ID: 321439
Cookbook: browseurl.jbs
Time: 06:11:18
Date: 22/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

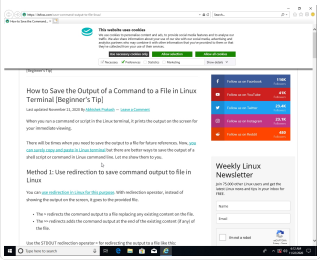
Analysis Report https://itsfoss.com/save-command-out…

Overview

General Information

Sample URL:	http://https://itsfoss.com/save-command-output-to-file-linux/
Analysis ID:	321439

Most interesting Screenshot:



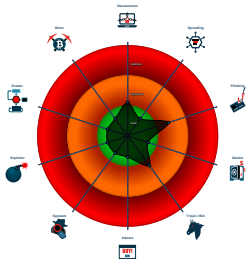
Detection

Score:	2
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Connects to several IPs in different …
- Form action URLs do not match mai…
- Found iframes
- HTML title does not match URL

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 4952 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5640 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4952 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 7896 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4952 CREDAT:82962 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 8024 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4952 CREDAT:17424 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 8152 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4952 CREDAT:82970 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

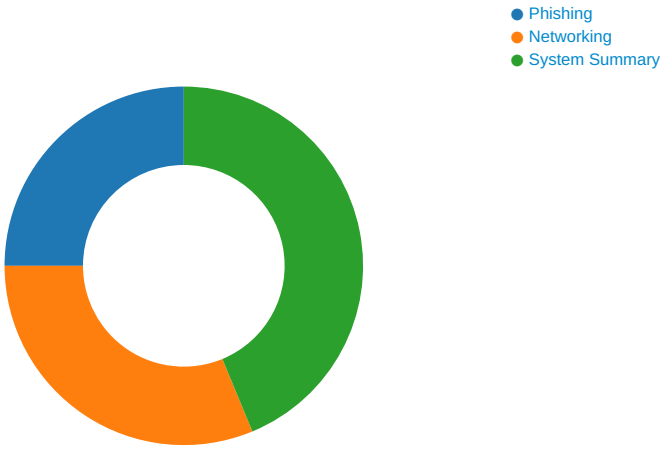
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



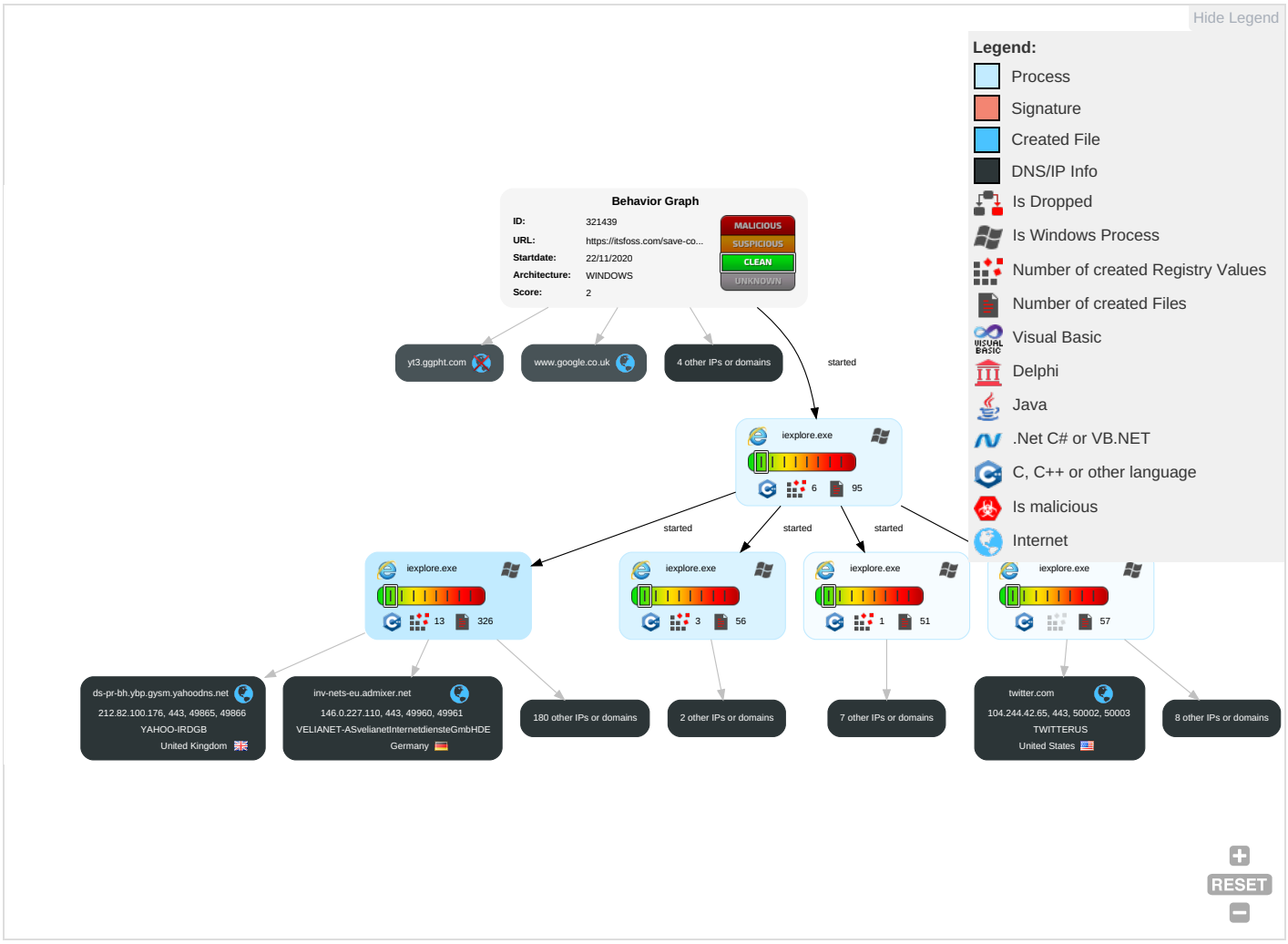
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

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
Drive-by Compromise 1	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory 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
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups

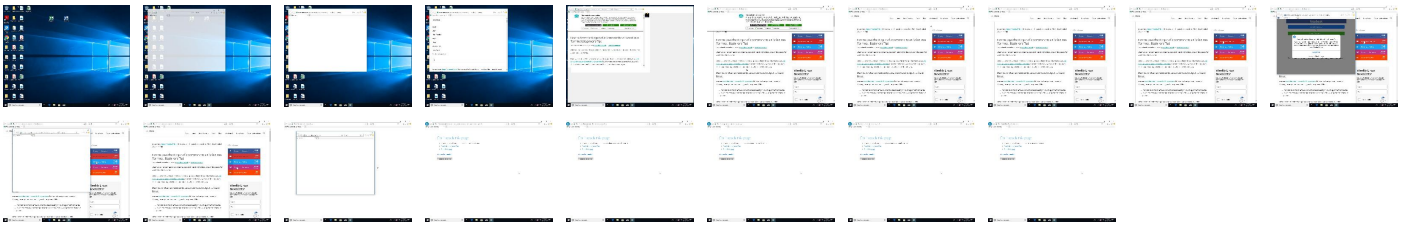
Behavior Graph

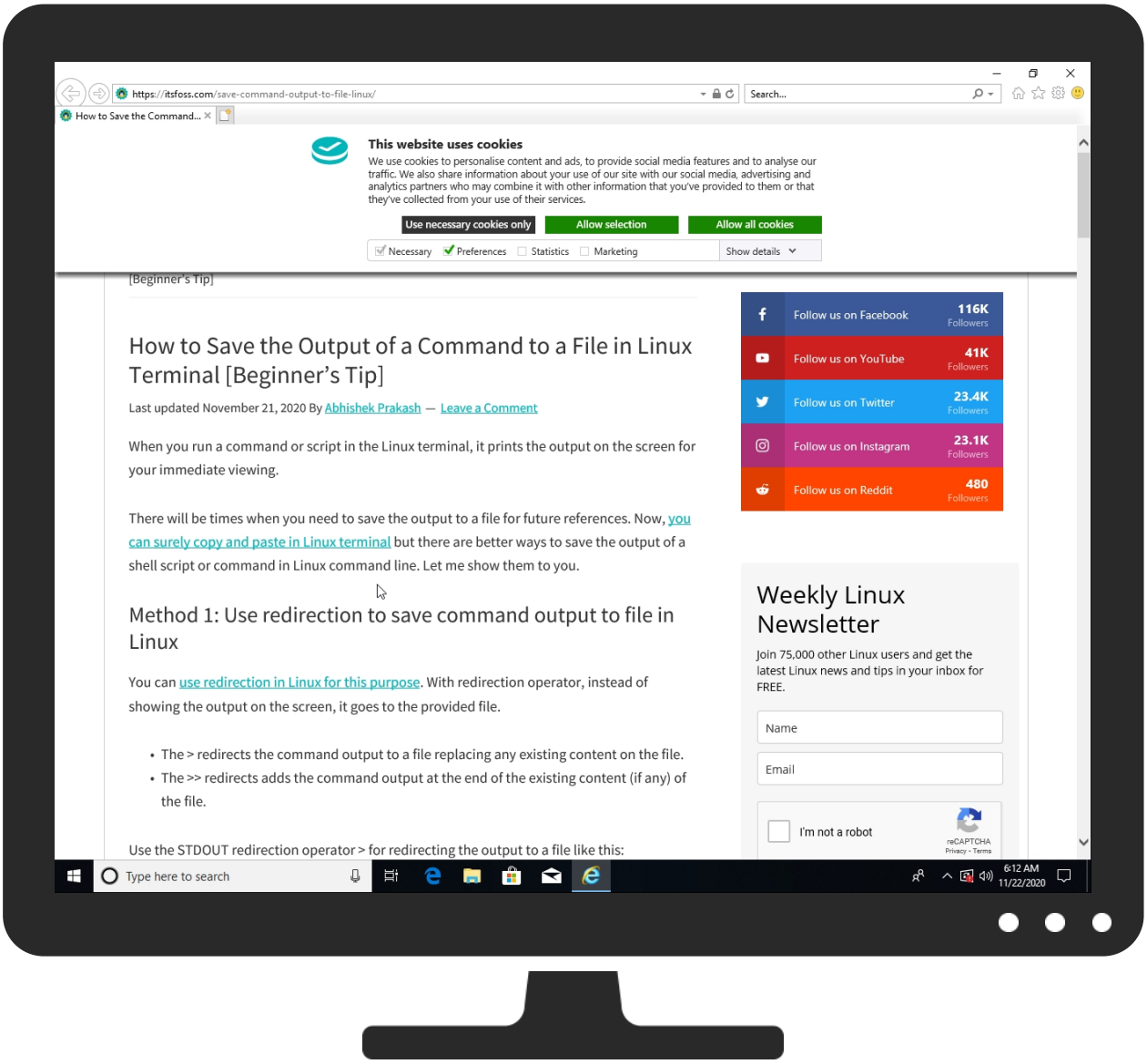


Screenshots

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://itsfoss.com/save-command-output-to-file-linux/	0%	Virustotal		Browse
http://https://itsfoss.com/save-command-output-to-file-linux/	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
acuityplatform.com	0%	Virustotal		Browse
tls13.taboola.map.fastly.net	0%	Virustotal		Browse
pub.searchiq.co	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://ssp.programattik.com/hb	0%	Avira URL Cloud	safe	
http://polymer.github.io/AUTHORS.txt	0%	Avira URL Cloud	safe	
http://https://www.internalfb.com/intern/invariant/	0%	URL Reputation	safe	
http://https://www.internalfb.com/intern/invariant/	0%	URL Reputation	safe	
http://https://www.internalfb.com/intern/invariant/	0%	URL Reputation	safe	
http://https://itsfoss.cd-choices-opt-out/interest-based-advertising-policy-and-opt-out/xt/html$	0%	Avira URL Cloud	safe	
http://fontello.comdashiconsRegulardashiconsdashiconsVersion	0%	Avira URL Cloud	safe	
http://https://linuxhandbook.com/redirection-linux/	0%	Avira URL Cloud	safe	
http://polymer.github.io/PATENTS.txt	0%	Avira URL Cloud	safe	
http://https://ssp.programattik.com/sync	0%	Avira URL Cloud	safe	
http://https://a.omappapi.com/app/js/api.min.js	0%	Avira URL Cloud	safe	
http://https://www.internedservices.nl/disclaimer-privacy-policy/tising-policy-and-opt-out/	0%	Avira URL Cloud	safe	
http://https://itsfoss.c/privacy-policyt/interest-based-advertising-policy-and-opt-out/xt/html$	0%	Avira URL Cloud	safe	
http://https://id5-sync.com/g/v1/	0%	Avira URL Cloud	safe	
http://https://wa.me/?text=	0%	Avira URL Cloud	safe	
http://https://www.google.%/ads/ga-audiences?	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences?	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences?	0%	URL Reputation	safe	
http://https://itsfoss.cRoot	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
stats.wp.com	192.0.76.3	true	false		high
um.simpli.fi	159.253.128.188	true	false		high
acuityplatform.com	154.59.122.74	true	false	• 0%, Virustotal, Browse	unknown
lga-bh-bgp.contextweb.com	198.148.27.140	true	false		high
tls13.taboola.map.fastly.net	151.101.1.44	true	false	• 0%, Virustotal, Browse	unknown
global.px.quantserve.com	91.228.74.133	true	false		high
pixel-a.sitescout.com	66.155.71.150	true	false		high
pub.searchiq.co	172.67.156.77	true	false	• 0%, Virustotal, Browse	unknown
omappapi.awesomemotive.netdna-cdn.com	23.111.11.71	true	false		high
ads-1460635594.eu-central-1.elb.amazonaws.com	18.185.216.221	true	false		high
facebook.com	185.60.216.35	true	false		high
match-1943069928.eu-west-1.elb.amazonaws.com	52.50.156.162	true	false		high
csync.loopme.me	116.202.114.114	true	false		high
eu2-ice.360yield.com	52.58.204.249	true	false		high
cs510.wpc.edgecastcdn.net	152.199.21.141	true	false		high
match.prod.bidr.io	54.171.14.147	true	false		unknown
static.am5.vip.prod.criteo.net	178.250.2.130	true	false		high
ssp-ats-prod-eu-central-1.one-mobile-prod.aws.oath.cloud	18.156.195.47	true	false		unknown
uip.semasio.net	77.243.60.138	true	false		high
gum.par.vip.prod.criteo.com	178.250.0.157	true	false		high
i0.wp.com	192.0.77.2	true	false		high
pixel.onaudience.com	51.210.112.66	true	false		unknown
i2.wp.com	192.0.77.2	true	false		high
d1ykf07e75w7ss.cloudfront.net	13.224.103.105	true	false		high
fbsbx.com	185.60.216.35	true	false		high
pugm-lhr.pubmatic.com	185.64.190.78	true	false		high
www.google.co.uk	172.217.21.227	true	false		unknown
googlehosted.l.googleusercontent.com	172.217.21.193	true	false		high
r5.sn-4g5e6nz7.googlevideo.com	173.194.187.170	true	false		high
spug-lhr.pubmatic.com	185.64.190.81	true	false		high
d1azc1qln24ryf.cloudfront.net	13.224.89.144	true	false		high
hb-api-fra02.omnitagjs.com	185.255.84.151	true	false		high
naeu.geo.cloudwm-cdn.com	185.127.17.52	true	false		unknown
static.apester.com	35.190.72.53	true	false		high
api.searchiq.co	172.67.156.77	true	false		unknown
itx5.smartadserver.com	185.86.138.32	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
scontent.xx.fbcdn.net	185.60.216.19	true	false		high
load-ams1.exelator.com	147.75.102.200	true	false		high
tag.1rx.io	213.19.147.210	true	false		high
d5p.de17a.com	213.155.156.181	true	false		high
pixel.tapad.com	35.227.248.159	true	false		high
pagead46.l.doubleclick.net	172.217.23.130	true	false		high
twitter.com	104.244.42.65	true	false		high
i1.wp.com	192.0.77.2	true	false		high
fbcdn.net	185.60.216.35	true	false		high
dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com	35.158.49.68	true	false		high
jita-rtk-io-dmyt03fgsksh5xx.stackpathdns.com	151.139.240.35	true	false		high
match.adsby.bidtheatre.com	174.138.12.104	true	false		unknown
ib.anycast.adnxs.com	185.33.220.243	true	false		high
prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud	3.126.56.137	true	false		unknown
static.mailerlite.com	104.18.2.159	true	false		high
btlr-ecs-eu-central-1.sharethrough.com	52.28.154.93	true	false		high
pug-lhr.pubmatic.com	185.64.190.80	true	false		high
i.ytimg.com	216.58.212.150	true	false		high
eu-u.openx.net	34.98.64.218	true	false		high
a.pub.network	104.26.0.139	true	false		unknown
hbopenbid22000nf.pubmatic.com	185.64.189.112	true	false		high
tpop-api.twitter.com	104.244.42.66	true	false		high
c0.wp.com	192.0.77.37	true	false		high
elb-aws-fr-verona-1711955695.eu-central-1.elb.amazonaws.com	18.159.79.175	true	false		high
widget.par.vip.prod.criteo.com	178.250.0.163	true	false		high
pagead.l.doubleclick.net	216.58.212.130	true	false		high
tagr-gcp-odr-euw4.mookie1.com	34.98.67.61	true	false		high
sync.crwdcntrl.net	52.49.190.28	true	false		high
photos-ugc.l.googleusercontent.com	172.217.23.161	true	false		high
renderer.apester.com	35.186.220.219	true	false		high
ds-pr-bh.ybp.gysm.yahoodns.net	212.82.100.176	true	false		unknown
sync.1rx.io	213.19.147.150	true	false		high
track.mailerlite.com	104.18.2.159	true	false		high
ads.playground.xyz	52.57.47.66	true	false		unknown
d1lpgznae1530s.cloudfront.net	13.224.102.94	true	false		high
33xchange-1576862511.us-east-1.elb.amazonaws.com	54.165.26.185	true	false		high
star-mini.c10r.facebook.com	185.60.216.35	true	false		high
bidder.par.vip.prod.criteo.com	178.250.0.165	true	false		high
itsfoss.com	104.26.8.105	true	false		high
us-u.openx.net	35.244.159.8	true	false		high
dsp.adfarm1.adition.com	85.114.159.118	true	false		high
bucket.rtk.io	147.75.84.99	true	false		high
ams01.sync.search.spotxchange.com	185.94.180.125	true	false		high
a.tribalfusion.com	104.18.12.5	true	false		high
live-eu-am.sekindo.com	185.220.204.220	true	false		high
sync.audiencepixel.com	45.61.136.49	true	false		unknown
pixel-origin.mathtag.com	185.29.133.199	true	false		high
s.tribalfusion.com	104.18.12.5	true	false		high
secure.gravatar.com	192.0.73.2	true	false		high
cs45.wac.edgecastcdn.net	93.184.220.70	true	false		high
u.openx.net	34.98.64.218	true	false		high
alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com	52.57.142.16	true	false		high
geolocation-db.com	46.101.248.169	true	false		unknown
apester-d.openx.net	35.244.159.8	true	false		high
inv-nets-eu.admixer.net	146.0.227.110	true	false		high
events.apester.com	35.190.63.234	true	false		high
rtb.gumgum.com	108.129.8.178	true	false		high
pixel.33across.com	67.202.110.21	true	false		high
org-481-0bf84-dmyt03fgsksh5xx.stackpathdns.com	151.139.240.22	true	false		high
prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud	35.156.106.231	true	false		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
static.searchiq.co	104.18.53.245	true	false		unknown
pug22000nf.pubmatic.com	185.64.189.110	true	false		high
spug22000nf.pubmatic.com	185.64.189.114	true	false		high
partnerad.l.doubleclick.net	172.217.21.226	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://smartstream.tv/de/datenschutz	false		unknown
http://www.bidswitch.com/privacy-policy/	false		high
http://https://www.admedo.com/privacy-policy	false		high

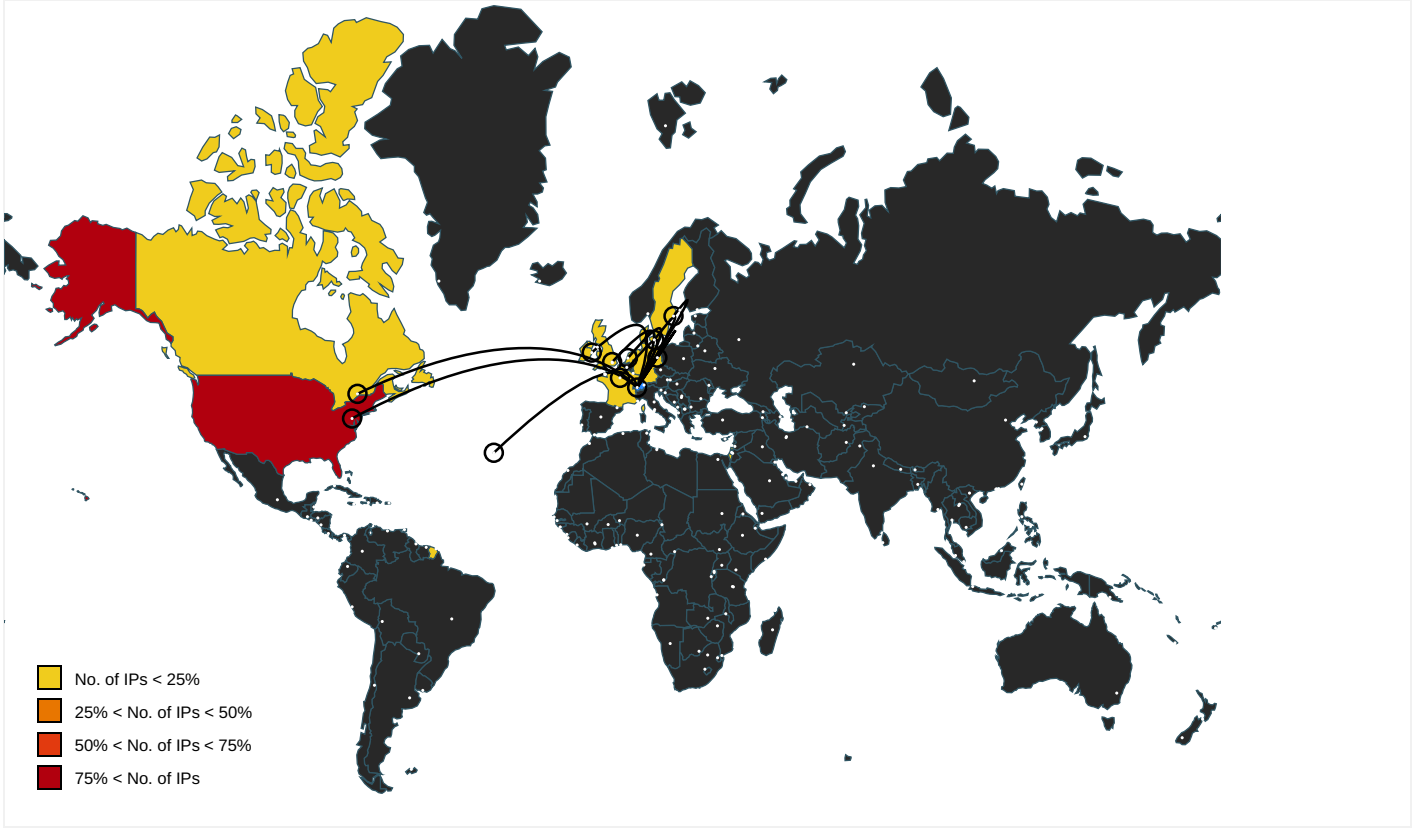
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://itsfoss.com/wp-content/plugins/socialsnap-plus/assets/css/socialsnap.css?ver=1.1.13	save-command-output-to-file-linux[1].htm.2.dr	false		high
http://https://mobile.twitter.com/i/nojs_router?path=%2Fitsfoss2%2F	itsfoss2[1].htm.17.dr	false		high
http://33across.com/privacy-policy/put-to-file-linux/rop4294967295	~DFCF7A576ABFFB88AA.TMP.1.dr	false		high
http://https://live.sekindo.com/live/liveView.php?njs=1&ito=1&vid_event=42&serverTime=1606021930&vid_player	liveVideo[1].htm.2.dr	false		high
http://https://twitter.com/itsfoss2/?lang=fa	itsfoss2[1].htm.17.dr	false		high
http://https://itsfoss.com/bootable-windows-usb-linux/	liveVideo[1].htm.2.dr	false		high
http://https://itsfoss.com/save-command-output-to-file-linux/?primis_content=embed4e69akmqnlur	liveVideo[1].htm.2.dr	false		high
http://https://ssp.programattik.com/hb	prebidVid.3.19.0_10.min[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://twitter.com/itsfoss2/?lang=fi	itsfoss2[1].htm.17.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web-legacy/icon-svg.9e211f65.svg	itsfoss2[1].htm.17.dr	false		high
http://https://itsfoss.com/favicon.ico	imagestore.dat.2.dr	false		high
http://https://itsfoss.com/wp-content/themes/genesis/lib/js/skip-links.min.js?ver=3.3.3	save-command-output-to-file-linux[1].htm.2.dr	false		high
http://www.optomaton.com/privacy.html	{B2129D5D-2CCC-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://twitter.com/itsfoss2/?lang=fr	itsfoss2[1].htm.17.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web-legacy/vendors~main.68b1d365.js	itsfoss2[1].htm.17.dr	false		high
http://https://itsfoss.com/save-command-output-to-file-linux/?primis_content=embed73642xyvqthg	liveVideo[1].htm.2.dr	false		high
http://https://live.sekindo.com/live/liveView.php?njs=1&ito=1&vid_event=35&serverTime=1606021930&vid_player	liveVideo[1].htm.2.dr	false		high
http://https://live.sekindo.com/live/liveView.php?njs=1&ito=1&vid_event=31&serverTime=1606021930&vid_player	liveVideo[1].htm.2.dr	false		high
http://polymer.github.io/AUTHORS.txt	desktop_polymer_inlined_html_polymer_flags_legacy_browsers[1].js.16.dr	false	• Avira URL Cloud: safe	unknown
http://https://itsfoss.com/sa	{B2129D5D-2CCC-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://cm.g.doubleclick.net/pixel?google_nid=openx&google_cm&google_sc	pd[1].htm.2.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web-legacy/polyfills.78d11e15.js.m	polyfills.78d11e15[1].js.17.dr	false		high
http://https://www.internalfb.com/intern/invariant/	m3riRLHGxZh[1].js.15.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.opensource.org/licenses/mit-license.php	superfish.min[1].js.2.dr	false		high
http://https://schema.org/WPSideBar	save-command-output-to-file-linux[1].htm.2.dr	false		high
http://https://i2.wp.com/itsfoss.com/wp-content/uploads/2020/02/ask-here.jpg?resize=300%2C86&ssl=1	save-command-output-to-file-linux[1].htm.2.dr	false		high
http://https://twitter.com/itsfoss2/?lang=ga	itsfoss2[1].htm.17.dr	false		high
http://https://itsfoss.com/wp-json/	save-command-output-to-file-linux[1].htm.2.dr	false		high
http://https://itsfoss.cd-choices-opt-out/interest-based-advertising-policy-and-opt-out/xt/html$	{B2129D5D-2CCC-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.cookiebot.com	cc[1].js.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://twitter.com/itsfoss2/?lang=gl	itsfoss2[1].htm.17.dr	false		high
http://https://i2.wp.com/itsfoss.com/wp-content/uploads/2020/02/ask-here.jpg?w=350&ssl=1	save-command-output-to-file-linux[1].htm.2.dr	false		high
http://https://secure.gravatar.com/images/grav-share-sprite.png);background-repeat:no-repeat;width:16px;hei	jetpack[1].css.2.dr	false		high
http://https://d1azc1qln24ryf.cloudfront.net	5cda8d66e3665c12b2113301[1].htm.2.dr	false		high
http://https://live.sekindo.com/live/liveView.php?njs=1&ito=1&vid_event=24&serverTime=1606021930&vid_player	liveVideo[1].htm.2.dr	false		high
http://https://twitter.com/itsfoss2/?lang=gu	itsfoss2[1].htm.17.dr	false		high
http://https://live.sekindo.com/live/liveView.php?njs=1&ito=1&vid_event=20&serverTime=1606021930&vid_player	liveVideo[1].htm.2.dr	false		high
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web-legacy/bundle.NetworkInstrumen	bundle.NetworkInstrument.e3ff3b25[1].js.17.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/y6/l/0	Its-FOSS-Linux-Blog--184328509 9062669[1].htm.15.dr	false		high
http://https://itsfoss.com/save-command-output-to-file-linux/redirecting_command_output_to_file/	save-command-output-to-file-linux[1].htm.2.dr	false		high
http://https://twitter.com/itsfoss2/?lang=de	itsfoss2[1].htm.17.dr	false		high
http://fontello.comdashiconsRegulardashiconsdashiconsVersion	dashicons[1].eot.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://renderer.apester.com/v2/static/main.0e32b39aad0081b2af83.bundle.js	5cda8d66e3665c12b2113301[1].htm.2.dr	false		high
http://https://twitter.com/itsfoss2/?lang=da	itsfoss2[1].htm.17.dr	false		high
http://https://video.sekindo.com/uploads/cn19/video/users/converted/25204/video_5b5845c36cf6d068557072/vid5	liveVideo[1].htm.2.dr	false		high
http://https://itsfoss.com/save-command-output-to-file-linux/tHow	{B2129D5D-2CCC-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://itsfoss.com/save-command-output-to-file-linux/?primis_content=embed4ed92gxjypls	liveVideo[1].htm.2.dr	false		high
http://https://linuxhandbook.com/redirection-linux/	save-command-output-to-file-linux[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://live.sekindo.com/live/liveJsonVid.php?vidUrl=	liveVideo[1].htm.2.dr	false		high
http://polymer.github.io/PATENTS.txt	desktop_polymer_inlined_html_polymer_flags_legacy_browsers[1].js.16.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.primis.tech?utm_source=promoted	liveVideo[1].htm.2.dr	false		high
http://https://video.sekindo.com/uploads/cn21/video/users/converted/25204/video_5b5845c36cf6d068557072/vid5	liveVideo[1].htm.2.dr	false		high
http://https://display.apester.com	5cda8d66e3665c12b2113301[1].htm.2.dr	false		high
http://https://ssp.programattik.com/sync	prebidVid.3.19.0_10.min[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.beeswax.com/cookies/zy/y/i.aspxicy/	~DFCF7A576ABFFB88AA.TMP.1.dr	false		high
http://https://www.youtube.com/channel/UCEU9D6KIShdLeTRyH3IdSvw	UCEU9D6KIShdLeTRyH3IdSvw[1].htm.16.dr	false		high
http://https://a.omappapi.com/app/js/api.min.js	save-command-output-to-file-linux[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://schema.org/ImageObject	UCEU9D6KIShdLeTRyH3IdSvw[1].htm.16.dr	false		high
http://https://schema.org/ListItem	save-command-output-to-file-linux[1].htm.2.dr	false		high
http://https://c0.wp.com/c/5.5.3/wp-includes/css/dist/block-library/style.min.css	save-command-output-to-file-linux[1].htm.2.dr	false		high
http://https://pixel.tapad.com/idsync/ex/receive/check?partner_id=PUBMATIC_RTB	{B2129D5D-2CCC-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://www.internedservices.nl/disclaimer-privacy-policy/tising-policy-and-opt-out/	~DFCF7A576ABFFB88AA.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://schema.org/WPHeader	save-command-output-to-file-linux[1].htm.2.dr	false		high
http://www.opensource.org/licenses/mit-license.php)	ml_jQuery.inputmask.bundle.min[1].js.2.dr	false		high
http://https://itsfoss.c/privacy-policyt/interest-based-advertising-policy-and-opt-out/xt/html$	{B2129D5D-2CCC-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://itsfoss.com/wp-content/plugins/wp-coupons/css/style.min.css?ver=1.7.4	save-command-output-to-file-linux[1].htm.2.dr	false		high
http://https://stats.g.doubleclick.net/j/collect?	ga[1].js.2.dr	false		high
http://https://www.youtube.com/ads/	UCEU9D6KIShdLeTRyH3IdSvw[1].htm.16.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ads.pubmatic.com/AdServer/js/showad.js	{B2129D5D-2CCC-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://itsfoss.com/save-command-output-to-file-linux/rop4294967295	~DFCF7A576ABFFB88AA.TMP.1.dr	false		high
http://https://interaction.apester.com	5cda8d66e3665c12b2113301[1].htm.2.dr	false		high
http://https://twitter.com/itsfoss2/?lang=en	itsfoss2[1].htm.17.dr	false		high
http://https://twitter.com/itsfoss2/?lang=el	itsfoss2[1].htm.17.dr	false		high
http://https://id5-sync.com/g/v1/	prebidVid.3.19.0_10.min[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ssc-cms.33across.com/ps/?m=xch&rt=html&ru=deb&id=dyh8gwOhar6jXyaKkv7mNO&gdpr_consent=undefin	{B2129D5D-2CCC-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://twitter.com/itsfoss2/?lang=eu	itsfoss2[1].htm.17.dr	false		high
http://https://wa.me/?text=	liveVideo[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://twitter.com/itsfoss2/?lang=es	itsfoss2[1].htm.17.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/ya/r/O2aKM2iSbOw.png	imagestore.dat.15.dr	false		high
http://https://itsfoss.com/wp-content/plugins/stackable-ultimate-gutenberg-blocks-premium/dist/frontend_blo	save-command-output-to-file-linux[1].htm.2.dr	false		high
http://https://itsfoss.com/feedback/	save-command-output-to-file-linux[1].htm.2.dr	false		high
http://https://itsfoss.com/wp-content/plugins/atomic-blocks/dist/assets/js/dismiss.js?ver=1603943004	save-command-output-to-file-linux[1].htm.2.dr	false		high
http://https://d1azc1qln24ryf.cloudfront.net/124741/ApesterPlayer/Apester-Font.eot?u8c17e	style-cf[1].css.2.dr	false		high
http://https://i0.wp.com/itsfoss.com/wp-content/uploads/2020/11/pipe-output-to-file-linux.png?resize=150%2C	save-command-output-to-file-linux[1].htm.2.dr	false		high
http://https://www.instagram.com/itsfoss/	save-command-output-to-file-linux[1].htm.2.dr	false		high
http://https://www.linkedin.com/cws/share	save-command-output-to-file-linux[1].htm.2.dr	false		high
http://https://itsfoss.com/wp-content/plugins/searchiq/assets/3.5/css/frontend/stylesheet.css?ver=160599932	save-command-output-to-file-linux[1].htm.2.dr	false		high
http://www.twitter.com/	msapplication.xml5.1.dr	false		high
http://https://static.mailerlite.com/js/w/webforms.min.js?v5c5d99c28cfe49b41fe82455507d7558	save-command-output-to-file-linux[1].htm.2.dr	false		high
http://https://mastodon.social/	save-command-output-to-file-linux[1].htm.2.dr	false		high
http://https://www.youtube.com/error_204?t=jserror&level=ERROR	UCEU9D6KIShdLeTRyH3IdSvw[1].htm.16.dr	false		high
http://https://www.bannerflow.com/privacy	{B2129D5D-2CCC-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://www.google.%/ads/ga-audiences?	ga[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://platform.twitter.com/widgets.js	configuration[1].js.2.dr	false		high
http://https://itsfoss.cRoot	{B2129D5D-2CCC-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://twitter.com/itsfoss2/?lang=ko	itsfoss2[1].htm.17.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
178.250.0.157	unknown	France		44788	ASN-CRITEO-EUROPEFR	false
46.101.248.169	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	false
87.98.128.108	unknown	France		16276	OVHFR	false
185.220.204.220	unknown	Israel		41436	CLOUDWEBMANAGE-EUGB	false
172.67.156.77	unknown	United States		13335	CLOUDFLARENETUS	false
185.64.190.80	unknown	United Kingdom		62713	AS-PUBMATICUS	false
185.64.190.81	unknown	United Kingdom		62713	AS-PUBMATICUS	false
52.50.156.162	unknown	United States		16509	AMAZON-02US	false
216.58.212.150	unknown	United States		15169	GOOGLEUS	false
35.227.248.159	unknown	United States		15169	GOOGLEUS	false
185.33.220.244	unknown	Netherlands		29990	ASN-APPNEXUS	false
185.33.220.243	unknown	Netherlands		29990	ASN-APPNEXUS	false
35.158.49.68	unknown	United States		16509	AMAZON-02US	false
192.0.77.2	unknown	United States		2635	AUTOMATTICUS	false
213.19.147.151	unknown	United Kingdom		26120	RHYTHMONEUS	false
178.250.0.163	unknown	France		44788	ASN-CRITEO-EUROPEFR	false
213.19.147.150	unknown	United Kingdom		26120	RHYTHMONEUS	false
192.0.73.2	unknown	United States		2635	AUTOMATTICUS	false
178.250.0.165	unknown	France		44788	ASN-CRITEO-EUROPEFR	false
185.60.216.35	unknown	Ireland		32934	FACEBOOKUS	false
151.101.1.44	unknown	United States		54113	FASTLYUS	false
18.185.216.221	unknown	United States		16509	AMAZON-02US	false
216.58.212.162	unknown	United States		15169	GOOGLEUS	false
104.18.12.5	unknown	United States		13335	CLOUDFLARENETUS	false
185.86.138.32	unknown	France		201081	SMARTADSERVERFR	false
147.75.84.99	unknown	Switzerland		54825	PACKETUS	false
54.171.14.147	unknown	United States		16509	AMAZON-02US	false
185.255.84.151	unknown	France		200271	IGUANE-FR	false
185.29.133.199	unknown	United Kingdom		30419	MEDIAMATH-INCUS	false
172.217.21.226	unknown	United States		15169	GOOGLEUS	false
185.64.189.110	unknown	United Kingdom		62713	AS-PUBMATICUS	false
185.64.189.112	unknown	United Kingdom		62713	AS-PUBMATICUS	false
185.64.189.114	unknown	United Kingdom		62713	AS-PUBMATICUS	false
152.199.21.141	unknown	United States		15133	EDGECASTUS	false
151.139.240.22	unknown	United States		33438	HIGHWINDS2US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
178.250.2.130	unknown	France		44788	ASN-CRITEO-EUROPEFR	false
91.228.74.133	unknown	United Kingdom		27281	QUANTCASTUS	false
213.19.147.210	unknown	United Kingdom		26120	RHYTHMONEUS	false
192.0.76.3	unknown	United States		2635	AUTOMATTICUS	false
185.64.190.78	unknown	United Kingdom		62713	AS-PUBMATICUS	false
35.190.72.53	unknown	United States		15169	GOOGLEUS	false
146.0.227.110	unknown	Germany		29066	VELIANET-ASvelianetInternetdiensteGmbHDE	false
147.75.102.200	unknown	Switzerland		54825	PACKETUS	false
66.155.71.150	unknown	Canada		13768	COGECO-PEER1CA	false
67.202.110.21	unknown	United States		32748	STEADFASTUS	false
52.57.47.66	unknown	United States		16509	AMAZON-02US	false
13.224.103.105	unknown	United States		16509	AMAZON-02US	false
52.49.190.28	unknown	United States		16509	AMAZON-02US	false
85.114.159.118	unknown	Germany		24961	MYLOC-ASIPBackboneofmyLocmanagedITAGDE	false
52.28.154.93	unknown	United States		16509	AMAZON-02US	false
77.243.60.138	unknown	Denmark		42697	NETIC-ASDK	false
172.217.23.130	unknown	United States		15169	GOOGLEUS	false
212.82.100.176	unknown	United Kingdom		34010	YAHOO-IRDGB	false
35.156.106.231	unknown	United States		16509	AMAZON-02US	false
104.26.0.139	unknown	United States		13335	CLOUDFLARENETUS	false
213.155.156.181	unknown	European Union		1299	TELIANETTeliaCarrierEU	false
52.57.142.16	unknown	United States		16509	AMAZON-02US	false
13.224.89.144	unknown	United States		16509	AMAZON-02US	false
104.26.8.105	unknown	United States		13335	CLOUDFLARENETUS	false
35.186.220.219	unknown	United States		15169	GOOGLEUS	false
108.129.8.178	unknown	United States		16509	AMAZON-02US	false
192.0.77.37	unknown	United States		2635	AUTOMATTICUS	false
18.159.79.175	unknown	United States		16509	AMAZON-02US	false
3.126.56.137	unknown	United States		16509	AMAZON-02US	false
151.139.240.35	unknown	United States		33438	HIGHWINDS2US	false
34.98.67.61	unknown	United States		15169	GOOGLEUS	false
154.59.122.74	unknown	United States		174	COGENT-174US	false
51.210.112.66	unknown	France		16276	OVHFR	false
52.58.204.249	unknown	United States		16509	AMAZON-02US	false
13.224.102.94	unknown	United States		16509	AMAZON-02US	false
45.61.136.49	unknown	United States		40676	AS40676US	false
104.18.53.245	unknown	United States		13335	CLOUDFLARENETUS	false
159.253.128.188	unknown	Netherlands		36351	SOFTLAYERUS	false
104.18.2.159	unknown	United States		13335	CLOUDFLARENETUS	false
116.202.114.114	unknown	Germany		24940	HETZNER-ASDE	false
35.244.159.8	unknown	United States		15169	GOOGLEUS	false
185.94.180.125	unknown	Netherlands		35220	SPOTX-AMSNL	false
54.165.26.185	unknown	United States		14618	AMAZON-AESUS	false
104.26.12.50	unknown	United States		13335	CLOUDFLARENETUS	false
216.58.212.130	unknown	United States		15169	GOOGLEUS	false
172.217.16.162	unknown	United States		15169	GOOGLEUS	false
23.111.11.71	unknown	United States		33438	HIGHWINDS2US	false
104.244.42.66	unknown	United States		13414	TWITTERUS	false
89.207.16.140	unknown	Sweden		25751	VALUECLICKUS	false
104.244.42.65	unknown	United States		13414	TWITTERUS	false
198.148.27.140	unknown	United States		19189	PULSEPOINTUS	false
174.138.12.104	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
35.190.63.234	unknown	United States		15169	GOOGLEUS	false
185.60.216.19	unknown	Ireland		32934	FACEBOOKUS	false
34.98.64.218	unknown	United States		15169	GOOGLEUS	false
93.184.220.70	unknown	European Union		15133	EDGECASTUS	false
185.127.17.52	unknown	Israel		210329	CLOUDWEBMANAGE-UK-1GB	false
18.156.195.47	unknown	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321439
Start date:	22.11.2020
Start time:	06:11:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://itsfoss.com/save-command-output-to-file-linux/
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:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean2.win@9/345@123/94
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: http://33across.com/privacy-policy/ • Browsing link: https://4finance.com/ad-choices-opt-out/interest-based-advertising-policy-and-opt-out/ • Browsing link: https://www.admedo.com/privacy-policy • Browsing link: https://www.int ernedservices.nl/disclaimer-privacy-policy/ • Browsing link: http://www.programattik.com/gizlilik-politikasi.aspx • Browsing link: https://www.sportradar.com/about-us/privacy/ • Browsing link: http://www.opto maton.com/privacy.html • Browsing link: http://www.bidswitch.com/privacy-policy/ • Browsing link: https://smartst ream.tv/de/datenschutz • Browsing link: https://www.bannerflow.com/privacy • Browsing link: https://www.beeswax.com/cookies/
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): 104.43.193.48, 104.43.139.144, 104.83.120.32, 95.101.20.192, 95.101.20.161, 216.58.210.4, 172.217.18.106, 92.123.45.62, 216.58.205.227, 151.101.2.217, 151.101.66.217, 151.101.130.217, 151.101.194.217, 172.217.18.168, 172.217.18.99, 2.20.85.92, 2.20.85.164, 2.20.142.210, 2.20.142.209, 40.88.32.150, 172.217.22.74, 172.217.23.142, 172.217.23.161, 172.217.23.97, 69.173.144.140, 69.173.144.141, 69.173.144.143, 151.101.2.49, 151.101.66.49, 151.101.130.49, 151.101.194.49, 2.20.85.83, 104.83.125.139, 37.157.4.23, 37.157.6.246, 37.157.2.236,

