8555A3144
SHA-512:	899A9CCC791F27CFEF92A5D45BC9171CED80EF5BE0A574E9625422F0CC09528505CAAF59D9D3A3194B5FDD6C0A76769FF0A560CEE93A67516CA359D9CE0F28F
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1614392645.025859,"host":"Dg14fIaciUHGX6Lc+OnYmaNiAA/ADiwumtIyPrC3d6U=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1611800645.025863},{"expiry":1627352646.111733,"host":"HS0xQK8RrrSZ/KdSgKIC7bLU+xijlimr9JuWvTPbfkE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1611800646.111737},{"expiry":1622687045.120903,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1611800645.120907},{"expiry":1643336582.154742,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1611800582.154747},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1643336646.500605,"host":"Y1cbV6ziZu1KjdKdxBzKmgzsZCYqaDEHWONjJAo942Q=","mode":"force-https","sts_include_subdomains":false,"sts_ob

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.470871652687531
Encrypted:	false
SSDEEP:	3:tUKaesFIFZZmwv3ceLFJ1V8sceLFJ1WGv:m7/uXZmwPcahVvcahtv
MD5:	2FF540D0FCD75D0C339E602A8E5E905D
SHA1:	1EC60DC9F2785AE37EA88F3930E965828FE503B2
SHA-256:	1CF5269886A27580941E4E9FC0D8F3201CB85FB1FB825DFD17434CC9EC16F165
SHA-512:	997453671BE89A3D5F7E092AD821CEBD69DCEB739DE5724C93A7245F6148D96FACECCAE4086CE550A529B6E111A0EB1FDB2F8DEED40EA7B208BCC8F50696B AE4
Malicious:	false
Reputation:	low
Preview:	2021/01/27-18:23:07.356 12b0 Recovering log #3.2021/01/27-18:23:07.406 12b0 Delete type=0 #3.2021/01/27-18:23:07.406 12b0 Delete type=3 #2.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e63f3b59-4081-494e-b1b3-dfab30b6ef23.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):	5385
Entropy (8bit):	5.190687190510504
Encrypted:	false
SSDEEP:	96:nj7pCpFszKyYVt0ecVayk0JCKL8yRk3/jDjbOEQVuwn:nj7pCpA7Y/0ec94KdRk3/Hq
MD5:	BCBE650AD2485549E1EFF18BBCABE6CA
SHA1:	821FAD3E0D1092BAA97AF8A885E72CD2ED9C5916
SHA-256:	87A6465E4EA5D983C593BCF147F3BBB41705854E30BA3D3EA61D25C4ADBD3E2E
SHA-512:	6A08C703648C9304EF584FBC344DE23FCFBA2ADC8E78FDF95D6C5AA19ADD1B4BBC07EE7D562469AEBEF5205D09A52D54A5401B45FD6F0F22671767F8D8F7F2 AF
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e63f3b59-4081-494e-b1b3-dfab30b6ef23.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13256274178468160","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e8d35ddb-9a8d-4495-9588-7aabd118ab15.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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):	5.232406011209822
Encrypted:	false
SSDEEP:	6:m7l9+q2PWXp+N23iKKdKfrzAdIFUtpcv8JZmwPcv89VkwOWXp+N23iKKdKfrzILJ:sf+va5Kk9FUtpcW/PcSV5f5Kk2J
MD5:	FB226DE1A7C22FD33CDEB110B62BE206
SHA1:	178B8458048A7FD000489AA8E9107FCA4ADD12A7
SHA-256:	CE80EBF0041F5E7E2B21EE52F2AE290E31B3243F93F730C79218DF834C8C1738
SHA-512:	D36EDE208CA83EFE4C8CD6FC8E64154E883BAEA153D24A0D665EA2DFDE8F5C542D41D6D1CD7FD030643E53E4B83CEE8103D97777DD15A00144EAE445EC38I 2B1
Malicious:	false
Reputation:	low
Preview:	2021/01/27-18:23:08.631 15bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/01/27-18:23:08.632 15bc Recovering log #3.2021/01/27-18:23:08.632 15bc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691 724
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
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\Subresource Filter\Indexed Rules\27\9.18.0\Indexing in Progress	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Reputation:	low
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir6132_2135469203\Ruleset Data	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	235624
Entropy (8bit):	4.967847153665615
Encrypted:	false
SSDEEP:	3072:EtV4WVaR1c58AVLz5LTmUbHqrzpxmHBoET2N42aq5tETVoQ6MGnr9/ipKiao5u9V:WL8lVZT2+85tThEKl
MD5:	4AFE0BFD28E65161E164F53178A96836
SHA1:	498E6448FAC9E2901F65124C8A3D79077B5256BF
SHA-256:	3F8EA1BE3A593F8309C89B6A59249EFF593EF90911FED8205D9C964594BC112B
SHA-512:	1FD7BC2FC2114A9D1CA79CFD730D19BEF72159D54DBF962D6E3BFDB39F7F2E13833B236C6C9B8A5C9AABD7822820E42D28C9E7310F98CD74C2F371C75D1CF75
Malicious:	false
Reputation:	low
Preview:	.....<)..... .....`...D.....|.....t...p.....h...d..`.....t...L...T...8...@...<...8...4.....,...(...p.....uocca.....l.....ozama.....`.. .....0iupb.....@.....g.bat.....onwod.....ennab.....`.....nozam.....geips.....|...0.....rekoj.....H.....lgoog.....q..`.....uotpo.....D..... ..lreko.....t...+.....t.....l...P.....,.....h.....H.....|...$...t...p...l...h.....`.....X.....P.....\|...D...@...<...8...4...L...,...,..$... ... .d.....D.....l.....|...x...@...p... .....\.....T...P.....H...h...L...0...8.....0...,...(...$... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\e20777de-d3c7-4e5c-a273-661c6bf2fe86.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7521457082067338
Encrypted:	false
SSDEEP:	384:FTduakbh8rYWVTV6RNGrzvay3JSMNHolGtErPMesxBwc0vrHKmLof8eqCRO48SNx:VWa1RCsR1Mer8usEfXGuKs6uBJ
MD5:	D57E49C2AF97C11141F015CFB4A8A591
SHA1:	F5481D1C5570063B4A410F361E2039D49F69E9AB
SHA-256:	E9553E864D407A941C345929FF54AB8013FBA3FF2BEA4152EA90F5882189B5C9
SHA-512:	00FCFAE1F9108334A746F0420220402826CE557C31C73F6820F7B54FC659003E7EAA4823501F548931308F924EBD9C2403236783D50FE49D73F1BB4312F83407
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\e20777de-d3c7-4e5c-a273-661c6bf2fe86.tmp	
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\e2cc4708-c326-40e4-ac23-62c2e6059909.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):	163488
Entropy (8bit):	6.081591729845753
Encrypted:	false
SSDEEP:	3072:iDzWZ9M5muYQcRjh2bN53qzK89AFcbXafIB0u1GOJmA3iuRi:QS9MIuYT8afYaqfIlUOoSiuRi
MD5:	067D5BB83FEE68EBCBACAAF716351215
SHA1:	575A7CE0AD27CD69A2E8022DF8612DD3D8207DF1
SHA-256:	41C25A4DA759751F90464E822B8136678DC76F334A007C5F0EDC709D088BC36E
SHA-512:	9F31345E138D264EE05AF0EA36AEFF581EFF69322EDCAC36C9ECD48B2FE12078F2BB34DB7CA0A51E0E922CD6277C43ED5797E5DE2F6EE0FB8977687A5471AC 97
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.611800580172949e+12,"network":1.61176818e+12,"ticks":98173914.0,"uncertainty":2768664.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\78UZHHEC\dough-bolts[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Reputation:	low
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{CCED0D32-610F-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33368
Entropy (8bit):	1.8735267978608354
Encrypted:	false
SSDEEP:	96:rMZzZG2H9WpdtpMfpsxMpEpupOpttpfS3:rMZzZG2H9WXtOf6xMWMoftdS3
MD5:	D7637F92148FDB474E54442B4EB5A0B1
SHA1:	3DF31C5C12CF5EBB9F5172422CAF4B39032BCCE3
SHA-256:	94E01E25684428F171019827B2B0692CDFC565CEA503E0CC48CD759CCA4148A7
SHA-512:	2ED5377DEDFE7B689F44DA572EEDAF03025AC8DE7B3B99D8396D1CEDD9C994C2A8209B94493F9766C85C9963348CEF386E0A7801E6BD728B995514AC03EBDF 9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{CCED0D32-610F-11EB-90E4-ECF4BB862DED}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