37.157.4.28, 37.157.6.242, 37.157.2.237, 37.157.4.41, 37.157.6.252, 46.228.164.11, 173.231.180.197, 51.104.139.180, 152.199.19.161, 2.20.84.85, 20.54.26.129, 172.217.21.238, 216.58.205.238, 216.58.207.78, 216.58.206.14, 172.217.16.174, 216.58.210.14, 172.217.23.110, 216.58.212.142, 172.217.22.46, 172.217.18.110, 172.217.22.110, 216.58.212.174, 142.250.74.206, 172.217.23.174, 172.217.22.78, 172.217.18.173, 92.122.213.247, 92.122.213.194

- Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, consent.cookiebot.com.edgekey.net, uipglob.trafficmanager.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, afp.dotomi.weighted.com.akadns.net, www.google.com, ssl-google-analytics.l.google.com, watson.telemetry.microsoft.com, www.gstatic.com, au-bg-shim.trafficmanager.net, secure-adnxs.edgekey.net, www.google-analytics.com, fonts.googleapis.com, pagead-googlehosted.l.google.com, e8960.b.akamaiedge.net, fs.microsoft.com, ajax.googleapis.com, 2-01-275d-0028.cdx.cedexis.net, ris-prod.trafficmanager.net, skypedataprdcolcus16.cloudapp.net, pagead2.googlesyndication.com, skypedataprdcolcus15.cloudapp.net, e34372.dsca.akamaiedge.net, ris.api.iris.microsoft.com, youtube-ui.l.google.com, rtb.adgrx.com.tech.akadns.net, blobcollector.events.data.trafficmanager.net, e6603.g.akamaiedge.net, eus.rubiconproject.com.edgekey.net, h2.shared.global.fastly.net, cs9.wpc.v0cdn.net, au.download.windowsupdate.com.edgesuite.net, cs2-wac.apr-8315.edgecastdns.net, t2.shared.global.fastly.net, adservice.google.com, track.adformnet.akadns.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, tagged-by.rubiconproject.net.akadns.net, arc.msn.com, iecvlist.microsoft.com, go.microsoft.com, e8037.g.akamaiedge.net, 1e853f314c0997eb2ba831bbd90178d3.safeframe.googlesyndication.com, pubmatic.edgekey.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, consentcdn.cookiebot.com-v1.edgekey.net, e3849.dsca.akamaiedge.net, www-google-analytics.l.google.com, accounts.google.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, ad.turn.com.akadns.net, sync.search-gtm.spotxchange.com.akadns.net, ssl.google-analytics.com, as-sec.casalemedia.com.edgekey.net, tpc.googlesyndication.com, go.microsoft.com.edgekey.net, ssum-sec.casalemedia.com.edgekey.net, e6115.g.akamaiedge.net
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	117872
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	1536:i/LAvEZrGclx0hoW6qCLdNz2p+/LAvEZrGclx0hoW6qCLdNz2pj:UcMqZVCp8pwcMqZVCp8pj
MD5:	DB381E85D86EA4484D20078E9EC667A6
SHA1:	4871FDAF0C2EEC8183FC3CE7710B18FD3C647CEA
SHA-256:	C3520E3A6EB43F6D416852C454414C5D7823A96FB9070BC30301ADDEBB334D4D
SHA-512:	D9E03A617D1D9505D3ADA3C41FC8A53504F4F1C44F92AF00869F2FE150D6677FD4450E85EB1E3D920D32BA01F190E7F14BF130F8CC69EB47D834CCE43CAA765 0
Malicious:	false
Reputation:	low
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:.(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC... 3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.... ....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G..... ..b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u. .s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`...........A$:.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.120749303734162
Encrypted:	false
SSDEEP:	12:skvkPlE99SNxAhUegeTQawvkPlE99SNxAhUegeT2:skvkPcUQU76MvkPcUQU762
MD5:	32068917B454BC05FEA93CB95B00B423
SHA1:	347F873C2FBCD49BEC2EF561F945EC61545D1B09
SHA-256:	A13D809D332449459B7E6CDC6D4F7BE770539E92ACD24E5FB6BA8AB479C0466D
SHA-512:	65807806EC129A81826B7D01DDF72455C4794C55713553FDD043984AEE2E83DB7CF582B4B95B4FBCF0146A46C7E533CBA04763461DFA114B6CDAE9CE5D9237E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Preview:	p..... .....U.x....(..... .....Y.....$.....8...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...p..... .....s.x....(..... .....Y.....$.....8...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...".0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\9JTW3P5P\ads.pubmatic[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	594
Entropy (8bit):	4.964415277428922
Encrypted:	false
SSDEEP:	12:JsrUHVlgP4CSMRrT69J4NOrUHVlgP4CR0RrT69GNOrUHVlI4vRrTxP4CR0RrT69q:WUy4RQrTEKIUy4EorTEGIUU4JrTt4Eor
MD5:	49EB982EB4FE4EA2D02B1ED243781B3F
SHA1:	966358310CE0EBCD0BB2F39BFF4E252A5C17C4DF
SHA-256:	F1FCBFD6C97B3893B4EB680321FFAC9FB620CDC2610289947FA15D6C23734B2A
SHA-512:	4DDE274DF84BC5F382534B8D88875BF57F6D7834DB9A00ABE5F1F99490A6EF1394ECC0717FB4865340C40A5CD27DADB53FAC311C8D4BAD12324E99E682C35E3
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="PubMatic_USP" value="{"159196":{"t":1606054338794,"c":"1---"}}" ltime="2093515456" htime="30851289" /></root><root><item name="PubMatic_USP" value="{"159196":{"t":1606054338803,"c":"1---"}}" ltime="2093555456" htime="30851289" /></root><root><item name="PubMatic_USP" value="{"156559":{"t":1606054346909,"c":"1---"},"159196":{"t":1606054338803,"c":"1---"}}" ltime="2174675456" htime="30851289" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\9JTW3P5P\www.youtube[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	238
Entropy (8bit):	4.447817208801295
Encrypted:	false
SSDEEP:	6:JFK1rFK1rUFWcqa/m2liSyiz1rFK1rFK1rFK1rUFWcqa/l5liSyiz1rFKb:JsrsrUua/cNOrsrsrsrUua/l5cNOrS
MD5:	20840F163F3CD5D214DDF48569518820
SHA1:	EB8DD12D5B02CD6F21CBDDF090F9793A38EC0455
SHA-256:	16A7CAB398D949C6C8F4B3B26B6B4E5D19A6A8EF7A470D19F7CDC364568D7CFF
SHA-512:	CC635317DB38983DEE969DC53A7E2EBD121DC68D2530A57C6CBBBFD8320C7D7A24F4B677E0588D976B9DEC7A5A14659BF6ED589363C1C30AB52FC4CCC68667
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root><item name="__sak" value="1" ltime="2614345456" htime="30851289" /></root><root></root><root></root><root></root><root><item name="__sak" value="1" ltime="2670025456" htime="30851289" /></root><root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\BDVTOSXC\www.google[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	108
Entropy (8bit):	4.905454290645922
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwsW+pEeAqKJthFJ580XRJAqSSUNclbaKb:JFK1rUFy+pEeAqKJ5/iSyizb
MD5:	05577E0673A502D5D3DA2129B681162E
SHA1:	A1A60632E133B571825CBE444EF7DB343684DC3A
SHA-256:	731DD009D2A99E0FF97B1CA4C41039280288380D06D4B3488B1670E96944CEA7
SHA-512:	01E974BA442579571019CE724DD6FA9AD93E991DFC9568844A7B69BD20F0FB0A2828833F527974F15938C27DBC30C5A8089F9867D008C07CC4927F44A332204B
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="rc::a" value="YndmMjE3dHJrbXJl" ltime="2131435456" htime="30851289" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\BFUVPUHP\consentcdn.cookiebot[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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\BFUVPUHP\consentcdn.cookiebot[1].xml	
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\DOMStore\BFUVPUHP\twitter[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	105
Entropy (8bit):	4.401104944461469
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwsDAqvl97RQNRJAqSSUNclbaK1r0aKb:JFK1rUFvAqyV8iSyiz1rFKb
MD5:	A472E22C4285B4CC4E2A5FEC726821C5
SHA1:	7D67E3D33945B7668375BC7EEA4056B021820E14
SHA-256:	34EEFFE0D4281E02342955CC0E23E11EA23D131295FB862569F61E5024D35E06
SHA-512:	83CC78C5BA147CCC73D46AC219F9DB308CC304DECDF2BDA7483F21A1E24831E9895BCDFF9FAC94C8E3C9934E0F464A252D7B02824F70DF0F045EAEB489BF9 82
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="test" value="a" ltime="2557995456" htime="30851289" /></root><root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\NF3IQ4OM\itsfoss[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	244790
Entropy (8bit):	5.614276760130006
Encrypted:	false
SSDEEP:	3072:VmHk93ZG/1GclP7Bgjn3mHk93ZG/1GclP7BgjnX:Gk93ZG/8cl+jnsk93ZG/8cl+jnX
MD5:	FA438237ABB8131D8ECAE960652F5E9B
SHA1:	1E3B29E742766FB67143FAE01A3357E20CAC867F
SHA-256:	A4CB97BB016E05F6BC526C59C114C3CBAD2F63EB1EC8002BF66C5662A0561834
SHA-512:	37D129C2B0267A9B27627216DA33F504EC7CE29D2E3D397D5E72CB429CFEE038D47D2422ACFEF277A79883E888C04E143DF2B4FE04C6653F6D8C88CB0D6CDC E
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="__sync_id" value="approved" ltime="1997115456" htime="30851289" /></root><root><item name="__sync_id" value="approved" ltime="1997115456" htime="30851289" /></root><root><item name="__sync_id" value="approved" ltime="1997115456" htime="30851289" /></root><root><item name="__sync_id" value="approved" ltime="1997115456" htime="30851289" /><item name="omVisitsFirst" value="{"path":"save-command-output-to-file-linux","queryArgs":{},"timestamp":1606054329,"referrer":""}" ltime="1997585456" htime="30851289" /></root><root><item name="__sync_id" value="approved" ltime="1997115456" htime="30851289" /><item name="omVisitsFirst" value="{"path":"save-command-output-to-file-linux","queryArgs":{},"timestamp":1606054329,"referrer":""}" ltime="1997585456" htime="30851289" /><item name="prebid.cookieTest" value="1" ltime="2006165456" htime="30851289" />

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\NF3IQ4OM\m.facebook[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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\NF3IQ4OM\m.facebook[1].xml	
Reputation:	low
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{B2129D5B-2CCC-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	98664
Entropy (8bit):	2.4893330690002253
Encrypted:	false
SSDEEP:	384:r4xepULyryu7P8hgClswgOI61+insGsjRaPm:mal
MD5:	D2FC91D4F4F587E3972638C966AC423E
SHA1:	46C490C00417417BDB158012EC7889713F567B01
SHA-256:	DCA2C57496AFE51B622F7C681FF2D11FBF9A0D097AD05BBB89D8698234906303
SHA-512:	314CEB318E521214A4C6B3ED66A218201834AA899A51A1554014D02E86CCF02D1E3ADE07D2588AEB64C37F40F07EBBB59C5058DB5CD2FA13E49723A21BD7FC8
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B2129D5D-2CCC-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	1295884
Entropy (8bit):	3.7628853209744486
Encrypted:	false
SSDEEP:	6144:pvXouuvXoqjvXoyr5vXoaWvXoeFxvXou7:pvXouuvXoqjvXoyVvXoaWvXoePvXou7
MD5:	54CF582EBDFBF38E1AE69FEB776BBFC1
SHA1:	19F25894BCC5323149CDCAAD1E6558C13D7370B5
SHA-256:	5C65D3300A1FBDC5EBB7B590DF83922A0B38A710CDA99F797F518AD7BA5FD607
SHA-512:	86B6772511504DCD1C008501B82F146EB6B1A21976BE79231E9A46F278A2A74EF1A3C7326E6E56987E396269784F8374BB095851319CFC2C3D953ABD521C8FA2
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B2129D5E-2CCC-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5643736114934617
Encrypted:	false
SSDEEP:	48:IwpZGcprlGwpaMZG4pQKGrapbS95rGQpK0G7HpRIsTGIpG:rp/ZvQM768BSfFA/TI4A
MD5:	19875A5BA57184C282272FBB4AB66F0F
SHA1:	A11528151A111E6CE0EA37053A78A23E4E31A791
SHA-256:	200434A613295737E7AD165FA1382C8F68F48DE80FAE23F93980A66DE3DBBC04
SHA-512:	6A8E076A4FBA61505D91E3B005EEF22114E28C197552CECC4883C9EFFDAB5C0B44B137DD67FB69257C709ACC26DA72DCFFA6A2394F7E73C1E707EEEE1ED456C
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{D0936BEF-2CCC-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{D0936BEF-2CCC-11EB-90E4-ECF4BB862DED}.dat	
Category:	dropped
Size (bytes):	30240
Entropy (8bit):	1.902925692160542
Encrypted:	false
SSDEEP:	96:r3/ZlQ2769BSFFjy2ykWgMLYXs4BUhYBWGPhsMoqVoB0o+93Xkh:rvZlQW69kFFjy2ykWgMLYXs4yhYgK8h
MD5:	A961396FD4A3924765451C5B4A33D3B7
SHA1:	99EE3AC1F277C0DC883F99F173D921C2E17175E0
SHA-256:	4C71C1D59BAEBD7DA028485067DF9EAE8E897800986744F9754A68438C6DF055
SHA-512:	5AA43759666DC5F0FEAF77252B84B5502EC5AC8BCAA8BEED9021AC804B5F8767B45C3C796DB5014A89B2EB7BE80D41A97E3817581E718642A8038CEBA30E8C9
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{D0936BF1-2CCC-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24224
Entropy (8bit):	1.6411510505014455
Encrypted:	false
SSDEEP:	96:rK/Z8Q676ABSQFjlf2lskWlsMlQY73uzg:r+Z8QK6AkQFjx2qkWaMaY7Cg
MD5:	30CD6066B3F83418169514B88D329A68
SHA1:	3DFE30268B70C43B7186C46851707E3A22359927
SHA-256:	7FF55972AA1A3E498B728F98558A4B3F1F433CC95A252BB19DA95585DC92D375
SHA-512:	3531C67953CE50939720FBFB114EF5AFF446EDD62D24667DC4FF7D3F84E7A63FEB14CA9CCFE1312C30BFD63DCF17F35CE215A7330DF726070CC0DFC14C8A37D
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{D0936BF3-2CCC-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27628
Entropy (8bit):	1.805725943364365
Encrypted:	false
SSDEEP:	96:rX/ZYQsE76+8BShFjx2hkW+MyYkDvXD52QL0lx3or:rPZYQR6XkhFjx2hkW+MyYkDvXD5cr
MD5:	51388399C9BCE5CAC1C77D0F4048F0C4
SHA1:	9E909D1FEE58BB69305689B38736DC22CC33B645
SHA-256:	800B0E4FB35ADCDC35D28A3963861467B791530B6EA974AE1B3D612A8971A5AE
SHA-512:	7BF05A009665C816EE48A37DA3F366C4F13A55CC995D1258C34957E4BFB88E56878C6EFC02E64884F9A30A4C0320E8A760BA5D3D507A774CE947DFE9D4913BF
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.086581427337948
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEAsiPsFnWimI002EtM3MHdNMNxOEAsiPsFnWimI00ObVbkEtMb:2d6NxOVsKsFSZHKd6NxOVsKsFSZ76b
MD5:	9DAA963C4D0948D96559408A8C5B165C

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
SHA1:	4A50D05ED5D502E87EADD4DD1DF7163CD7120E7F
SHA-256:	CF5DC94EE618213D24AFC7AE44616173F293AC59D3AF6DDEB45B73F2A34EC2F3
SHA-512:	63AC6A2D1B05DB5EE6F02C461816B9445C1E6EB80B3F9EF26E3D16470A5649D9BE9BBD6F7C6398040A951D82F71F4FBFE7E6FA4AC5E617F460572BCC9EFD5F6
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x87f863fc,0x01d6c0d9</date><accdate>0x87f863fc,0x01d6c0d9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x87f863fc,0x01d6c0d9</date><accdate>0x87f863fc,0x01d6c0d9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.110845705631094
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2k6wui9wuFnWimI002EtM3MHdNMNxe2k6wui9srFnWimI00Obkak6Es:2d6Nxr7NkNFSZHKd6Nxr7NksrFSZ7Aan
MD5:	EF512033B0F6FBC5C40C8FC200415F68
SHA1:	EB98FF2DA81DDB628715D9D8CAD2B0F7296B2781
SHA-256:	5658301057AAB1CA4FB7D11C32366ABABC9DC51E399BB7712C52641D7E6E17AB
SHA-512:	BA74A2A2E98D3287A6E291DF874D8D600258C8F1563601A978799E9E1EE5818497624FFE3F2549D4E246E05CE0BBDB0096F686D6AD4CAA7519ECBC390C95E83
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x87ef3c4f,0x01d6c0d9</date><accdate>0x87ef3c4f,0x01d6c0d9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x87ef3c4f,0x01d6c0d9</date><accdate>0x87efd883,0x01d6c0d9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.118022676028228
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLEi7FnWimI002EtM3MHdNMNxvLEiyFFnWimI00ObmZEtMb:2d6NxvQCFSZHKd6NxvQtFSZ7mb
MD5:	7178AE7491C7979F3C5CD59FF5C5B52D
SHA1:	22C5BC97636027FBC7491CE635A7B6A48011B545
SHA-256:	7F23683FE5394A7A35623A2F9C1BA90FF8FE3AB5E046035CC09F84A040538917
SHA-512:	37394B499B787D7D25AE8C244DE8F3FC2307ADB08AEFB56B8BCE95F04A0C83E0483E0E43F6D492D2F8460D69F902998FD96C596BC92076ACD4478039DD30158
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x87f9004b,0x01d6c0d9</date><accdate>0x87f9004b,0x01d6c0d9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x87f9004b,0x01d6c0d9</date><accdate>0x87f99c89,0x01d6c0d9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.109944961320645
Encrypted:	false
SSDEEP:	12:TMHdNMNxinIieIFnWimI002EtM3MHdNMNxinIiBFnWimI00Obd5EtMb:2d6NxfCFSZHKd6NxfQFSZ7Jjb
MD5:	18757D4A9A1F174638B30EC3BE595E7C
SHA1:	86F1A8D9EF3E1F857AC29FF358C6AB69CFF49713
SHA-256:	5A697206DD741E6DE4657C5BF343B88E04AD836F4AC76027B7EC14C5ABA03A43
SHA-512:	04DD739B60526B211806A8A814FFBF0C3D8B7D47C131C47994D2729D25DC99CA5045B5539A9B2DD26BAFE2F53441973F758F79E3E5A36B0C801259942397AEC5
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x87f5f310,0x01d6c0d9</date><acc date>0x87f5f310,0x01d6c0d9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x87f5f310,0x01d6c0d9</date><accdate>0x87f68 f4e,0x01d6c0d9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.123989840906497
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGw5FiyFFnWimI002EtM3MHdNMNxhGw5FieuFnWimI00Ob8K075EtMb:2d6NxQOtFSZHKd6NxQOqFSZ7YKajb
MD5:	37F1975A6B8BBADA793E89AAE3938863
SHA1:	6BD67171767DFD8E4F50BEE2A1CC5367A9607922
SHA-256:	4F5DE510FBFE59426835BCB6908D259F0D52251D5312F1F5B36B4FD8D850C8C8
SHA-512:	5D9F74D6354CAC71FDC00FDEFF30D16B7A7493781B8B283915290A9734B02E43B244687389EB96AB75C95A4B02020DED3E1BE5D32F293F7D7A43015FD9AAEB3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x87f99c89,0x01d6c0d9</date>< accdate>0x87f99c89,0x01d6c0d9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x87f99c89,0x01d6c0d9</date><accdate>0 x87fa38c6,0x01d6c0d9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.0707621445537985
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nlJri4JrFnWimI002EtM3MHdNMNx0nlJri4JrFnWimI00ObxEtMb:2d6Nx0Hr9rFSZHKd6Nx0Hr9rFSZ7nb
MD5:	ECD59C0B4EBB0BB3F6222090D13E9F8B
SHA1:	B44D916DA94CA33246F5341C1683F3ACE84D331B
SHA-256:	B258CADA266E0EDF987277C05A38F04F40C421D4FB18FE0918FF10B7A46F4B80
SHA-512:	7E45B89B957BEA57F93EDF4739EB82EF9BB7CC31AB4C6719BB888DF63B4C64B642C2A0B4C614C1EEA0F771210105A6F0B5E8F81DD37D865D29F15D544095F82 8
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x87f7c7c8,0x01d6c0d9</date><a ccdate>0x87f7c7c8,0x01d6c0d9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x87f7c7c8,0x01d6c0d9</date><accdate>0x8 7f7c7c8,0x01d6c0d9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.1528989679548625
Encrypted:	false
SSDEEP:	12:TMHdNMNxxRiKFnWimI002EtM3MHdNMNxxRiKFnWimI00Ob6Kq5EtMb:2d6NxPnFSZHKd6NxPnFSZ7ob
MD5:	568C751AD32FBD132D751D0EBB863418
SHA1:	AC060C0FCBA4C98117D2911C1C7C1A84DAE9F97E
SHA-256:	559EA3245688651178848E6367B8B298B5E031564D24A0E80024D1DFA29EC378
SHA-512:	D888F41FE11C7E56FC39A3379A9A1E0D929D00B977ABCF48146B33EB4AA9833EC33FD22D4197C9FB0C0E3231884DF4BCCF3C8E96E9FEC62956D47AA93A62D6 E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x87f72b81,0x01d6c0d9</date>< accdate>0x87f72b81,0x01d6c0d9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x87f72b81,0x01d6c0d9</date><accdate>0 x87f72b81,0x01d6c0d9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.098996422680809
Encrypted:	false
SSDEEP:	12:TMHdNMNxcVuuikuuFnWimI002EtM3MHdNMNxcVuuikuuFnWimI00ObVEtMb:2d6NxOuuDuuFSZHKd6NxOuuDuuFSZ7Db
MD5:	44F4F8AAFC458D09C1290809CEBF1299
SHA1:	80FDE24422DA39648F689AD8A65461E89C9BE5EF
SHA-256:	D47E30D13D9FBABA20FBC38C74456A10E5221F02C1089CEAE8010D2E0BE5C0DE
SHA-512:	48A86CA2ED3E5E04129568EB1D6FE4F61C44BC923B93BCCCC01A52CA6BC6A10892130EF8F2733AA15C42D49F20A8390539310271BD686674BA6D3C245C393BE
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x87f1ad4d,0x01d6c0d9</date><accdate>0x87f1ad4d,0x01d6c0d9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x87f1ad4d,0x01d6c0d9</date><accdate>0x87f1ad4d,0x01d6c0d9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.139235224222256
Encrypted:	false
SSDEEP:	12:TMHdNMNxfn6c/iZc/FnWimI002EtM3MHdNMNxfn6c/inuFnWimI00Obe5EtMb:2d6Nxf/J/FSZHKd6Nxf/iuFSZ7ijb
MD5:	703C553C042DFDB7ACBAD2DFC25A06D8
SHA1:	91FEA4B7C2248A7FB4C3455A7C4760B6C7AD4E1D
SHA-256:	5BD1FCDFCBC758D889DADD32A8A43D3A2B92CFF8CC823A89EC6A74E409E36D0A
SHA-512:	AF49CA98DFB95861B8DE3A75FF43E8DB9913BEB77056D3B96F3AD56D1B79D3C0E5B91813D7BFE3F9482000CBDA3218F0440FE095A5FFE0913AAF36176A32EEC A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x87f24998,0x01d6c0d9</date><accdate>0x87f24998,0x01d6c0d9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x87f24998,0x01d6c0d9</date><accdate>0x87f556f4,0x01d6c0d9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	1034
Entropy (8bit):	7.458329119735551
Encrypted:	false
SSDEEP:	24:pqCYBWexLZs78de/zI4gBabzeiqYMfD91MVnfkHU:pxYBRkode/k4yamiqYMfZb0
MD5:	3F863E3081976F5DF3F1664D88344000
SHA1:	485167860C010C806BED7542EAF8914278E51109
SHA-256:	B84ADF0B0F798D788DF07DF8E02548815A2320213E73B94F9EF664944C526741
SHA-512:	FA2DDD2197503B3CE67FA473FE23C0FF4CCB36DAE6711A0E9D5C8ADCA58163DA37FD83EF45669743565E00AE7EA00F932D8BFEFB56DDFD50C54FB0F8D8794 10
Malicious:	false
Reputation:	low
Preview:	*.h.t.t.p.s.:././.a.b.s...t.w.i.m.g...c.o.m./.f.a.v.i.c.o.n.s./.t.w.i.t.t.e.r...i.c.o.....PNG.....IHDR... ... .szz.....sRGB.....JIDATX..VMh.Q..yIlR.)J.T..Z....P.J.....P...,.O..z...=...A..4A.C.DEEoV*T.,m..I.R....I.l....u7....<....7?.....\...@t3..#..HP.H_..r...p...*...J.ol/&..&..?.....uU!...%.kD.B.G.I.....ou.Pq.....".....{..CiY~.....G..*.Z..._.Beg...=Mt.....S..V.K....c&..#.,.S....e.Re....W....Y96..{.I.....ZN}..oD3.....W?..J.T.6.....Nk.4....{.....T.-'..r.....=..|.....3.....H...1....H...Ci.r.tgF....m...#...f.h....6..rAhd.8"....J.93K^..>.W.8.K.=..%\....&=.@z.S.B!j.hj...-.vs...s./.....[;.*bF.By<.....0.\.E.8..8o...g....&...c8(..r&..).....>d..[...'..$..b.1RZ*O.....2 .A...../.a_i..!...E..Q.6S...N...o.....I7.".(7...%.....X..h.\.hF...*8S+../.6..!.e_:f.s.P..mM.t..[...H6.....!.]i8x...9..?F...`!.....X..P.W0..e....$u...wS.N..@....9C.....No.D.s.,6.:.".._..w2tR.O.eH5r.w.#b....U<!.@8.y.`z.[5..Q.....+.....3.....1..x*....IEND.B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\408081[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	30868

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\408081[1].json	
Entropy (8bit):	5.195795851277327
Encrypted:	false
SSDEEP:	768:py7XHo8pXS7AR0qRySOtDYsXx3RJNcuy7Rw5:2XI8pH+BJ4C5
MD5:	3D5603ADEF47DFDC0164CE394E26EE04
SHA1:	DA22F91CA4ED2E680A10C8C223755185A4F95CBB
SHA-256:	3AD6833F1AA76890389CC1B3B939120D818709FA9D92C7C49D398D096C018BE7
SHA-512:	92A481A9C4D38A2F2FF6973B6F4EC84A077B00EFD685AA1738556F062AA978C01815AD1E1D501D91F2CD1D4455D5F70DDF7047F5D234869A8D915F3D5AA7734
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://api.omappapi.com/v1/optin/447/408081
Preview:	{"408081":{"type":"lightbox","theme":"metro","builderv3":1,"namespace":"dallas","ga_account":"55a587cb9c57e","cookie":30,"cookie_success":365,"automatic_toggle" :0,"yesno":{"theme":"default","privacy":{"show":false},"backlink":{"show":false}},"content_lock":false,"rules_engine":{"rulesets":"[{\"name\":\"Default Ruleset\",\"rules\":[{\"rule \":\"time-delay\",\"active\":false,\"conditions\":[[{\"type\":\"page-time\",\"operator\":\"more-than-equal-to\",\"value\":5,\"unit\":0}]]},{\"rule\":\"exit-intent\",\"active\":false,\"condit ions\":[[{\"type\":\"exit-sensitivity\",\"value\":1}]]},{\"rule\":\"scroll\",\"active\":false,\"conditions\":[[{\"type\":\"scroll\",\"operator\":\"more-than-equal-to\",\"value\":50,\"unit\":0}]]}, {\"rule\":\"monsterlink\",\"active\":true,\"conditions\":[[{\"type\":\"monsterlink\",\"operator\":\"wildcard\",\"value\":false}]]},{\"rule\":\"datetime\",\"active\":false,\"conditions\":[[{\"type\":\"time\",\"operator\":\"on-before\",\"value\":false}]]},{\"rule\":\"url-path

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\470037[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	30891
Entropy (8bit):	5.198823380427105
Encrypted:	false
SSDEEP:	768:9y7hFUGDXUV2faY5IwOtDYsX83RhyuuymhwT:yh6GDTtBh4yT
MD5:	C885FB16C0E13C0529BEC8B59ED55372
SHA1:	5D67B6DBDF6C4BF7B9F7EF3A81F31EC43511B6F0
SHA-256:	70709C7E0D5B2D2EBDA1D0E46EAD1FB55F1FBB14FDBD0F4F2283207DDCE3B3E2
SHA-512:	2D0D5D27250BFA4529D7674DEC569DDB3ADC4A8A9B7FA05D8761F0CB0E2C3972605FB5BA7A9018B920827919EAD2703E33A29BEBDFDD1BE46EDF4C69DB68C CA8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://api.omappapi.com/v1/optin/447/470037
Preview:	{"470037":{"type":"lightbox","theme":"metro","builderv3":1,"namespace":"dallas","ga_account":"55a587cb9c57e","cookie":30,"cookie_success":365,"automatic_toggle" :0,"yesno":{"theme":"default","privacy":{"show":false},"backlink":{"show":false}},"content_lock":false,"rules_engine":{"rulesets":"[{\"name\":\"Default Ruleset\",\"rules\":[{\"rule \":\"time-delay\",\"active\":false,\"conditions\":[[{\"type\":\"page-time\",\"operator\":\"more-than-equal-to\",\"value\":5,\"unit\":0}]]},{\"rule\":\"exit-intent\",\"active\":false,\"condit ions\":[[{\"type\":\"exit-sensitivity\",\"value\":1}]]},{\"rule\":\"scroll\",\"active\":false,\"conditions\":[[{\"type\":\"scroll\",\"operator\":\"more-than-equal-to\",\"value\":50,\"unit\":0}]]}, {\"rule\":\"monsterlink\",\"active\":true,\"conditions\":[[{\"type\":\"monsterlink\",\"operator\":\"wildcard\",\"value\":false}]]},{\"rule\":\"datetime\",\"active\":false,\"conditions\":[[{\"type\":\"time\",\"operator\":\"on-before\",\"value\":false}]]},{\"rule\":\"url-path