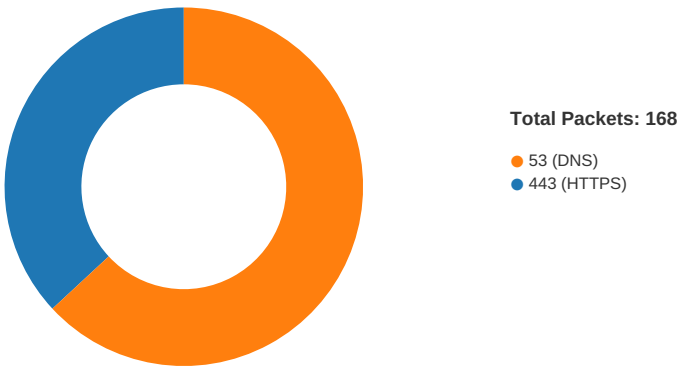
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{CCED0D34-610F-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	54448
Entropy (8bit):	2.7369866804994385
Encrypted:	false
SSDEEP:	192:rNZqQO6Vk8FjZ2ikWBQMDYOtLwJuJn6rQmt/ZuhKAt5wJuJn6rQmt/ZuhEAzFDlB:rjnZe8ho2XDjYZQmDKKZQmDE5J40/28d
MD5:	0A4B8450CF26F6705E9155DBFF80E41E
SHA1:	24E32F4323D25446C4ACB4468A3430141333A0C3
SHA-256:	0F4F1E04047426E2623B0D7D32650A132FF04FA1E34CF50C848560A843221791
SHA-512:	012689BD0F3F140C124C0B8290900D4572DFB26E11CD8BAC179B78C39A449F8085D881F25F772BEB838BA6653AB9B861DDA45CA3974AD0F0AF0216FD47DA913
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 18:23:00.583399057 CET	49723	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:00.584443092 CET	49725	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:00.765533924 CET	49727	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:00.781533003 CET	443	49723	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:00.781646967 CET	49723	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:00.781923056 CET	49723	443	192.168.2.3	44.238.32.151

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 18:23:00.784666061 CET	443	49725	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:00.784795046 CET	49725	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:00.784986973 CET	49725	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:00.965817928 CET	443	49727	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:00.965971947 CET	49727	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:00.966557026 CET	49727	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:00.981530905 CET	443	49723	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:00.982383013 CET	443	49723	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:00.982423067 CET	443	49723	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:00.982440948 CET	443	49723	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:00.982462883 CET	443	49723	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:00.982497931 CET	49723	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:00.982517958 CET	49723	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:00.986857891 CET	443	49725	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:00.987766981 CET	443	49725	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:00.987787008 CET	443	49725	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:00.987801075 CET	443	49725	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:00.987827063 CET	443	49725	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:00.988327980 CET	49725	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:01.025487900 CET	49723	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:01.026439905 CET	49725	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:01.026567936 CET	49725	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:01.026678085 CET	49723	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:01.026848078 CET	49723	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:01.168405056 CET	443	49727	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:01.168473005 CET	443	49727	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:01.168510914 CET	443	49727	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:01.168555975 CET	443	49727	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:01.168598890 CET	443	49727	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:01.168983936 CET	49727	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:01.174397945 CET	49727	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:01.226089001 CET	443	49723	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:01.226121902 CET	443	49723	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:01.226216078 CET	49723	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:01.226444960 CET	49723	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:01.229151964 CET	443	49723	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:01.229186058 CET	443	49725	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:01.229212046 CET	443	49725	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:01.229295015 CET	49725	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:01.229320049 CET	49725	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:01.251507998 CET	443	49723	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:01.251549006 CET	443	49723	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:01.251635075 CET	49723	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:01.251671076 CET	443	49723	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:01.251688957 CET	49723	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:01.251719952 CET	443	49723	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:01.251751900 CET	49723	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:01.253592968 CET	443	49723	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:01.253690958 CET	49723	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:01.322252989 CET	443	49723	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:01.325615883 CET	443	49723	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:01.325731039 CET	49723	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:01.367129087 CET	49731	443	192.168.2.3	99.86.154.21
Jan 27, 2021 18:23:01.367625952 CET	49732	443	192.168.2.3	99.86.154.21
Jan 27, 2021 18:23:01.368019104 CET	49733	443	192.168.2.3	99.86.154.21
Jan 27, 2021 18:23:01.372994900 CET	443	49727	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:01.373429060 CET	443	49727	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:01.373512030 CET	49727	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:01.411475897 CET	443	49732	99.86.154.21	192.168.2.3
Jan 27, 2021 18:23:01.411566019 CET	49732	443	192.168.2.3	99.86.154.21
Jan 27, 2021 18:23:01.412087917 CET	49732	443	192.168.2.3	99.86.154.21
Jan 27, 2021 18:23:01.413003922 CET	443	49731	99.86.154.21	192.168.2.3
Jan 27, 2021 18:23:01.413088083 CET	49731	443	192.168.2.3	99.86.154.21
Jan 27, 2021 18:23:01.413284063 CET	49731	443	192.168.2.3	99.86.154.21

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 18:23:01.413461924 CET	443	49733	99.86.154.21	192.168.2.3
Jan 27, 2021 18:23:01.413561106 CET	49733	443	192.168.2.3	99.86.154.21
Jan 27, 2021 18:23:01.413764000 CET	49733	443	192.168.2.3	99.86.154.21
Jan 27, 2021 18:23:01.424058914 CET	443	49723	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:01.424101114 CET	443	49723	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:01.424127102 CET	49723	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:01.424151897 CET	49723	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:01.424201012 CET	443	49723	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:01.424246073 CET	443	49723	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:01.424263954 CET	49723	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:01.424314022 CET	49723	443	192.168.2.3	44.238.32.151
Jan 27, 2021 18:23:01.449537992 CET	443	49723	44.238.32.151	192.168.2.3
Jan 27, 2021 18:23:01.457700014 CET	443	49732	99.86.154.21	192.168.2.3
Jan 27, 2021 18:23:01.459001064 CET	443	49732	99.86.154.21	192.168.2.3
Jan 27, 2021 18:23:01.459019899 CET	443	49732	99.86.154.21	192.168.2.3
Jan 27, 2021 18:23:01.459036112 CET	443	49732	99.86.154.21	192.168.2.3
Jan 27, 2021 18:23:01.459055901 CET	443	49732	99.86.154.21	192.168.2.3
Jan 27, 2021 18:23:01.459079981 CET	49732	443	192.168.2.3	99.86.154.21
Jan 27, 2021 18:23:01.459105968 CET	49732	443	192.168.2.3	99.86.154.21
Jan 27, 2021 18:23:01.460144997 CET	443	49731	99.86.154.21	192.168.2.3
Jan 27, 2021 18:23:01.460978031 CET	443	49733	99.86.154.21	192.168.2.3
Jan 27, 2021 18:23:01.461477995 CET	443	49733	99.86.154.21	192.168.2.3
Jan 27, 2021 18:23:01.461502075 CET	443	49733	99.86.154.21	192.168.2.3
Jan 27, 2021 18:23:01.461513996 CET	443	49733	99.86.154.21	192.168.2.3
Jan 27, 2021 18:23:01.461527109 CET	443	49733	99.86.154.21	192.168.2.3
Jan 27, 2021 18:23:01.461601019 CET	49733	443	192.168.2.3	99.86.154.21
Jan 27, 2021 18:23:01.461631060 CET	49733	443	192.168.2.3	99.86.154.21
Jan 27, 2021 18:23:01.463458061 CET	443	49733	99.86.154.21	192.168.2.3
Jan 27, 2021 18:23:01.463480949 CET	443	49732	99.86.154.21	192.168.2.3
Jan 27, 2021 18:23:01.463799953 CET	443	49731	99.86.154.21	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 18:22:53.545191050 CET	58361	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:22:53.593688011 CET	53	58361	8.8.8.8	192.168.2.3
Jan 27, 2021 18:22:54.466634035 CET	63492	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:22:54.517515898 CET	53	63492	8.8.8.8	192.168.2.3
Jan 27, 2021 18:22:55.425990105 CET	60831	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:22:55.478533983 CET	53	60831	8.8.8.8	192.168.2.3
Jan 27, 2021 18:22:56.609488964 CET	60100	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:22:56.660531998 CET	53	60100	8.8.8.8	192.168.2.3
Jan 27, 2021 18:22:59.642431974 CET	49563	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:22:59.692459106 CET	53	49563	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:00.516489983 CET	51352	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:00.518527985 CET	59349	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:00.520051956 CET	57084	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:00.522097111 CET	58823	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:00.524332047 CET	57568	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:00.572709084 CET	53	51352	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:00.574863911 CET	53	59349	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:00.580607891 CET	53	57568	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:00.581125021 CET	53	58823	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:00.581443071 CET	53	57084	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:00.649976969 CET	50540	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:00.700670004 CET	53	50540	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:00.996978998 CET	54366	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:01.078710079 CET	53	54366	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:01.188452959 CET	53034	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:01.252381086 CET	53	53034	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:01.305710077 CET	57762	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:01.365709066 CET	53	57762	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:01.704092979 CET	55435	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:01.751847029 CET	53	55435	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 18:23:01.945768118 CET	50713	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:01.947489977 CET	56132	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:02.005536079 CET	53	50713	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:02.014480114 CET	53	56132	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:02.775957108 CET	58987	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:02.836023092 CET	53	58987	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:03.145287991 CET	56579	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:03.201809883 CET	53	56579	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:03.389669895 CET	60633	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:03.395514965 CET	61292	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:03.397731066 CET	63619	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:03.452478886 CET	53	60633	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:03.453335047 CET	53	61292	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:03.456430912 CET	53	63619	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:03.459736109 CET	64938	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:03.459947109 CET	61946	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:03.510612965 CET	53	61946	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:03.516052961 CET	53	64938	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:03.683980942 CET	64910	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:03.688685894 CET	52123	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:03.742769003 CET	53	64910	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:03.748140097 CET	53	52123	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:03.789889097 CET	56130	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:03.852209091 CET	53	56130	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:04.122586012 CET	56338	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:04.151742935 CET	59420	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:04.179732084 CET	53	56338	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:04.199862957 CET	53	59420	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:04.271984100 CET	58784	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:04.273119926 CET	63978	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:04.274298906 CET	62938	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:04.331989050 CET	53	58784	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:04.335055113 CET	53	63978	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:04.339241982 CET	53	62938	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:05.099387884 CET	55708	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:05.160429955 CET	53	55708	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:05.202980995 CET	55709	443	192.168.2.3	108.177.15.157
Jan 27, 2021 18:23:05.219082117 CET	56803	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:05.221235991 CET	57145	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:05.221998930 CET	55359	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:05.223078966 CET	58306	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:05.223727942 CET	64124	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:05.255714893 CET	443	55709	108.177.15.157	192.168.2.3
Jan 27, 2021 18:23:05.255750895 CET	443	55709	108.177.15.157	192.168.2.3
Jan 27, 2021 18:23:05.258121967 CET	55709	443	192.168.2.3	108.177.15.157
Jan 27, 2021 18:23:05.266859055 CET	53	56803	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:05.270809889 CET	53	58306	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:05.271378040 CET	53	64124	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:05.278994083 CET	53	57145	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:05.289086103 CET	53	55359	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:05.296396017 CET	63150	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:05.304946899 CET	53279	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:05.307884932 CET	56881	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:05.310349941 CET	53642	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:05.310728073 CET	443	55709	108.177.15.157	192.168.2.3