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\6xK1dSBYKcSV-LCoeQqfX1RYOo3qPZ7nsDdB9cme[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 14 tables, 1st "GDEF", 8 names, Microsoft, language 0x409, Copyright 2010, 2012, 2014 Adobe Systems Incorporated (http://www.adobe.com/), with Reserved Fo
Category:	downloaded
Size (bytes):	27548
Entropy (8bit):	5.880007332186799
Encrypted:	false
SSDEEP:	768:jgLCql3xYdv8LHXTaPIt0VyZ1lmt+lDX3HA3:jgOC3xRr0VQlmt4DX34
MD5:	AA3461AE48B9B6248D21E792F206DF1E
SHA1:	BCF70EF7812400325834AE410654005D77BB7F9F
SHA-256:	B222C8A0E93E7D0D2AD5B2C986A67B205F38711B6BB871FAB7B672A2D8104F4C
SHA-512:	038EDDE925D66724A8850C107B3665958A4D345AA1F2702D19B99D8121937C9ECAD90D62BD16A4F53A7AB6F8C6EFAC16776B5641AF8AD35B0994FA928AD5734
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://itsfoss.com/fonts.gstatic.com/s/sourcesanspro/v14/6xK1dSBYKcSV-LCoeQqfX1RYOo3qPZ7nsDdB9cme.ttf
Preview:	.....`GDEF.\....Q....:GPOS...5..R8...bGSUB#.#...i.....OS/2Z.tl...h...`cmap..I.....gasp.....Q.....glyf.....@..@<head.....6hhea.....$...$hmtx.)&.....DlocaDPT... .....$maxp.+.Z...H... nameZ.r...J\|....post.....M(.....u0.m._.<.....N.....?\..-...R.....x.-...R.....p...u.....s.....X...K...X.D.^.2.#..... .....ADBO... ....t.$.....G.#.&.9.P.#...#...#.L.9.n.#...#...../.#...#...#.k.#.y.<.&.#.y.<.+.#.....].h.O...R..._.....S.....'.....%...'...%...+.....,..... .....'.....'.V.....E.<...8...;...F.....#...&.9...#...#...#...#...#...#...#...#.k.#.y.<.y.<.y.<.y.<.y...0.<.h.O.h.O.h.O.h.O...S.b./.2.#...'...'...'...'...'...'... ...%...% ...%...%...%.....'...'...'...'...'.....,'.+.....8...8...8...8.....+.....(.+.1.+.F.....*.....3...k...#.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\6xK3dSBYKcSV-LCoeQqfX1RYOo3qOK7gujVj9w[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 14 tables, 1st "GDEF", 8 names, Microsoft, language 0x409, Copyright 2010, 2012, 2014 Adobe Systems Incorporated (http://www.adobe.com/), with Reserved Fo
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\6xK3dSBYKcSV-LCoeQqfX1RYOo3qOK7gujVj9w[1].ttf	
Size (bytes):	29808
Entropy (8bit):	5.770209350186367
Encrypted:	false
SSDEEP:	768:CtHEby3GL9oI6CJqdyQJ8z2SLSApJHCeqor/FX:6EbzuQgq2SLNp9/rdX
MD5:	F10CD8E2AC6BF3E3FD1F17144121CEF7
SHA1:	1B538D196AB46D29C05DBA1DC240AC07A0145AEC
SHA-256:	EECCAB635520EAFAD0017505B523EE0E884D91EAE3C1700D5E6C503B1C2C24E8
SHA-512:	F9CFD4105EDF45926072CD251CC34B44EBB6BA9F55E78D6FDB6A4D0BC37CABE88F721D851283E8288EBDE61A8FD8AB38308DFF358C36843437512DCDC4FE58D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://itsfoss.com/fonts.gstatic.com/s/sourcesanspro/v14/6xK3dSBYKcSV-LCoeQqfX1RYOo3qOK7gujVj9w.ttf
Preview:	..........`GDEF.....V....FGPOS.x.{..V....fGSUBJ.c...qP... OS/2[.t....h...`cmap..3.....gasp.....V.....glyff..G...T..?.head..........6hhea.....$...$hmtx.=).....Plocaa.RI...(...*maxp.3.z...H... name[.s...N.....post.SF...Q.....`.r.k_.<.....?\.:....o.....:.:.o.....v.....s.....X...K...X...^.2.#.....'.....ADBO.@. ....Y..... ...L.Z.;.4.g.Z...Z...Z.i.4...Z...Z.....C.Z...Z...Z...Z...4.6.Z...4.9.Z...*.....W.....-...4.).R.....+./....$.....-. .R...C.....R...R.=.R.#.R.....+.R.+./.[.R.....R... .K..... .. ..6...;.4...Z...Z...Z...Z.....M.....Z...4...4...4...4...4...2.O.4...W...W...W...W.....~.!.G.Z...4...4...4...4...4...:.....C.....R.#.R.....G...@.R. .K. .K. .K. .K.....!.5.+.R.A...R...o...2.R.a. ...,...O...$.....0...,...)...(...A.../

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\6xKydSBYKcSV-LCoeQqfX1RYOo3i54rwlxdr3cOWxw[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 14 tables, 1st "GDEF", 8 names, Microsoft, language 0x409, Copyright 2010, 2012, 2014 Adobe Systems Incorporated (http://www.adobe.com/), with Reserved Fo
Category:	downloaded
Size (bytes):	29508
Entropy (8bit):	5.770873847089662
Encrypted:	false
SSDEEP:	768:Z3+HEbac1u6+E3Dj4EJ7jD6vylAHUPKbIfUtSHrQUOpJ/BQ+iFX:ZAEb3vD8EJD6qlKpTQ+sX
MD5:	47B0E1F0585C9B8A8DA18EEFEC79B254
SHA1:	4A32BBD43AA8A006C4ACB9297D95081D2F745A6F
SHA-256:	AE9E9BA146E2AE878C8D5CA690D0032F5DC8739AC96581A61A96675C97BB906C
SHA-512:	89138D2BD3262FA0A645AC94A1F9F27BC42C22B51BB2639233672F5ECAA16E7FFFF347A7F24ED3051256BF7F83E23B6B4CAA626C2A80E3DB6B1BACA2B95E0D30
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://itsfoss.com/fonts.gstatic.com/s/sourcesanspro/v14/6xKydSBYKcSV-LCoeQqfX1RYOo3i54rwlxdr3cOWxw.ttf
Preview:	..........`GDEF.....U....FGPOS...z..U....TGSUBJ.c...p$... OS/2[.u....h...`cmap..3.....gasp.....U.....glyf..5....T..>.head..........6hhea.....$...$hmtx.7%.....Ploca5|&i...(...*maxp.3.p...H... nameX.qE..M.....post.SF...P.....`...?_.<.....?\..8...n.....8.8.n.....k.....s.....X.....X...K...X...^.2.&.....'.....ADBO.@. ....T.....U.S.@.1.q.S...S...S.t.1...S...S.....U.S...S...S...S...1.F.S...1.P.S.!.&.".....P..... .....(.../.3.I...).4.+...).=.....(...I...<.....I...I.K.I.0.I.%.).4.I.4.+.u.I.....i...,.D.....".....B...@.1...S...S...S...S.....L.....S...1...1...1...1...1...-.[.1...P...P...P...P.....X.S.../.../.../.../.../...4...)...)...)...)...).....H.....I.0.I.%.).%.).%.).%.).%.).>.).\.I.,.D.,.D.,.D.,.D.....(.0.4.I.j.....B.I.....(...J...!.....,...,...)...%...?.../

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\6xKydSBYKcSV-LCoeQqfX1RYOo3ig4vwlxdr3cOWxw[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 14 tables, 1st "GDEF", 8 names, Microsoft, language 0x409, Copyright 2010, 2012, 2014 Adobe Systems Incorporated (http://www.adobe.com/), with Reserved Fo
Category:	downloaded
Size (bytes):	29536
Entropy (8bit):	5.769341103623475
Encrypted:	false
SSDEEP:	768:lNlHEbffdWBdXUxPZ4cXC+9BFnKpJvX1bRFX:lNZEbtU8hdIpTX
MD5:	DE7AB4B12A803FD2A0A868BD8F2F460E
SHA1:	AEFA766F5DF7ED8C33748BDB56AE58EBF3A2DC21
SHA-256:	FA6464A1FD029592C65A116891480C02E46509088884BF044BC05E0C79CD8752
SHA-512:	3E1BF71B2A27946E1B913BD11355F1E173A0584D272AFA15880303EDF625375A7196DFC7C9A45615DB15941D9CBB30ED9360560C7305B0300CC52B1C481F3D19
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://itsfoss.com/fonts.gstatic.com/s/sourcesanspro/v14/6xKydSBYKcSV-LCoeQqfX1RYOo3ig4vwlxdr3cOWxw.ttf
Preview:	..........`GDEF.....U....FGPOS.o....U....fGSUBJ.c...p@... OS/2\?v....h...`cmap..3.....gasp.....U.....glyfy..R...T..>.head..........6hhea.....$...$hmtx.k!N.....Ploca3a$+...(...*maxp.3.r...H... nameX.p...N.....post.SF...P.....`.'._.<.....?\..7...m.....7.7.m.....m.....s.....,.....X...K...X...^.2.).....'.....ADBO. . ...P.....=...].M.F...{.M.$.M...M.~.....M.-.M.....f.M...M...M.....T.M.....e.M.,.#.,.....I.,...-...7.....$...*.=.A...$.=.'...$.U.....".;.A...5.....$.A...A.Y.A.<.A.+.$.=.A.=.'...A.....8.<.....&.=...=...=...=...=...=...M...F...$.M.$.M.$.M.$.M.-...-.J.-...-.....M.....(.g.....I...I...I...I.....i.M...*...*...*...*...*...*.../...$...$...$...$...$.....A.....A.<.A.+.$.+.$.+.$.+.$.+.$.+.$.6.$.x.A.8.<.8.<.8.<.8.<.....0.*.=.A.....R.A.....%...F.....).....,...*...".,.=,,.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\836AED64-FCB7-4098-8161-8F980A7BAC3E[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\836AED64-FCB7-4098-8161-8F980A7BAC3E[1].gif	
Size (bytes):	43
Entropy (8bit):	3.5257351171929923
Encrypted:	false
SSDEEP:	3:CUEIHh/:i4/
MD5:	13E1C7A2184E36D7AE519E99B1AA226F
SHA1:	355CCAD4EAC39838E1CC76FD0B670FD2EA1E5AA3
SHA-256:	48A33CA9F42B91902D57AD8AC52E1CE32B92C8C10C732F2DBB6FE960EBFD9438
SHA-512:	B1A6CFA7B21DBB0B281D241AF609F3BA7F3A63E5668095BBA912BF7CFD7F0320BAF7C3B0BFABD0F8609448F39902BAEB145BA7A2D8177FE22A6FCEA03DD29BE1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pr-bh.ybp.yahoo.com/sync/pubmatic/836AED64-FCB7-4098-8161-8F980A7BAC3E?gdpr=0&gdpr_consent=
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\DetectGDPR2.v1.1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	8795
Entropy (8bit):	5.338001034916449
Encrypted:	false
SSDEEP:	192:0JGwJeGYWmLgSeap0XzcpV08YFYLH6phH2pYaLCLPCLyCrc0jZo6Yx35YgYuKt3T:0sdHqy0XzWVeGLH6nH2pYaLCLPCLy0cm
MD5:	3DE79992D0CEF104B76350C3B21BB251
SHA1:	A5291BC84F1274976B2C40E0E79EC92FE2211EEC
SHA-256:	0CF25ABE73B03E246C0A820C825A1F433E36949C2CF456CE889D86E8DD9EC427
SHA-512:	E443D2FAAFAFAF77E82AA6D32E6CE35E4A58282526D6CBE33B8292321BDBB8B0AAC2C4B39A1E3E6B860C1514F45781DAF1F671B6A084A70E4FC2D1865F7D46BE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://live.sekindo.com/content/ClientDetections/DetectGDPR2.v1.1.js
Preview:	/* CMP v2 Implementation - TCF 2.0 */.var SekindoClientDetections_GDPR_v2 = function (isDebug, globalTimeout, onConsentAvail) {...this.CONSENT_SDK_NOT_AVAILABLE = -100;..this.CONSENT_STILL_RUNNING = -2;..this.CONSENT_REJECTED = 0;..this.CONSENT_APPROVED = 1;..this.CONSENT_NOT_APPLY = 2;..this.CONSENT_ANOTHER_VER = 3;...this.VERSION = 2;...this.PRIVACY_DETECTION_TIMEOUT_STEP_MS = 50;....this.VENDOR_ID = 228;..this.PURPOSES = [1,2,5,6,7,8];...this.isCmpLoaded = false;..this.cmpVersion = '';..this.consentState = this.CONSENT_STILL_RUNNING;..this.consentRawData = null;..this.debug = isDebug;..this.requestTimeout = globalTimeout;..this.isListeningStarted = false;...this.startTs = new Date().getTime();...if (onConsentAvail && typeof onConsentAvail == 'function')...this.onConsentAvail = onConsentAvail;..else...this.onConsentAvail = null;...this.tcfCallsList = {};...if (typeof window.Sekindo == 'undefined')...window.Sekindo = {};..if (typeof window.Sekindo.clientConsentEncoded == 'undefined').

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\lts-FOSS-Linux-Blog--1843285099062669[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	132768
Entropy (8bit):	5.235611382840236
Encrypted:	false
SSDEEP:	3072:tTSmQR4ah7oSacG8LSyO9R/eiQ26VfOyAi2ixa4JWy:tAR7h7oSacG8LSyUR/eiQ268YQS
MD5:	228A26517D3026FA3F69931D097B84F3
SHA1:	2451A1876F25AA102DF00471EDF04D8AED1CFDAA
SHA-256:	70DCDBADCBD9B077F5B452DFAF686CCE003C83C2A5DABD5C1867487F830E7F38
SHA-512:	78072A65553902D8C4CF1B58FEFEE2116FD18B3AD9EA28E05F662BBEB8B4EC09B65768F2245C3B4967D8C7B5DB19BC0448D18A3196AC8E0858D88A89C46DF37
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html><html><head><title>Content Not Found</title><meta name="viewport" content="user-scalable=no,initial-scale=1,maximum-scale=1" /><link href="https://static.xx.fbcdn.net/rsrc.php/v3/ya/r/O2aKM2iSbOw.png" rel="shortcut icon" sizes="196x196" /><meta name="referrer" content="default" id="meta_referrer" /><link type="text/css" rel="stylesheet" href="https://static.xx.fbcdn.net/rsrc.php/v3/yn/l/0,cross/V2KLVLHMzX-.css?_nc_x=Ij3Wp8lg5Kz" data-bootloader-hash="wi0bt" data-nonblocking="1" /><link type="text/css" rel="stylesheet" href="https://static.xx.fbcdn.net/rsrc.php/v3/yl/l/0,cross/ZCcUn0Z7yEy.css?_nc_x=Ij3Wp8lg5Kz" data-bootloader-hash="l3s9d" /><link type="text/css" rel="stylesheet" href="https://static.xx.fbcdn.net/rsrc.php/v3/y6/l/0,cross/7U_-wuTAXEq.css?_nc_x=Ij3Wp8lg5Kz" data-bootloader-hash="vu/4d" /><script id="u_0_8" nonce="nkkCQSk7">function envFlush(a){function b(b){for(var c in a)b[c]=a[c]}window.requireLazy?window.requireLazy(["Env"],b):(window.Env=window.Env||{},

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\KFOjCnqEu92Fr1Mu51S7ACc6CsI[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 21564, version 1.1
Category:	downloaded
Size (bytes):	21564

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\KFOjCnqEu92Fr1Mu51S7ACc6CsI[1].woff	
Entropy (8bit):	7.9688026243536
Encrypted:	false
SSDEEP:	384:bc6bX9TFqgFUvxQi0W1jHYHwnSthN/yiJsMw52R5oBAvhPFx466gfwu5:bcCV4aUlxHSw8ZyixnFP3N6U5
MD5:	FFCC050B2D92D4B14A4FCB527EE0BCC8
SHA1:	DE3033F27DB6BBDA89A0E6F16EC51E8C877739AB
SHA-256:	C8912EBD82B4DF2EB87E37B1F66432FA2186182E08BB8A533BA4C2DF6CE67FBA
SHA-512:	7D517BB33DE3D088B8EE4EC9250AB1645CF76B35B25F57C004BF82B5A9A30C15252C865765EFFD4679A68ACDF6EFB89E4B0319283914880935D8D1AC823FE65
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOjCnqEu92Fr1Mu51S7ACc6CsI.woff
Preview:	wOFF.....T<.....GDEF.....G...d....GPOS.....GSUB.....7b..OS/2.....Q...`t.#ycmap...4.....L....cvt .....\...\1..Mfpgm...@...2.....$.gasp...t..... ....glyf.....@...p.N..Hhdmx..M(...f.....head..M....6...6...vhhea..M...."...$....hmtx..M....k.....3.loca..PX.....G.*"maxp..R4... ... .name..RT.....!.>gpost..S0..... .a.dprep.. SH.....X9..x...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R.....2.x...pfK.G...1.c>..`9..m<+;..m.x...bg.M.T...O.....l...XU.../{.[_..W....c._..72.. ." z.+..F.....&.& ...`e..T].....K=..K2S....q..d...xf.$~i..$?.d..dU.....@R-/LMO-J6...[]..Z..O.C_."lf..d....fS....$d.G>eL`....Tf1.....9.c>..`1.TR..x./d-.....q.....7....{...v.....!.....1.QG=.4.D3-..F;=. .1'.'q.rw...9..e!.....Q....f.....qV.n.h.V.Z]..B..C.[B...V.....v...o.w.{...w..zRO.i=..._.....-.m....].=...[...(1.(.#.....O0/.0?..04rL.G.9.....i6..l..|.(o.....\|$,..{|&|....YJ...x.e8B.#..t;R8.{+....\=.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\KFOkCnqEu92Fr1Mu51xIIzQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 21528, version 1.1
Category:	downloaded
Size (bytes):	21528
Entropy (8bit):	7.973887568128485
Encrypted:	false
SSDEEP:	384:uy/NCb8EbjU+Fos6gaUFZ3qR474EAqAG3w/Qpt/uxMsucMgwtDw031F:7/4zb7o6XqR4+3QptcuLg0w031F
MD5:	9680D5A0C32D2FD084E07BBC4C8B2923
SHA1:	8020B21E3DB55FF7A02100FAEBD92C2305E7156E
SHA-256:	2CFE69657C55133DAC6EA017B4452EFFF2131422ABD9E90500A072DF7CA5A9C8
SHA-512:	E19A498866F69F3D8136A65A5AB4E92CC047170673ED00B506E325165A84216267B9FEF1E5CFD66458E85ED820C12E9C345CEC9BEE4DE48E1C2E2B1A784F179
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOkCnqEu92Fr1Mu51xIIzQ.woff
Preview:	wOFF.....T.....GDEF.....G...d....GPOS.....hGSUB.....7b..OS/2.....R...`tq#gcmap.....L....cvt .....R...R..-.fpgm.....4....s...gasp...<..... ....glyf...H..@...o..Na.hdmx..M....g.....head..Mp...6...6...ehhea..M...."...$...{hmtx..M....k.....1<.loca..P8.....6...maxp..R.... ... .name..R4.....:.post..S..... .a.dprep.. S$.....D..].x...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R.....2.x.....[....#N..m.m.m.mfm....SP..NuM..9]..=.U..!...[.....w...|.....^p....H.....;...).....;..EoDo. ...E.E.D...`.0.GG.aA.H.V.Mx\xA...../..d3.Eb_.J...R.^v.....\^ob.}.z..k.x).v$f$..O)+.2..*....y}6`C6b.6cs...l.....!.....<..|.|..|..|..|....o....I%.4.L.SI.&C.6..!`...{...c..\.J.(.2.C....V. A..?.M<nG.....v..m.;..R.C..aj.H...=..{.>.:.....}i_Y.....:...o.&k..KY.2..6k....i]..{.p}../.....VO3.o].fJ....R-TZ..;...RN..&V...C...3.?.....&..z.s&.D....r,.I...t.R..a$k..Mm..Y.U...+b.%kQ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3224
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	48:5m73jcJqQep89TEw7UxkZCm73jcJqQep89TEw7Uxkk:5nqrehEw7U6ZCnqrehEw7U6k
MD5:	3A35614D9A6156057F7D30C91C1ED4F2
SHA1:	7DDE5D14A15F465C9BFD0B0C0B3416175E69D1BC
SHA-256:	D544FAC44B7B2CD937726C401B5C9C726F900CEF22980A7B39F8756581901B73
SHA-512:	8A31C0C90EF443E3B7AC5B930466CD8CEF1D540D2D436A7DC4D12F38686368303882A9610A57B2A1CF9AB973DB684FDA0B1831B116EAEB4D86BE816FDD627C 8
Malicious:	false
Reputation:	low
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #00 0000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\O2aKM2iSbOw[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 196 x 196, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	6787
Entropy (8bit):	7.92313117554656
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\O2aKM2iSbOw[1].png	
SSDEEP:	192:CTErdfzHKZ1NCr7aOs6U7ve1H5rJKVeuqr:JsjNg+ZfvU51gtK
MD5:	AEBBF2D6313BBC20D85BA08F39A2C6BC
SHA1:	B27B7590E678293FEBE8B845D02804C637677C8A
SHA-256:	CCB2E0ACFEB57DA9AB6AA6BD3CCE09BFB2F8DFDA8979D89A0CED773D5B3948A1
SHA-512:	C7E5DCD750667FAE1E73DDC377590A6F092A66D8C5554997E2DFEDDD98BAC4946504200CE262B2A3C62389BBF0070FF0BFE3FBE7176EC84FE3B0136872C1BEA4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3/ya/r/O2aKM2iSbOw.png
Preview:	.PNG.....IHDR.....x~Y...pPLTEc..c..b..b..b..b..a..a..a..`..`..`.._.._..]..]..]..]..\..]..\..[..[~.[~.Z~.Y|.Y|.X{.Wz.]~.m.....w..Wz.....Vw.Tv.....St.Y}....Rs.....Uu....Qr.Vz.Oo.Xz.Wz._}....Vx.{..Mn....Tw.Rt.Tv....St....|.....Oq....Tq.Ge.Hg.Kk.Lm.Qs.....bz.Kl.Pq....Mo.Cc.No....Dd.c~.Oo.Mn.....Gh.Jk.Ij.Ln.Hi....Kl....Ik.....A_.Ff.Ee.Bb.Fg.A`.....>].....Dd.....=[.Cc....;Y.@_.?^.....9V.>]....<Z.7S....2O.=\.:X.....6S....<[.9W.;Z....8V....;Y.:X.7V.....3Q.0L.6U..0K.1N.5S.4R....3Q.2P.-J.,G.....K.....?...gtRNS.....N.ec...[IDATx..O.n.0..,[....<..!..v(...:2....G.4;.h..6Y?.`.`wZ.....: .!o.T.k...m....Y..:.(.89.\U9n.k.....L.3...%...._.aF.u..xX.C..Sl.R&.g..Z..(L.B^.....St.<.D...|.nZ*,6o.K....3.{.4.....WP..D....]u.fm.E&%.\..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\O5P04DWH.gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	35
Entropy (8bit):	2.9302005337813077
Encrypted:	false
SSDEEP:	3:CUkrllHh/:qJ/
MD5:	C2196DE8BA412C60C22AB491AF7B1409
SHA1:	5FBD472222FEB8A22CF5B8AA5DC5B8E13AF88E2B
SHA-256:	6ADC3D4C1056996E4E8B765A62604C78B1F867CCEB3B15D0B9BEDB7C4857F992
SHA-512:	84E24A70B78E9DE9C9D0DFEB49F3F4247DBC1C715D8844471EE40669270682E199D48F5FBEC62BD984C9C0270534B407C4D2561DD6C05ADEC3C83C1534F32DC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pixel.onaudience.com/?partner=161&icm&mapped=16e1612ed06391c52bd2a0c9dd9cecc1
Preview:	GIF89a.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Pug[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	84
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEqjdfXPQE/xlEy:1QEoqh3QEoy
MD5:	6A3F2D147842187CD48B1546EDDD5BA0
SHA1:	AB278C31189DF2939428CF81A3850A2C6DBF5E2E
SHA-256:	D4990F907BCA02F02B3D41216EEA5461609D4BCBA07A3CBEE0D7CF28A6D0D864
SHA-512:	998F55BF5C3D4A71CB3C23782B788F71E7625DF83A37FE8A18F915AAA3BDE5420183A3C709816664E262069EE2FE245CA44799E3476B6DE507B5D68FC86F8960
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D.;GIF89a.....!.....,.....D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\S6u9w4BMUTPHh50XSwiPHw[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 27524, version 1.1
Category:	downloaded
Size (bytes):	27524
Entropy (8bit):	7.981057931878512
Encrypted:	false
SSDEEP:	768:zzAiDCpYbY5aqoCp71Q19fHbqjJjqBGBRnwjK+5qmsQCns:zz7l5ltp7U9fHbqjMBeRnwmAqB/s
MD5:	A82FF6AC9208656F9A21A65DFACBCAE3
SHA1:	80F8216F458F74EBB649641FA617195DFC8BF836
SHA-256:	7831E273F41FEF8485564286F3578D2847754DB375BEFDB48B8CE37E1E1F3A57
SHA-512:	F119CD55C01A595D216E61F7CCBE77E1D28190E383457E089347161D0E6B97A33958E290D974B9C0F016E05A767559FD59CF0FE25F297248B7A873EE11FF5A1D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/lato/v17/S6u9w4BMUTPHh50XSwiPHw.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\S6u9w4BMUTPHh50XSwiPHw[1].woff	
Preview:	wOFF.....k.....GPOS...l.....z.a.RGSUB...\...S...p.:.|OS/2.....[...`{0f.cmap.....cvt .....y..fpgm.....rZr@gasp...H.....glyf...P..U.....6.x.head..d $...6...6...ghhea..d\.....$.1..hmtx..d\.....v..5.loca..f.....Y.maxp..hL... ... ....name..hl...2....8.Q.post..i.....EX...prep..k8...K...K....x.T..I Q.EO....m.m.m;X...Fl..?us..p.$z 3.....G.f.N...`Yv...p.a.N.*."b.3...]p..`...l,.5...]=.%U..D…]v?.xX.w...;.w>.....mt?....+.....]..G.>]:(.JO.+.J.R.=.k.....@9.+.....:(.UP.k.bZ...B..a....U....6\..Q.10....H'...../....1.!.e....HF1. .Lf...l.0.y,`.KY.rV....b7{....p...,.8...r.+..>.x.#....%.x.[...\|.....7.._.....$.H..&.X.'.D.I!.^xX...=.....$.....i.%..p.....X.a.h&n4..R.....9rS.p.z. .....x.3. .r.(7...?...n..?.....vp+(... ...k..1.4...Oy.K...g.A..&.....[.f..v.c..o8.-.H.2....>..?.<.)0.z).o..$...PF9..S.Ax?x(V..A..&|..RG.1...f...n.n;...4...Wb..^...G.c..&.bF_+.]e.u6.b.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\S6u9w4BMUTPHh6UVSwiPHw[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 28052, version 1.1
Category:	downloaded
Size (bytes):	28052
Entropy (8bit):	7.983868615364949
Encrypted:	false
SSDEEP:	384:n2zorz2U1eBym14fE/b3/DcgrjaYWTS1XrXUl44Eap54pSptB1Xg7a+:2krz22eYmAE/trmY+C14Eekexea+
MD5:	874B8E7BC7E8D1507B50F56BC6C9B536
SHA1:	B7AC18BD6D3ACECDFA5931FA4A59C005ADB02F38
SHA-256:	9F5A6FB49257579436C7BD8D42FA5D052336132B6F9F8972A7C9C00D93ED18B4
SHA-512:	C8771C91135DD24E6345DAF39728DC4986FAEDED05161CF4428360D538C3E7984FBBF416FA7B8B6F3956AEBF10817C604231EAA37EE3174B82B7BD16E52368D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/lato/v17/S6u9w4BMUTPHh6UVSwiPHw.woff
Preview:	wOFF.....m.....GPOS...l...i...B.#..GSUB.....S...p.:.|OS/2...,...Z...`z]d.cmap.....cvt .....*.....fpgm...@.....rZr@gasp.....glyf.....V[.....b.head..f(. ..6...6...Ghhea..f`.....$....hmtx..f.....v..BWloca..h.....%..1maxp..j\... ... .name..j\|...1....8.P.post..k.....EW...prep..mH...K...K....x.L...$Q.EO.....m.m...k.....1..a..q.....p..2j.. ...P.7.. A.-.Z.x...R.H%..U....p.k.l3[.df.....9o.f.!%W..X..w...jo4.=..Bu{#|_..j.....W.=...Y..`....{...f....l....._.....U"..*Tw..h....bv.....T..=b...LN(. ...AdTt.L,...&4.9.iC[:.Nt.+..N.z..../...0.3 .1.c<...d.3...b.+Y.j...lb3....vs....0G8.q.p..\."...U.q.....w..=..<..Oy.s...|.#...O~..D.C,q.@"!$.J...#.FwFa...]..G....C#.v.2.....>.....hiY..Q...JD:K-& j,...Y... ...E.SQY.-a).a..... XG..O.(5.....S.~L.l.>....{..R..m7.....=..eL7=..G?.,.....q....$.`....g<gW}.~..^...!.L.<...g![...Cn.$.S@!E\.7..f..kBq|9....C9.TQMM.....z.7...&.f.x9...].P.).

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\S6uyw4BMUTPHjx4wWA[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 28660, version 1.1
Category:	downloaded
Size (bytes):	28660
Entropy (8bit):	7.986798426962959
Encrypted:	false
SSDEEP:	768:Rr8uuUMtVCqVsUnrZAT9vaxw9pi95vSVc+Dfpy:R9uZV9VnndAJvaCGPvwDhy
MD5:	B8EE546ACD6CC0C49F42AD3D48EF244F
SHA1:	7D8BFF4143A36AA9CC1C2801F60FA0E99969E3F6
SHA-256:	04050BAE4CC3B9CCD20D3C7F57F5B1BA249D4A54D6EFF75A1E4DF504362E8C00
SHA-512:	700D04F4CAF24A20919C2136DD3700BBE07F509F5BD0045084063B78EA8B6FD72BFEA6BBF2A94A5865A75CD6C7197DAB500B809122AA5A3910F46E1D9816D00
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/lato/v17/S6uyw4BMUTPHjx4wWA.woff
Preview:	wOFF.....o.....l.....GPOS...l.....z....GSUB...<...S...p.:.|OS/2.....Z...`y$aycmap.....cvt ...x...+.....fpgm.....rZr@gasp...$.....glyf...0..YY...H@ ...head..h....6...6...#hhea..h.....$...whmtx..h.....v}.O7loca..j.....9maxp..l.... ... ....name..l....8....:.TApost..n.....EW..xprep..o....K...K....x.T..I Q.EO....m.m.m;X...Fl..? us..p.$z3.....G.f.N...`Yv...p.a.N.*."b.3...]p..`...l,.5...]=.%U..D…]v?.xX.w...;.w>.....mt?....+.....]..G.>]:(.JO.+.J.R.=.k.....@9.+.....:(.UP.k.bZ...B..a....U....6\..Q.10....H'...../....1. !.e....HF1..Lf...l.0.y,`.KY.rV....b7{....p...,.8...r.+..>.x.#....%.x.[...|.....7.._.....$.H..&.X.'.D.I!.^xX...=.....{XC.hySQy....p...n)..h..M.(..f)"..)..j...L.qw..R`).E..8..1*.X..7...\..9(q(. .32.PJ)K).....#)I(.X...{.....7.g..\s.:..7dL...K.>..0H.!.Y.v.U.Xg...m.-..a.=.:...<!..c.9~....?B...w...-..l(.>..TQM...X..5...G.J..P.\..=4.H31Z....q.j.6.....v.#..z.G..e.q

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\V2KLVLHMzX-[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	5469
Entropy (8bit):	5.151316310535322
Encrypted:	false
SSDEEP:	48:V5hIeP3l5NkFWcU+Fb1/t9LmQldUsZ0QMEEbDt6a7xiqPcaTWZwNQ4Iijo:n/P3l3kYcvJlUsZ0QMbbEaQACp8o
MD5:	75BD3CED9D1B7B9DE99A4911A0EFF06F
SHA1:	BBA4BB94E59F0E2756444378059DB6CB34F832E8
SHA-256:	2A63065F67DE1CAF285C129DF3ABE5701FE2B1494F1B866375283B456ABABD4B
SHA-512:	7866B87FB06FB360D1C7B22C1B590E7F8741FF098970C10C2CD2D6C0141A3DF879F38D5D5D053CFC4B32B5E74EC66CDDC3ED67AA67E99E3B994DCE95122723D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\V2KLVLHMzX-[1].css	
Preview:	.sp_kTPczrZnksk{background-image:url(/rsrc.php/v3/yf/r/-YLipmEFntl.png);background-size:auto;background-repeat:no-repeat;display:inline-block;height:16px;width:16px}.sp_kTPczrZnksk.sx_0bb90f{width:12px;height:12px;background-position:-105px -244px}.sp_kTPczrZnksk.sx_6539bf{width:20px;height:20px;background-position:-50px -143px}.sp_kTPczrZnksk.sx_0fcb28{width:24px;height:24px;background-position:-47px -110px}.sp_kTPczrZnksk.sx_34ec04{width:24px;height:24px;background-position:-72px -110px}.sp_kTPczrZnksk.sx_b98d02{width:24px;height:24px;background-position:-97px -110px}.sp_kTPczrZnksk.sx_303210{width:20px;height:20px;background-position:-71px -143px}.sp_kTPczrZnksk.sx_0ee1fd{width:12px;height:12px;background-position:0 -259px}.sp_kTPczrZnksk.sx_f770dc{width:12px;height:12px;background-position:-13px -259px}.sp_kTPczrZnksk.sx_2d6bda{width:20px;height:20px;background-position:-92px -143px}.sp_kTPczrZnksk.sx_5df003{width:24px;height:24px;background-position:0 -143px}.sp_kTPczrZnksk.sx_222

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\adsbygoogle.0e32b39aad0081b2af83.bundle[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	98
Entropy (8bit):	4.871587268794003
Encrypted:	false
SSDEEP:	3:lD3ORZy/LBdORZzZqVRNxhCJiEZLDHEyqYSL9J:lD3r1daZurCJiEZ3EyqF9J
MD5:	0DE025C4E10577505D4BE7D018A2EAF7
SHA1:	AE91AFDBE0A2DC7567F174189C21E67B63F937DB
SHA-256:	D6B87189F2250EA0DCDBB2DDACE715469013A7F2C2B5D3861DF3FB449839C621
SHA-512:	C90EBD0B4921979AA928EAC98224FE2FF5E5FEE0FB89BE1DFF561777C05CE8EF461DB1FE17906A77C3E17A621CE3121913A8B0CFC91699592DE1589BE0D3237D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://renderer.apester.com/v2/static/adsbygoogle.0e32b39aad0081b2af83.bundle.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([["adsbygoogle"],{"1b6bf":function(o,n,w){}}]);