Jan 27, 2021 18:23:05.311191082 CET	55709	443	192.168.2.3	108.177.15.157
Jan 27, 2021 18:23:05.311361074 CET	55709	443	192.168.2.3	108.177.15.157
Jan 27, 2021 18:23:05.313394070 CET	55667	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:05.346070051 CET	53	63150	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:05.355781078 CET	53	56881	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:05.358194113 CET	53	53642	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:05.363903999 CET	443	55709	108.177.15.157	192.168.2.3
Jan 27, 2021 18:23:05.363935947 CET	443	55709	108.177.15.157	192.168.2.3
Jan 27, 2021 18:23:05.363986969 CET	53	55667	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 18:23:05.385190964 CET	55709	443	192.168.2.3	108.177.15.157
Jan 27, 2021 18:23:05.405817986 CET	53	53279	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:05.691971064 CET	55669	443	192.168.2.3	172.217.22.227
Jan 27, 2021 18:23:05.750602961 CET	443	55669	172.217.22.227	192.168.2.3
Jan 27, 2021 18:23:05.750631094 CET	443	55669	172.217.22.227	192.168.2.3
Jan 27, 2021 18:23:05.751843929 CET	55669	443	192.168.2.3	172.217.22.227
Jan 27, 2021 18:23:06.308070898 CET	55669	443	192.168.2.3	172.217.22.227
Jan 27, 2021 18:23:06.327272892 CET	54833	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:06.327518940 CET	62476	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:06.327981949 CET	49705	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:06.328206062 CET	61477	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:06.375587940 CET	53	49705	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:06.378372908 CET	55949	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:06.378453016 CET	443	55669	172.217.22.227	192.168.2.3
Jan 27, 2021 18:23:06.380266905 CET	443	55669	172.217.22.227	192.168.2.3
Jan 27, 2021 18:23:06.380825043 CET	55669	443	192.168.2.3	172.217.22.227
Jan 27, 2021 18:23:06.386337042 CET	53	54833	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:06.388897896 CET	53	61477	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:06.391571999 CET	53	62476	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:06.431936979 CET	53	55949	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:06.440188885 CET	49342	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:06.490792990 CET	53	49342	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:06.737371922 CET	56253	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:06.796510935 CET	53	56253	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:06.798222065 CET	56254	443	192.168.2.3	172.217.20.226
Jan 27, 2021 18:23:06.854115963 CET	443	56254	172.217.20.226	192.168.2.3
Jan 27, 2021 18:23:06.854135990 CET	443	56254	172.217.20.226	192.168.2.3
Jan 27, 2021 18:23:06.856559038 CET	56254	443	192.168.2.3	172.217.20.226
Jan 27, 2021 18:23:06.857316017 CET	56254	443	192.168.2.3	172.217.20.226
Jan 27, 2021 18:23:06.924767017 CET	443	56254	172.217.20.226	192.168.2.3
Jan 27, 2021 18:23:06.926250935 CET	443	56254	172.217.20.226	192.168.2.3
Jan 27, 2021 18:23:06.927064896 CET	56254	443	192.168.2.3	172.217.20.226
Jan 27, 2021 18:23:06.944730997 CET	443	56254	172.217.20.226	192.168.2.3
Jan 27, 2021 18:23:06.944789886 CET	443	56254	172.217.20.226	192.168.2.3
Jan 27, 2021 18:23:06.945380926 CET	56254	443	192.168.2.3	172.217.20.226
Jan 27, 2021 18:23:06.946825981 CET	56254	443	192.168.2.3	172.217.20.226
Jan 27, 2021 18:23:07.014827013 CET	443	56254	172.217.20.226	192.168.2.3
Jan 27, 2021 18:23:07.426907063 CET	49667	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:07.485271931 CET	53	49667	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:07.560926914 CET	55439	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:07.625438929 CET	53	55439	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:08.371153116 CET	57069	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:08.443687916 CET	53	57069	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:09.378377914 CET	56639	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:10.019309044 CET	51856	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:10.389172077 CET	56639	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:11.015990019 CET	51856	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:11.064029932 CET	53	51856	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:11.408159971 CET	56639	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:11.469504118 CET	53	56639	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:15.905643940 CET	56546	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:15.956506968 CET	53	56546	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:17.240277052 CET	62152	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:17.291029930 CET	53	62152	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:18.425014019 CET	53470	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:18.474591970 CET	53	53470	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:19.521970987 CET	56446	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:19.570245028 CET	53	56446	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:20.313702106 CET	55709	443	192.168.2.3	108.177.15.157
Jan 27, 2021 18:23:20.390753031 CET	443	55709	108.177.15.157	192.168.2.3
Jan 27, 2021 18:23:26.823694944 CET	59631	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:26.879944086 CET	53	59631	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:28.223753929 CET	55515	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:28.281469107 CET	53	55515	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 18:23:28.973066092 CET	64547	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:29.037878036 CET	53	64547	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:30.037911892 CET	51759	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:30.098705053 CET	53	51759	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:30.499093056 CET	59207	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:30.561039925 CET	53	59207	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:33.995455027 CET	54269	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:34.046292067 CET	53	54269	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:42.246300936 CET	54856	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:42.302465916 CET	53	54856	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:43.545097113 CET	64140	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:44.340048075 CET	62271	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:44.546672106 CET	64140	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:45.343615055 CET	62271	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:45.545984983 CET	53	64140	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:45.552541971 CET	53	62271	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:46.276386976 CET	57404	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:46.337131977 CET	53	57404	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:46.649101973 CET	62997	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:46.709139109 CET	53	62997	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:47.052248001 CET	57712	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:47.111795902 CET	53	57712	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:47.585474014 CET	60065	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:47.620224953 CET	55068	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:47.642398119 CET	53	60065	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:47.669836998 CET	64700	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:47.678791046 CET	53	55068	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:47.728874922 CET	53	64700	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:47.739027977 CET	61998	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:47.762083054 CET	53724	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:47.796792030 CET	53	61998	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:47.856144905 CET	52328	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:47.857224941 CET	53	53724	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:47.914875984 CET	53	52328	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:50.228703976 CET	58051	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:50.289376974 CET	53	58051	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:54.565946102 CET	64130	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:54.625704050 