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\anchor[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	14417
Entropy (8bit):	5.9457725099366145
Encrypted:	false
SSDEEP:	384:3/Shze4ieoqFAxcQCBdwQT91840punhVa7dEsRQpKA:3/Sh64iWuCQC7FEunhORQpKA
MD5:	1CE5FD64CBA82894026FD5BBE6A82212
SHA1:	C3A78EEF07905224CE4ABFAC88BEF26807B237D3
SHA-256:	71B4FCACAB169AEEC45E26EA0E84667085B6B787311D503DD61BC1DCAB428EFA
SHA-512:	9C680094BE4D5D9FFDF713CB485A510801CF23DC59A6C1D53E79D8A803DFAD9B6E01C35B2E10F9C340056F95DB48F20A28134E41FBF802B9C521A81F0762944
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML><html dir="ltr" lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.<meta http-equiv="X-UA-Compatible" content="IE=edge">.<style type="text/css">.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxP.ttf) format('truetype');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 500;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc9.ttf) format('truetype');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 900;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmYUtfBBc9.ttf) format('truetype');.}..</style>.<link rel="stylesheet" type="text/css" href="https://www.gstatic.com/recaptcha/releases/UFwvoDBMjc8LiYc1DKXiAomK/styles__ltr.css" nonce="svxo6So3FvPlAqp6jXMu4g">.<script nonce="svxo6So3FvPlAqp6jXMu4g" type="text/javascript">window['__recaptcha_api'] = 'https://www.google.c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\apester-javascript-sdk.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	238907
Entropy (8bit):	5.336658946777202
Encrypted:	false
SSDEEP:	3072:gl1QuKGnUuRaVrZcpQAzy92P5kbAtoQ66UCnZV5PoLySSYm8URSEJn:gl1QuK/V+rP5kooQ66UCnZVdoaYu
MD5:	1378D122C8C5D1496CFC5A8D6691B545
SHA1:	CA989945BCF9C01BC11EF3195429C0465D6F98C5
SHA-256:	BB2D19AFD24ACB7BC6FB2D1CA57BB3D857254FC7D936034D57E10C67DF688887
SHA-512:	FB0679CF9D98CF63B3892794AE89F38DE14D5AC6753EE68CBEDE12F90F13664BC931E8E7C4D0CC241F20B61458365297B496BFC684B544F74873DAB9DA6AA25
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.apester.com/js/sdk/latest/apester-javascript-sdk.min.js?ver=5.5.3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\apester-javascript-sdk.min[1].js	
Preview:	try {.(function(){.. !function(e){function t(i){if(n[i])return n[i].exports;var r=n[i]={i:i,l:!1,exports:{}};return e[i].call(r.exports,r,r.exports,t),r.l=!0,r.exports}var n={};t.m=e,t.c=n,t .i=function(e){return e},t.d=function(e,n,i){t.o(e,n)||Object.defineProperty(e,n,{configurable:!1,enumerable:!0,get:i})},t.n=function(e){var n=e&&e.__esModule?function(){ return e.default}:function(){return e};return t.d(n,"a",n),n},t.o=function(e,t){return Object.prototype.hasOwnProperty.call(e,t)},t.p="https://static.apester.com/",t(t.s=158)}([fun ction(e,t,n){(function(t,n){!function(t,n){e.exports=n()}(0,function(){"use strict";function e(e){var t=typeof e;return null!==e&&("object"===t||"function"===t)}function i(e){retur n"function"==typeof e}function r(e){U=e}function o(e){F=e}function a(){return void 0!==j?function(){j(l)}:s()}function s(){var e=setTimeout;return function(){return e(l,1)}}function l(){for(var e=0;e<V;e+=2){(0,G[e])(G[e+1]),G[e]=void 0,G[e+1]=void 0}V=0}function c(e,t){var n=thi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bidRequest[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	62
Entropy (8bit):	4.518397116698908
Encrypted:	false
SSDEEP:	3:YMb+dAO9e14nEuHY:YMbiRgeEuHY
MD5:	A06756314BF6D3DF08DDA148B93EAE2D
SHA1:	6D23CA032F0BD7A4BBB998269BEF2EF927059977
SHA-256:	F4EB9F05F942445D14BF91CDAFD1A6B5C5865F80E13B8636E83DF0B61E4AB2A6
SHA-512:	582457E2D9D4231B677BB76E1C3ACD430F31AECD9B802F1D8EFAC55131972966585060AB7F0589B9FA9E7EFFD608AF052462F4D25D780DBABCB953FEA205621
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c2shb.ssp.yahoo.com/bidRequest?dcn=8a96945901757509a7550d8502ed01c1&pos=8a96945901757509a7550d88005e01c7&cmd=bid&secure=1
Preview:	{"id":"a705542f6ceb4ffa83cbaf125cc96331","nbr":1,"seatbid":[]}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bid[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	23
Entropy (8bit):	3.914866303883101
Encrypted:	false
SSDEEP:	3:8WiCLViemVh:8WilUemf
MD5:	EAE5EE6C7E3134A287AA23FCD63D64F0
SHA1:	3B17DC8EB29B01BD80C12C7D64159D0434EDFDAC
SHA-256:	745A085B52B8371EC6705413FCA70A28C6D8BFF0DB480E6B124BD08C54E95EF8
SHA-512:	3A534A5E4557ACC431634EBA78950183078C2F78816C6E156679F3A8753C4C6514353111E6CE3F52C91219D036351D090970E8097CB4D41D65A1EC39D0E450EF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.amazon-adsystem.com/e/dtb/bid?src=600&u=https%3A%2F%2Fitsfoss.com%2Fsave-command-output-to-file-linux%2F&pid=4tAqxu3C2LHDH&cb=0&ws=300x150&v=7.57.00&t=1600&slots=%5B%7B%22sd%22%3A%220%22%2C%22s%22%3A%5B%22300x250%22%2C%22300x100%22%2C%22300x250%22%2C%22300x50%22%2C%22300x75%22%2C%22320x50%22%2C%22300x300%22%5D%2C%22sn%22%3A%22%2F57806026%2FItsFoss_DT_Dis%22%7D%5D&pubid=f67fb912-2d88-4326-8009-bd2154299562&gdprl=%7B%22status%22%3A%22no-cmp%22%7D
Preview:	apstag.punt({"cb":"0"})

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\blocks.style.build[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	45111
Entropy (8bit):	4.9499604069953715
Encrypted:	false
SSDEEP:	768:K5OLIfDTZ+/S2eIfSLpKnBo2yVY7gQiTFkjoFw:Fm+/S2eIfSLony2yVY7gQiTFkjoS
MD5:	30F0C5757823F9CF82D4549D9A3F65D2
SHA1:	77EC180E6A59771EC49030FCB2975B15DD767CCB
SHA-256:	030452EBBF37A3EA0014F9E22A179DC31A3EF4D82D5E804864A208B75FD9A85B
SHA-512:	0612E6803F4059EE8D50833D1B49DF53E5B96745A51CC6591CE929F507902E5CD0DAA7F7F61FC55731CF7253D317A84EC71759973B1E955CE3CAAF7CC9060FC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://itsfoss.com/wp-content/plugins/genesis-blocks/dist/blocks.style.build.css?ver=1604544077
Preview:	.gb-block-testimonial{background:#f2f2f2;color:#293038;margin:0 auto;padding:5%;border-radius:5px;margin-bottom:1.2em}.gb-block-testimonial .gb-testimonial-info {position:relative;display:inline-block;width:100%;margin-top:15px;min-height:55px;padding-top:5px;line-height:1.4}.gb-block-testimonial .gb-testimonial-info .blocks-edit able{padding-left:0}.gb-block-testimonial .gb-testimonial-info .gb-testimonial-avatar-wrap{position:absolute;left:0;top:0}.gb-block-testimonial .gb-testimonial-avatar-wra p+.gb-testimonial-name,.gb-block-testimonial .gb-testimonial-avatar-wrap+.gb-testimonial-name+.gb-testimonial-title,.gb-block-testimonial .gb-testimonial-avatar-wrap+.gb-testimonial-title,.gb-block-testimonial .gb-testimonial-avatar-wrap+.editor-rich-text,.gb-block-testimonial .gb-testimonial-avatar-wrap+.editor-rich-text+.editor-rich-tex t{margin-left:70px;padding-left:0}.gb-block-testimonial .gb-testimonial-text p{line-height:1.6}.gb-block-testimonial .gb-testimonial-text a{color:inherit;box-sh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bundle.NetworkInstrument.e3ff3b25[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	6220
Entropy (8bit):	5.241394376522417
Encrypted:	false
SSDEEP:	96:q7In7xuigJ071fbdoDRVSHyXuRj0NHhn6R/odFWqmUfUNREy:fn7E01zdoDRsH2E/sEUa6y
MD5:	EEB47C646221A975BED130F207912F7D
SHA1:	FB46F36A96FF9A5F0EA6D434370B0ED866C6E8C6
SHA-256:	C3DAE5F44A1E3755EE97222E63DA9AFF2E92C485F343E3A5E006B21D6883D9FD
SHA-512:	435D292EEFC14AD918C086507202C0F847C5FEBD56424D02AE3C05A0AC6362FFE7305D4149BFDC251C6F240E5E5591868FCD2A92D2A08A207D42B93C3704E0D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://abs.twimg.com/responsive-web/client-web-legacy/bundle.NetworkInstrument.e3ff3b25.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[57],{ujfh:function(e,t,r){"use strict";r.r(t),r.d(t,"default",(function(){return b}));r("1t7P"),r("LW0h"),r("jwue"),r("vrRf"),r("lTEL"),r("z84l"),r("Ee2X"),r("ho0z"),r("daRM"),r("FtHn"),r("+KXO"),r("7x/C"),r("87if"),r("+oxZ"),r("kYxP"),r("Cm4o");var n=r("m3Bd"),o=r.n(n),i=r("VrFO"),s=r.n(i),a=r("Y9Ll"),u=r.n(a),c=r("KEM+"),p=r.n(c),_=r("pXBW"),d=r("k49u"),f=r("ZjLa"),h=r("Myq3"),m=r("EhiH"),l=r("/NU0");function v(e,t){var r=Object.keys(e);if(Object.getOwnPropertySymbols){var n=Object.getOwnPropertySymbols(e);t&&(n=n.filter((function(t){return Object.getOwnPropertyDescriptor(e,t).enumerable}))),r.push.apply(r,n)}return r}function w(e){for(var t=1;t<arguments.length;t++){var r=null!=arguments[t]?arguments[t]:{};t%2?v(Object(r),!0).forEach((function(t){p()(e,t,r[t])})):Object.getOwnPropertyDescriptors?Object.defineProperties(e,Object.getOwnPropertyDescriptors(r)):v(Object(r)).forEach((function(t){Object.defineProperty(e,t,Object.getOwnP

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\c[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 6 x 5
Category:	downloaded
Size (bytes):	50
Entropy (8bit):	3.8488255736198
Encrypted:	false
SSDEEP:	3:CN+ltRPQEsJen2sSX:xvQEsJ42sSX
MD5:	E4D673A55C5656F19EF81563FB10884C
SHA1:	1F2D8ED221D39329251AD3A6FF1EDB20B7219443
SHA-256:	F3A8992ACB9AB911E0FA4AE12F4B85EF8E61008619F13EE51C7A121FF87F63B1
SHA-512:	E0B03411282A979CF772F700D9E5634B0C25C612E380AD33C0D59059B1B479D027016D5BEB148403EF185430DB35F5FAED362F36CE2C8ECAD0E6D8E30CEA97E4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pixel.wp.com/c.gif?s=2&u=https%3A%2F%2Fwww.youtube.com%2Fchannel%2FUCEU9D6KIShdLeTRyH3IdSvw&r=nofollow%20noopener&b=37237282&p=85345&rand=0.8329526349966203
Preview:	GIF89a.....!.....,.....bx..j....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	750
Entropy (8bit):	5.167270294510424
Encrypted:	false
SSDEEP:	12:jFMY3Q6ZRoT6pncqFMY3Q6ZN76p6qFMO6ZRoT6pIFqFMO6ZN76pYnJY:5MY3QYs0nMY3QYN7YMOYsiMOYN7M
MD5:	D7427F8811D90D07D2E2D4D5D863011F
SHA1:	B83F4B0212E90A1DBB49A3718A399253AEA8B093
SHA-256:	36DE425207CB62C32B2D559BA2938034E15A9FDAA5434BA58CBF756940A1B5F9
SHA-512:	E5B82F682143D05E5D5CF8DC1631540FFCFB96968E86824198D891E27700A72A67052256A14DCD3A1AFC54E6E1CBF526C3069F112D67D3D977775D682C6FC0E
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/opensans/v18/mem6YaGs126MiZpBA-UFUK0Zdcs.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKWiUNhrIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/opensans/v18/mem8YaGs126MiZpBA-UFVZ0d.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UN7rgOUuhv.woff) format('woff');.}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\custom[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	6943

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\custom[1].css	
Entropy (8bit):	4.9204326849344895
Encrypted:	false
SSDEEP:	192:0DH31/INBY49HLB4C1BSje8PuOFf0hyzq3tX7XyXDw+lPz:OpIA
MD5:	1F4F543DEC78A6B9C6267750B9F30CC0
SHA1:	FE03B7A22FB83C8AA3D9C21A1F2717EB3DCD9C92
SHA-256:	EB7FAC32CAFBB4D2568C5ECFAFE71F2F2A8E3147EA7CB24D81C0CB7C766E63FF
SHA-512:	8A9419EC5E5CDF1EE1297F677829FC40D2644FA591A2BB4835D0E23C41EBD5F2500550F6653D1041192A207708E21EAB99E0032A6A52E95D0A2930DFE8F57825
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://api.searchiq.co/api/css/f72c700acb39b7cb641df8a9ef845ffc/custom.css?v=2.2.56&cb=6270431
Preview:	body #siq_search_results .siq_searchForm .siq_searchWrapper .siq_searchTop .siq_searchInner .siq_searchBox{background-color:#FFFFFF;color:#323232}.body #siq_search_results .srch-poweredbysiq div, body #siq_search_results .srch-poweredbysiq a{color: #AAAAAA}.body #siq_search_results .search-results-row, body #siq_search_results .search-sponsored-row,#siq_search_results div.siq-prodfacet-contR div.siq-prdrslts-row div.siq-prdrslts-box{background-color:#FFFFFF}.body #siq_search_results .search-results-R div.search-results-title a, body #siq_search_results .siq-ads h2.srch-sponsored-title a, #siq_search_results div.siq-prodfacet-contR div.siq-prdrslts-row div.siq-prdrslts-box a.siq-prdbx div.siq-prdtls h3{font-size:20px;line-height:24px;color:#000000}.body #siq_search_results .search-results-R div.sr-R-author{font-size:13px;line-height:15px;color:#959595}.body #siq_search_results .search-results-R .sr-R-cont div, body #siq_search_results .siq-ads .srch-sponsored-R-cont p{font-size:15px;lin

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\dashicons.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	59009
Entropy (8bit):	6.036875180346838
Encrypted:	false
SSDEEP:	768:oey/Z24B3P3aXOhUzSv16CAyLquqSfurIdUMbs73KO08QSJ2BQH02CRqxMWs5HJq:ox/ZvB/qPWMiquqioMUXQSJYIMW+HJq
MD5:	D2678BBFDB083928CABB16F0B85D0F1C
SHA1:	087B89DC6890740318D68DFF5550B0E624D254CF
SHA-256:	DC1A3A3BF97EADA084F65B5D87085DDB8D3A76A9E450C6A41211E1698048DE91
SHA-512:	888217472B406413F5FA4F69823E87B04B9B76828C97902C52C8D96B1DCB09DE43AAFE26BCD38131733C74C8FBD23608362DC0FB9BC2FF87EA8A5B64205C087
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c0.wp.com/c/5.5.3/wp-includes/css/dashicons.min.css
Preview:	/*! This file is auto-generated */.@font-face{font-family:dashicons;src:url(../fonts/dashicons.eot?99ac726223c749443b642ce33df8b800);src:url(../fonts/dashicons.eot?99ac726223c749443b642ce33df8b800#iefix) format("embedded-opentype"),url("data:application/x-font-woff;charset=utf-8;base64,d09GRgABAAAAAHwAAsAAAAA3EgAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAABHU1VCAAABCAAAADMAAABCsP6z7U9TLzIAAAE8AAAAQAAAAFZAuk8lY21hcAAAAXwAAAk/AAAU9l+BPsxnbHlmAAAKvAAAYwIAAKlAcWTMRWhlYWQAAG3AAAAALwAAADYXkmaRaGhlYQAAbfAAAAAfAAAAJAQ3A0hobXR4AABuEAAAACUAAAVQpgT/9mxvY2EAAG44AAACqgAAAqps5EEYbWF4cAAAcOQAAAAfAAAAIAJvAKBuYW1lAABxBAAAATAAAAIiwytf8nBvc3QAAHI0AAAJvAAAEhojMlz2eJxjYGRgYOBikGPQYWB0cfMJYeBgYGGAAJAMY05meiJQDMoDyrGAaQ4gZoOIAgCKIwNPAHicY2Bk/Mc4gYGVgYOBhzGNgYHBHUp/ZZBkaGFgYGJgZWbACgLSXFMYHD4yfHVnAnH1mBgZGIE0CDMAAI/zCGl4nN3Y93/eVRnG8c/9JE2bstLdQIF0N8x0t8w0pSMt0BZKS5ml7F32lrL3hlKmCxEQtzjAhQMRRcEJijhQQWV4vgNBGV4nl3+B/mbTd8+reeVJvuc859znvgL0A5pkO2nW3xcJ8qee02ej7/NNDOz7fHPTw/r/LnTo60ale4ooWov2orOYXXQXPWVr2V52lrPL3qq3WlmtqlZXx

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\desktop_polymer_inlined_html_polymer_flags_legacy_browsers[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	6551638
Entropy (8bit):	5.500427929871944
Encrypted:	false
SSDEEP:	49152:5fECLwgkjsXPc2saVtk++UIzID4MmEMnS1asGYKcO4CznZ0TzZpIua///PAcmwAi:zMqZZcm6
MD5:	59F5B2EFBEAD1096DA8C31E71D733955
SHA1:	0462BE120D5B3A697C4AC81FE844DAABB883ED21
SHA-256:	7DB3B7AB19616817198C1718702A028BBB82708F4DC986A3561195988757D3E4
SHA-512:	96F9FF45F56252027CA4AF63098000E9B450ACB075EAD08BCF7DC9E1F11580D97E3F3C727B50A4ED9C33C58549461097FCB1A0FD4EE811FF80E835EC59F7B2B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube.com/s/desktop/a386e432/jsbin/desktop_polymer_inlined_html_polymer_flags_legacy_browsers.vflset/desktop_polymer_inlined_html_polymer_flags_legacy_browsers.js
Preview:	if(ytcsi){ytcsi.tick("rses_dpj")}.(function(){./* HTML content inlined from HTML import */.const d=document.createElement("div");.d.setAttribute("inlined-html","");.d.innerHTML=" \n@license\nCopyright (c) 2016 The Polymer Project Authors. All rights reserved.\nThis code may only be used under the BSD style license found at http://polymer.github.io/LICENSE.txt\nThe complete set of authors may be found at http://polymer.github.io/AUTHORS.txt\nThe complete set of contributors may be found at http://polymer.github.io/CONTRIBUTORS.txt\nCode distributed by Google as part of the polymer project is also\nsubject to an additional IP rights grant found at http://polymer.github.io/PATENTS.txt\n--> \n@license\nCopyright (c) 2015 The Polymer Project Authors. All rights reserved.\nThis code may only be used under the BSD style license found at http://polymer.github.io/LICENSE.txt\nThe complete set of authors may be found at http://polymer.github.io/AUTHORS.txt\nThe complete set of contributors

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5994
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8RrN7u5V4VyhhV2lFUW29vj0RkpNc7KpS:vIlJ6G7Ao8RilIJ6G7Ao8Ra
MD5:	713ADD0E98C772CE39C7B2452806602B
SHA1:	7888DE86275AE869D6E82EE4D392C71EB9BCCD25
SHA-256:	6DE0370BA485689D411FF66EEA6EBCC577A1D19CFD489FA4DC7E22BD91F65806
SHA-512:	ABFB3EF6B1EA2A12B9A1E425BD94F807A4CE1C8FCE8CC618FBC700222CE573CFAB47BA9FCDCDE7157142F43CD3349014AAD1DC720EB8C327000B9211BAB3 39F
Malicious:	false
Reputation:	low
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMo reInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t.,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\e-202047[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	8972
Entropy (8bit):	5.193120646441914
Encrypted:	false
SSDEEP:	192:SOfIRscXT3FySXv/r8o6NAAWOT4LpWYNO9DqWXWv66LyHxTD:SOfIzwSJ6NAAD4LpWYgTQ2Rn
MD5:	BA6F15831404DC46DA2DDE617BDA1653
SHA1:	1F356C00C142ACAB972807BAEE47FD3F54C9CB11
SHA-256:	0EBBC7FBA9A50D36EF5422345F624431710DB4528F25749D1D438C2C10BB69F2
SHA-512:	001FED834A366D386F9FC60FD30DB3505AEDA99B27FF4C683BED599F4534051EDDF7C36DBDAE1C39810BCB140757D9AF01CD46522E12ED029648A673CE97DE 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://stats.wp.com/e-202047.js
Preview:	window.wpcom=window.wpcom||{};window._stq=window._stq||[];function st_go(a){window._stq.push(['view',a]);};function linktracker_init(b,p){window._stq.push(['cli ckTrackerInit',b,p]);};window.wpcom.stats=(function(){var _clickTracker=(function(){var _blog,_post;var _addEvent=function(el,t,cb){if('function'===typeof el.addEventList ener){el.addEventListener(t,cb);}else if('object'===typeof el.attachEvent){el.attachEvent('on'+t,cb);}};var _getClickTarget=function(e){if('object'===typeof e&&e.target){return e.target;}else{return window.event.srcElement;}};var _clickTrack=function(e){var d=0;if('object'===typeof InstallTrigger)d=100;if(7===_getIEVer())d=100;_processLin k(_getClickTarget(e),d);};var _contextTrack=function(e){_processLink(_getClickTarget(e),0);};var _isSameHost=function(a){var l=document.location;if(l.host===a.h ost)return true;if(''===a.host)return true;if(l.protocol===a.protocol&&l.host===a.hostname){if('http:'===l.protocol&&l.host+':80'===a.host)return true;if('https:'===l.pro

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[1]	
Category:	downloaded
Size (bytes):	9440
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	192:JsUOG1yNlX6ZzWpHOWLia16Cb7b4sUOG1yNlX6ZzWpHOWLia16Cb7bk:JsDhpNOWLiIb7b4sDhpNOWLiIb7bk
MD5:	9FDEE838E7C036092E81A4E7CC949643
SHA1:	364FC6C36972FFD803E5999AD501F3D7A2216FDF
SHA-256:	C6BF586821E13F7F6D6EF75AA82E69BD5E3E1336615C85AE513C70704F5C0787
SHA-512:	622BC3BD9F0615C191B03F2E8D018867C9D9ADCF1015DA5FB4D3462D71512B72558B32CA9F74A925C150B57FD232ABD48AFFC8D32128C50540DF02FCA8ECBE B
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\f[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	9700
Entropy (8bit):	6.017814501214815
Encrypted:	false
SSDEEP:	192:zLUVB44di8DwNE+wFVNgjHgYoEjDPcaGgO5q/qGzT2uei8rDMA3fy/+ZJ:+B4ai8DwOFJJMbWgO56qRDNPy/+ZJ
MD5:	F1E28DA8053BA8532595151AF4393BD6
SHA1:	27F34B366867AD2C66D61506AA631823BDCD8538
SHA-256:	1984345F00DF435B623A7F59BC216A6DADF199138C064CBDFC5DC7EE4610A48F
SHA-512:	D52F7942A5F646A32C72AABFDE9FDE46C4C8BE28F310ABBDC3F431D53215D04375ED2CE02ED8195EFFDFBA9899B1F5E1C8CFEA2C9F1A4911079ECC7631C38 CD2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pagead2.googlesyndication.com/getconfig/sodar?sv=200&tid=gpt&tv=2020111701&st=env
Preview:	{"sodar_query_id":"MPO5X4_KC_rI7_UP5M-HmA0","injector_basename":"sodar2","bg_hash_basename":"h-M7V3DIqUYi9kK3fFWRC5fS_RbIlX9Nvskvt3Cq0cY","bg_binary":"RzRk6tQZhAMVonEHn/co3amr+amVqghJVIdj8AwkzhbjHpzhjrTOonV57uxjTTE2bZ9sdgvz933DpEEsMjsDZAa216mEfT+wrMHAVHaGC5GcVUrnaChYr31ojNNRALJ2YI8ayE4KbOs72UiIuviVCIX1ileCIPCFD0Qk3HuukOoI7fMAGEz86xMMupCJyp7lY9XRnSZv+d1VhKjtUcdS7xNk8QQh4oxUQwb3Uj0z4A1Xa2p76Oc3owaFzqAP4DmE6W1sMsZdQBAhxwS8ZpRstad+rjMpyiDAbhT9LrhdTmrLNScuCw2TRmbB4ArQBeFtLGJFMr+wwcNdCHopbEUWaZhUTNXX2ZCqxcJ7vCIjTEw6x4dFSxIHedkPvfv7eHl2m0EjxATWppWy2bEPkIxFPKBBk1RRQSzqXbjPEQnSg1yfkee6e/qAEenfcRPtVNo6xhXDXXXUj7G+bfPD4fsFhifrsoRElU5cDp4e9DgWAjpnqwj+mhCsFHfk7lFoyrc/5j/BaltHNiHTLdUwcUgU3rHON2WK9CLFUrkCYpcks5dpVLz5PX4bnfmAYDaujnb5OpoDmkaMKtVmmmIOXZtJMNSzr4A6a1UQLGcYqZqCA6v3U8aczf58Ugf+UUEiRaXccqC9ae0trdZdBxluuXNA1EPg7MmNNop5op9w+ALXqlJ1IvHcQkXt2oK9dchFiGI/nRS1PRRoSBqsqsQr4pM0Iofs9DuWoIsdehNpNcnmTKEr5O8kThodrvpve6NnxIbh7p/vkovYcTNEL7+Q3r4M7/VzRGj/KFUgOKNTlVYhlxsRHJMa6rhvFIR3hV4SMFbbwL2Xtg0aC0c+Ww2st

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\fetch-polyfill[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Pascal source, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	8543
Entropy (8bit):	5.238064281324506
Encrypted:	false
SSDEEP:	192:oQHdiEslZc0rsNYNU5mSJHqI03aej6tZoaMLQO/x5/P80+HcW:ocHslLsP5muHqI0Jj6tZcUO/x5+V
MD5:	04E3CC8A9641B3F9F9C9370F4E9B5BDD
SHA1:	9602A891F583094BB04FD407B253ABCAFFB8C8D0
SHA-256:	DE6C4FFA2BD9FD283610E28D0DB2EC48607AAB39D213A51AEF248673A0A7E980
SHA-512:	58942BCC0F39D620A475B65C1AEB4F18872F68F22C89DEC076906A0DB8BC2B7CCA9357710A7824A0FA7404FF73F41013AECA34609CAACD2187414F7BD0D490D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube.com/s/desktop/a386e432/jsbin/fetch-polyfill.vflset/fetch-polyfill.js
Preview:	/*.. Copyright (c) 2014-2016 GitHub, Inc... Permission is hereby granted, free of charge, to any person obtaining. a copy of this software and associated documentation files (the. "Software"), to deal in the Software without restriction, including. without limitation the rights to use, copy, modify, merge, publish,. distribute, sublicense, and/or sell copies of the Software, and to. permit persons to whom the Software is furnished to do so, subject to. the following conditions:.. The above copyright notice and this permission notice shall be. included in all copies or substantial portions of the Software... THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,. EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF. MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND. NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE. LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION. OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\frontend_blocks[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	91946
Entropy (8bit):	4.858685059719977
Encrypted:	false
SSDEEP:	1536:l8cA1JCntOjdfXH+P5eD7LfnWHPI8kLCu:vO1XH+P5eD78kv
MD5:	B18AD10A66E254BC46C9986232B6F565
SHA1:	DE9DEDF17B2A8A45F46B35C0C4398C087CC4A4DA
SHA-256:	A0DCCC63C1C808FF164AF14F7D3722217C4C4DDC0A06BBF00153DA7F3B2B0371
SHA-512:	4120FFB080DA3B2B870927A6C00F8AF1D521071CA164CB017FD303C1E0D0F1D2D5E378367B53C400F9A5930A0D954B5706E5FF1264957460F193D1B080A9020F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://itsfoss.com/wp-content/plugins/stackable-ultimate-gutenberg-blocks-premium/dist/frontend_blocks.css?ver=2.12.2
Preview:	.ugb-accordion.ugb-accordion--v2.ugb-accordion--open .ugb-accordion__heading .ugb-accordion__arrow{transform:rotate(180deg)}.ugb-accordion.ugb-accordion--v2.ugb-accordion.ugb-accordion--design-basic .ugb-accordion__heading{box-shadow:0 5px 5px 0 rgba(18,63,82,.035),0 0 0 1px rgba(176,181,193,.2);background-color:#fff;border-radius:12px;overflow:hidden;padding:17.5px 35px}.ugb-accordion.ugb-accordion--v2 .ugb-accordion__heading{margin:0;display:flex;align-items:center;justify-content:space-between;cursor:pointer;transition:margin .3s ease-in-out;will-change:margin}.ugb-accordion.ugb-accordion--v2 .ugb-accordion__heading .ugb-accordion__title{flex:1;margin:0!important;order:1}.ugb-accordion.ugb-accordion--v2 .ugb-accordion__heading .ugb-accordion__arrow{flex-shrink:0;order:3;transition:transform .3s ease-in-out;transform:rotate(0deg)}.ugb-accordion.ugb-accordion--v2 .ugb-accordion__heading:after{content:"";width:26.25px;display:block;order:2;flex-shrink:0}.ugb-accordion.ugb-accordion--v2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\frontend_blocks__premium_only[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	94800
Entropy (8bit):	4.8581756950628945
Encrypted:	false
SSDEEP:	1536:xYeIoRFF0ytpoQIrdqleMTu3ENRgNa1ruVj47xz8r:WeIjGz8r
MD5:	E28E830F5FFCF5E08D51C9E90BAD0362
SHA1:	4A311E2A90CF0D550231080EABA9CFF03D3608E8
SHA-256:	90503602FF019C16204AFD8063F2BFD01826ADD168E7F6E181B55E0DF21AB09B
SHA-512:	940D04D31342FF15745A945E1BE2CE6BAE4B7B9802FA3AC149274AEE4942FE690CDD923AEB4E68FDAA6D46C0A64E2D3F7582A208FE80032F387D4B89F82E4FE5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://itsfoss.com/wp-content/plugins/stackable-ultimate-gutenberg-blocks-premium/dist/frontend_blocks__premium_only.css?ver=2.12.2
Preview:	.ugb--hover-lift,.ugb--hover-lift-more,.ugb--hover-lift-shadow,.ugb--hover-lift-shadow-staggered,.ugb--hover-lift-staggered,.ugb--hover-lower,.ugb--hover-lower-more,.ugb--hover-scale,.ugb--hover-scale-more,.ugb--hover-scale-shadow,.ugb--hover-shadow{transition:all .3s cubic-bezier(.84,.12,.59,.83)!important}.ugb--hover-lift-shadow-staggered,.ugb--hover-lift-staggered{transition-delay:.15s!important}.ugb--hover-lift-shadow-staggered h1,.ugb--hover-lift-shadow-staggered h2,.ugb--hover-lift-shadow-staggered h3,.ugb--hover-lift-shadow-staggered h4,.ugb--hover-lift-shadow-staggered h5,.ugb--hover-lift-shadow-staggered img,.ugb--hover-lift-staggered h1,.ugb--hover-lift-staggered h2,.ugb--hover-lift-staggered h3,.ugb--hover-lift-staggered h4,.ugb--hover-lift-staggered h5,.ugb--hover-lift-staggered img{transition:all .3s cubic-bezier(.84,.12,.59,.83)!important}.ugb--hover-lift-shadow-staggered:hover,.ugb--hover-lift-staggered:hover{transform:translateY(-10px)}.ugb--hover-lift-shadow-staggered:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ga[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	46274
Entropy (8bit):	5.48786904450865
Encrypted:	false
SSDEEP:	768:aqNVrKn0VGhn+K7U1r2p/Y60fyy3/g3OMZht1z1prkfw1+9NZ5VA:RHrLVGhnpIwp/Y7cnz1RkLL5m
MD5:	E9372F0EBBCF71F851E3D321EF2A8E5A
SHA1:	2C7D19D1AF7D97085C977D1B69DCB8B84483D87C
SHA-256:	1259EA99BD76596239BFD3102C679EB0A5052578DC526B0452F4D42F8BCDD45F
SHA-512:	C3A1C74AC968FC2FA366D9C25442162773DB9AF1289ADFB165FC71E7750A7E62BD22F424F241730F3C2427AFFF8A540C214B3B97219A360A231D4875E6DDEE6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.google-analytics.com/ga.js
Preview:	(function(){var E;var g=window,n=document,p=function(a){var b=g._gaUserPrefs;if(b&&b.ioo&&b.ioo()||a&&!0===g["ga-disable-"+a])return!0;try{var c=g.external;if(c&&c._gaUserPrefs&&"oo"==c._gaUserPrefs)return!0}catch(f){}a=[];b=n.cookie.split(";");c=/^\s*AMP_TOKEN=\s*(.*?)\s*$/;for(var d=0;d<b.length;d++){var e=b[d].match(c);e&&a.push(e[1])}for(b=0;b<a.length;b++)if("$OPT_OUT"==decodeURIComponent(a[b]))return!0;return!1};var q=function(a){return encodeURIComponent?encodeURIComponent(a).replace(/\(/g,"%28").replace(/\)/g,"%29"):a},r=/^(www\.)?google(\.com?)?(\.[a-z]{2})?$/,u=/(^|\.)doubleclick\.net$/i;function Aa(a,b){switch(b){case 0:return""+a;case 1:return 1*a;case 2:return!!a;case 3:return 1E3*a}return a}function Ba(a){return"function"==typeof a}function Ca(a){return void 0!=a&&-1<(a.constructor+"").indexOf("String")}function F(a,b){return void 0==a||"-"==a&&!b||""==a}function Da(a){if(!a||""==a)return"";for(;a&&-1<" \n\r\t".indexOf(a.charAt(0));)a=a.substring(1);for(;a&&-1<" \n\r\t".i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\hsts-pixel[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	2.7374910194847146
Encrypted:	false
SSDEEP:	3:CU9yltxlHh/:m/
MD5:	DF3E567D6F16D040326C7A0EA29A4F41
SHA1:	EA7DF583983133B62712B5E73BFFBCD45CC53736
SHA-256:	548F2D6F4D0D820C6C5FFBEFFCBD7F0E73193E2932EEFE542ACCC84762DEEC87
SHA-512:	B2CA25A3311DC42942E046EB1A27038B71D689925B7D6B3EBB4D7CD2C7B9A0C7DE3D10175790AC060DC3F8ACF3C1708C336626BE06879097F4D0ECAA7F5670 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fbsbx.com/security/hsts-pixel.gif
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Reputation:	low
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\iePolyfills.0e32b39aad0081b2af83.bundle[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with NEL line terminators
Category:	downloaded
Size (bytes):	92117
Entropy (8bit):	5.36225991231486
Encrypted:	false
SSDEEP:	1536:BGsc/xM6y6j3qLj5m3arBobjMxqv85Ew7+:xP83qL2aybjEL+
MD5:	5F84E1E8D9E4B502168F1B6D338A9103
SHA1:	4ED8D3A222C87EA7651CE0FA45C50E59B64857C4
SHA-256:	5192F051646C02416AB929F7A3EC0AB7EE6A423FFC0EEEDFA4C7F8C3221C9B3B
SHA-512:	FFFD0BCD945576CCFB9F1846AAA3C625F83D57C7DE6B761F460CB1CE114525322272B01BF59DA2C525E840CE901D99DD0F160931AC18C943EF8F6060B30A93
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://renderer.apester.com/v2/static/iePolyfills.0e32b39aad0081b2af83.bundle.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([["iePolyfills"],{"000d7":function(t,n,e){var r=Date.prototype,i=r.toString,o=r.getTime;new Date(NaN)+""!="Invalid Date"&&e("e3856")(r,"toString",(function(){var t=o.call(this);return t==t?i.call(this):"Invalid Date"}))},"009d1":function(t,n,e){var r=e("ef372"),i=e("a97ab")(!1);r(r.S,"Object",{values:function(t){return i(t)}})},"00a5a":function(t,n,e){var r=e("402c0"),i=e("904aa"),o=e("25a61"),c=e("ef372"),f=e("194e2"),u=e("8c7ed");c(c.S,"Reflect",{get:function t(n,e){var c,a,s=arguments.length<3?n:arguments[2];return u(n)===s?n[e]:(c=r.f(n,e))?o(c,"value")?c.value:void 0!==c.get?c.get.call(s):void 0:f(a=i(n))?t(a,e,s):void 0}})},"0139b":function(t,n,e){var r=e("ef372");r(r.S,"Number",{MIN_SAFE_INTEGER:-9007199254740991})},"01b06":function(t,n){t.exports=Object.is||function(t,n){return t===n?0!==t||1/t==1/n:t!=t&&n!=n}},"03d8d":function(t,n,e){var r=e("e3856");t.exports=function(t,n,e){for(var i in n)r(t,i,n[i],e);return t}},"04027":fu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jetpack[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	76995

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jetpack[1].css	
Entropy (8bit):	5.035269893158372
Encrypted:	false
SSDEEP:	1536:aMSPAMZpO8I2V9aW0kPQtV09/oJ7ozeA2J3nQJtQZ+:DV0ZoJ7Y2J3nQJtQZ+
MD5:	F61C4B029FC7B95F4203B65093D4908C
SHA1:	66B3FD56EB72F845068A414DA04F45D7C165B0BB
SHA-256:	7772A9CC35FC902C0CCCB8871670EC3E45E4695E1BC6941AEE1C24DB3DE8C544
SHA-512:	2C676A5E3320D36AE7AC20FE1E2806DD7E3AAE410871B7EC0C5817C9C4364251741E7F8720116C52A8C0ED43354EC51A5090F66E0E7B5AAD6D243DB3559BB8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c0.wp.com/p/jetpack/9.1/css/jetpack.css
Preview:	/*!.* Do not modify this file directly. It is concatenated from individual module CSS files..*/.[data-carousel-extra]{cursor:pointer}.jp-carousel-wrap *{line-height:inherit}.jp-carousel-overlay{background:#000}div.jp-carousel-fadeaway{background:-moz-linear-gradient(bottom,rgba(0,0,0,.5),rgba(0,0,0,0));background:-webkit-gradient(linear,left bottom,left top,from(rgba(0,0,0,.5)),to(rgba(0,0,0,0)));position:fixed;bottom:0;z-index:2147483647;width:100%;height:15px}.jp-carousel-next-button span,.jp-carousel-previous-button span{background:url(../modules/carousel/images/arrows.png) no-repeat center center;background-size:200px 126px}.jp-carousel-msg{font-family:"Open Sans",sans-serif;font-style:normal;display:inline-block;line-height:19px;padding:11px 15px;font-size:14px;text-align:center;margin:25px 20px 0 2px;background-color:#fff;border-left:4px solid #ffba00;box-shadow:0 1px 1px 0 rgba(0,0,0,.1)}@media only screen and (-webkit-min-device-pixel-ratio:1.5),only screen and (-o-min-device-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jita[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	409283
Entropy (8bit):	5.41525009209989
Encrypted:	false
SSDEEP:	6144:uWyxInKW9ilV9O6D6iHPbtb4GAQ1hkZiwQLh:u6P43O62TYkZBQV
MD5:	CD050645B5DB5D9AFA88FCDE7DC662E4
SHA1:	AB432E5ABE3ACD7997B1B0693C9FE478D5E659ED
SHA-256:	ABB3B499EB71C4A4F36CD0A9E00E8471462EA24ED16301EA87D0450DA4C54A1E
SHA-512:	179FE1138F06957CDEA641C83DE0AB2821AB9164845EFBA90E26A42E69DB80A8C0CCA4E2CFAFD24438B75CCF93F88B24979E5E436EB91613A95A6964398D45E6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://481.hostedprebid.com/k8Es/jita.js?dfp=1
Preview:	if (!window.JITA || !window.JITA.init).{.// prebid-core.js./* prebid.js v2.44.5.Updated : 2020-04-06 */.!function(u){var s=window.JITAPBChunk;window.JITAPBChunk=function(e,t,n){for(var r,i,o,a=0,c=[];a<e.length;a++)i=e[a],d[i]&&c.push(d[i][0]),d[i]=0;for(r in t)Object.prototype.hasOwnProperty.call(t,r)&&(u[r]=t[r]);for(s&&s(e,t,n);c.length;)c.shift()();if(n)for(a=0;a<n.length;a++)o=f(f.s=n[a]);return o};var n={},d={293:0};function f(e){if(n[e])return n[e].exports;var t=n[e]={i:e,l:!1,exports:{}};return u[e].call(t.exports,t,t.exports,f),t.l=!0,t.exports}f.m=u,f.c=n,f.d=function(e,t,n){f.o(e,t)||Object.defineProperty(e,t,{configurable:!1,enumerable:!0,get:n})},f.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};return f.d(t,"a",t),t},f.o=function(e,t){return Object.prototype.hasOwnProperty.call(e,t)},f.p="",f.oe=function(e){throw console.error(e),e},f(f.s=720)}({0:function(e,t,n){"use strict";Object.defineProperty(t,"__esModule",{value:!0}),n.d(t,"int