CET	53	64130	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:56.822161913 CET	50491	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:56.870465040 CET	53	50491	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:57.591005087 CET	53004	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:57.649777889 CET	53	53004	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:57.831619978 CET	50491	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:57.879748106 CET	53	50491	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:58.548481941 CET	52529	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:58.597202063 CET	53004	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:58.625679016 CET	53	52529	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:58.644886017 CET	53	53004	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:58.851026058 CET	50491	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:58.907275915 CET	53	50491	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:59.059185982 CET	62724	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:59.107074022 CET	53	62724	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:59.231281042 CET	56059	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:59.289338112 CET	53	56059	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:59.416246891 CET	63060	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:59.464061022 CET	51498	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:59.474603891 CET	53	63060	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:59.524033070 CET	53	51498	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:59.593971968 CET	59943	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:59.602015018 CET	53004	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:23:59.653573990 CET	53	53004	8.8.8.8	192.168.2.3
Jan 27, 2021 18:23:59.663345098 CET	53	59943	8.8.8.8	192.168.2.3
Jan 27, 2021 18:24:00.851660967 CET	50491	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:24:00.899435997 CET	53	50491	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 18:24:01.617335081 CET	53004	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:24:01.665744066 CET	53	53004	8.8.8.8	192.168.2.3
Jan 27, 2021 18:24:05.906961918 CET	53004	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:24:05.917458057 CET	50491	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:24:05.954860926 CET	53	53004	8.8.8.8	192.168.2.3
Jan 27, 2021 18:24:05.965282917 CET	53	50491	8.8.8.8	192.168.2.3
Jan 27, 2021 18:24:10.385584116 CET	50118	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:24:10.444269896 CET	53	50118	8.8.8.8	192.168.2.3
Jan 27, 2021 18:24:19.582250118 CET	58357	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:24:19.649758101 CET	53	58357	8.8.8.8	192.168.2.3
Jan 27, 2021 18:24:19.772962093 CET	55804	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:24:19.829202890 CET	53	55804	8.8.8.8	192.168.2.3
Jan 27, 2021 18:24:19.892210960 CET	58079	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:24:19.948771000 CET	53	58079	8.8.8.8	192.168.2.3
Jan 27, 2021 18:24:27.085242033 CET	52080	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:24:27.134279966 CET	53	52080	8.8.8.8	192.168.2.3
Jan 27, 2021 18:24:27.460649014 CET	55238	53	192.168.2.3	8.8.8.8
Jan 27, 2021 18:24:27.525012970 CET	53	55238	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 18:23:00.522097111 CET	192.168.2.3	8.8.8.8	0xed3a	Standard query (0)	quip.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:01.305710077 CET	192.168.2.3	8.8.8.8	0xa5b	Standard query (0)	quip-cdn.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:02.775957108 CET	192.168.2.3	8.8.8.8	0x4eb2	Standard query (0)	listenweb4.quip.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:03.145287991 CET	192.168.2.3	8.8.8.8	0xf347	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:03.389669895 CET	192.168.2.3	8.8.8.8	0x3a6c	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:03.395514965 CET	192.168.2.3	8.8.8.8	0xcfb	Standard query (0)	s.adroll.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:03.397731066 CET	192.168.2.3	8.8.8.8	0xf1d4	Standard query (0)	scripts.demandbase.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:03.459736109 CET	192.168.2.3	8.8.8.8	0xbcbd	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:03.683980942 CET	192.168.2.3	8.8.8.8	0x765b	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:03.688685894 CET	192.168.2.3	8.8.8.8	0x5324	Standard query (0)	d.adroll.mgr.consensu.org	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:04.122586012 CET	192.168.2.3	8.8.8.8	0x3eee	Standard query (0)	d.adroll.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:04.151742935 CET	192.168.2.3	8.8.8.8	0x1e6f	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:04.271984100 CET	192.168.2.3	8.8.8.8	0x4617	Standard query (0)	match.prod.bidr.io	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:04.273119926 CET	192.168.2.3	8.8.8.8	0xdd2	Standard query (0)	id.rlcdn.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:04.274298906 CET	192.168.2.3	8.8.8.8	0xda0d	Standard query (0)	api.company-target.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.219082117 CET	192.168.2.3	8.8.8.8	0xcec6	Standard query (0)	pixel.advertising.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.221235991 CET	192.168.2.3	8.8.8.8	0xf8b2	Standard query (0)	dsum-sec.casalemedia.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.221998930 CET	192.168.2.3	8.8.8.8	0xdd51	Standard query (0)	pixel.rubiconproject.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.223078966 CET	192.168.2.3	8.8.8.8	0x39a7	Standard query (0)	sync.outbrain.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.223727942 CET	192.168.2.3	8.8.8.8	0x772d	Standard query (0)	simage2.pubmatic.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.296396017 CET	192.168.2.3	8.8.8.8	0xa07a	Standard query (0)	ads.yahoo.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.304946899 CET	192.168.2.3	8.8.8.8	0xdea	Standard query (0)	sync.taboola.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.307884932 CET	192.168.2.3	8.8.8.8	0x6898	Standard query (0)	eb2.3lift.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.310349941 CET	192.168.2.3	8.8.8.8	0x4f1	Standard query (0)	x.bidswitch.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 18:23:05.313394070 CET	192.168.2.3	8.8.8.8	0x32ee	Standard query (0)	ib.adnxs.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:06.327272892 CET	192.168.2.3	8.8.8.8	0xdbb1	Standard query (0)	segments.company-target.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:06.327518940 CET	192.168.2.3	8.8.8.8	0x9f24	Standard query (0)	cm.g.doubleclick.net	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:06.327981949 CET	192.168.2.3	8.8.8.8	0x2373	Standard query (0)	us-u.openx.net	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:06.328206062 CET	192.168.2.3	8.8.8.8	0xcbe9	Standard query (0)	idsync.rlcdn.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:06.378372908 CET	192.168.2.3	8.8.8.8	0x55db	Standard query (0)	ups.analytics.yahoo.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:06.737371922 CET	192.168.2.3	8.8.8.8	0xce58	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:07.560926914 CET	192.168.2.3	8.8.8.8	0xc2be	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:28.223753929 CET	192.168.2.3	8.8.8.8	0xd7bf	Standard query (0)	dough-bolts.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:30.037911892 CET	192.168.2.3	8.8.8.8	0xbdce	Standard query (0)	static.sharepointonline.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:30.499093056 CET	192.168.2.3	8.8.8.8	0xdec2	Standard query (0)	spoprod-a.akamaihd.net	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:44.340048075 CET	192.168.2.3	8.8.8.8	0x570e	Standard query (0)	dough-bolts.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:45.343615055 CET	192.168.2.3	8.8.8.8	0x570e	Standard query (0)	dough-bolts.