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	96873
Entropy (8bit):	5.372169393547772
Encrypted:	false
SSDEEP:	1536:HYE1fGBiByJsbfXXeRJ/shgWCeLLccJdZVHk04ssx+/mvaSIFSet43tpXJIGVyp3:fsAg0psxTva/FSeKy2bDD5a98Hrq
MD5:	49EDCCEA2E7BA985CADC9BA0531CBED1
SHA1:	F8747F8EE704D9AF31D0950015E01D3F9635B070
SHA-256:	1DB21D816296E6939BA1F42962496E4134AE2B0081E26970864C40C6D02BB1DF
SHA-512:	F766DF685B673657BDF57551354C149BE2024385102854D2CA351E976684BB88361EAE848F11F714E6E5973C061440831EA6F5BE995B89FD5BD2D4559A0DC4A6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c0.wp.com/c/5.5.3/wp-includes/js/jquery/jquery.js
Preview:	/*! jQuery v1.12.4 | (c) jQuery Foundation | jquery.org/license | WordPress 2019-05-16 */.!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="1.12.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?a<0?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return this.pushStack(n.map(this,fu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\libs-frontend.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	65422

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\libs-frontend.min[1].js	
Entropy (8bit):	5.395908851931914
Encrypted:	false
SSDEEP:	1536:xVTddVk0LbvFWkuwF+Zs733vA60EpBAzxL3mDU:7nVk0XbfF+22zB3D
MD5:	8DCEE1C0C95911B2C8510710865ECDEA
SHA1:	EFC3ABFB8FCB9ACB688848E0B3505B3C491EBF98
SHA-256:	F04025594BF92A417ECFF83BB70B8D0122100892D7192D529BB5E3E0BC20D14E
SHA-512:	780F6FE72DEC9E53C5B15AF4D782D9A978DDF3E8830D4C98B25E315622E9A3C1E3B1BA7307610D3F12D1EC25E7197E86D6B9EBB9CE0B38A9C4089B53197CDD93
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://itsfoss.com/wp-content/plugins/thrive-comments/assets/js/libs-frontend.min.js?ver=1.4.10
Preview:	/*! Thrive Comments - 2020-11-04.* http://www.thrivethemes.com/.* Copyright (c) 2020 Thrive Themes */..!function(a,b,c,d){"use strict";function e(a,b,c){return setTimeout(k(a,c),b)}function f(a,b,c){return!!Array.isArray(a)&&(g(a,c[b],c),!0)}function g(a,b,c){var e;if(a)if(a.forEach)a.forEach(b,c);else if(a.length!==d)for(e=0;e<a.length;)b.call(c,a[e],e,a),e++;else for(e in a)a.hasOwnProperty(e)&&b.call(c,a[e],e,a)}function h(a,b,c){for(var e=Object.keys(b),f=0;f<e.length;)(!c||c&&a[e[f]]===d)&&(a[e[f]]=b[e[f]]),f++;return a}function i(a,b){return h(a,b,!0)}function j(a,b,c){var d,e=b.prototype;d=a.prototype=Object.create(e),d.constructor=a,d._super=e,c&&h(d,c)}function k(a,b){return function(){return a.apply(b,arguments)}}function l(a,b){return typeof a==ka?a.apply(b?b[0]||d:d,b):a}function m(a,b){return a===d?b:a}function n(a,b,c){g(r(b),function(b){a.addEventListener(b,c,!1)})}function o(a,b,c){g(r(b),function(b){a.removeEventListener(b,c,!1)})}function p(a,b){for(;a;){if(a==b)retur

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\live[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1 x 1, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	68
Entropy (8bit):	4.3336655487943405
Encrypted:	false
SSDEEP:	3:yionv//thPlE+tJ8/V+5Gfjul2g1p:6v/lhPfA/UY7ulVp
MD5:	978C1BEE49D7AD5FC1A4D81099B13E18
SHA1:	AFCB011CFE6B924F202EE9544F17F631B32A01B1
SHA-256:	93AE7D494FAD0FB30CBF3AE746A39C4BC7A0F8BBF87FBB587A3F3C01F3C5CE20
SHA-512:	81F251D1CA407945457425B681A96D1E7743706FAFA47ACE26F5F569E69337E9AAF726BFF1A854B1A5A47A22E55C4BD285A4D21F695D126DA631A1C891D10F48
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://api.searchiq.co/live?engineKey=f72c700acb39b7cb641df8a9ef845ffc
Preview:	.PNG.....IHDR.....IDATx.c.....1q....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\logo-white[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3343
Entropy (8bit):	3.7402451696991013
Encrypted:	false
SSDEEP:	96:yJJCEa/7LWWZmmKZZX55z23JCVsssKetmD3xxKa:yJLdoSxxB
MD5:	CE8CA0460F4CDC30DE7E89B83A5D9529
SHA1:	A6E709B0F4D0D320553707FEDACB32EFD568722A
SHA-256:	C4A0FB4DA7F6DB6EA3BE9B26968272FD292B94084B4F85652C21A91E106613FF
SHA-512:	8FEFC805538C79D1EACF255FA00AC1D4B6F262E5C5660E12C099F720B84B60399D625ECE2F35CE0600D3ACAF6ACD4E1292D1F4CDF23914381EE9C507B71F4ED
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.apester.com/js/assets/logo-white.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" preserveAspectRatio="xMidYMid" viewBox="0 0 221 43">. <defs>. <style>. .cls-2 {. fill: #ffffff;. }. </style>. </defs>. <path d="M212.4 27C212.4 27 212.9 27.7 213.8 29.3 213.8 29.3 221 42.4 221 42.4 221 42.4 210.9 42.4 210.9 42.4 210.9 42.4 204.4 29.8 204.4 29.8 204.4 29.8 200.1 29.8 200.1 29.8 200.1 29.8 200.1 42.4 200.1 42.4 200.1 42.4 191.1 42.4 191.1 42.4 191.1 42.4 191.1 42.4 191.1 4.9 191.1 4.9 191.1 4.9 204 4.9 204 4.9 207.7 4.9 209.5 5.2 211.1 5.8 215.3 7.5 218 11.3 218 16.7 218 20.7 216.1 25 212.4 26.9 212.4 26.9 212.4 27 212.4 27ZM203.2 12.8C203.2 12.8 200.1 12.8 200.1 12.8 200.1 12.8 200.1 12.8 200.1 21.9 200.1 21.9 200.1 21.9 204.1 21.9 204.1 21.9 207 21.9 208.8 20.3 208.8 17.3 208.8 14.5 207.7 12.8 203.2 12.8ZM162.6 4.9C162.6 4.9 185.7 4.9 185.7 4.9 185.7 4.9 185.7 12.8 185.7 12.8 185.7 12.8 185.7 12.8 171.6 12.8 171.6 12.8 171.6 12.8 171.6 12.8 171.6 19.6 171.6 19.6 171.6 19.6 182.8 19.6 182.8 19.6 182.8 19.6 182.8 27.5 182.8 27.5 182.8 27.5 171.6 27.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\logo_48[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	2228
Entropy (8bit):	7.82817506159911
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\logo_48[1].png	
SSDEEP:	48:4/6MuQu6DYYEcBDlBVzqawiHl1Oupgl8m7NCnagQJFknwD:4SabhtXqMHyCl8m7N0ag6D
MD5:	EF9941290C50CD3866E2BA6B793F010D
SHA1:	4736508C795667DCEA21F8D864233031223B7832
SHA-256:	1B9EFB22C938500971AAC2B2130A475FA23684DD69E43103894968DF83145B8A
SHA-512:	A0C69C70117C5713CAF8B12F3B6E8BBB9CDAF72768E5DB9DB5831A3C37541B87613C6B020DD2F9B8760064A8C7337F175E7234BFE776EEE5E3588DC5662419D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/recaptcha/api2/logo_48.png
Preview:	.PNG.....IHDR...0...0.....W.....gAMA.....a.... cHRM..z&.....u0...`..:....p..Q<....bKGD.....C.....pHYs.....IDATh...P....=..8.....Nx. ..PlP8..;.C.1iL#6...*.Z..!.....3.po .o.L.i.l..1fl..4..ujL&6$.....w.....,Z..z. ~....\.._.C.eK...g..%..P..L7...96..q....L.....k6...*..,xz.._.....B."#...L(n..f..Yb...*.8.;....K)N...H).%.F"Ic.LB.....jG.uD..B....Tm....T. .).A.}D.f..3.V.....O.....t_..].x.{o.....*....x?!W...j..@..G=Ed.XF.....J..E?../]..?p..W..H..d5% WA+.....)2r..+..'qk8.../HS.[...u..z.P.*....-.A.}.....I .P.....S....|...)..KS4....I.....W...@....S. s..s..$`.X9.....E.x.=.u.*iJ.....k.....'...!.a....*+.....(...S..\h....@.....I.$..%.2....l.....a.|.....U....y.....t..8....TF.o.p.+.@<.g.....-.M....:.@..(.....@.....>..=.ofm.WM{...e..,..D.r.. .....w....T.L.os..T@Rv..;.....9....56<.x.....2.k.1....dd.V.....m..y5../4|...G.p.V.....6...}.....B.....5...&..v..yTd.6...../m.K...(.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\m3riRLHGxZh[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	234418
Entropy (8bit):	5.393302773231366
Encrypted:	false
SSDEEP:	3072:inElRZsMR9hHPlNhNlRxdx3JVDCuvw4Im+gSUrBmAP2TxNB7fXDUH:0EdsEBmAPGxNNY
MD5:	E53C10DBE24C541A9DCB0E6998F1F69E
SHA1:	D3462F883828CC5FC7B360667CF0C119E7E8C438
SHA-256:	BDCC597C5B5C39BE39EFE00E019F397E2D58F2FA58160A44C9FFCA6E1CDFE3F7
SHA-512:	0C4FDC24AF6D92662013CD5A25B5DF0E91150758BEF5C41D15F60042ECDD60FE08CCAB9CA85A3AD439FAC0A7A386DAC7555B2425D459C86A90740D0C3E8B171
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3/yV/r/m3riRLHGxZh.js?_nc_x=Ij3Wp8lg5Kz
Preview:	if (self.CavalryLogger) { CavalryLogger.start_js(["QPGh+"]); }..self.__DEV__=self.__DEV__||0,self.emptyFunction=function(){};."use strict";.Array.from||(Array.from=function(a){if(a==null)throw new TypeError("Object is null or undefined");var b=arguments[1],c=arguments[2],d=this,e=Object(a),f=typeof Symbol==="function"?typeof Symbol==="function"?Symbol.iterator:"@@iterator":"@@iterator",g=typeof b==="function",h=typeof e[f]==="function",i=0,j,k;if(h){j=typeof d==="function"?new d():[];var l=e[f]( ),m;while(!(m=l.next()).done)k=m.value,g&&(k=b.call(c,k,i)),j[i]=k,i+=1;j.length=i;return j}var n=e.length;(isNaN(n)||n<0)&&(n=0);j=typeof d==="function"?new d(n):new Array(n);while(i<n)k=e[i],g&&(k=b.call(c,k,i)),j[i]=k,i+=1;j.length=i;return j});.Array.isArray||(Array.isArray=function(a){return Object.prototype.toString.call(a)=="[object Array]"});.(function(){var a=Object.prototype.toString,b=Object("a"),c=b[0]!="a";function d(a){a=+a;a!==a?a=0:a!==0&&a!==1/0&&a!==-(1/0)&&(a=(a>0||-1)*Math.fl

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\nuNGGHVvpr7[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 144 x 142, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	13062
Entropy (8bit):	7.975072357529135
Encrypted:	false
SSDEEP:	384:gV/ulMVXsCAvfXr2adAxgu6xVmdpA1oR10XN7Q:plpLvPZA5GUdO1oR1mQ
MD5:	D186B6092C3FF6D63D46439344509A98
SHA1:	A18BD5DA3C3A409F6E2DD88EC64C95B81EB790A9
SHA-256:	B5887504C28947A2526772B2FA00652E438A3E43F3C0174F6A65E105A424F2E8
SHA-512:	8D8F5B65F5D345C7F4363E157C71F8935D6F416C0C20B4C094FEB7463A200686B322C5D5BBC2BF03606F7E95812D774A087A08E1CDA655F732F3987C4C1A8E92
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3/yp/r/nuNGGHVvpr7.png
Preview:	.PNG.....IHDR.....S....sRGB.....pHYs.....YiTXtXML:com.adobe.xmp.....<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="XMP Core 5.4.0">. <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">. <rdf:Description rdf:about="". xmlns:tiff="http://ns.adobe.com/tiff/1.0/">. <tiff:Orientation>1</tiff:Orientation>. </rdf:Description>. </rdf:RDF>.</x:xmpmeta>.L.'Y..1FIDATx..}.`T...y....!{.$..'aU..E.VDM..n.Z.K.j..|m.....V..QA."K. ....I&.6....3..j..Lf.d...}...g..j.+ .P`....$Cggg.....0..lF.+p....(Q.....S....."S.)YQ5.....U.wl...>.K....T[[...o....jb.:a.....A....8-.....,...FB....o. .l...o...8p...../1..sPE....q[f.O^.....>U.T....H..Ca.../t.t.o...S..'...8Q ...a@.o0<...@..Rn..?>..1..x.F....C.=....!._.....1.....LUT.#..j8..I....>{M.....|K}}.{xB'.V.p~..y...d..M.....p>..]...zta.x..V.!#%.7"UKM.j.....n_@.....H..#.....~../?...{8..T.w.". OBJ....r...9.U(fp.-....e.Q..E.....;h.:...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\openx[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	70
Entropy (8bit):	3.577769619550495
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\openx[1].gif	
SSDEEP:	3:CUul/Re/FemxhkYltxlzeze:E07ize
MD5:	58A7930CD4577FC33C35828C271EAB8F
SHA1:	406E57F86DC101E10F3A57BE1E2F7B93C4580474
SHA-256:	8D70B3E6BADB6973663B398D297BB32EAEDD08826A1AF98D0A1CFCE5324FFCE0
SHA-512:	F7A5F748F4C0D3096A3CA972886FE9A9DFF5DCE7792779EC6FFC42FA880B3815E2E4C3BDEA452352F3844B81864C9BFB7861F66AC961CFA66CB9CB4FEBE5688
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!..NETSCAPE2.0.....!.....,.....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\placeHolder[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 350 x 350, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	23999
Entropy (8bit):	7.97611219512239
Encrypted:	false
SSDEEP:	384:vzygszDch26IMhpExEipWpIDWW0bUbHgKXma2M3acwpOov5FeJk6rL+Co3N+gJbp:vzygs5cpIDPXmS3cOQeJkyXo3ICx
MD5:	F44F469E45876F0B6A017C2F58A053F2
SHA1:	DDD9FC1E6C62D4BFC7BD93BF306E6FF6821EF3A0
SHA-256:	76102878C1198DE858725194952BA1C6B35BDEE0F870CC6A124E93D17385E64E
SHA-512:	DF4DB61AEFE925CE7A3F4466B449E0A13A3358A0835D35277CE8E1F9B1B18540568E4685ECCF70C99CB6A15CF6A1CBBBA31CE36F9DBF3BC315E97A8576A7354E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://live.sekindo.com/content/video/splayer/assets/placeHolder.png
Preview:	.PNG.....IHDR...^...^.....+w.....tEXtSoftware.Adobe ImageReadyq.e<..]aIDATx....dWy.[...hF..t.S...$B....y.....K..1&1.a]..o.l...8<L..r....v...v._cC.E.xc..@G."..3...G=....^s.....O[.T..:u...^U]].s.....c....[.....Q-V...333...c,1==.....p....p.M...m2..Me.7g.S[...9X.....l.>...3.....s.c..6.....Y.....p....V.\..#-...61..!....,...x\.bE....+.{.1...chK....G[.kK.m{.G....?|.1.~2.....g....=.....:V.v}hO...g.y.r.5+V.^.Z.jUK.4.VDZ. _}_?...wC .>..C..s.Zz<{,,.}.....=.=.....1(\....=;.g....[.v..d[.\r...6.....44.u.....'._.....>].N..^.]..... ..@..d.\z.-.6<_")4.P.3.}...^;.....H..o9}.4d.M...})./..7-..;....w'..\....0...n7n.x.u.H.&..#.....'.....>..i..@..dN.....^...6.j...-.8i....i..SK.....6.O.v{F..'^'.Q.1..C..2...Ys%[g.&.'.j...D .v..Y..>.._....9.:....}qh.A..$.i..Kd..C.Q.....'x.....Yh..Z.Av8.:.6..gd.ch..h.o.....(...C....q1.._C./.....oM...-.n ..7o^"[?.k.8....;....ok-{L8.x.x..Bm

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\polyfills.78d11e15[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	47894
Entropy (8bit):	5.272665851348083
Encrypted:	false
SSDEEP:	768:zj1lQh/eA43auGkR+5sPLngJEG+A1KEQBfeVoVEsmiGrv4:VlQX++5k7gJ3b1tQBfeyVEyGj4
MD5:	2DC41A564D5B69185F0DF8D7A7727DB7
SHA1:	230568855C28EB48306244DAB9DCB97E90D479FB
SHA-256:	BEB8196C90EC0E1775ABE8AC52860D9B76755035166B128ADD385EB81ACA6B58
SHA-512:	90B6FA9CB9CC7ABCB30DB484628C2FF1A64A362DC9FE5E52556C38907954C3E3FAFC2B04139046CE4F87158BABA157766B09672D991F99CF0FD8AA76ACB45D9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://abs.twimg.com/responsive-web/client-web-legacy/polyfills.78d11e15.js
Preview:	window.__SCRIPTS_LOADED__.runtime&&((window.webpackJsonp=window.webpackJsonp||[]).push([[283],{"+kY7":function(t,e,n){var r=n("q9+l").f,o=n("8aeu"),i=n("fVMg")("toStringTag");t.exports=function(t,e,n){t&&!o(t=n?t:t.prototype,i)&&r(t,i,{configurable:!0,value:e})}},"/4m8":function(t,e,n){"use strict";var r,o,i,c=n("DjlN"),u=n("WxKw"),a=n("8aeu"),f=n("fVMg"),s=n("DpO5"),l=f("iterator"),p=!1;[].keys&&("next"in(i=[].keys())?(o=c(c(i)))!==Object.prototype&&(r=o):p=!0),null==r&&(r={}),s||a(r,l)||u(r,l,(function(){return this})),t.exports={IteratorPrototype:r,BUGGY_SAFARI_ITERATORS:p}},"0FSu":function(t,e,n){var r=n("lRf+"),o=n("g6a+"),i=n("N9G2"),c=n("tJVe"),u=n("aoZ+"),a=[].push,f=function(t){var e=1==t,n=2==t,f=3==t,s=4==t,l=6==t,p=5==t||l;return function(h,v,d,y){for(var g,m,b=i(h),w=o(b),x=r(v,d,3),O=c(w.length),_=0,j=y||u,S=e?j(h,O):n?j(h,0):void 0;O>_;_++)if((p||_ in w)&&(m=x(g=w[_],_,b),t))if(e)S[_]=m;else if(m)switch(t){case 3:return!0;case 5:return g;case 6:return _;case 2:a.call(S,g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\prebidVid.3.19.0_10.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	309454
Entropy (8bit):	5.3672905890657665
Encrypted:	false
SSDEEP:	3072:3rWwvxyY7ARdHnELT3w4oEA2cAMMw1FE7QqWWWtflWn47li6wx2TO0fyd:Jxjs/SUEhI/EQflWKI162y0f0
MD5:	0DFB6D5A5670264C233DFEEED920283D
SHA1:	F1630906AF735463CAA83B5F95572A4B77427E1C
SHA-256:	C1A7ABF4985379F74AF7244DB4954A0305C8F73C2F64F4F80A09D86DC3AE9596

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\prebidVid.3.19.0_10.min[1].js	
SHA-512:	98C46D0F825CC56F6635DF3B55C5AF0B470252C9D40383E5A68357094A4A1EC92B5027AC254EBC4E8886A5CF79D481ADDD0B2DF0E422A044C1CAF528BCBB3E B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://live.sekindo.com/content/prebid/prebidVid.3.19.0_10.min.js
Preview:	/* prebid.js v3.19.0.Updated : 2020-09-13 */.!function(u){var s=window.SKpbjsChunk;window.SKpbjsChunk=function(e,t,r){for(var n,o,i,a=0,c=[];a<e.length;a++)o=e[a],d[o]&&c.push(d[o][0]),d[o]=0;for(n in t)Object.prototype.hasOwnProperty.call(t,n)&&(u[n]=t[n]);for(s&&s(e,t,r);c.length;)c.shift()();if(r)for(a=0;a<r.length;a++)i=f(f.s=r[a]);re turn i};var r={},d={305:0};function f(e){if(r[e])return r[e].exports;var t=r[e]={i:e,l:!1,exports:{}};return u[e].call(t.exports,t,t.exports,f),t.l=!0,t.exports}f.m=u,f.c=r,f.d=function(e,t,r) {f.o(e,t)||Object.defineProperty(e,t,{configurable:!1,enumerable:!0,get:r})},f.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};return f.d(t, "a",t),t},f.o=function(e,t){return Object.prototype.hasOwnProperty.call(e,t)},f.p="",f.oe=function(e){throw console.error(e),e},f(f.s=815)}([function(e,t,r){"use strict";Object.def ineProperty(t,"__esModule",{value:!0}),r.d(t,"internal",function(){return k}),r.d(t,"bind",function(){return N

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\primisslate[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	17864
Entropy (8bit):	4.912183002285288
Encrypted:	false
SSDEEP:	192:QnbtHDnzpr8XrYDxM66lZL6GP/LYFB8Rz+D43lryl5N8j4Ywzxe2fXHoja7GNIcg:8HzMrYDxM66DsD43RmXbcfY
MD5:	AE75067760956DE94B97B90B253712FE
SHA1:	B2372CD932B7513BA538D078BF062EAF6BC50335
SHA-256:	4F7CD55655BAFCA4DB9B67255125ED52CD91D21B1727E9F28F71219AA1341DE5
SHA-512:	2200CEE7FC194FC7D8281ADAD5E298166AC04F6C9999086B65F6D77152B07AC7AE4528071AA47552066273C7B49294C69CD329CBA9FE70BE3CF85302C67EE20
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://live.sekindo.com/content/video/css/primisslate.css
Preview:	/*!.* primisslate.* github.com/premasagar/primisslate.*.*//*. An extreme CSS reset stylesheet, for normalising the styling of a container element and its children... by Premasagar Rose. dharmafly.com.. license. opensource.org/licenses/mit-license.php.. **.. v0.10.1..*/.. /* == BLANKET RESET RULES == */.. /* HTML 4.01 */..primisslate, .primisslate h1, .primisslate h2, .primisslate h3, .primisslate h4, .primisslate h5, .primisslate h6, .primisslate p, .primisslate td, .primisslate dl, .primisslate tr, .primisslate dt, .primisslate ol, .primisslate form, .primisslate select, .primisslate option, .primisslate pre, .primisslate div, .primisslate table, .primisslate th, .primisslate tbody, .primisslate tfoot, .primisslate caption, .primisslate thead, .primisslate ul, .primisslate li, .primisslate address, .primisslate blockquote, .primisslate dd, .primisslate fieldset, .primisslate li, .primisslate iframe, .primisslate strong, .primisslate legend, .primi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\red_x[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4692
Entropy (8bit):	7.929034471918412
Encrypted:	false
SSDEEP:	96:Sn/2mON/mv8Z7QuHy9TZhjR0ZmegAmURrkxeDlOyMX:SnO8i7QhVTvUbDlq
MD5:	5F3C13A459A72438E42B2289C7AF2034
SHA1:	F43551BE102CD1EB0B2E87DC24F980720194A56B
SHA-256:	A7A63CA1370CD6FC3470FA81BB1DCB21BCE31B0048A36E5BCE8914EEB88DAAB1
SHA-512:	14E82E281DC91ED57EAB780279D167413185DB3FA7BE49FBDB4942888E7F4E30B1A0536B269258FB8C3975BCF2BC189B51AAC4F70BF44887BC17506DF6ECB50 7
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/red_x.png
Preview:	.PNG.....IHDR...0...0.....W.....IDATx^.Y.tTe....RK.....D..6.....(.*G..d;c..8.`.....3.....2"Qq.g@.0.aK.I.V.R{.en..?.N<8.8...%.{.....+....^.j<...$..('.....F..'.....7...7._A:..... ..6...0X^^.V2jTV^^.....+L<.w...Q]]]...G....}kk.....N..V.....4.....3gfO.<.P..Xw7.g."x.4.jk...G.....UQ...1p.8%/..`.9r.....kok...x.....I~:.o.Y\.....V..4....o.....P.f..m..T.....c."-';...6 t...O=...c...h.M.,((.w...._q..'..G..._.....7.>u..h{.....8z.i..H.6.zO...].}.0.!X..L].....=`.0M..3.D.Q._s.*(.U\IVWW7n.=..D....r..$....,]Z.....UUp....4D...z{;.....7T..Z0M.2.q....t)..a.....{. ...g?./..o...s..)b... .U...../Y2...._z....G.B.....B..$i..L..#..,..+ s...A.bX.`@7.)"@.'M.G.EzQ..u....kj..>"l.#?a.E./..b..7m.UWB!.?.....$*..I..0. m).8'..P..h..k@...]..C..{.*L..qm9...W_.yX .....@.Kh..7/^<..Q.~=..N...;..D4ZD%i...B....0O.f.....ua1a5(.....~..>. .#.i.&.|.(....H~.'...pE..Ekx.Yd^r.b'O"~..RHDe..P...n... ....%lA.....a.b..F.i.X..a.....i,....f.q...7=.`[..l.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\runner[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	12318
Entropy (8bit):	5.314366444111888
Encrypted:	false
SSDEEP:	192:I7UTGaZMNZU5mFCD+hgnFGzb90VzsiKvWJ9jky688:y4AFcZn8F0VzseJd8
MD5:	689EC0B5962F97BB6F4B9EDDC7247179
SHA1:	B8AEE6499B776B9E5133F184B4B8F5453592984D
SHA-256:	15A6E70E27BBE74B154C0A5281BE1774D648BEC1B24F18E92FD072F0BC51E55B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\runner[1].htm	
SHA-512:	DEFA96B7A645F7073AE3EE88B6CC5C92DDBC73A59DFA2E11AEE2CF27D4CF77A8D3A6D21A466ED5C03D5B537821B8ECA573FEFBDEFB0FE6A045A1A0087A8EC768
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/sodar/sodar2/219/runner.html
Preview:	<!DOCTYPE html>.<meta charset=utf-8><script>.(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.'use strict';function m(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}function p(a){var b="undefined"!=typeof t.Symbol&&u(t.Symbol,"iterator")&&a[u(t.Symbol,"iterator")];return b?b.call(a):{next:m(a)}}var aa="function"==typeof Object.create?Object.create:function(a){function b(){}b.prototype=a;return new b},v="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,d){if(a==Array.prototype||a==Object.prototype)return a;a[b]=d.value;return a};.function ba(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var d=a[b];if(d&&d.Math==Math)return d}throw Error("Cannot find global object");}var w=ba(this),x="function"===typeof Symbol&&"symbol"===typeof Symbol("x"),t={},y={};function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sd[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	2.9889835948335506
Encrypted:	false
SSDEEP:	3:CUkxl7/lHh/:slf/
MD5:	B4491705564909DA7F9EAF749DBBFBB1
SHA1:	279315D507855C6A4351E1E2C2F39DD9CD2FCCD8
SHA-256:	4E0705327480AD2323CB03D9C450FFCAE4A98BF3A5382FA0C7882145ED620E49
SHA-512:	B8D82D64EC656C63570B82215564929ADAD167E61643FD72283B94F3E448EF8AB0AD42202F3537A0DA89960BBDC69498608FC6EC89502C6C338B6226C8BF5E14
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\state[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	30
Entropy (8bit):	3.764735178725505
Encrypted:	false
SSDEEP:	3:ADKLMRsXhUe:AMMRG
MD5:	8FABFD3BB9B067B11AD664181B30FA66
SHA1:	0F93D4D0300C0C736A8C18DBD91ECCDB4DBEBD4B
SHA-256:	B97BAB9BF4FCA8D386EF5FC83CD58B492F2132E2D28053ADE2F212A8B151B0C4
SHA-512:	D5DFC67915A2ED567667FCF04BC807A3771F4938198CC7297FE9E37B5550AB57B7386017A6E9A6DA56DB68CE92B2876BE2514525B6E0B8C94DA53F4EB584758
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://consentcdn.cookiebot.com/consentconfig/21a90315-060b-44e5-9a12-6df9da9c40f8/state.js
Preview:	CookieConsent.latestVersion=1;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\style.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	53907
Entropy (8bit):	4.940786840491388
Encrypted:	false
SSDEEP:	384:F5Tku7HBZDO/KRUEqXMXRLrO+AwlVHI+vg7LKclyvNSX2GVX5Ttfr:0RXMXRLrO+AwlxI+vg7LKNcF5Bfr
MD5:	2E7E1D1C1D4D446A1B6B63295757D859
SHA1:	27A1D9DCBDC4AFF486016B5C9F3ECE6AD0C028C1
SHA-256:	8C626F0F9B5C109539B256B73E72C02B300A184F46B4535C2EB86599215C78AF
SHA-512:	7526B0ADCE5C1751D3E55BA5077C4BB5F334FAE6A73CB519E2BE07AA602ED25C307A8462AF380DA0550F56AE29C871A663F9A01E523462DFB9A378E8F26888A3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c0.wp.com/c/5.5.3/wp-includes/css/dist/block-library/style.min.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\style.min[1].css	
Preview:	:root{--wp-admin-theme-color:#007cba;--wp-admin-theme-color-darker-10:#006ba1;--wp-admin-theme-color-darker-20:#005a87}#start-resizable-editor-section{display:none}.wp-block-audio figcaption{margin-top:.5em;margin-bottom:1em}.wp-block-audio audio{width:100%;min-width:300px}.wp-block-button__link{color:#fff;background-color:#32373c;border:none;border-radius:28px;box-shadow:none;cursor:pointer;display:inline-block;font-size:18px;padding:12px 24px;text-align:center;text-decoration:none;overflow-wrap:break-word}.wp-block-button__link:active,.wp-block-button__link:focus,.wp-block-button__link:hover,.wp-block-button__link:visited{color:#fff}.wp-block-button__link.aligncenter{text-align:center}.wp-block-button__link.alignright{text-align:right}.wp-block-button.is-style-squared,.wp-block-button__link.wp-block-button.is-style-squared{border-radius:0}.wp-block-button.no-border-radius,.wp-block-button__link.no-border-radius{border-radius:0!important}.is-style-outline .wp-block-button__link,.wp-bl

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\stylesheet[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	7903
Entropy (8bit):	4.832084717773727
Encrypted:	false
SSDEEP:	192:oHI4c2BEhs4asitnQVaE7rY8zdUIYXPnyYwVzwt5wkAwNPxxVWyITW6btQD0ReHg:Ho240q2D9tr
MD5:	3393B3AB29229EC4E39CF7FAC895EC69
SHA1:	78FB8EB5BA7069AC97A8FE91775DCDD3B5BE50C7
SHA-256:	FA46821BA001DB4BEFE90ADAEED1C68E868EA952C8417C7BEDB876E4B4190AA6
SHA-512:	27AFC627C3CEBD8CB445B5924E2E890D04611800B6EF65A9F9F9308E75A0CAC22A8F3B2A45C0E6C247522AAE5B3AF9EFB0343E557120D726AA359659CDAD883 4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://itsfoss.com/wp-content/plugins/searchiq/assets/3.5/css/frontend/stylesheet.css?ver=1605999323
Preview:	#menu-item-siq-selectbox,.siq-icon-item-siq-selectbox{position:relative!important;width:40px!important;height:46px;left:auto;right:auto}.siq-icon-item-siq-selectbox{height:auto;clear:both}#menu-item-siq-selectbox.moveToExtremeRight{position:absolute!important;right:0;height:auto;left:auto}.siq-icon-item-siq-selectbox.moveToExtremeRight{float:right;height:46px}.siq-icon-item-siq-selectbox.moveToExtremeRight .siq-icon-searchbox-wrap{position:absolute;right:0}#menu-item-siq-selectbox a,.siq-icon-item-siq-selectbox a{outline:none}#siq-menu-searchbox-wrap{position:absolute;right:0;z-index:9}.siq-icon-item-siq-selectbox .siq-icon-searchbox-wrap{}#siq-menu-searchbox-wrap.siq-search-open,.siq-icon-item-siq-selectbox .siq-icon-searchbox-wrap.siq-search-open{width:300px}#siq-menu-searchbox-wrap #siq-expsearch-cont{}#siq-menu-searchbox-wrap #siq-expsearch-cont .siq-expsearch,.siq-icon-searchbox-wrap .siq-expsearch-cont .siq-expsearch{position:relative;min-width:50px;width:50px;height:46px;float:r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\t1h9m7[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	2.7374910194847146
Encrypted:	false
SSDEEP:	3:CUnl/7yltxlHh/:/+/
MD5:	07FFF40B5DD495ACA2AC4E1C3FBC60AA
SHA1:	E8AC224BA9EE97E87670ED6F3A2F0128B7AF9FE4
SHA-256:	A065920DF8CC4016D67C3A464BE90099C9D28FFE7C9E6EE3A18F257EFC58CBD7
SHA-512:	49B8DAF1F5BA868BC8C6B224C787A75025CA36513EF8633D1D8F34E48EE0B578F466FCC104A7BED553404DDC5F9FAFF3FEF5F894B31CD57F32245E550FAD65 A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://track.mailerlite.com/webforms/o/2516912/t1h9m7?v1597657573
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\uc[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	72833
Entropy (8bit):	5.195088836600577
Encrypted:	false
SSDEEP:	1536:IzuFfSDfTBgSqdCInODofztv/smLaYr5Lo7d8M3ufl7mqRj+3:efTpcdVGPufl7mqR63
MD5:	316DB25309CEA526D38998E3BA95D08E
SHA1:	4DC376DFA9E459DBF3004D66504D80BD582298C9
SHA-256:	8E0D2AB4F0A4A7E5A6C1755ABF9D48AC795A9AB41C35802BBDA956E4338FF50F
SHA-512:	5FAF29FFFE920BEC21E60EDB68FEC89503CFC471719965F7F5903D309756600D3A3D87C323E9FCA1273618CE3450C7CC06976FB7F27AAAF7DB15B6DD702585E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://consent.cookiebot.com/uc.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\uc[1].js	
Preview:	function __uspapi(e,t,o){var n=null,i=!0,s=!0;CookieConsent&&""!=CookieConsent.userCountry&&-1==CookieConsent.regulationRegions.ccpa.indexOf(CookieConsent.userCountry.toLowerCase())&&(s=!1),1==t&&"getUSPData"==e?n=s?(s=1..toString(),s+="Y",CookieConsent&&CookieConsent.hasResponse?CookieConsent.consent.marketing?s+="N":s+="Y":CookieConsent&&!CookieConsent.hasResponse?s+="N":s+="Y",{version:1,uspString:s+="Y"}):{version:1,uspString:1..toString()+"---"}:i=!1,o&&o(n,i)}function addUspapiLocatorFrame(){var e;window.frames.__uspapiLocator||(document.body?((e=document.createElement("iframe")).style.cssText="display:none;position:absolute;width:1px;height:1px;top:-9999px;",e.name="__uspapiLocator",e.tabIndex=-1,e.setAttribute("role","presentation"),e.setAttribute("aria-hidden","true"),e.setAttribute("title","Blank"),document.body.appendChild(e)):setTimeout(addUspapiLocatorFrame,5))}function __handleUspapiMessage(o){var n=o&&o.data&&o.data.__uspapiCall;n&&"function"==typeof window.__uspapi&&win

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\user_sync[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	8056
Entropy (8bit):	5.471697420871033
Encrypted:	false
SSDEEP:	96:mYtUQ3cA1ynMRkPpcZpNb5UcTCZpdRFu+Zuj6ZuwBLGKaKnIes2gYAGn2hCV79kT:mYtUQhynWk1cIrIc/KCV7ykHbSP
MD5:	3C021FDA9B9CA38FE0925363556460BE
SHA1:	59C717D8DAAA5400650B500688D88B146EE130D6
SHA-256:	23371B5319A53A0A2D3C59D738D679C384822C244EA4E791EF87A4110B8A291E
SHA-512:	72D76C61C1B300641C5A189BF733000B199BF9433B8C03297B2A825358923369F87EB441C415DB2C4A337CD5F13359278800E6CEE504EB97F31DD1B8D4188582
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ads.pubmatic.com/AdServer/js/user_sync.html?p=156578&predirect=
Preview:	<html><body><script type="text/javascript">(function(){var n={},h,e=location.href.slice(location.href.indexOf("?")+1).split("&"),y,z=e.length,o="https://ads.pubmatic.com/AdServer/js/showad.js#PIX&kdntuid=1&SPug=true";var g=window,a=function(i){return typeof i==="function"},C=console.log.bind(console,"PubMatic:"),s=function(K,J){var H=0,G=K.length,I=false;for(;H<G;H++){if(K[H]===J){I=true;break}}return I},u=function(){return"https:"},d=function(G){var H="";for(var i in G){if(G.hasOwnProperty(i)){H+=i+"="+encodeURIComponent(G[i])+"&"}}return H},w=function(G){var i=g.document.createElement("iframe");i.src=G;i.style.height="0px";i.style.width="0px";i.style.display="none";i.height=0;i.width=0;i.border="0px";i.hspace="0";i.vspace="0";i.marginWidth="0";i.marginHeight="0";i.style.border="0";i.scrolling="no";i.frameBorder="0";g.document.getElementsByTagName("script")[0].parentNode.appendChild(i)},p=function(i,I){var H=document.createElement("script");H.type="text/javascript";H.src=i;if(a(I)){H.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\vendors~main.68b1d365[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with LF, NEL line terminators
Category:	downloaded
Size (bytes):	439928
Entropy (8bit):	5.4559761027348594
Encrypted:	false
SSDEEP:	6144:YF0cmyU3pwv3O1LQfEAeUSo/YzArrWBV6S:Yo5M3O1LQfluzjb
MD5:	EDBCCAA9067E2FA872B6E7206CA16AFB
SHA1:	DDAB4AFF563BB455A9D0D07186451703A1547377
SHA-256:	45E82FB2AA89EFECBF43E1401B0C6208BF32D35E6CFE94B421B964AA361599E2
SHA-512:	BCB9B81029574BA3872E5623754E6A0FC1A7C4C5B6A7A9711C4FF613CABFF98A777D060377664A98F910DEC8B559433CA6FF7B8C20AF6448AA148F10C30578F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://abs.twimg.com/responsive-web/client-web-legacy/vendors~main.68b1d365.js
Preview:	window.__SCRIPTS_LOADED__.polyfills&&((window.webpackJsonp=window.webpackJsonp||[]).push([[2],{"+/1j":function(e,t,n){"use strict";var r=n("ERkP"),u=n("k/Ka"),o=n("9MNk"),i=n("QAqE"),a=n("Nw+a"),c=n("Nfwf"),l=n("r3Qg"),s=n("CYzn"),f=n("vlSS"),d=n("zCvs"),p={accessibilityLabel:!0,accessibilityLiveRegion:!0,accessibilityRole:!0,accessibilityState:!0,accessibilityValue:!0,accessible:!0,children:!0,classList:!0,dir:!0,importantForAccessibility:!0,lang:!0,nativeID:!0,onBlur:!0,onClick:!0,onClickCapture:!0,onContextMenu:!0,onFocus:!0,onKeyDown:!0,onKeyUp:!0,onTouchCancel:!0,onTouchCancelCapture:!0,onTouchEnd:!0,onTouchEndCapture:!0,onTouchMove:!0,onTouchMoveCapture:!0,onTouchStart:!0,onTouchStartCapture:!0,pointerEvents:!0,ref:!0,style:!0,testID:!0,dataSet:!0,onMouseDown:!0,onMouseEnter:!0,onMouseLeave:!0,onMouseMove:!0,onMouseOver:!0,onMouseOut:!0,onMouseUp:!0,onScroll:!0,onWheel:!0,href:!0,rel:!0,target:!0},h=Object(r.forwardRef)((function(e,t){var n=e.dir,o=e.numberOfLines,f=e.onClick,h=e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\vid5c7ea78307296482649144[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	"Lavc58.47.100", baseline, precision 8, 640x360, frames 3
Category:	downloaded
Size (bytes):	13103
Entropy (8bit):	7.63044585743299
Encrypted:	false
SSDEEP:	192:SsSTrbm6ynHQIZoPA+sRofAMrjWuMxpMNbykLjK4fDTIwUsVb2QpHdGZ+b:SsB284IRorjWdxpMNb/jPfT7V6QXGZW
MD5:	12F918DDCB869C5DC0B7D527F1ADB754
SHA1:	497A392FB9EE392B7EED60E0FDFBC074AFFB71D3
SHA-256:	DED5D4E74DD4EAB04E868C9A58E64DB54100BBBF0204D5D54AE0C6807E2585FF
SHA-512:	03EF4072D931B73CCA57BCDA63DD7908B8C22D68A716503B3D4477FFB64DDD58BE090E8DE7199A6335B3BADF29B8F40050FDF55FE9CBE0B0927DD443864C531
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\vid5c7ea78307296482649144[1].jpg	
Reputation:	low
IE Cache URL:	http://https://video.sekindo.com/uploads/cn10/video/users/converted/25204/video_5b5845c36cf6d068557072/vid5c7ea78307296482649144.jpg?cbuster=1591786229
Preview:	......JFIF.....Lavc58.47.100....C..... . !!! !!!$$$***$$$!!$$((**./.++*+//222<<99FFHVVg.....1.!R.4ArQ.q.a.."3.2..S. ...CBbc..#...s$5..%.....!...1AR"aqQ23.B.4#..C.r.S.b.....h...."...?..... .....I..w....c.n...^....k.F@.yv.....G..Dd.7.n...^.r....K..~.F@.yv.....G..Dd.7.n...^.r....K..~.F@.yv.....G..Dd.7.n...^.r....K..~.F@.yv.....G. .Dd.7.n...^.r....K..~.F@.yv.....G..Dd.7.n...^.r....K..~.F@.yv.....G..Dd.7.n...^.r....K..~.F@.yv.....G..Dd.7.n...^.r....K..~.F@.yv..... ...G..Dd.7.n...^.r....K..~.F@.yv.....G..Dd.7.n...^.r....K..~.F@.yv.....G..Dd.7.n...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\vid5c91ee7d09143568428664[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	"Lavc58.47.100", baseline, precision 8, 640x360, frames 3
Category:	downloaded
Size (bytes):	11201
Entropy (8bit):	7.744169145349814
Encrypted:	false
SSDEEP:	192:ffgED5KeSQ1k80q5QXXvzD5JVazN8wBu4olBmMPtwfECyJegWfMXx1NLUe0rV:ff3DfRk8J5wztJVazNxBGnmzfkJtnXF0
MD5:	E7243CA7E80E37A3506F8A7E84D3A1C5
SHA1:	6E39D0E717597D415C3F4CF8FCD33EBD22179CB7
SHA-256:	A1FA081EAC1D0B14B60BDFAB8C62EA6DF208202B6ADD5A548ADF8801D8ADA5C1
SHA-512:	083838110D3BE178E03000D104FC00E3E45185636E6CE2E975166A671E392682041EC5AE76815046D2F9A14A58078615EB5EBB0BB516EF4D4E3B337A0BEF2B2F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://video.sekindo.com/uploads/cn19/video/users/converted/25204/video_5b5845c36cf6d068557072/vid5c91ee7d09143568428664.jpg?cbuster=1591786229
Preview:	......JFIF.....Lavc58.47.100....C..... . !!! !!!$$$***$$$!!$$((**./.++*+//222<<99FFHVVg.....!.1.a.Q....qAU.Tr...2..."5 s.4...S.36R.#.Bb.c..E..D.....a..Q..!..R1qA.2.B".....h...."...?..... .....R....n..L....)s.R..&....R....*M3.L....9K.T.g..79K.r.0.4.-0nr.0..aRi.Z`...a.\..8....\...I.qi.s...)s..L....)s.R..&....R....*M3.L....9K.T.g..79K.r.0.4.-0nr.0..aRi.Z`...a.\..8....\.. 0.4.- or.0..aRi.A..]h9K..I.....)s.R.ARi.A..]h9K..I.....)u.....&.[KD.....T.ym-.or.Z.R.ARi.A..]h9K..I.....)s..\..8....\...I.qi.s...)s..L....)s.R..&....R....*M3.L.o...)s..L.-@m.0..aRi.....R ....*M3.....\...I.v..6.K.r.0.4.....)s.R..&..Z....a.\..;KP.|..9K.T.gij.o...)s..L.-@m.0..aRi.....R....*M3.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\vid5c93817e6f424092606247[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	"Lavc58.47.100", baseline, precision 8, 640x360, frames 3
Category:	downloaded
Size (bytes):	11201
Entropy (8bit):	7.744169145349814
Encrypted:	false
SSDEEP:	192:ffgED5KeSQ1k80q5QXXvzD5JVazN8wBu4olBmMPtwfECyJegWfMXx1NLUe0rV:ff3DfRk8J5wztJVazNxBGnmzfkJtnXF0
MD5:	E7243CA7E80E37A3506F8A7E84D3A1C5
SHA1:	6E39D0E717597D415C3F4CF8FCD33EBD22179CB7
SHA-256:	A1FA081EAC1D0B14B60BDFAB8C62EA6DF208202B6ADD5A548ADF8801D8ADA5C1
SHA-512:	083838110D3BE178E03000D104FC00E3E45185636E6CE2E975166A671E392682041EC5AE76815046D2F9A14A58078615EB5EBB0BB516EF4D4E3B337A0BEF2B2F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://video.sekindo.com/uploads/cn22/video/users/converted/25204/video_5b5845c36cf6d068557072/vid5c93817e6f424092606247.jpg?cbuster=1591786229
Preview:	......JFIF.....Lavc58.47.100....C..... . !!! !!!$$$***$$$!!$$((**./.++*+//222<<99FFHVVg.....!.1.a.Q....qAU.Tr...2..."5 s.4...S.36R.#.Bb.c..E..D.....a..Q..!..R1qA.2.B".....h...."...?..... .....R....n..L....)s.R..&....R....*M3.L....9K.T.g..79K.r.0.4.-0nr.0..aRi.Z`...a.\..8....\...I.qi.s...)s..L....)s.R..&....R....*M3.L....9K.T.g..79K.r.0.4.-0nr.0..aRi.Z`...a.\..8....\.. 0.4.- or.0..aRi.A..]h9K..I.....)s.R.ARi.A..]h9K..I.....)u.....&.[KD.....T.ym-.or.Z.R.ARi.A..]h9K..I.....)s..\..8....\...I.qi.s...)s..L....)s.R..&....R....*M3.L.o...)s..L.-@m.0..aRi.....R ....*M3.....\...I.v..6.K.r.0.4.....)s.R..&..Z....a.\..;KP.|..9K.T.gij.o...)s..L.-@m.0..aRi.....R....*M3.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\vid5caf37df7a6ec897857758[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	"Lavc58.47.100", baseline, precision 8, 640x360, frames 3
Category:	downloaded
Size (bytes):	8482
Entropy (8bit):	7.1222394764524
Encrypted:	false
SSDEEP:	192:bB+BYHULvj6OZ6u7kGFz4gTkQO3dnPQ9X:Um0L76OLkGFnkQCdno9X
MD5:	3088D498A98E03E5D1574276FA9D8EFD
SHA1:	F6E18E0DDDC4072CBFBC1903C4CC83F857EF99D7
SHA-256:	60F7072277F66EB0CECED773BE07468FDAC1CEBA0106CC1244956933ADAB0EED
SHA-512:	79DB53C79AA0A26F34F55EF9D80DF72096C94280C45BC05F21C7AD3B7F201557E74A7E42E0005C766AE529F5AED303FC385BE4658F994A8B504A1CA8263C641
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://video.sekindo.com/uploads/cn19/video/users/converted/25204/video_5b5845c36cf6d068557072/vid5caf37df7a6ec897857758.jpg?cbuster=1591786229

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\vid5caf37df7a6ec897857758[1].jpg	
Preview:	......JFIF.....Lavc58.47.100....C..... . !!! !!!$$$***$$$!!$$((**./.++*+//222<<99FFHVVg.....!1.rQA..aR.qs...42"5..B.3T. .#b.c....S...%$C...d.....ba!RQ2B.Aq".....h....".....?.....U&..J^%..>ru..oR.xn;...p.....O.<..8...q..lm9.Mo.^.H.7.'^.....'...`nk9T..Q.MI... <_y...S.lfe.8J/.5.tr..\....e^..T.&...../.....h.....(.,.]>#L{.<....8%.....8.X6...]?.F-8.....y}....&..Mb_.....M(.9._...K..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\webcomponents-lite-noPatch[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	123591
Entropy (8bit):	5.416605148511316
Encrypted:	false
SSDEEP:	1536:YDlZVg/ZylWUGuP+dYjOKhjFBNb/Awg+SHYHvB6RExoFPaYK4jJ/n4E41Kj:mt8rjGAz4HsU2b4y
MD5:	01CF271DACDE4B1D5CDB1FF0E4D5D4EF
SHA1:	EC60121EB520C8BBAA460FA468D3E72A222F537E
SHA-256:	8A4CC7E7A47BA745A302AEC5C8A50B3F50FC1145A31D99F6A04C87E6B5E7CDE0
SHA-512:	9CCF7B23049A9880CCB08AC9CF634BDDC5225DE3527B58009655DCE17044C657D7C7EDD068C6A594EDFC043D9ADB5D078AF25E3834C163930DBA670C0AEF2 62
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube.com/s/desktop/a386e432/jsbin/webcomponents-lite-noPatch.vflset/webcomponents-lite-noPatch.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var n;function ba(a){var b=0;return function(){return b<a.length?{done:!1, value:a[b++]}:{done:!0}}}function ca(a){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return b?b.call(a):{next:ba(a)}}function y(a){if(!(a instanc eof Array)){a=ca(a);for(var b,c=[];!(b=a.next()).done;)c.push(b.value);a=c}return a}.function da(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&& window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}var fa=da(this);/*.. Copyright (c) 2016 The Polymer Project Authors. All rights reserved.. This code may only be used under the BSD style license found at http://p olymer.github.io/LICENSE.txt. The complete set of authors may be found at http://polymer.github.io/AUTHORS.txt. The complete set of contributors may b

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\webfont[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	16587
Entropy (8bit):	5.527990125851192
Encrypted:	false
SSDEEP:	384:N1+8TmpUiz+NX+qFObMuhR/bfgN4TV97KW2b4t6FbGl2TAL8Z/VJOT2m:N9Tmpx+h+qFObMuhRzfgN4TVdtQi8VOr
MD5:	593E60AD549E46F8CA9A60755336C7DF
SHA1:	9C030800712C832F2A15040CF02F546884A99808
SHA-256:	CE261EB163FCAEE6953CEDC35059732A133766AB824DC512BBDF9424D48601E4
SHA-512:	7EBCAB12AE8B469723BE43224A1DA8A4AF0CE7B45550501411627467 1A5787E5BEBD7A7D170CE0FCBB283382D4B44CC05E4E0CC0CA9D50A728C32CFF0393A5 C7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/webfont/1.5.18/webfont.js
Preview:	/*. * Copyright 2015 Small Batch, Inc.. *. * Licensed under the Apache License, Version 2.0 (the "License"); you may not. * use this file except in compliance with the Li cense. You may obtain a copy of. * the License at. *. * http://www.apache.org/licenses/LICENSE-2.0. *. * Unless required by applicable law or agreed to in writing, softwa re. * distributed under the License is distributed on an "AS IS" BASIS, WITHOUT. * WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the. * License for the specific language governing permissions and limitations under. * the License.. */* Web Font Loader v1.5.18 - (c) Adobe Systems, Google. License: Apache 2.0 */.;(function(window,document,undefined){function aa(a,b,c){return a.call.apply(a.bind,arguments)}function ba(a,b,c){if(!a)throw Error();if(2<arguments.length) {var d=Array.prototype.slice.call(arguments,2);return function(){var c=Array.prototype.slice.call(arguments);Array.prototype.unshift.apply(c,d);return a.apply(b,c)}}ret

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\wp-auth-check.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1915
Entropy (8bit):	5.0526640641102
Encrypted:	false
SSDEEP:	24:Q77AgH6YVZvpXALmVon10FRuk0M+pJ0cil9N555WpJlkBk5tG4qXhDg5KteFzGzW:Q78CjVZBXAiVCQo6gii755hZ52xD6KJW
MD5:	AA04FC708866D04DBD758E16AC9293C1
SHA1:	737F3DB1D732B2D030A5D8DF87520BA4E832C11C
SHA-256:	3076557D91DB6D6217E358C687C914060B1B08E0C3EC416C39941BACCA8A0898
SHA-512:	E9EBA56C2614749B7C2E1969758A2A3374C8A5FFE585ED0AAD44C89D2A6257613525D26F4CD1B5AE59488CD96EB32034F152BA72447576E13F018F5FD39C191F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c0.wp.com/c/5.5.3/wp-includes/css/wp-auth-check.min.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\wp-auth-check.min[1].css	
Preview:	/*! This file is auto-generated */.#wp-auth-check-wrap.hidden{display:none}#wp-auth-check-wrap #wp-auth-check-bg{position:fixed;top:0;bottom:0;left:0;right:0;background:#000;opacity:.7;z-index:1000010}#wp-auth-check-wrap #wp-auth-check{position:fixed;left:50%;overflow:hidden;top:40px;bottom:20px;max-height:415px;width:380px;margin:0 0 0 -190px;padding:30px 0 0;background-color:#f1f1f1;z-index:1000011;box-shadow:0 3px 6px rgba(0,0,0,.3)}@media screen and (max-width:380px){#wp-auth-check-wrap #wp-auth-check{left:0;width:100%;margin:0}}#wp-auth-check-wrap.fallback #wp-auth-check{max-height:180px;overflow:auto}#wp-auth-check-wrap #wp-auth-check-form{height:100%;position:relative;overflow:auto;-webkit-overflow-scrolling:touch}#wp-auth-check-form.loading:before{content:"";display:block;width:20px;height:20px;position:absolute;left:50%;top:50%;margin:-10px 0 0 -10px;background:url(../images/spinner.gif) no-repeat center;background-size:20px 20px;transform:translateZ(0)}@media print,(-webkit-m

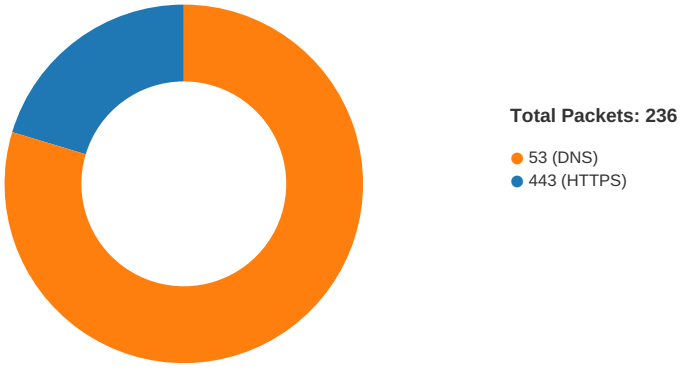
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\HSl8ex4j-oG[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	231
Entropy (8bit):	5.431470415321234
Encrypted:	false
SSDEEP:	6:C3HpTvL4nviLo4dfu6AV9yEwDyCHyEJyEJdyDpVQVHf:wDBfdfuJVQXWCJy6wDpVQJ
MD5:	FD7E886B420B3DB45D6431FC991D8842
SHA1:	A922F1976C93E99F551FDE3447A85432273272F0
SHA-256:	DEBE37C7E68B02B31B47249B674336B63AA71FE8458AD9EDB33A98145DA290EB
SHA-512:	66B24B9AF4F107AAB4D904A08DEF63B893ADD8920612F291B37CF7ACE34ACB12C0402737FD9BAF3E87DB559C937153253783A33BA6F587A34ECBA3DD7C2358AF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.xx.fbcdn.net/rsrc.php/v3/ye/r/HSl8ex4j-oG.js?_nc_x=Ij3Wp8lg5Kz
Preview:	if (self.CavalryLogger) { CavalryLogger.start_js(["GwiMv"]); }..__d("ODS",["ODSWithBanzaiImpl","ODSWithFalcoImpl","gkx"],(function(a,b,c,d,e,f){a=b("gkx")("1836351")?b("ODSWithFalcoImpl"):b("ODSWithBanzaiImpl");e.exports=a}),null);

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 06:12:06.183444023 CET	49717	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.183593988 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.200278044 CET	443	49717	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.200309992 CET	443	49716	104.26.8.105	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 06:12:06.200400114 CET	49717	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.200437069 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.204916954 CET	49717	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.204946995 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.221601963 CET	443	49717	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.221632957 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.224165916 CET	443	49717	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.224256992 CET	443	49717	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.224967003 CET	49717	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.225112915 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.225138903 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.225203037 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.225229025 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.283983946 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.285300970 CET	49717	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.290127993 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.290287018 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.296155930 CET	49717	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.300539970 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.300707102 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.300726891 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.300791979 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.300817013 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.301390886 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.301701069 CET	443	49717	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.302037954 CET	443	49717	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.302057981 CET	443	49717	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.302104950 CET	49717	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.302129984 CET	49717	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.302596092 CET	49717	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.306586981 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.306612015 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.307159901 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.307240963 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.313133955 CET	443	49717	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.313468933 CET	443	49717	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.313534021 CET	49717	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.321584940 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.321611881 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.321629047 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.321646929 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.321708918 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.321723938 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.321746111 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.321753025 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.321780920 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.321856022 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.321904898 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.321927071 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.321943045 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.321959972 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.321970940 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.321976900 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.321983099 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.321997881 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.322017908 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.322026014 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.322035074 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.322043896 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.322051048 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.322165966 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.322392941 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.322467089 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.322468996 CET	49716	443	192.168.2.3	104.26.8.105