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:47.585474014 CET	192.168.2.3	8.8.8.8	0x128a	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:47.762083054 CET	192.168.2.3	8.8.8.8	0x22b0	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 18:23:00.581125021 CET	8.8.8.8	192.168.2.3	0xed3a	No error (0)	quip.com		44.238.32.151	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:00.581125021 CET	8.8.8.8	192.168.2.3	0xed3a	No error (0)	quip.com		54.191.147.46	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:00.581125021 CET	8.8.8.8	192.168.2.3	0xed3a	No error (0)	quip.com		52.39.66.75	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:01.365709066 CET	8.8.8.8	192.168.2.3	0xa5b	No error (0)	quip-cdn.com		99.86.154.21	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:01.365709066 CET	8.8.8.8	192.168.2.3	0xa5b	No error (0)	quip-cdn.com		99.86.154.85	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:01.365709066 CET	8.8.8.8	192.168.2.3	0xa5b	No error (0)	quip-cdn.com		99.86.154.50	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:01.365709066 CET	8.8.8.8	192.168.2.3	0xa5b	No error (0)	quip-cdn.com		99.86.154.9	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:02.836023092 CET	8.8.8.8	192.168.2.3	0x4eb2	No error (0)	listenweb4.quip.com		52.39.66.75	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:02.836023092 CET	8.8.8.8	192.168.2.3	0x4eb2	No error (0)	listenweb4.quip.com		44.238.32.151	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:02.836023092 CET	8.8.8.8	192.168.2.3	0x4eb2	No error (0)	listenweb4.quip.com		54.191.147.46	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:03.201809883 CET	8.8.8.8	192.168.2.3	0xf347	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:03.201809883 CET	8.8.8.8	192.168.2.3	0xf347	No error (0)	stats.l.doubleclick.net		108.177.15.157	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:03.201809883 CET	8.8.8.8	192.168.2.3	0xf347	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 18:23:03.201809883 CET	8.8.8.8	192.168.2.3	0xf347	No error (0)	stats.l.doubleclick.net		108.177.15.156	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:03.201809883 CET	8.8.8.8	192.168.2.3	0xf347	No error (0)	stats.l.doubleclick.net		108.177.15.155	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:03.452478886 CET	8.8.8.8	192.168.2.3	0x3a6c	No error (0)	snap.licdn.com	wildcard.licdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:03.453335047 CET	8.8.8.8	192.168.2.3	0xcfb	No error (0)	s.adroll.com	wildcard.adroll.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:03.456430912 CET	8.8.8.8	192.168.2.3	0xf1d4	No error (0)	scripts.demandbase.com		143.204.11.81	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:03.456430912 CET	8.8.8.8	192.168.2.3	0xf1d4	No error (0)	scripts.demandbase.com		143.204.11.23	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:03.456430912 CET	8.8.8.8	192.168.2.3	0xf1d4	No error (0)	scripts.demandbase.com		143.204.11.42	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:03.456430912 CET	8.8.8.8	192.168.2.3	0xf1d4	No error (0)	scripts.demandbase.com		143.204.11.7	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:03.516052961 CET	8.8.8.8	192.168.2.3	0xbcbd	No error (0)	www.google.co.uk		172.217.22.227	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:03.742769003 CET	8.8.8.8	192.168.2.3	0x765b	No error (0)	px.ads.linkedin.com	mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:03.742769003 CET	8.8.8.8	192.168.2.3	0x765b	No error (0)	mix.linkedin.com	pop-tln1-alpha.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:03.742769003 CET	8.8.8.8	192.168.2.3	0x765b	No error (0)	pop-tln1-alpha.mix.linkedin.com		185.63.144.5	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:03.748140097 CET	8.8.8.8	192.168.2.3	0x5324	No error (0)	d.adroll.mgr.consensu.org	d.adroll.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:03.748140097 CET	8.8.8.8	192.168.2.3	0x5324	No error (0)	d.adroll.com	adserver-vpc-alb-3-890571764.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:03.748140097 CET	8.8.8.8	192.168.2.3	0x5324	No error (0)	adserver-vpc-alb-3-890571764.eu-west-1.elb.amazonaws.com		34.254.169.151	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:03.748140097 CET	8.8.8.8	192.168.2.3	0x5324	No error (0)	adserver-vpc-alb-3-890571764.eu-west-1.elb.amazonaws.com		3.248.28.111	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:04.179732084 CET	8.8.8.8	192.168.2.3	0x3eee	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 18:23:04.179732084 CET	8.8.8.8	192.168.2.3	0x3eee	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 18:23:04.179732084 CET	8.8.8.8	192.168.2.3	0x3eee	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 18:23:04.199862957 CET	8.8.8.8	192.168.2.3	0x1e6f	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:04.331989050 CET	8.8.8.8	192.168.2.3	0x4617	No error (0)	match.prod.bidr.io		52.49.193.31	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:04.331989050 CET	8.8.8.8	192.168.2.3	0x4617	No error (0)	match.prod.bidr.io		52.214.70.9	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 18:23:04.331989050 CET	8.8.8.8	192.168.2.3	0x4617	No error (0)	match.prod.bidr.io		52.31.242.159	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:04.331989050 CET	8.8.8.8	192.168.2.3	0x4617	No error (0)	match.prod.bidr.io		52.215.8.160	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:04.331989050 CET	8.8.8.8	192.168.2.3	0x4617	No error (0)	match.prod.bidr.io		54.72.203.0	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:04.331989050 CET	8.8.8.8	192.168.2.3	0x4617	No error (0)	match.prod.bidr.io		54.228.192.197	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:04.335055113 CET	8.8.8.8	192.168.2.3	0xdd2	No error (0)	id.rlcdn.com		34.120.207.148	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:04.339241982 CET	8.8.8.8	192.168.2.3	0xda0d	No error (0)	api.company-target.com		99.86.154.35	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:04.339241982 CET	8.8.8.8	192.168.2.3	0xda0d	No error (0)	api.company-target.com		99.86.154.15	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:04.339241982 CET	8.8.8.8	192.168.2.3	0xda0d	No error (0)	api.company-target.com		99.86.154.58	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:04.339241982 CET	8.8.8.8	192.168.2.3	0xda0d	No error (0)	api.company-target.com		99.86.154.83	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.266859055 CET	8.8.8.8	192.168.2.3	0xcec6	No error (0)	pixel.advertising.com	prod.ups-adcom.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:05.266859055 CET	8.8.8.8	192.168.2.3	0xcec6	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 18:23:05.266859055 CET	8.8.8.8	192.168.2.3	0xcec6	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 18:23:05.266859055 CET	8.8.8.8	192.168.2.3	0xcec6	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 18:23:05.266859055 CET	8.8.8.8	192.168.2.3	0xcec6	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.197.47.23	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.266859055 CET	8.8.8.8	192.168.2.3	0xcec6	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 18:23:05.266859055 CET	8.8.8.8	192.168.2.3	0xcec6	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		52.59.102.119	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.266859055 CET	8.8.8.8	192.168.2.3	0xcec6	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 18:23:05.266859055 CET	8.8.8.8	192.168.2.3	0xcec6	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 18:23:05.266859055 CET	8.8.8.8	192.168.2.3	0xcec6	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 18:23:05.270809889 CET	8.8.8.8	192.168.2.3	0x39a7	No error (0)	sync.outbrain.com	alldcs.outbrain.org		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:05.270809889 CET	8.8.8.8	192.168.2.3	0x39a7	No error (0)	alldcs.outbrain.org	nydc1.outbrain.org		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:05.270809889 CET	8.8.8.8	192.168.2.3	0x39a7	No error (0)	nydc1.outbrain.org		64.202.112.159	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.271378040 CET	8.8.8.8	192.168.2.3	0x772d	No error (0)	simage2.pubmatic.com	pug-lhrc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 18:23:05.271378040 CET	8.8.8.8	192.168.2.3	0x772d	No error (0)	pug-lhrc.pubmatic.com	pug-lhr.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:05.271378040 CET	8.8.8.8	192.168.2.3	0x772d	No error (0)	pug-lhr.pubmatic.com		185.64.190.80	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.278994083 CET	8.8.8.8	192.168.2.3	0xf8b2	No error (0)	dsum-sec.casalemedia.com	dsum-sec.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:05.289086103 CET	8.8.8.8	192.168.2.3	0xdd51	No error (0)	pixel.rubiconproject.com	pixel.rubiconproject.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:05.346070051 CET	8.8.8.8	192.168.2.3	0xa07a	No error (0)	ads.yahoo.com	edge.gycpi.b.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:05.346070051 CET	8.8.8.8	192.168.2.3	0xa07a	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.23	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.346070051 CET	8.8.8.8	192.168.2.3	0xa07a	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.22	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.355781078 CET	8.8.8.8	192.168.2.3	0x6898	No error (0)	eb2.3lift.com	eu-eb2.3lift.