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 06:12:06.322531939 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.322575092 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.322597027 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.322627068 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.322638988 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.322643995 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.322659016 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.322663069 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.322678089 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.322680950 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.322699070 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.322699070 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.322721004 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.322765112 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.327292919 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.327318907 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.327368975 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.327392101 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.327413082 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.327435017 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.327452898 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.327464104 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.327471018 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.327471972 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.327491045 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.327505112 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.327514887 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.327527046 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.327533007 CET	443	49716	104.26.8.105	192.168.2.3
Nov 22, 2020 06:12:06.327547073 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.327574968 CET	49716	443	192.168.2.3	104.26.8.105
Nov 22, 2020 06:12:06.327584982 CET	443	49716	104.26.8.105	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 06:12:00.917187929 CET	65110	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:00.944695950 CET	53	65110	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:01.858819008 CET	58361	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:01.886099100 CET	53	58361	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:02.658834934 CET	63492	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:02.686028004 CET	53	63492	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:03.552192926 CET	60831	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:03.579657078 CET	53	60831	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:04.352276087 CET	60100	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:04.379609108 CET	53	60100	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:05.067082882 CET	53195	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:05.104640007 CET	53	53195	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:05.355942965 CET	50141	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:05.391976118 CET	53	50141	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:06.129188061 CET	53023	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:06.170231104 CET	53	53023	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:06.303973913 CET	49563	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:06.331181049 CET	53	49563	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:06.389081955 CET	51352	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:06.399183989 CET	59349	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:06.426244020 CET	53	51352	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:06.426280022 CET	53	59349	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:06.481060028 CET	57084	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:06.516652107 CET	53	57084	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:06.577085972 CET	58823	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:06.596986055 CET	57568	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:06.601452112 CET	50540	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:06.612188101 CET	53	58823	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 06:12:06.620753050 CET	54366	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:06.628361940 CET	53	50540	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:06.632113934 CET	53	57568	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:06.634130955 CET	53034	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:06.647664070 CET	53	54366	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:06.661079884 CET	53	53034	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:06.840351105 CET	57762	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:06.840981007 CET	55435	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:06.841466904 CET	50713	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:06.847115993 CET	56132	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:06.859896898 CET	58987	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:06.867302895 CET	53	57762	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:06.876995087 CET	53	50713	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:06.882385969 CET	53	56132	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:06.884254932 CET	53	55435	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:06.896846056 CET	53	58987	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:06.969696045 CET	56579	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:06.996932030 CET	53	56579	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:07.037676096 CET	60633	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:07.075359106 CET	53	60633	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:07.211818933 CET	61292	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:07.247412920 CET	53	61292	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:08.860379934 CET	63619	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:08.886759996 CET	64938	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:08.887500048 CET	53	63619	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:08.923837900 CET	53	64938	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:08.983109951 CET	61946	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:08.994898081 CET	64910	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:09.021362066 CET	53	61946	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:09.030380964 CET	53	64910	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:09.097843885 CET	52123	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:09.141298056 CET	56130	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:09.148123980 CET	53	52123	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:09.157989979 CET	56338	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:09.185215950 CET	53	56130	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:09.193581104 CET	53	56338	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:09.310430050 CET	59420	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:09.351239920 CET	53	59420	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:09.364732027 CET	58784	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:09.400331974 CET	53	58784	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:09.422523975 CET	63978	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:09.468852997 CET	53	63978	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:09.696050882 CET	62938	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:09.723165989 CET	53	62938	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:09.821326971 CET	55708	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:09.848319054 CET	53	55708	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:10.348678112 CET	56803	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:10.358035088 CET	57145	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:10.384469986 CET	53	56803	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:10.402674913 CET	53	57145	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:10.657289028 CET	55359	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:10.695648909 CET	53	55359	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:10.715389967 CET	58306	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:10.742641926 CET	53	58306	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:10.814120054 CET	64124	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:10.857980013 CET	53	64124	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:11.208477020 CET	49361	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:11.217349052 CET	63150	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:11.231887102 CET	53279	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:11.235769033 CET	53	49361	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:11.240427971 CET	56881	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:11.247555017 CET	53642	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:11.254376888 CET	53	63150	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:11.254833937 CET	55667	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 06:12:11.267374992 CET	53	53279	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:11.274632931 CET	53	53642	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:11.277482033 CET	53	56881	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:11.281833887 CET	53	55667	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:11.426523924 CET	54833	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:11.452760935 CET	62476	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:11.465425968 CET	53	54833	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:11.496635914 CET	53	62476	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:11.854813099 CET	49705	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:11.856966019 CET	61477	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:11.892364025 CET	53	49705	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:11.892605066 CET	53	61477	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:13.210822105 CET	61633	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:13.238115072 CET	53	61633	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:13.484766960 CET	55949	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:13.530416012 CET	53	55949	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:14.395206928 CET	57601	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:14.431018114 CET	53	57601	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:14.502192974 CET	49342	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:14.546222925 CET	53	49342	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:14.839124918 CET	56253	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:14.866734982 CET	53	56253	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:14.966521025 CET	49667	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:14.975447893 CET	55439	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:15.010947943 CET	53	49667	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:15.019546986 CET	53	55439	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:15.535901070 CET	57069	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:15.571515083 CET	53	57069	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:15.585438013 CET	57659	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:15.629432917 CET	53	57659	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:16.078434944 CET	54717	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:16.123420954 CET	53	54717	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:16.155411005 CET	63975	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:16.182430983 CET	53	63975	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:16.244689941 CET	56639	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:16.250194073 CET	51856	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:16.283154964 CET	53	56639	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:16.288022995 CET	53	51856	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:16.365772009 CET	56546	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:16.392872095 CET	53	56546	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:17.251874924 CET	62152	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:17.279043913 CET	53	62152	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:17.659326077 CET	53470	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:17.715848923 CET	53	53470	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:18.276891947 CET	56446	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:18.284344912 CET	59631	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:18.289539099 CET	55515	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:18.301157951 CET	64547	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:18.304846048 CET	51759	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:18.313879013 CET	59207	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:18.316605091 CET	53	56446	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:18.322630882 CET	54269	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:18.324038029 CET	53	59631	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:18.326438904 CET	54856	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:18.327599049 CET	53	55515	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:18.331916094 CET	53	51759	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:18.334166050 CET	64140	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:18.337635040 CET	62271	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:18.341104984 CET	53	59207	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:18.356861115 CET	57404	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:18.358002901 CET	53	54269	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:18.360367060 CET	53	64547	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:18.362129927 CET	62997	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:18.363966942 CET	53	54856	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 06:12:18.373542070 CET	53	64140	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:18.375050068 CET	53	62271	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:18.383774042 CET	53	57404	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:18.397624969 CET	53	62997	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:18.515788078 CET	57712	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:18.533792019 CET	60065	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:18.551419973 CET	53	57712	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:18.581639051 CET	53	60065	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:19.640008926 CET	55068	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:19.677923918 CET	53	55068	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:19.720757961 CET	64700	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:19.726722956 CET	61998	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:19.733285904 CET	53724	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:19.748099089 CET	53	64700	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:19.754164934 CET	53	61998	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:19.764703989 CET	52328	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:19.777168989 CET	53	53724	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:19.804461002 CET	53	52328	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:21.396285057 CET	58051	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:21.423571110 CET	53	58051	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:21.805772066 CET	64130	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:21.832881927 CET	53	64130	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:22.041951895 CET	50491	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:22.085942984 CET	53	50491	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:22.195914984 CET	53004	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:22.223018885 CET	53	53004	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:24.888170004 CET	52529	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:24.909200907 CET	53656	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:24.927825928 CET	53	52529	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:24.932646036 CET	62724	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:24.943927050 CET	56059	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:24.944967985 CET	53	53656	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:24.957751036 CET	63060	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:24.959669113 CET	53	62724	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:24.971118927 CET	53	56059	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:24.996651888 CET	53	63060	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:25.537240982 CET	51498	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:25.545393944 CET	59943	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:25.562064886 CET	50118	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:25.564335108 CET	53	51498	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:25.572412014 CET	53	59943	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:25.579137087 CET	58357	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:25.589045048 CET	53	50118	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:25.591768026 CET	55804	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:25.616000891 CET	53	58357	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:25.618824959 CET	53	55804	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:25.662695885 CET	58079	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:25.666506052 CET	52080	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:25.686574936 CET	55238	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:25.689728022 CET	53	58079	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:25.693528891 CET	53	52080	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:25.713685036 CET	53	55238	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:25.868326902 CET	49289	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:25.916671991 CET	53	49289	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:25.924417973 CET	61034	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:25.937812090 CET	51964	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:25.940541029 CET	58241	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:25.959439039 CET	59571	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:25.961321115 CET	53	61034	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:25.962651014 CET	51708	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:25.967587948 CET	53	58241	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:25.973644018 CET	60709	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:25.974994898 CET	53	51964	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:25.996500969 CET	53	59571	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 06:12:26.005753040 CET	53	51708	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:26.013334036 CET	53	60709	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:26.032418966 CET	63643	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:26.059250116 CET	53	63643	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:26.257164001 CET	62823	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:26.284157991 CET	53	62823	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:26.429636002 CET	63750	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:26.439207077 CET	61959	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:26.443269968 CET	63554	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:26.452785969 CET	57723	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:26.454159021 CET	58663	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:26.458759069 CET	50980	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:26.459785938 CET	50067	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:26.461064100 CET	52992	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:26.469073057 CET	53	63750	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:26.470351934 CET	53	63554	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:26.477459908 CET	55129	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:26.479840040 CET	53	57723	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:26.486720085 CET	53	50067	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:26.488176107 CET	53	61959	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:26.491595030 CET	53	58663	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:26.496150970 CET	53	50980	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:26.507817984 CET	53	52992	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:26.515645027 CET	53	55129	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:26.524844885 CET	60959	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:26.538399935 CET	58319	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:26.566313982 CET	53	60959	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:26.578867912 CET	53	58319	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:26.594142914 CET	64785	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:26.597229004 CET	50208	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:26.617685080 CET	62477	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:26.632822037 CET	53	50208	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:26.637465000 CET	53	64785	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:26.663953066 CET	53	62477	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:26.775423050 CET	54467	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:26.782362938 CET	60548	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:26.790491104 CET	59623	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:26.802341938 CET	53	54467	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:26.809231997 CET	53	60548	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:26.829673052 CET	53	59623	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:26.847923994 CET	51689	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:26.885437965 CET	53	51689	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:26.966417074 CET	64806	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:26.975300074 CET	49686	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:26.993470907 CET	53	64806	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:27.002202988 CET	53	49686	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:28.576905012 CET	56195	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:28.604115963 CET	53	56195	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:31.139811993 CET	62241	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:31.167316914 CET	53	62241	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:35.062856913 CET	50543	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:35.102758884 CET	53	50543	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:35.425415993 CET	56445	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:35.463237047 CET	53	56445	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:35.756087065 CET	56709	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:35.791795015 CET	53	56709	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:36.067682028 CET	50543	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:36.103401899 CET	53	50543	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:36.753952026 CET	56709	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:36.789721966 CET	53	56709	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:37.139489889 CET	50543	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:37.166810036 CET	53	50543	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:37.757925034 CET	56709	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:37.793978930 CET	53	56709	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 06:12:39.580116034 CET	50543	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:39.615925074 CET	53	50543	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:39.762026072 CET	56709	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:39.800081015 CET	53	56709	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:43.582571030 CET	50543	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:43.618515015 CET	53	50543	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:43.766328096 CET	56709	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:43.803136110 CET	53	56709	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:50.097028971 CET	51248	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:50.134308100 CET	53	51248	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:50.301484108 CET	49679	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:50.345416069 CET	53	49679	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:56.933294058 CET	50263	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:56.971002102 CET	53	50263	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:57.120764017 CET	49215	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:57.158099890 CET	53	49215	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:57.385808945 CET	64372	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:57.422029972 CET	53	64372	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:57.443068027 CET	50016	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:57.480936050 CET	53	50016	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:57.591173887 CET	61325	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:57.628443003 CET	53	61325	8.8.8.8	192.168.2.3
Nov 22, 2020 06:12:58.953318119 CET	49160	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:12:58.980429888 CET	53	49160	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:00.137408972 CET	51265	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:00.164752007 CET	53	51265	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:00.642067909 CET	52006	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:00.682306051 CET	58697	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:00.688498974 CET	53	52006	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:00.725655079 CET	53	58697	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:00.771722078 CET	51530	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:00.807012081 CET	53	51530	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:00.843389988 CET	50989	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:00.878998041 CET	53	50989	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:03.155175924 CET	53323	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:03.182440996 CET	53	53323	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:04.888030052 CET	59034	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:04.923911095 CET	53	59034	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:07.327308893 CET	53106	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:07.357321024 CET	62132	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:07.364917994 CET	53	53106	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:07.384556055 CET	53	62132	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:09.305939913 CET	54489	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:09.333358049 CET	53	54489	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:20.455199957 CET	64390	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:20.492981911 CET	53	64390	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:26.289179087 CET	58369	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:26.327419996 CET	53	58369	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:26.334598064 CET	64203	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:26.370449066 CET	53	64203	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:27.304158926 CET	49232	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:27.338598013 CET	64203	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:27.348834038 CET	53	49232	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:27.374440908 CET	53	64203	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:27.464507103 CET	52558	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:27.508265972 CET	53	52558	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:28.807427883 CET	64203	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:28.843564034 CET	53	64203	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:30.999537945 CET	64203	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:31.035947084 CET	53	64203	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:31.051238060 CET	53555	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:31.078792095 CET	53	53555	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:32.096388102 CET	53555	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:32.132657051 CET	53	53555	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 06:13:32.734368086 CET	50083	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:32.770534992 CET	53	50083	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:33.007829905 CET	49804	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:33.054316998 CET	53	49804	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:33.100167036 CET	53555	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:33.138070107 CET	53	53555	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:33.874336958 CET	50083	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:33.901806116 CET	53	50083	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:34.924274921 CET	50083	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:34.951669931 CET	53	50083	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:35.016796112 CET	64203	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:35.044337988 CET	53	64203	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:35.110446930 CET	53555	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:35.146452904 CET	53	53555	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:37.001909018 CET	50083	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:37.029306889 CET	53	50083	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:38.270092010 CET	62963	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:38.295181990 CET	63695	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:38.314400911 CET	53	62963	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:38.331439972 CET	53	63695	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:39.133964062 CET	53555	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:39.161417007 CET	53	53555	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:41.012118101 CET	50083	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:41.039664984 CET	53	50083	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:51.200110912 CET	64296	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:51.227638960 CET	53	64296	8.8.8.8	192.168.2.3
Nov 22, 2020 06:13:52.938924074 CET	60844	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:13:52.985243082 CET	53	60844	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 22, 2020 06:12:06.129188061 CET	192.168.2.3	8.8.8.8	0x7cfe	Standard query (0)	itsfoss.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.389081955 CET	192.168.2.3	8.8.8.8	0xb4b5	Standard query (0)	consent.cookiebot.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.399183989 CET	192.168.2.3	8.8.8.8	0x33a4	Standard query (0)	c0.wp.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.481060028 CET	192.168.2.3	8.8.8.8	0x46c8	Standard query (0)	static.apester.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.577085972 CET	192.168.2.3	8.8.8.8	0xad8e	Standard query (0)	a.pub.network	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.596986055 CET	192.168.2.3	8.8.8.8	0x399	Standard query (0)	live.sekindo.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.601452112 CET	192.168.2.3	8.8.8.8	0xfb2c	Standard query (0)	i1.wp.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.620753050 CET	192.168.2.3	8.8.8.8	0xfb11	Standard query (0)	i2.wp.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.634130955 CET	192.168.2.3	8.8.8.8	0x7e37	Standard query (0)	i0.wp.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.840351105 CET	192.168.2.3	8.8.8.8	0xaa08	Standard query (0)	secure.gravatar.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.847115993 CET	192.168.2.3	8.8.8.8	0xdd63	Standard query (0)	track.mailerlite.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.859896898 CET	192.168.2.3	8.8.8.8	0x1fb1	Standard query (0)	consentcdn.cookiebot.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.969696045 CET	192.168.2.3	8.8.8.8	0x57de	Standard query (0)	static.mailerlite.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:07.037676096 CET	192.168.2.3	8.8.8.8	0x4894	Standard query (0)	stats.wp.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:08.860379934 CET	192.168.2.3	8.8.8.8	0x74ab	Standard query (0)	events.apester.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:08.886759996 CET	192.168.2.3	8.8.8.8	0xde16	Standard query (0)	display.apester.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:08.983109951 CET	192.168.2.3	8.8.8.8	0x1541	Standard query (0)	pub.searchiq.co	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:09.097843885 CET	192.168.2.3	8.8.8.8	0xce76	Standard query (0)	a.omappapi.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 22, 2020 06:12:09.157989979 CET	192.168.2.3	8.8.8.8	0x7ba	Standard query (0)	api.searchiq.co	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:09.310430050 CET	192.168.2.3	8.8.8.8	0x8171	Standard query (0)	static.searchiq.co	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:09.364732027 CET	192.168.2.3	8.8.8.8	0xd2ca	Standard query (0)	sync.audiencepixel.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:09.422523975 CET	192.168.2.3	8.8.8.8	0xb9f4	Standard query (0)	api.omappapi.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:09.821326971 CET	192.168.2.3	8.8.8.8	0x88f2	Standard query (0)	pixel.wp.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:10.348678112 CET	192.168.2.3	8.8.8.8	0xbfca	Standard query (0)	renderer.apester.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:10.358035088 CET	192.168.2.3	8.8.8.8	0x7215	Standard query (0)	www.googletagservices.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:10.657289028 CET	192.168.2.3	8.8.8.8	0x85fc	Standard query (0)	c.amazon-adsystem.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:10.814120054 CET	192.168.2.3	8.8.8.8	0xebc	Standard query (0)	video.sekindo.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:11.208477020 CET	192.168.2.3	8.8.8.8	0x496	Standard query (0)	x.bidswitch.net	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:11.217349052 CET	192.168.2.3	8.8.8.8	0x8064	Standard query (0)	ads.pubmatic.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:11.231887102 CET	192.168.2.3	8.8.8.8	0xab0e	Standard query (0)	csync.loopme.me	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:11.240427971 CET	192.168.2.3	8.8.8.8	0xf5c2	Standard query (0)	ssum-sec.casalemedia.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:11.247555017 CET	192.168.2.3	8.8.8.8	0xd704	Standard query (0)	sync.search.spotxchange.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:11.254833937 CET	192.168.2.3	8.8.8.8	0x5441	Standard query (0)	u.openx.net	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:11.426523924 CET	192.168.2.3	8.8.8.8	0xf898	Standard query (0)	481.hostedprebid.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:11.452760935 CET	192.168.2.3	8.8.8.8	0x879	Standard query (0)	securepubads.g.doubleclick.net	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:13.210822105 CET	192.168.2.3	8.8.8.8	0xc6a	Standard query (0)	geolocation-db.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:14.395206928 CET	192.168.2.3	8.8.8.8	0x730f	Standard query (0)	jita.rtk.io	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:14.966521025 CET	192.168.2.3	8.8.8.8	0x3954	Standard query (0)	adservice.google.co.uk	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:16.155411005 CET	192.168.2.3	8.8.8.8	0x446b	Standard query (0)	image6.pubmatic.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:16.244689941 CET	192.168.2.3	8.8.8.8	0x4e22	Standard query (0)	ads.adaptv.advertising.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:16.250194073 CET	192.168.2.3	8.8.8.8	0xe7c6	Standard query (0)	d1azc1qln24ryf.cloudfront.net	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.276891947 CET	192.168.2.3	8.8.8.8	0x46b1	Standard query (0)	prg.smartadserver.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.284344912 CET	192.168.2.3	8.8.8.8	0x2243	Standard query (0)	hb-api.omnitagjs.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.289539099 CET	192.168.2.3	8.8.8.8	0x25ef	Standard query (0)	c2shb.ssp.yahoo.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.301157951 CET	192.168.2.3	8.8.8.8	0xa052	Standard query (0)	grid.bidswitch.net	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.304846048 CET	192.168.2.3	8.8.8.8	0xf2fc	Standard query (0)	ib.adnxs.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.313879013 CET	192.168.2.3	8.8.8.8	0x15d	Standard query (0)	bidder.criteo.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.322630882 CET	192.168.2.3	8.8.8.8	0x2af9	Standard query (0)	btlr.sharethrough.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.326438904 CET	192.168.2.3	8.8.8.8	0x325b	Standard query (0)	tag.1rx.io	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.334166050 CET	192.168.2.3	8.8.8.8	0x2f93	Standard query (0)	as-sec.casalemedia.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.337635040 CET	192.168.2.3	8.8.8.8	0xf6af	Standard query (0)	ice.360yield.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.356861115 CET	192.168.2.3	8.8.8.8	0x6d59	Standard query (0)	hbopenbid.pubmatic.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.362129927 CET	192.168.2.3	8.8.8.8	0x98c7	Standard query (0)	apester-d.openx.net	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.515788078 CET	192.168.2.3	8.8.8.8	0x3b6a	Standard query (0)	ssc.33across.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 22, 2020 06:12:18.533792019 CET	192.168.2.3	8.8.8.8	0x234b	Standard query (0)	fastlane.rubiconproject.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:19.640008926 CET	192.168.2.3	8.8.8.8	0x474d	Standard query (0)	bucket.rtk.io	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:19.720757961 CET	192.168.2.3	8.8.8.8	0xa92e	Standard query (0)	match.adsrvr.org	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:19.726722956 CET	192.168.2.3	8.8.8.8	0xe76e	Standard query (0)	pr-bh.ybp.yahoo.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:19.733285904 CET	192.168.2.3	8.8.8.8	0x5707	Standard query (0)	cm.g.doubleclick.net	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:19.764703989 CET	192.168.2.3	8.8.8.8	0xb2e2	Standard query (0)	sync-tm.everesttech.net	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:21.396285057 CET	192.168.2.3	8.8.8.8	0xd4c4	Standard query (0)	pixel.advertising.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:21.805772066 CET	192.168.2.3	8.8.8.8	0x64e4	Standard query (0)	static.criteo.net	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:22.041951895 CET	192.168.2.3	8.8.8.8	0x420e	Standard query (0)	ups.analytics.yahoo.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:22.195914984 CET	192.168.2.3	8.8.8.8	0xbaaa	Standard query (0)	gum.criteo.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:24.888170004 CET	192.168.2.3	8.8.8.8	0x83ce	Standard query (0)	acdn.adnxs.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:24.909200907 CET	192.168.2.3	8.8.8.8	0x73b9	Standard query (0)	ssc-cms.33across.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:24.932646036 CET	192.168.2.3	8.8.8.8	0xd3e1	Standard query (0)	odr.mookie1.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:24.943927050 CET	192.168.2.3	8.8.8.8	0x87d8	Standard query (0)	eu-u.openx.net	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:24.957751036 CET	192.168.2.3	8.8.8.8	0xaa2f	Standard query (0)	eus.rubiconproject.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.537240982 CET	192.168.2.3	8.8.8.8	0xf838	Standard query (0)	uipglob.semasio.net	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.545393944 CET	192.168.2.3	8.8.8.8	0xb5bb	Standard query (0)	visitor.fiftyt.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.562064886 CET	192.168.2.3	8.8.8.8	0x849	Standard query (0)	pixel.onaudience.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.579137087 CET	192.168.2.3	8.8.8.8	0x9fc5	Standard query (0)	um.simpli.fi	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.591768026 CET	192.168.2.3	8.8.8.8	0xf712	Standard query (0)	image2.pubmatic.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.662695885 CET	192.168.2.3	8.8.8.8	0x4831	Standard query (0)	simage2.pubmatic.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.666506052 CET	192.168.2.3	8.8.8.8	0x14de	Standard query (0)	d5p.de17a.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.686574936 CET	192.168.2.3	8.8.8.8	0xd6ac	Standard query (0)	dis.criteo.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.868326902 CET	192.168.2.3	8.8.8.8	0x4aae	Standard query (0)	c1.adform.net	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.924417973 CET	192.168.2.3	8.8.8.8	0xebcd	Standard query (0)	ad.turn.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.937812090 CET	192.168.2.3	8.8.8.8	0x8d19	Standard query (0)	pixel.quantserve.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.940541029 CET	192.168.2.3	8.8.8.8	0xf558	Standard query (0)	sync.mathtag.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.959439039 CET	192.168.2.3	8.8.8.8	0xa8e6	Standard query (0)	pubmatic-match.dotomi.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.962651014 CET	192.168.2.3	8.8.8.8	0x38f0	Standard query (0)	sync.crwdcntrl.net	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.973644018 CET	192.168.2.3	8.8.8.8	0x3990	Standard query (0)	acuityplatform.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.032418966 CET	192.168.2.3	8.8.8.8	0xbe63	Standard query (0)	image4.pubmatic.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.257164001 CET	192.168.2.3	8.8.8.8	0xdf81	Standard query (0)	dsp.adfarm1.adition.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.429636002 CET	192.168.2.3	8.8.8.8	0xc3de	Standard query (0)	pixel-sync.sitescout.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.439207077 CET	192.168.2.3	8.8.8.8	0x8e37	Standard query (0)	match.prod.bidr.io	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.443269968 CET	192.168.2.3	8.8.8.8	0xe0d9	Standard query (0)	match.adsby.bidtheatre.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.452785969 CET	192.168.2.3	8.8.8.8	0xb484	Standard query (0)	green.erne.co	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.454159021 CET	192.168.2.3	8.8.8.8	0x26a1	Standard query (0)	sync.1rx.io	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 22, 2020 06:12:26.458759069 CET	192.168.2.3	8.8.8.8	0x16e1	Standard query (0)	ads.playground.xyz	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.459785938 CET	192.168.2.3	8.8.8.8	0xc32	Standard query (0)	a.tribalfusion.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.461064100 CET	192.168.2.3	8.8.8.8	0x3c28	Standard query (0)	bh.contextweb.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.477459908 CET	192.168.2.3	8.8.8.8	0xea34	Standard query (0)	rtb.gumgum.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.524844885 CET	192.168.2.3	8.8.8.8	0x6ef6	Standard query (0)	cm.adgrx.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.538399935 CET	192.168.2.3	8.8.8.8	0x4911	Standard query (0)	trc.taboola.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.594142914 CET	192.168.2.3	8.8.8.8	0xdfa4	Standard query (0)	loada.exelator.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.597229004 CET	192.168.2.3	8.8.8.8	0x89fb	Standard query (0)	pm.w55c.net	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.617685080 CET	192.168.2.3	8.8.8.8	0xabf6	Standard query (0)	pixel.tapad.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.775423050 CET	192.168.2.3	8.8.8.8	0xe3d7	Standard query (0)	secure.adnxs.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.782362938 CET	192.168.2.3	8.8.8.8	0xf86d	Standard query (0)	s.tribalfusion.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.790491104 CET	192.168.2.3	8.8.8.8	0xfb25	Standard query (0)	match.taboola.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.847923994 CET	192.168.2.3	8.8.8.8	0xb51f	Standard query (0)	sync.targeting.unrulymedia.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.966417074 CET	192.168.2.3	8.8.8.8	0xbd49	Standard query (0)	inv-nets.admixer.net	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.975300074 CET	192.168.2.3	8.8.8.8	0x8b3f	Standard query (0)	us-u.openx.net	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:28.576905012 CET	192.168.2.3	8.8.8.8	0xfc5b	Standard query (0)	simage4.pubmatic.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:56.933294058 CET	192.168.2.3	8.8.8.8	0x8fc1	Standard query (0)	facebook.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:57.120764017 CET	192.168.2.3	8.8.8.8	0xfc02	Standard query (0)	m.facebook.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:57.385808945 CET	192.168.2.3	8.8.8.8	0xd6f1	Standard query (0)	static.xx.fbcdn.net	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:57.443068027 CET	192.168.2.3	8.8.8.8	0x304c	Standard query (0)	fbcdn.net	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:57.591173887 CET	192.168.2.3	8.8.8.8	0x6cdc	Standard query (0)	fbsbx.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:58.953318119 CET	192.168.2.3	8.8.8.8	0x7e0b	Standard query (0)	i1.wp.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:13:00.137408972 CET	192.168.2.3	8.8.8.8	0x9e08	Standard query (0)	www.youtube.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:13:00.682306051 CET	192.168.2.3	8.8.8.8	0xdb76	Standard query (0)	i.ytimg.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:13:03.155175924 CET	192.168.2.3	8.8.8.8	0xca57	Standard query (0)	twitter.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:13:04.888030052 CET	192.168.2.3	8.8.8.8	0x17a7	Standard query (0)	abs.twimg.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:13:07.327308893 CET	192.168.2.3	8.8.8.8	0xe231	Standard query (0)	pbs.twimg.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:13:07.357321024 CET	192.168.2.3	8.8.8.8	0x54fa	Standard query (0)	api.twitter.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:13:27.304158926 CET	192.168.2.3	8.8.8.8	0x6f43	Standard query (0)	yt3.ggpht.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:13:27.464507103 CET	192.168.2.3	8.8.8.8	0xbd7c	Standard query (0)	s2.googleusercontent.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:13:33.007829905 CET	192.168.2.3	8.8.8.8	0x9a2	Standard query (0)	r5---sn-4g5e6nz7.googlevideo.com	A (IP address)	IN (0x0001)
Nov 22, 2020 06:13:38.270092010 CET	192.168.2.3	8.8.8.8	0x6448	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 06:12:06.170231104 CET	8.8.8.8	192.168.2.3	0x7cfe	No error (0)	itsfoss.com		104.26.8.105	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 06:12:06.170231104 CET	8.8.8.8	192.168.2.3	0x7cfe	No error (0)	itsfoss.com		172.67.75.102	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.170231104 CET	8.8.8.8	192.168.2.3	0x7cfe	No error (0)	itsfoss.com		104.26.9.105	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.426244020 CET	8.8.8.8	192.168.2.3	0xb4b5	No error (0)	consent.cookiebot.com	consent.cookiebot.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:06.426280022 CET	8.8.8.8	192.168.2.3	0x33a4	No error (0)	c0.wp.com		192.0.77.37	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.516652107 CET	8.8.8.8	192.168.2.3	0x46c8	No error (0)	static.apester.com		35.190.72.53	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.612188101 CET	8.8.8.8	192.168.2.3	0xad8e	No error (0)	a.pub.network		104.26.0.139	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.612188101 CET	8.8.8.8	192.168.2.3	0xad8e	No error (0)	a.pub.network		104.26.1.139	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.612188101 CET	8.8.8.8	192.168.2.3	0xad8e	No error (0)	a.pub.network		172.67.68.60	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.628361940 CET	8.8.8.8	192.168.2.3	0xfb2c	No error (0)	i1.wp.com		192.0.77.2	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.632113934 CET	8.8.8.8	192.168.2.3	0x399	No error (0)	live.sekindo.com	live-eu-am.sekindo.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:06.632113934 CET	8.8.8.8	192.168.2.3	0x399	No error (0)	live-eu-am.sekindo.com		185.220.204.220	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.632113934 CET	8.8.8.8	192.168.2.3	0x399	No error (0)	live-eu-am.sekindo.com		63.250.56.23	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.632113934 CET	8.8.8.8	192.168.2.3	0x399	No error (0)	live-eu-am.sekindo.com		185.220.204.204	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.632113934 CET	8.8.8.8	192.168.2.3	0x399	No error (0)	live-eu-am.sekindo.com		185.220.205.205	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.632113934 CET	8.8.8.8	192.168.2.3	0x399	No error (0)	live-eu-am.sekindo.com		63.250.56.119	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.632113934 CET	8.8.8.8	192.168.2.3	0x399	No error (0)	live-eu-am.sekindo.com		194.146.38.23	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.632113934 CET	8.8.8.8	192.168.2.3	0x399	No error (0)	live-eu-am.sekindo.com		185.220.205.220	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.632113934 CET	8.8.8.8	192.168.2.3	0x399	No error (0)	live-eu-am.sekindo.com		194.146.38.205	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.647664070 CET	8.8.8.8	192.168.2.3	0xfb11	No error (0)	i2.wp.com		192.0.77.2	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.661079884 CET	8.8.8.8	192.168.2.3	0x7e37	No error (0)	i0.wp.com		192.0.77.2	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.867302895 CET	8.8.8.8	192.168.2.3	0xaa08	No error (0)	secure.gravatar.com		192.0.73.2	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.882385969 CET	8.8.8.8	192.168.2.3	0xdd63	No error (0)	track.mailerlite.com		104.18.2.159	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.882385969 CET	8.8.8.8	192.168.2.3	0xdd63	No error (0)	track.mailerlite.com		104.18.3.159	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.896846056 CET	8.8.8.8	192.168.2.3	0x1fb1	No error (0)	consentcdn.cookiebot.com	consentcdn.cookiebot.com-v1.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:06.996932030 CET	8.8.8.8	192.168.2.3	0x57de	No error (0)	static.mailerlite.com		104.18.2.159	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:06.996932030 CET	8.8.8.8	192.168.2.3	0x57de	No error (0)	static.mailerlite.com		104.18.3.159	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 06:12:07.075359106 CET	8.8.8.8	192.168.2.3	0x4894	No error (0)	stats.wp.com		192.0.76.3	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:08.887500048 CET	8.8.8.8	192.168.2.3	0x74ab	No error (0)	events.apester.com		35.190.63.234	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:08.923837900 CET	8.8.8.8	192.168.2.3	0xde16	No error (0)	display.apester.com	t2.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:09.021362066 CET	8.8.8.8	192.168.2.3	0x1541	No error (0)	pub.searchiq.co		172.67.156.77	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:09.021362066 CET	8.8.8.8	192.168.2.3	0x1541	No error (0)	pub.searchiq.co		104.18.52.245	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:09.021362066 CET	8.8.8.8	192.168.2.3	0x1541	No error (0)	pub.searchiq.co		104.18.53.245	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:09.148123980 CET	8.8.8.8	192.168.2.3	0xce76	No error (0)	a.omappapi.com	omappapi.awesomemotive.netdna-cdn.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:09.148123980 CET	8.8.8.8	192.168.2.3	0xce76	No error (0)	omappapi.awesomemotive.netdna-cdn.com		23.111.11.71	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:09.193581104 CET	8.8.8.8	192.168.2.3	0x7ba	No error (0)	api.searchiq.co		172.67.156.77	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:09.193581104 CET	8.8.8.8	192.168.2.3	0x7ba	No error (0)	api.searchiq.co		104.18.52.245	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:09.193581104 CET	8.8.8.8	192.168.2.3	0x7ba	No error (0)	api.searchiq.co		104.18.53.245	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:09.351239920 CET	8.8.8.8	192.168.2.3	0x8171	No error (0)	static.searchiq.co		104.18.53.245	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:09.351239920 CET	8.8.8.8	192.168.2.3	0x8171	No error (0)	static.searchiq.co		104.18.52.245	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:09.351239920 CET	8.8.8.8	192.168.2.3	0x8171	No error (0)	static.searchiq.co		172.67.156.77	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:09.400331974 CET	8.8.8.8	192.168.2.3	0xd2ca	No error (0)	sync.audiencepixel.com		45.61.136.49	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:09.468852997 CET	8.8.8.8	192.168.2.3	0xb9f4	No error (0)	api.omappapi.com	d1lpgznae1530s.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:09.468852997 CET	8.8.8.8	192.168.2.3	0xb9f4	No error (0)	d1lpgznae1530s.cloudfront.net		13.224.102.94	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:09.468852997 CET	8.8.8.8	192.168.2.3	0xb9f4	No error (0)	d1lpgznae1530s.cloudfront.net		13.224.102.47	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:09.468852997 CET	8.8.8.8	192.168.2.3	0xb9f4	No error (0)	d1lpgznae1530s.cloudfront.net		13.224.102.46	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:09.468852997 CET	8.8.8.8	192.168.2.3	0xb9f4	No error (0)	d1lpgznae1530s.cloudfront.net		13.224.102.10	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:09.848319054 CET	8.8.8.8	192.168.2.3	0x88f2	No error (0)	pixel.wp.com		192.0.76.3	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:10.384469986 CET	8.8.8.8	192.168.2.3	0xbfca	No error (0)	renderer.apester.com		35.186.220.219	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:10.402674913 CET	8.8.8.8	192.168.2.3	0x7215	No error (0)	www.googletagservices.com	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:10.402674913 CET	8.8.8.8	192.168.2.3	0x7215	No error (0)	pagead46.l.doubleclick.net		172.217.23.130	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:10.695648909 CET	8.8.8.8	192.168.2.3	0x85fc	No error (0)	c.amazon-adsystem.com	d1ykf07e75w7ss.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:10.695648909 CET	8.8.8.8	192.168.2.3	0x85fc	No error (0)	d1ykf07e75w7ss.cloudfront.net		13.224.103.105	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 06:12:10.857980013 CET	8.8.8.8	192.168.2.3	0xebc	No error (0)	video.sekindo.com	naeu.geo.cloudwm-cdn.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:10.857980013 CET	8.8.8.8	192.168.2.3	0xebc	No error (0)	naeu.geo.cloudwm-cdn.com		185.127.17.52	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:10.857980013 CET	8.8.8.8	192.168.2.3	0xebc	No error (0)	naeu.geo.cloudwm-cdn.com		185.167.96.211	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:10.857980013 CET	8.8.8.8	192.168.2.3	0xebc	No error (0)	naeu.geo.cloudwm-cdn.com		185.127.16.51	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:10.857980013 CET	8.8.8.8	192.168.2.3	0xebc	No error (0)	naeu.geo.cloudwm-cdn.com		185.167.97.84	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:10.857980013 CET	8.8.8.8	192.168.2.3	0xebc	No error (0)	naeu.geo.cloudwm-cdn.com		45.83.41.218	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:10.857980013 CET	8.8.8.8	192.168.2.3	0xebc	No error (0)	naeu.geo.cloudwm-cdn.com		63.250.60.138	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:10.857980013 CET	8.8.8.8	192.168.2.3	0xebc	No error (0)	naeu.geo.cloudwm-cdn.com		185.127.17.54	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:10.857980013 CET	8.8.8.8	192.168.2.3	0xebc	No error (0)	naeu.geo.cloudwm-cdn.com		185.167.96.10	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:10.857980013 CET	8.8.8.8	192.168.2.3	0xebc	No error (0)	naeu.geo.cloudwm-cdn.com		212.115.110.216	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:10.857980013 CET	8.8.8.8	192.168.2.3	0xebc	No error (0)	naeu.geo.cloudwm-cdn.com		45.83.41.102	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:10.857980013 CET	8.8.8.8	192.168.2.3	0xebc	No error (0)	naeu.geo.cloudwm-cdn.com		185.167.98.14	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:10.857980013 CET	8.8.8.8	192.168.2.3	0xebc	No error (0)	naeu.geo.cloudwm-cdn.com		185.127.16.53	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:11.235769033 CET	8.8.8.8	192.168.2.3	0x496	No error (0)	x.bidswitch.net	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:11.235769033 CET	8.8.8.8	192.168.2.3	0x496	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		52.57.142.16	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:11.235769033 CET	8.8.8.8	192.168.2.3	0x496	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		35.158.172.137	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:11.235769033 CET	8.8.8.8	192.168.2.3	0x496	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		18.158.221.94	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:11.235769033 CET	8.8.8.8	192.168.2.3	0x496	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		52.29.191.126	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:11.235769033 CET	8.8.8.8	192.168.2.3	0x496	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		52.28.21.247	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:11.235769033 CET	8.8.8.8	192.168.2.3	0x496	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		35.157.13.31	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:11.235769033 CET	8.8.8.8	192.168.2.3	0x496	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		52.28.120.199	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 06:12:11.235769033 CET	8.8.8.8	192.168.2.3	0x496	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		35.156.158.150	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:11.254376888 CET	8.8.8.8	192.168.2.3	0x8064	No error (0)	ads.pubmatic.com	pubmatic.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:11.267374992 CET	8.8.8.8	192.168.2.3	0xab0e	No error (0)	csync.loopme.me		116.202.114.114	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:11.267374992 CET	8.8.8.8	192.168.2.3	0xab0e	No error (0)	csync.loopme.me		116.202.172.174	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:11.267374992 CET	8.8.8.8	192.168.2.3	0xab0e	No error (0)	csync.loopme.me		116.202.161.117	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:11.274632931 CET	8.8.8.8	192.168.2.3	0xd704	No error (0)	sync.search.spotxchange.com	sync.search-gtm.spotxchange.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:11.274632931 CET	8.8.8.8	192.168.2.3	0xd704	No error (0)	ams01.sync.search.spotxchange.com		185.94.180.125	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:11.274632931 CET	8.8.8.8	192.168.2.3	0xd704	No error (0)	ams01.sync.search.spotxchange.com		185.94.180.126	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:11.277482033 CET	8.8.8.8	192.168.2.3	0xf5c2	No error (0)	ssum-sec.casalemedia.com	ssum-sec.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:11.281833887 CET	8.8.8.8	192.168.2.3	0x5441	No error (0)	u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:11.281833887 CET	8.8.8.8	192.168.2.3	0x5441	No error (0)	u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:11.465425968 CET	8.8.8.8	192.168.2.3	0xf898	No error (0)	481.hosted prebid.com	org-481-0bf84-dmyt03fgsksh5xx.stackpathdns.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:11.465425968 CET	8.8.8.8	192.168.2.3	0xf898	No error (0)	org-481-0bf84-dmyt03fgsksh5xx.stackpathdns.com		151.139.240.22	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:11.496635914 CET	8.8.8.8	192.168.2.3	0x879	No error (0)	securepubads.g.doubleclick.net	partnerad.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:11.496635914 CET	8.8.8.8	192.168.2.3	0x879	No error (0)	partnerad.l.doubleclick.net		172.217.21.226	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:13.238115072 CET	8.8.8.8	192.168.2.3	0xc6a	No error (0)	geolocation-db.com		46.101.248.169	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:14.431018114 CET	8.8.8.8	192.168.2.3	0x730f	No error (0)	jita.rtk.io	jita-rtk-io-dmyt03fgsksh5xx.stackpathdns.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:14.431018114 CET	8.8.8.8	192.168.2.3	0x730f	No error (0)	jita-rtk-io-dmyt03fgsksh5xx.stackpathdns.com		151.139.240.35	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:15.010947943 CET	8.8.8.8	192.168.2.3	0x3954	No error (0)	adservice.google.co.uk	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:15.010947943 CET	8.8.8.8	192.168.2.3	0x3954	No error (0)	pagead46.l.doubleclick.net		172.217.16.162	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:15.019546986 CET	8.8.8.8	192.168.2.3	0x9846	No error (0)	pagead46.l.doubleclick.net		216.58.212.162	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:16.123420954 CET	8.8.8.8	192.168.2.3	0xdebd	No error (0)	pagead46.l.doubleclick.net		172.217.21.226	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:16.182430983 CET	8.8.8.8	192.168.2.3	0x446b	No error (0)	image6.pubmatic.com	pugm-lhrc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:16.182430983 CET	8.8.8.8	192.168.2.3	0x446b	No error (0)	pugm-lhrc.pubmatic.com	pugm-lhr.pubmatic.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 06:12:16.182430983 CET	8.8.8.8	192.168.2.3	0x446b	No error (0)	pugm-lhr.pubmatic.com		185.64.190.78	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:16.283154964 CET	8.8.8.8	192.168.2.3	0x4e22	No error (0)	ads.adaptv.advertising.com	control-geo.adap.tv		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:16.283154964 CET	8.8.8.8	192.168.2.3	0x4e22	No error (0)	control-geo.adap.tv	ads-1460635594.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:16.283154964 CET	8.8.8.8	192.168.2.3	0x4e22	No error (0)	ads-1460635594.eu-central-1.elb.amazonaws.com		18.185.216.221	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:16.283154964 CET	8.8.8.8	192.168.2.3	0x4e22	No error (0)	ads-1460635594.eu-central-1.elb.amazonaws.com		18.185.185.10	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:16.283154964 CET	8.8.8.8	192.168.2.3	0x4e22	No error (0)	ads-1460635594.eu-central-1.elb.amazonaws.com		18.185.141.152	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:16.283154964 CET	8.8.8.8	192.168.2.3	0x4e22	No error (0)	ads-1460635594.eu-central-1.elb.amazonaws.com		3.123.45.128	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:16.283154964 CET	8.8.8.8	192.168.2.3	0x4e22	No error (0)	ads-1460635594.eu-central-1.elb.amazonaws.com		52.28.38.201	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:16.283154964 CET	8.8.8.8	192.168.2.3	0x4e22	No error (0)	ads-1460635594.eu-central-1.elb.amazonaws.com		18.197.185.70	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:16.283154964 CET	8.8.8.8	192.168.2.3	0x4e22	No error (0)	ads-1460635594.eu-central-1.elb.amazonaws.com		18.197.37.94	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:16.283154964 CET	8.8.8.8	192.168.2.3	0x4e22	No error (0)	ads-1460635594.eu-central-1.elb.amazonaws.com		18.196.202.129	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:16.288022995 CET	8.8.8.8	192.168.2.3	0xe7c6	No error (0)	d1azc1qln24ryf.cloudfront.net		13.224.89.144	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:16.288022995 CET	8.8.8.8	192.168.2.3	0xe7c6	No error (0)	d1azc1qln24ryf.cloudfront.net		13.224.89.57	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:16.288022995 CET	8.8.8.8	192.168.2.3	0xe7c6	No error (0)	d1azc1qln24ryf.cloudfront.net		13.224.89.149	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:16.288022995 CET	8.8.8.8	192.168.2.3	0xe7c6	No error (0)	d1azc1qln24ryf.cloudfront.net		13.224.89.207	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.316605091 CET	8.8.8.8	192.168.2.3	0x46b1	No error (0)	prg.smartadserver.com	prga.smartadserver.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:18.316605091 CET	8.8.8.8	192.168.2.3	0x46b1	No error (0)	prga.smartadserver.com	2-01-275d-0028.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:18.316605091 CET	8.8.8.8	192.168.2.3	0x46b1	No error (0)	itx5.smartadserver.com		185.86.138.32	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.316605091 CET	8.8.8.8	192.168.2.3	0x46b1	No error (0)	itx5.smartadserver.com		185.86.138.16	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.316605091 CET	8.8.8.8	192.168.2.3	0x46b1	No error (0)	itx5.smartadserver.com		185.86.138.121	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.316605091 CET	8.8.8.8	192.168.2.3	0x46b1	No error (0)	itx5.smartadserver.com		185.86.138.122	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.324038029 CET	8.8.8.8	192.168.2.3	0x2243	No error (0)	hb-api.omnitagjs.com	hb-api-fra02.omnitagjs.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:18.324038029 CET	8.8.8.8	192.168.2.3	0x2243	No error (0)	hb-api-fra02.omnitagjs.com		185.255.84.151	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.324038029 CET	8.8.8.8	192.168.2.3	0x2243	No error (0)	hb-api-fra02.omnitagjs.com		185.255.84.150	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 06:12:18.327599049 CET	8.8.8.8	192.168.2.3	0x25ef	No error (0)	c2shb.ssp.yahoo.com	c2shb.one-mobile-prod.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:18.327599049 CET	8.8.8.8	192.168.2.3	0x25ef	No error (0)	c2shb.one-mobile-prod.aws.oath.cloud	ssp-ats-prod-eu-central-1.one-mobile-prod.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:18.327599049 CET	8.8.8.8	192.168.2.3	0x25ef	No error (0)	ssp-ats-prod-eu-central-1.one-mobile-prod.aws.oath.cloud		18.156.195.47	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.327599049 CET	8.8.8.8	192.168.2.3	0x25ef	No error (0)	ssp-ats-prod-eu-central-1.one-mobile-prod.aws.oath.cloud		35.157.246.167	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.327599049 CET	8.8.8.8	192.168.2.3	0x25ef	No error (0)	ssp-ats-prod-eu-central-1.one-mobile-prod.aws.oath.cloud		52.28.203.152	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.331916094 CET	8.8.8.8	192.168.2.3	0xf2fc	No error (0)	ib.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:18.331916094 CET	8.8.8.8	192.168.2.3	0xf2fc	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:18.331916094 CET	8.8.8.8	192.168.2.3	0xf2fc	No error (0)	ib.anycast.adnxs.com		185.33.220.243	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.331916094 CET	8.8.8.8	192.168.2.3	0xf2fc	No error (0)	ib.anycast.adnxs.com		185.33.221.13	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.331916094 CET	8.8.8.8	192.168.2.3	0xf2fc	No error (0)	ib.anycast.adnxs.com		185.33.220.240	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.331916094 CET	8.8.8.8	192.168.2.3	0xf2fc	No error (0)	ib.anycast.adnxs.com		185.33.220.242	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.331916094 CET	8.8.8.8	192.168.2.3	0xf2fc	No error (0)	ib.anycast.adnxs.com		185.33.221.88	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.331916094 CET	8.8.8.8	192.168.2.3	0xf2fc	No error (0)	ib.anycast.adnxs.com		185.33.220.145	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.331916094 CET	8.8.8.8	192.168.2.3	0xf2fc	No error (0)	ib.anycast.adnxs.com		185.33.221.53	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.331916094 CET	8.8.8.8	192.168.2.3	0xf2fc	No error (0)	ib.anycast.adnxs.com		185.33.221.15	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.341104984 CET	8.8.8.8	192.168.2.3	0x15d	No error (0)	bidder.criteo.com	bidder.par.vip.prod.criteo.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:18.341104984 CET	8.8.8.8	192.168.2.3	0x15d	No error (0)	bidder.par.vip.prod.criteo.com		178.250.0.165	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.358002901 CET	8.8.8.8	192.168.2.3	0x2af9	No error (0)	btlr.sharethrough.com	btlr-ecs-eu-central-1.sharethrough.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:18.358002901 CET	8.8.8.8	192.168.2.3	0x2af9	No error (0)	btlr-ecs-eu-central-1.sharethrough.com		52.28.154.93	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.358002901 CET	8.8.8.8	192.168.2.3	0x2af9	No error (0)	btlr-ecs-eu-central-1.sharethrough.com		35.158.189.107	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.358002901 CET	8.8.8.8	192.168.2.3	0x2af9	No error (0)	btlr-ecs-eu-central-1.sharethrough.com		3.127.95.92	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.358002901 CET	8.8.8.8	192.168.2.3	0x2af9	No error (0)	btlr-ecs-eu-central-1.sharethrough.com		52.59.41.102	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.358002901 CET	8.8.8.8	192.168.2.3	0x2af9	No error (0)	btlr-ecs-eu-central-1.sharethrough.com		3.126.224.165	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 06:12:18.358002901 CET	8.8.8.8	192.168.2.3	0x2af9	No error (0)	btlr-ecs-eu-central-1.sharethrough.com		52.58.195.54	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.360367060 CET	8.8.8.8	192.168.2.3	0xa052	No error (0)	grid.bidswitch.net	pool-aws-fr.verona.iponweb.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:18.360367060 CET	8.8.8.8	192.168.2.3	0xa052	No error (0)	pool-aws-fr.verona.iponweb.net	elb-aws-fr-verona-1711955695.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:18.360367060 CET	8.8.8.8	192.168.2.3	0xa052	No error (0)	elb-aws-fr-verona-1711955695.eu-central-1.elb.amazonaws.com		18.159.79.175	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.360367060 CET	8.8.8.8	192.168.2.3	0xa052	No error (0)	elb-aws-fr-verona-1711955695.eu-central-1.elb.amazonaws.com		18.193.182.58	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.360367060 CET	8.8.8.8	192.168.2.3	0xa052	No error (0)	elb-aws-fr-verona-1711955695.eu-central-1.elb.amazonaws.com		18.185.195.81	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.360367060 CET	8.8.8.8	192.168.2.3	0xa052	No error (0)	elb-aws-fr-verona-1711955695.eu-central-1.elb.amazonaws.com		3.123.125.171	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.363966942 CET	8.8.8.8	192.168.2.3	0x325b	No error (0)	tag.1rx.io		213.19.147.210	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.373542070 CET	8.8.8.8	192.168.2.3	0x2f93	No error (0)	as-sec.casalemedia.com	as-sec.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:18.375050068 CET	8.8.8.8	192.168.2.3	0xf6af	No error (0)	ice.360yield.com	eu2-ice.360yield.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:18.375050068 CET	8.8.8.8	192.168.2.3	0xf6af	No error (0)	eu2-ice.360yield.com		52.58.204.249	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.375050068 CET	8.8.8.8	192.168.2.3	0xf6af	No error (0)	eu2-ice.360yield.com		52.57.46.37	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.375050068 CET	8.8.8.8	192.168.2.3	0xf6af	No error (0)	eu2-ice.360yield.com		18.194.102.50	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.375050068 CET	8.8.8.8	192.168.2.3	0xf6af	No error (0)	eu2-ice.360yield.com		35.157.156.128	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.375050068 CET	8.8.8.8	192.168.2.3	0xf6af	No error (0)	eu2-ice.360yield.com		35.157.249.55	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.375050068 CET	8.8.8.8	192.168.2.3	0xf6af	No error (0)	eu2-ice.360yield.com		52.29.14.143	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.375050068 CET	8.8.8.8	192.168.2.3	0xf6af	No error (0)	eu2-ice.360yield.com		18.197.249.149	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.375050068 CET	8.8.8.8	192.168.2.3	0xf6af	No error (0)	eu2-ice.360yield.com		35.157.238.72	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.383774042 CET	8.8.8.8	192.168.2.3	0x6d59	No error (0)	hbopenbid.pubmatic.com	hbopenbid22000nfc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:18.383774042 CET	8.8.8.8	192.168.2.3	0x6d59	No error (0)	hbopenbid22000nfc.pubmatic.com	hbopenbid22000nf.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:18.383774042 CET	8.8.8.8	192.168.2.3	0x6d59	No error (0)	hbopenbid22000nf.pubmatic.com		185.64.189.112	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.397624969 CET	8.8.8.8	192.168.2.3	0x98c7	No error (0)	apester-d.openx.net		35.244.159.8	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 06:12:18.397624969 CET	8.8.8.8	192.168.2.3	0x98c7	No error (0)	apester-d.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.551419973 CET	8.8.8.8	192.168.2.3	0x3b6a	No error (0)	ssc.33across.com	33xchange-1576862511.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:18.551419973 CET	8.8.8.8	192.168.2.3	0x3b6a	No error (0)	33xchange-1576862511.us-east-1.elb.amazonaws.com		54.165.26.185	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.551419973 CET	8.8.8.8	192.168.2.3	0x3b6a	No error (0)	33xchange-1576862511.us-east-1.elb.amazonaws.com		52.45.248.59	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.551419973 CET	8.8.8.8	192.168.2.3	0x3b6a	No error (0)	33xchange-1576862511.us-east-1.elb.amazonaws.com		34.200.78.134	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.551419973 CET	8.8.8.8	192.168.2.3	0x3b6a	No error (0)	33xchange-1576862511.us-east-1.elb.amazonaws.com		54.210.38.109	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:18.581639051 CET	8.8.8.8	192.168.2.3	0x234b	No error (0)	fastlane.rubiconproject.com	tagged-by.rubiconproject.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:19.677923918 CET	8.8.8.8	192.168.2.3	0x474d	No error (0)	bucket.rtk.io		147.75.84.99	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:19.748099089 CET	8.8.8.8	192.168.2.3	0xa92e	No error (0)	match.adsrvr.org	match-1943069928.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:19.748099089 CET	8.8.8.8	192.168.2.3	0xa92e	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.50.156.162	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:19.748099089 CET	8.8.8.8	192.168.2.3	0xa92e	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		63.33.218.134	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:19.748099089 CET	8.8.8.8	192.168.2.3	0xa92e	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.210.149.10	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:19.748099089 CET	8.8.8.8	192.168.2.3	0xa92e	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		34.246.127.166	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:19.748099089 CET	8.8.8.8	192.168.2.3	0xa92e	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		18.203.78.129	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:19.748099089 CET	8.8.8.8	192.168.2.3	0xa92e	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		54.154.164.132	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:19.748099089 CET	8.8.8.8	192.168.2.3	0xa92e	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		54.195.113.118	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:19.748099089 CET	8.8.8.8	192.168.2.3	0xa92e	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.210.128.165	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:19.754164934 CET	8.8.8.8	192.168.2.3	0xe76e	No error (0)	pr-bh.ybp.yahoo.com	ds-pr-bh.ybp.gysm.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:19.754164934 CET	8.8.8.8	192.168.2.3	0xe76e	No error (0)	ds-pr-bh.ybp.gysm.yahoodns.net		212.82.100.176	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 06:12:19.777168989 CET	8.8.8.8	192.168.2.3	0x5707	No error (0)	cm.g.doubleclick.net	pagead.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:19.777168989 CET	8.8.8.8	192.168.2.3	0x5707	No error (0)	pagead.l.doubleclick.net		216.58.212.130	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:19.804461002 CET	8.8.8.8	192.168.2.3	0xb2e2	No error (0)	sync-tm.everesttech.net	sync.tubemogul.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:19.804461002 CET	8.8.8.8	192.168.2.3	0xb2e2	No error (0)	sync.tubemogul.com	syncf.tubemogul.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:19.804461002 CET	8.8.8.8	192.168.2.3	0xb2e2	No error (0)	syncf.tubemogul.com	h2.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:21.423571110 CET	8.8.8.8	192.168.2.3	0xd4c4	No error (0)	pixel.advertising.com	prod.ups-adcom.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:21.423571110 CET	8.8.8.8	192.168.2.3	0xd4c4	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)
Nov 22, 2020 06:12:21.423571110 CET	8.8.8.8	192.168.2.3	0xd4c4	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		35.156.106.231	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:21.423571110 CET	8.8.8.8	192.168.2.3	0xd4c4	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		35.156.153.71	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:21.423571110 CET	8.8.8.8	192.168.2.3	0xd4c4	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.197.47.23	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:21.423571110 CET	8.8.8.8	192.168.2.3	0xd4c4	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.197.99.6	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:21.423571110 CET	8.8.8.8	192.168.2.3	0xd4c4	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		3.124.119.192	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:21.423571110 CET	8.8.8.8	192.168.2.3	0xd4c4	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		3.126.63.176	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:21.423571110 CET	8.8.8.8	192.168.2.3	0xd4c4	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		52.28.239.147	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:21.423571110 CET	8.8.8.8	192.168.2.3	0xd4c4	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		52.28.254.214	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:21.832881927 CET	8.8.8.8	192.168.2.3	0x64e4	No error (0)	static.criteo.net	static.am5.vip.prod.criteo.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:21.832881927 CET	8.8.8.8	192.168.2.3	0x64e4	No error (0)	static.am5.vip.prod.criteo.net		178.250.2.130	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:22.085942984 CET	8.8.8.8	192.168.2.3	0x420e	No error (0)	ups.analytics.yahoo.com	prod.ups-ats.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:22.085942984 CET	8.8.8.8	192.168.2.3	0x420e	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)
Nov 22, 2020 06:12:22.085942984 CET	8.8.8.8	192.168.2.3	0x420e	No error (0)	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		3.126.56.137	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:22.085942984 CET	8.8.8.8	192.168.2.3	0x420e	No error (0)	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		18.156.0.31	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:22.223018885 CET	8.8.8.8	192.168.2.3	0xbaaa	No error (0)	gum.criteo.com	gum.par.vip.prod.criteo.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 06:12:22.223018885 CET	8.8.8.8	192.168.2.3	0xbaaa	No error (0)	gum.par.vip.prod.criteo.com		178.250.0.157	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:24.927825928 CET	8.8.8.8	192.168.2.3	0x83ce	No error (0)	acdn.adnxs.com	secure-adnxs.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:24.944967985 CET	8.8.8.8	192.168.2.3	0x73b9	No error (0)	ssc-cms.33across.com	pixel.33across.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:24.944967985 CET	8.8.8.8	192.168.2.3	0x73b9	No error (0)	pixel.33across.com		67.202.110.21	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:24.959669113 CET	8.8.8.8	192.168.2.3	0xd3e1	No error (0)	odr.mookie1.com	tagr-gcp-odr-euw4.mookie1.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:24.959669113 CET	8.8.8.8	192.168.2.3	0xd3e1	No error (0)	tagr-gcp-odr-euw4.mookie1.com		34.98.67.61	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:24.971118927 CET	8.8.8.8	192.168.2.3	0x87d8	No error (0)	eu-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:24.971118927 CET	8.8.8.8	192.168.2.3	0x87d8	No error (0)	eu-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:24.996651888 CET	8.8.8.8	192.168.2.3	0xaa2f	No error (0)	eus.rubiconproject.com	eus.rubiconproject.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:25.564335108 CET	8.8.8.8	192.168.2.3	0xf838	No error (0)	uipglob.semasio.net	uipglob.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:25.564335108 CET	8.8.8.8	192.168.2.3	0xf838	No error (0)	uip.semasio.net		77.243.60.138	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.572412014 CET	8.8.8.8	192.168.2.3	0xb5bb	No error (0)	visitor.fiftyt.com		104.26.12.50	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.572412014 CET	8.8.8.8	192.168.2.3	0xb5bb	No error (0)	visitor.fiftyt.com		104.26.13.50	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.572412014 CET	8.8.8.8	192.168.2.3	0xb5bb	No error (0)	visitor.fiftyt.com		172.67.73.8	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.589045048 CET	8.8.8.8	192.168.2.3	0x849	No error (0)	pixel.onaudience.com		51.210.112.66	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.589045048 CET	8.8.8.8	192.168.2.3	0x849	No error (0)	pixel.onaudience.com		51.210.112.63	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.589045048 CET	8.8.8.8	192.168.2.3	0x849	No error (0)	pixel.onaudience.com		51.210.112.236	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.589045048 CET	8.8.8.8	192.168.2.3	0x849	No error (0)	pixel.onaudience.com		51.210.112.64	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.616000891 CET	8.8.8.8	192.168.2.3	0x9fc5	No error (0)	um.simpli.fi		159.253.128.188	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.616000891 CET	8.8.8.8	192.168.2.3	0x9fc5	No error (0)	um.simpli.fi		159.253.128.183	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.616000891 CET	8.8.8.8	192.168.2.3	0x9fc5	No error (0)	um.simpli.fi		169.50.137.190	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.618824959 CET	8.8.8.8	192.168.2.3	0xf712	No error (0)	image2.pubmatic.com	pug-lhrc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:25.618824959 CET	8.8.8.8	192.168.2.3	0xf712	No error (0)	pug-lhrc.pubmatic.com	pug-lhr.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:25.618824959 CET	8.8.8.8	192.168.2.3	0xf712	No error (0)	pug-lhr.pubmatic.com		185.64.190.80	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.689728022 CET	8.8.8.8	192.168.2.3	0x4831	No error (0)	simage2.pubmatic.com	pug22000nfc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:25.689728022 CET	8.8.8.8	192.168.2.3	0x4831	No error (0)	pug22000nfc.pubmatic.com	pug22000nf.pubmatic.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 06:12:25.689728022 CET	8.8.8.8	192.168.2.3	0x4831	No error (0)	pug22000nf .pubmatic.com		185.64.189.110	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.693528891 CET	8.8.8.8	192.168.2.3	0x14de	No error (0)	d5p.de17a.com		213.155.156.181	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.693528891 CET	8.8.8.8	192.168.2.3	0x14de	No error (0)	d5p.de17a.com		213.155.156.169	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.693528891 CET	8.8.8.8	192.168.2.3	0x14de	No error (0)	d5p.de17a.com		213.155.156.183	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.693528891 CET	8.8.8.8	192.168.2.3	0x14de	No error (0)	d5p.de17a.com		213.155.156.166	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.693528891 CET	8.8.8.8	192.168.2.3	0x14de	No error (0)	d5p.de17a.com		213.155.156.168	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.693528891 CET	8.8.8.8	192.168.2.3	0x14de	No error (0)	d5p.de17a.com		213.155.156.165	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.693528891 CET	8.8.8.8	192.168.2.3	0x14de	No error (0)	d5p.de17a.com		213.155.156.180	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.693528891 CET	8.8.8.8	192.168.2.3	0x14de	No error (0)	d5p.de17a.com		213.155.156.184	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.693528891 CET	8.8.8.8	192.168.2.3	0x14de	No error (0)	d5p.de17a.com		213.155.156.167	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.693528891 CET	8.8.8.8	192.168.2.3	0x14de	No error (0)	d5p.de17a.com		213.155.156.182	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.693528891 CET	8.8.8.8	192.168.2.3	0x14de	No error (0)	d5p.de17a.com		213.155.156.164	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.693528891 CET	8.8.8.8	192.168.2.3	0x14de	No error (0)	d5p.de17a.com		213.155.156.185	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.713685036 CET	8.8.8.8	192.168.2.3	0xd6ac	No error (0)	dis.criteo.com	widget.par.vip.prod.criteo.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:25.713685036 CET	8.8.8.8	192.168.2.3	0xd6ac	No error (0)	widget.par .vip.prod. criteo.com		178.250.0.163	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.916671991 CET	8.8.8.8	192.168.2.3	0x4aae	No error (0)	c1.adform.net	track.adformnet.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:25.961321115 CET	8.8.8.8	192.168.2.3	0xebcd	No error (0)	ad.turn.com	ad.turn.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:25.967587948 CET	8.8.8.8	192.168.2.3	0xf558	No error (0)	sync.matht ag.com	pixel-origin.mathtag.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:25.967587948 CET	8.8.8.8	192.168.2.3	0xf558	No error (0)	pixel-orig in.mathtag.com		185.29.133.199	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.967587948 CET	8.8.8.8	192.168.2.3	0xf558	No error (0)	pixel-orig in.mathtag.com		185.29.135.190	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.967587948 CET	8.8.8.8	192.168.2.3	0xf558	No error (0)	pixel-orig in.mathtag.com		185.29.133.208	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.967587948 CET	8.8.8.8	192.168.2.3	0xf558	No error (0)	pixel-orig in.mathtag.com		185.29.135.233	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.974994898 CET	8.8.8.8	192.168.2.3	0x8d19	No error (0)	pixel.quan tserve.com	global.px.quantserve.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:25.974994898 CET	8.8.8.8	192.168.2.3	0x8d19	No error (0)	global.px. quantserve.com		91.228.74.133	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.974994898 CET	8.8.8.8	192.168.2.3	0x8d19	No error (0)	global.px. quantserve.com		91.228.74.226	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.974994898 CET	8.8.8.8	192.168.2.3	0x8d19	No error (0)	global.px. quantserve.com		91.228.74.189	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 06:12:25.974994898 CET	8.8.8.8	192.168.2.3	0x8d19	No error (0)	global.px.quantserve.com		91.228.74.198	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.974994898 CET	8.8.8.8	192.168.2.3	0x8d19	No error (0)	global.px.quantserve.com		91.228.74.134	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:25.996500969 CET	8.8.8.8	192.168.2.3	0xa8e6	No error (0)	pubmatic-match.dotomi.com	afp.dotomi.weighted.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:25.996500969 CET	8.8.8.8	192.168.2.3	0xa8e6	No error (0)	ams03-login-ds.dotomi.com		89.207.16.140	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.005753040 CET	8.8.8.8	192.168.2.3	0x38f0	No error (0)	sync.crwdcntrl.net		52.49.190.28	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.005753040 CET	8.8.8.8	192.168.2.3	0x38f0	No error (0)	sync.crwdcntrl.net		34.245.253.34	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.005753040 CET	8.8.8.8	192.168.2.3	0x38f0	No error (0)	sync.crwdcntrl.net		52.30.140.199	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.005753040 CET	8.8.8.8	192.168.2.3	0x38f0	No error (0)	sync.crwdcntrl.net		52.48.248.240	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.005753040 CET	8.8.8.8	192.168.2.3	0x38f0	No error (0)	sync.crwdcntrl.net		34.253.109.165	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.005753040 CET	8.8.8.8	192.168.2.3	0x38f0	No error (0)	sync.crwdcntrl.net		52.48.137.92	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.005753040 CET	8.8.8.8	192.168.2.3	0x38f0	No error (0)	sync.crwdcntrl.net		52.210.253.186	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.005753040 CET	8.8.8.8	192.168.2.3	0x38f0	No error (0)	sync.crwdcntrl.net		99.80.128.92	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.013334036 CET	8.8.8.8	192.168.2.3	0x3990	No error (0)	acuityplatform.com		154.59.122.74	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.059250116 CET	8.8.8.8	192.168.2.3	0xbe63	No error (0)	image4.pubmatic.com	spug22000nfc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:26.059250116 CET	8.8.8.8	192.168.2.3	0xbe63	No error (0)	spug22000nfc.pubmatic.com	spug22000nf.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:26.059250116 CET	8.8.8.8	192.168.2.3	0xbe63	No error (0)	spug22000nf.pubmatic.com		185.64.189.114	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.284157991 CET	8.8.8.8	192.168.2.3	0xdf81	No error (0)	dsp.adfarm1.adition.com		85.114.159.118	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.284157991 CET	8.8.8.8	192.168.2.3	0xdf81	No error (0)	dsp.adfarm1.adition.com		85.114.159.93	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.469073057 CET	8.8.8.8	192.168.2.3	0xc3de	No error (0)	pixel-sync.sitescout.com	pixel-a.sitescout.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:26.469073057 CET	8.8.8.8	192.168.2.3	0xc3de	No error (0)	pixel-a.sitescout.com		66.155.71.150	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.470351934 CET	8.8.8.8	192.168.2.3	0xe0d9	No error (0)	match.adsby.bidtheatre.com		174.138.12.104	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.470351934 CET	8.8.8.8	192.168.2.3	0xe0d9	No error (0)	match.adsby.bidtheatre.com		167.99.220.155	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.479840040 CET	8.8.8.8	192.168.2.3	0xb484	No error (0)	green.erne.co		87.98.128.108	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.479840040 CET	8.8.8.8	192.168.2.3	0xb484	No error (0)	green.erne.co		188.165.4.142	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.479840040 CET	8.8.8.8	192.168.2.3	0xb484	No error (0)	green.erne.co		188.165.27.173	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.479840040 CET	8.8.8.8	192.168.2.3	0xb484	No error (0)	green.erne.co		87.98.252.5	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 06:12:26.479840040 CET	8.8.8.8	192.168.2.3	0xb484	No error (0)	green.erne.co		94.23.73.243	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.479840040 CET	8.8.8.8	192.168.2.3	0xb484	No error (0)	green.erne.co		94.23.144.220	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.479840040 CET	8.8.8.8	192.168.2.3	0xb484	No error (0)	green.erne.co		87.98.242.60	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.479840040 CET	8.8.8.8	192.168.2.3	0xb484	No error (0)	green.erne.co		87.98.228.78	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.479840040 CET	8.8.8.8	192.168.2.3	0xb484	No error (0)	green.erne.co		94.23.171.206	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.479840040 CET	8.8.8.8	192.168.2.3	0xb484	No error (0)	green.erne.co		188.165.137.78	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.486720085 CET	8.8.8.8	192.168.2.3	0xc32	No error (0)	a.tribalfusion.com		104.18.12.5	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.486720085 CET	8.8.8.8	192.168.2.3	0xc32	No error (0)	a.tribalfusion.com		104.18.13.5	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.488176107 CET	8.8.8.8	192.168.2.3	0x8e37	No error (0)	match.prod.bidr.io		54.171.14.147	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.488176107 CET	8.8.8.8	192.168.2.3	0x8e37	No error (0)	match.prod.bidr.io		52.214.70.9	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.488176107 CET	8.8.8.8	192.168.2.3	0x8e37	No error (0)	match.prod.bidr.io		52.31.242.159	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.488176107 CET	8.8.8.8	192.168.2.3	0x8e37	No error (0)	match.prod.bidr.io		52.49.193.31	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.488176107 CET	8.8.8.8	192.168.2.3	0x8e37	No error (0)	match.prod.bidr.io		54.72.203.0	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.488176107 CET	8.8.8.8	192.168.2.3	0x8e37	No error (0)	match.prod.bidr.io		54.228.192.197	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.491595030 CET	8.8.8.8	192.168.2.3	0x26a1	No error (0)	sync.1rx.io		213.19.147.150	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.496150970 CET	8.8.8.8	192.168.2.3	0x16e1	No error (0)	ads.playground.xyz		52.57.47.66	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.496150970 CET	8.8.8.8	192.168.2.3	0x16e1	No error (0)	ads.playground.xyz		3.125.132.240	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.496150970 CET	8.8.8.8	192.168.2.3	0x16e1	No error (0)	ads.playground.xyz		3.121.163.163	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.507817984 CET	8.8.8.8	192.168.2.3	0x3c28	No error (0)	bh.contextweb.com	lga-bh.contextweb.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:26.507817984 CET	8.8.8.8	192.168.2.3	0x3c28	No error (0)	lga-bh.contextweb.com	lga-bh-bgp.contextweb.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:26.507817984 CET	8.8.8.8	192.168.2.3	0x3c28	No error (0)	lga-bh-bgp.contextweb.com		198.148.27.140	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.507817984 CET	8.8.8.8	192.168.2.3	0x3c28	No error (0)	lga-bh-bgp.contextweb.com		198.148.27.139	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.515645027 CET	8.8.8.8	192.168.2.3	0xea34	No error (0)	rtb.gumgum.com		108.129.8.178	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.515645027 CET	8.8.8.8	192.168.2.3	0xea34	No error (0)	rtb.gumgum.com		108.128.209.152	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.515645027 CET	8.8.8.8	192.168.2.3	0xea34	No error (0)	rtb.gumgum.com		34.250.108.63	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.515645027 CET	8.8.8.8	192.168.2.3	0xea34	No error (0)	rtb.gumgum.com		54.171.43.242	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 06:12:26.515645027 CET	8.8.8.8	192.168.2.3	0xea34	No error (0)	rtb.gumgum.com		54.154.144.178	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.515645027 CET	8.8.8.8	192.168.2.3	0xea34	No error (0)	rtb.gumgum.com		52.215.241.211	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.515645027 CET	8.8.8.8	192.168.2.3	0xea34	No error (0)	rtb.gumgum.com		34.250.244.32	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.515645027 CET	8.8.8.8	192.168.2.3	0xea34	No error (0)	rtb.gumgum.com		52.31.234.119	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.566313982 CET	8.8.8.8	192.168.2.3	0x6ef6	No error (0)	cm.adgrx.com	rtb.adgrx.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:26.566313982 CET	8.8.8.8	192.168.2.3	0x6ef6	No error (0)	rtb.adgrx.com	rtb.adgrx.com.tech.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:26.578867912 CET	8.8.8.8	192.168.2.3	0x4911	No error (0)	trc.taboola.com	tls13.taboola.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:26.578867912 CET	8.8.8.8	192.168.2.3	0x4911	No error (0)	tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.578867912 CET	8.8.8.8	192.168.2.3	0x4911	No error (0)	tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.578867912 CET	8.8.8.8	192.168.2.3	0x4911	No error (0)	tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.578867912 CET	8.8.8.8	192.168.2.3	0x4911	No error (0)	tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.632822037 CET	8.8.8.8	192.168.2.3	0x89fb	No error (0)	pm.w55c.net	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:26.632822037 CET	8.8.8.8	192.168.2.3	0x89fb	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		35.158.49.68	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.632822037 CET	8.8.8.8	192.168.2.3	0x89fb	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		3.125.82.176	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.632822037 CET	8.8.8.8	192.168.2.3	0x89fb	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		3.125.99.7	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.632822037 CET	8.8.8.8	192.168.2.3	0x89fb	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		35.157.48.14	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.632822037 CET	8.8.8.8	192.168.2.3	0x89fb	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		3.127.88.255	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.632822037 CET	8.8.8.8	192.168.2.3	0x89fb	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		18.158.113.188	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.632822037 CET	8.8.8.8	192.168.2.3	0x89fb	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		3.123.192.108	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.632822037 CET	8.8.8.8	192.168.2.3	0x89fb	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		52.59.61.242	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.637465000 CET	8.8.8.8	192.168.2.3	0xdfa4	No error (0)	loada.exelator.com	eu-west.load.exelator.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 06:12:26.637465000 CET	8.8.8.8	192.168.2.3	0xdfa4	No error (0)	eu-west.load.exelator.com	load-ams1.exelator.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:26.637465000 CET	8.8.8.8	192.168.2.3	0xdfa4	No error (0)	load-ams1.exelator.com		147.75.102.200	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.663953066 CET	8.8.8.8	192.168.2.3	0xabf6	No error (0)	pixel.tapad.com		35.227.248.159	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.802341938 CET	8.8.8.8	192.168.2.3	0xe3d7	No error (0)	secure.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:26.802341938 CET	8.8.8.8	192.168.2.3	0xe3d7	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:26.802341938 CET	8.8.8.8	192.168.2.3	0xe3d7	No error (0)	ib.anycast.adnxs.com		185.33.220.244	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.802341938 CET	8.8.8.8	192.168.2.3	0xe3d7	No error (0)	ib.anycast.adnxs.com		185.33.221.91	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.802341938 CET	8.8.8.8	192.168.2.3	0xe3d7	No error (0)	ib.anycast.adnxs.com		185.33.221.14	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.802341938 CET	8.8.8.8	192.168.2.3	0xe3d7	No error (0)	ib.anycast.adnxs.com		185.33.220.240	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.802341938 CET	8.8.8.8	192.168.2.3	0xe3d7	No error (0)	ib.anycast.adnxs.com		185.33.221.53	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.802341938 CET	8.8.8.8	192.168.2.3	0xe3d7	No error (0)	ib.anycast.adnxs.com		185.33.220.243	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.802341938 CET	8.8.8.8	192.168.2.3	0xe3d7	No error (0)	ib.anycast.adnxs.com		185.33.221.50	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.802341938 CET	8.8.8.8	192.168.2.3	0xe3d7	No error (0)	ib.anycast.adnxs.com		185.33.220.242	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.809231997 CET	8.8.8.8	192.168.2.3	0xf86d	No error (0)	s.tribalfusion.com		104.18.12.5	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.809231997 CET	8.8.8.8	192.168.2.3	0xf86d	No error (0)	s.tribalfusion.com		104.18.13.5	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.829673052 CET	8.8.8.8	192.168.2.3	0xfb25	No error (0)	match.taboola.com	tls13.taboola.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:26.829673052 CET	8.8.8.8	192.168.2.3	0xfb25	No error (0)	tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.829673052 CET	8.8.8.8	192.168.2.3	0xfb25	No error (0)	tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.829673052 CET	8.8.8.8	192.168.2.3	0xfb25	No error (0)	tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.829673052 CET	8.8.8.8	192.168.2.3	0xfb25	No error (0)	tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.885437965 CET	8.8.8.8	192.168.2.3	0xb51f	No error (0)	sync.targeting.unrulymedia.com	sync.1rx.io		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:26.885437965 CET	8.8.8.8	192.168.2.3	0xb51f	No error (0)	sync.1rx.io		213.19.147.151	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:26.993470907 CET	8.8.8.8	192.168.2.3	0xbd49	No error (0)	inv-nets.admixer.net	inv-nets-eu.admixer.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:26.993470907 CET	8.8.8.8	192.168.2.3	0xbd49	No error (0)	inv-nets-eu.admixer.net		146.0.227.110	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:27.002202988 CET	8.8.8.8	192.168.2.3	0x8b3f	No error (0)	us-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:27.002202988 CET	8.8.8.8	192.168.2.3	0x8b3f	No error (0)	us-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 06:12:28.604115963 CET	8.8.8.8	192.168.2.3	0xfc5b	No error (0)	simage4.pubmatic.com	spug-lhrc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:28.604115963 CET	8.8.8.8	192.168.2.3	0xfc5b	No error (0)	spug-lhrc.pubmatic.com	spug-lhr.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:28.604115963 CET	8.8.8.8	192.168.2.3	0xfc5b	No error (0)	spug-lhr.pubmatic.com		185.64.190.81	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:56.971002102 CET	8.8.8.8	192.168.2.3	0x8fc1	No error (0)	facebook.com		185.60.216.35	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:57.158099890 CET	8.8.8.8	192.168.2.3	0xfc02	No error (0)	m.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:57.158099890 CET	8.8.8.8	192.168.2.3	0xfc02	No error (0)	star-mini.c10r.facebook.com		185.60.216.35	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:57.422029972 CET	8.8.8.8	192.168.2.3	0xd6f1	No error (0)	static.xx.fbcdn.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:12:57.422029972 CET	8.8.8.8	192.168.2.3	0xd6f1	No error (0)	scontent.xx.fbcdn.net		185.60.216.19	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:57.480936050 CET	8.8.8.8	192.168.2.3	0x304c	No error (0)	fbcdn.net		185.60.216.35	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:57.628443003 CET	8.8.8.8	192.168.2.3	0x6cdc	No error (0)	fbsbx.com		185.60.216.35	A (IP address)	IN (0x0001)
Nov 22, 2020 06:12:58.980429888 CET	8.8.8.8	192.168.2.3	0x7e0b	No error (0)	i1.wp.com		192.0.77.2	A (IP address)	IN (0x0001)
Nov 22, 2020 06:13:00.164752007 CET	8.8.8.8	192.168.2.3	0x9e08	No error (0)	www.youtube.com	youtube-ui.l.google.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:13:00.725655079 CET	8.8.8.8	192.168.2.3	0xdb76	No error (0)	i.ytimg.com		216.58.212.150	A (IP address)	IN (0x0001)
Nov 22, 2020 06:13:03.182440996 CET	8.8.8.8	192.168.2.3	0xca57	No error (0)	twitter.com		104.244.42.65	A (IP address)	IN (0x0001)
Nov 22, 2020 06:13:03.182440996 CET	8.8.8.8	192.168.2.3	0xca57	No error (0)	twitter.com		104.244.42.1	A (IP address)	IN (0x0001)
Nov 22, 2020 06:13:04.923911095 CET	8.8.8.8	192.168.2.3	0x17a7	No error (0)	abs.twimg.com	cs510.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:13:04.923911095 CET	8.8.8.8	192.168.2.3	0x17a7	No error (0)	cs510.wpc.edgecastcdn.net		152.199.21.141	A (IP address)	IN (0x0001)
Nov 22, 2020 06:13:07.364917994 CET	8.8.8.8	192.168.2.3	0xe231	No error (0)	pbs.twimg.com	cs196.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:13:07.364917994 CET	8.8.8.8	192.168.2.3	0xe231	No error (0)	cs196.wac.edgecastcdn.net	cs2-wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:13:07.364917994 CET	8.8.8.8	192.168.2.3	0xe231	No error (0)	cs2-wac-eu.8315.ecdns.net	cs45.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:13:07.364917994 CET	8.8.8.8	192.168.2.3	0xe231	No error (0)	cs45.wac.edgecastcdn.net		93.184.220.70	A (IP address)	IN (0x0001)
Nov 22, 2020 06:13:07.384556055 CET	8.8.8.8	192.168.2.3	0x54fa	No error (0)	api.twitter.com	tpop-api.twitter.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:13:07.384556055 CET	8.8.8.8	192.168.2.3	0x54fa	No error (0)	tpop-api.twitter.com		104.244.42.66	A (IP address)	IN (0x0001)
Nov 22, 2020 06:13:07.384556055 CET	8.8.8.8	192.168.2.3	0x54fa	No error (0)	tpop-api.twitter.com		104.244.42.194	A (IP address)	IN (0x0001)
Nov 22, 2020 06:13:07.384556055 CET	8.8.8.8	192.168.2.3	0x54fa	No error (0)	tpop-api.twitter.com		104.244.42.2	A (IP address)	IN (0x0001)
Nov 22, 2020 06:13:07.384556055 CET	8.8.8.8	192.168.2.3	0x54fa	No error (0)	tpop-api.twitter.com		104.244.42.130	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 06:13:27.348834038 CET	8.8.8.8	192.168.2.3	0x6f43	No error (0)	yt3.ggpht.com	photos-ugc.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:13:27.348834038 CET	8.8.8.8	192.168.2.3	0x6f43	No error (0)	photos-ugc.l.googleusercontent.com		172.217.23.161	A (IP address)	IN (0x0001)
Nov 22, 2020 06:13:27.508265972 CET	8.8.8.8	192.168.2.3	0xbd7c	No error (0)	s2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:13:27.508265972 CET	8.8.8.8	192.168.2.3	0xbd7c	No error (0)	googlehosted.l.googleusercontent.com		172.217.21.193	A (IP address)	IN (0x0001)
Nov 22, 2020 06:13:33.054316998 CET	8.8.8.8	192.168.2.3	0x9a2	No error (0)	r5---sn-4g5e6nz7.googlevideo.com	r5.sn-4g5e6nz7.googlevideo.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 06:13:33.054316998 CET	8.8.8.8	192.168.2.3	0x9a2	No error (0)	r5.sn-4g5e6nz7.googlevideo.com		173.194.187.170	A (IP address)	IN (0x0001)
Nov 22, 2020 06:13:38.314400911 CET	8.8.8.8	192.168.2.3	0x6448	No error (0)	www.google.co.uk		172.217.21.227	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 22, 2020 06:12:06.224256992 CET	104.26.8.105	443	192.168.2.3	49717	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Aug 12 02:00:00 CEST 2020	Thu Aug 12 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 22, 2020 06:12:06.225138903 CET	104.26.8.105	443	192.168.2.3	49716	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Aug 12 02:00:00 CEST 2020	Thu Aug 12 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 22, 2020 06:12:06.485809088 CET	192.0.77.37	443	192.168.2.3	49719	CN=*.wp.com 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 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018	Tue Jul 05 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=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	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
							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
					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		
Nov 22, 2020 06:12:06.486282110 CET	192.0.77.37	443	192.168.2.3	49718	CN=*.wp.com 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 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Tue Jul 05 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031 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=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		
Nov 22, 2020 06:12:06.496866941 CET	192.0.77.37	443	192.168.2.3	49724	CN=*.wp.com 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 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Tue Jul 05 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031 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=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		
Nov 22, 2020 06:12:06.604460955 CET	35.190.72.53	443	192.168.2.3	49725	CN=static.apester.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Oct 20 07:41:35 CEST 2020 Thu Mar 17 17:40:46 CET 2016	Mon Jan 18 06:41:35 CET 2021 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Nov 22, 2020 06:12:06.604646921 CET	35.190.72.53	443	192.168.2.3	49726	CN=static.apester.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Oct 20 07:41:35 CEST 2020 Thu Mar 17 17:40:46 CET 2016	Mon Jan 18 06:41:35 CET 2021 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Nov 22, 2020 06:12:06.607798100 CET	192.0.77.37	443	192.168.2.3	49720	CN=*.wp.com 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 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Tue Jul 05 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031 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=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		
Nov 22, 2020 06:12:06.607836962 CET	192.0.77.37	443	192.168.2.3	49721	CN=*.wp.com 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 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Tue Jul 05 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031 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=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		
Nov 22, 2020 06:12:06.656094074 CET	104.26.0.139	443	192.168.2.3	49727	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Jul 17 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Sat Jul 17 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 22, 2020 06:12:06.656414986 CET	104.26.0.139	443	192.168.2.3	49728	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Jul 17 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Sat Jul 17 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 22, 2020 06:12:06.669528961 CET	192.0.77.2	443	192.168.2.3	49730	CN=*.wp.com 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 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Tue Jul 05 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031 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=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		
Nov 22, 2020 06:12:06.821223021 CET	192.0.77.2	443	192.168.2.3	49729	CN=*.wp.com 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 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Tue Jul 05 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031 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=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		
Nov 22, 2020 06:12:06.845958948 CET	192.0.77.2	443	192.168.2.3	49734	CN=*.wp.com 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 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Tue Jul 05 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031 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=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
Nov 22, 2020 06:12:06.846010923 CET	192.0.77.2	443	192.168.2.3	49733	CN=*.wp.com 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 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Tue Jul 05 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031 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=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		
Nov 22, 2020 06:12:06.859474897 CET	185.220.204.220	443	192.168.2.3	49732	CN=www.sekindo.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Oct 27 13:28:25 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Sun Nov 28 13:28:25 CET 2021 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Nov 22, 2020 06:12:06.859977007 CET	185.220.204.220	443	192.168.2.3	49731	CN=www.sekindo.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Oct 27 13:28:25 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Sun Nov 28 13:28:25 CET 2021 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Nov 22, 2020 06:12:06.874066114 CET	192.0.77.2	443	192.168.2.3	49736	CN=*.wp.com 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 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Tue Jul 05 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031 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=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		
Nov 22, 2020 06:12:06.874792099 CET	192.0.77.2	443	192.168.2.3	49737	CN=*.wp.com 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 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Tue Jul 05 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031 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=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		
Nov 22, 2020 06:12:06.914875984 CET	192.0.73.2	443	192.168.2.3	49739	CN=*.gravatar.com 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	Fri Aug 14 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Wed Nov 16 01:00:00 CET 2022 Wed Jan 01 00:59:59 CET 2031 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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		
Nov 22, 2020 06:12:06.915673018 CET	192.0.73.2	443	192.168.2.3	49738	CN=*.gravatar.com 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	Fri Aug 14 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Wed Nov 16 01:00:00 CET 2022 Wed Jan 01 00:59:59 CET 2031 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=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		
Nov 22, 2020 06:12:06.944160938 CET	104.18.2.159	443	192.168.2.3	49742	CN=mailerlite.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Aug 28 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Sat Aug 28 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 22, 2020 06:12:06.947066069 CET	104.18.2.159	443	192.168.2.3	49743	CN=mailerlite.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Aug 28 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Sat Aug 28 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 22, 2020 06:12:07.056785107 CET	104.18.2.159	443	192.168.2.3	49748	CN=mailerlite.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Aug 28 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Sat Aug 28 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 22, 2020 06:12:07.058556080 CET	104.18.2.159	443	192.168.2.3	49749	CN=mailerlite.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Aug 28 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Sat Aug 28 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 22, 2020 06:12:07.112881899 CET	192.0.76.3	443	192.168.2.3	49751	CN=*.wp.com 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 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Tue Jul 05 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031 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=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		
Nov 22, 2020 06:12:07.112921000 CET	192.0.76.3	443	192.168.2.3	49750	CN=*.wp.com 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 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Tue Jul 05 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031 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=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		
Nov 22, 2020 06:12:08.928440094 