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:05.355781078 CET	8.8.8.8	192.168.2.3	0x6898	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 18:23:05.355781078 CET	8.8.8.8	192.168.2.3	0x6898	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 18:23:05.355781078 CET	8.8.8.8	192.168.2.3	0x6898	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 18:23:05.355781078 CET	8.8.8.8	192.168.2.3	0x6898	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 18:23:05.355781078 CET	8.8.8.8	192.168.2.3	0x6898	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		35.157.234.72	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.355781078 CET	8.8.8.8	192.168.2.3	0x6898	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		18.159.63.118	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.355781078 CET	8.8.8.8	192.168.2.3	0x6898	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 18:23:05.355781078 CET	8.8.8.8	192.168.2.3	0x6898	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 18:23:05.355781078 CET	8.8.8.8	192.168.2.3	0x6898	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 18:23:05.358194113 CET	8.8.8.8	192.168.2.3	0x4f1	No error (0)	x.bidswitch.net	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:05.358194113 CET	8.8.8.8	192.168.2.3	0x4f1	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		18.195.193.185	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.358194113 CET	8.8.8.8	192.168.2.3	0x4f1	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		52.58.45.227	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.358194113 CET	8.8.8.8	192.168.2.3	0x4f1	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		3.120.242.149	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.358194113 CET	8.8.8.8	192.168.2.3	0x4f1	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		3.121.79.35	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.358194113 CET	8.8.8.8	192.168.2.3	0x4f1	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		52.57.230.211	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.358194113 CET	8.8.8.8	192.168.2.3	0x4f1	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		52.59.81.87	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.358194113 CET	8.8.8.8	192.168.2.3	0x4f1	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		35.157.13.124	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.358194113 CET	8.8.8.8	192.168.2.3	0x4f1	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		52.58.102.227	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.363986969 CET	8.8.8.8	192.168.2.3	0x32ee	No error (0)	ib.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:05.363986969 CET	8.8.8.8	192.168.2.3	0x32ee	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:05.363986969 CET	8.8.8.8	192.168.2.3	0x32ee	No error (0)	ib.anycast.adnxs.com		185.33.221.13	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.363986969 CET	8.8.8.8	192.168.2.3	0x32ee	No error (0)	ib.anycast.adnxs.com		185.33.220.244	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.363986969 CET	8.8.8.8	192.168.2.3	0x32ee	No error (0)	ib.anycast.adnxs.com		185.33.221.90	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.363986969 CET	8.8.8.8	192.168.2.3	0x32ee	No error (0)	ib.anycast.adnxs.com		185.33.221.50	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.363986969 CET	8.8.8.8	192.168.2.3	0x32ee	No error (0)	ib.anycast.adnxs.com		185.33.221.15	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.363986969 CET	8.8.8.8	192.168.2.3	0x32ee	No error (0)	ib.anycast.adnxs.com		185.33.220.145	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.363986969 CET	8.8.8.8	192.168.2.3	0x32ee	No error (0)	ib.anycast.adnxs.com		185.33.221.11	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:05.363986969 CET	8.8.8.8	192.168.2.3	0x32ee	No error (0)	ib.anycast.adnxs.com		185.33.221.52	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 18:23:05.405817986 CET	8.8.8.8	192.168.2.3	0xdea	No error (0)	sync.taboola.com	am-sync.taboola.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:05.405817986 CET	8.8.8.8	192.168.2.3	0xdea	No error (0)	am-sync.taboola.com	am-vip001.taboola.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:05.405817986 CET	8.8.8.8	192.168.2.3	0xdea	No error (0)	am-vip001.taboola.com		141.226.228.48	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:06.375587940 CET	8.8.8.8	192.168.2.3	0x2373	No error (0)	us-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:06.375587940 CET	8.8.8.8	192.168.2.3	0x2373	No error (0)	us-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:06.386337042 CET	8.8.8.8	192.168.2.3	0xdbb1	No error (0)	segments.company-target.com		99.86.154.45	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:06.386337042 CET	8.8.8.8	192.168.2.3	0xdbb1	No error (0)	segments.company-target.com		99.86.154.70	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:06.386337042 CET	8.8.8.8	192.168.2.3	0xdbb1	No error (0)	segments.company-target.com		99.86.154.17	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:06.386337042 CET	8.8.8.8	192.168.2.3	0xdbb1	No error (0)	segments.company-target.com		99.86.154.99	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:06.388897896 CET	8.8.8.8	192.168.2.3	0xcbe9	No error (0)	idsync.rlcdn.com		34.120.207.148	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:06.391571999 CET	8.8.8.8	192.168.2.3	0x9f24	No error (0)	cm.g.doubleclick.net	pagead.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:06.391571999 CET	8.8.8.8	192.168.2.3	0x9f24	No error (0)	pagead.l.doubleclick.net		172.217.22.194	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:06.431936979 CET	8.8.8.8	192.168.2.3	0x55db	No error (0)	ups.analytics.yahoo.com	prod.ups-ats.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:06.431936979 CET	8.8.8.8	192.168.2.3	0x55db	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 18:23:06.431936979 CET	8.8.8.8	192.168.2.3	0x55db	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 18:23:06.431936979 CET	8.8.8.8	192.168.2.3	0x55db	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 18:23:06.796510935 CET	8.8.8.8	192.168.2.3	0xce58	No error (0)	googleads.g.doubleclick.net	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:06.796510935 CET	8.8.8.8	192.168.2.3	0xce58	No error (0)	pagead46.l.doubleclick.net		172.217.20.226	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:07.625438929 CET	8.8.8.8	192.168.2.3	0xc2be	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:07.625438929 CET	8.8.8.8	192.168.2.3	0xc2be	No error (0)	googlehosted.l.googleusercontent.com		172.217.22.225	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:28.281469107 CET	8.8.8.8	192.168.2.3	0xd7bf	No error (0)	dough-bolts.com		162.241.120.76	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:30.098705053 CET	8.8.8.8	192.168.2.3	0xbdce	No error (0)	static.sharepointonline.com	static.sharepointonline.com-c.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:30.561039925 CET	8.8.8.8	192.168.2.3	0xdec2	No error (0)	spoprod-a.akamaihd.net	spoprod-a.akamaihd.net.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 18:23:45.552541971 CET	8.8.8.8	192.168.2.3	0x570e	No error (0)	dough-bolts.com		162.241.120.76	A (IP address)	IN (0x0001)
Jan 27, 2021 18:23:47.642398119 CET	8.8.8.8	192.168.2.3	0x128a	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 18:23:47.857224941 CET	8.8.8.8	192.168.2.3	0x22b0	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	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 18:23:00.982462883 CET	44.238.32.151	443	192.168.2.3	49723	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 18:23:00.987827063 CET	44.238.32.151	443	192.168.2.3	49725	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 18:23:01.168598890 CET	44.238.32.151	443	192.168.2.3	49727	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 18:23:03.236314058 CET	52.39.66.75	443	192.168.2.3	49737	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 18:23:03.875570059 CET	185.63.144.5	443	192.168.2.3	49746	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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 18:23:03.903568983 CET	34.254.169.151	443	192.168.2.3	49747	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		
Jan 27, 2021 18:23:04.307951927 CET	54.170.19.229	443	192.168.2.3	49749	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 18:23:04.466197014 CET	52.49.193.31	443	192.168.2.3	49751	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 18:23:05.380610943 CET	35.156.106.231	443	192.168.2.3	49756	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 18:23:05.435801983 CET	185.64.190.80	443	192.168.2.3	49758	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		

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 18:23:05.543962955 CET	64.202.112.159	443	192.168.2.3	49757	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 18:23:05.718118906 CET	18.185.170.181	443	192.168.2.3	49764	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		
Jan 27, 2021 18:23:05.718453884 CET	18.195.193.185	443	192.168.2.3	49762	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		

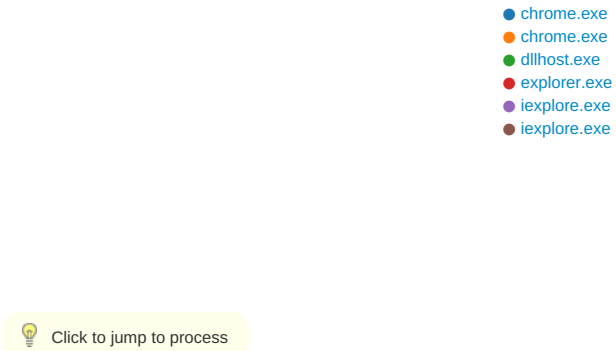
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 18:23:05.726902962 CET	141.226.228.48	443	192.168.2.3	49760	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS Hybrid ECC 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	Mon Dec 27 00:59:59 CET 2021	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=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 18:23:05.729970932 CET	185.33.221.13	443	192.168.2.3	49761	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 18:23:28.661216021 CET	162.241.120.76	443	192.168.2.3	49783	CN=dough-bolts.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Jan 25 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Mon Apr 26 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jan 27, 2021 18:23:28.671912909 CET	162.241.120.76	443	192.168.2.3	49784	CN=dough-bolts.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Jan 25 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Mon Apr 26 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

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 18:23:45.880692959 CET	162.241.120.76	443	192.168.2.3	49797	CN=dough-bolts.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Jan 25 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Mon Apr 26 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 6132 Parent PID: 1788

General

Start time:	18:22:57
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/OWCGAwI8CpAi'
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: chrome.exe PID: 1488 Parent PID: 6132

General

Start time:	18:22:58
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=1540,11308364918695712584,17961569525687617 14,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1796 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

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

Analysis Process: dllhost.exe PID: 6692 Parent PID: 792

General

Start time:	18:23:02
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:	0x7ff7bc440000
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: 3388 Parent PID: 6692

General

Start time:	18:23:04
Start date:	27/01/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
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

Analysis Process: iexplore.exe PID: 6348 Parent PID: 792

General

Start time:	18:23:26
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:	0x7ff793330000
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	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 6356 Parent PID: 6348

General

Start time:	18:23:26
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:6348 CREDAT:17410 /prefetch:2
Imagebase:	0x1350000
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	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis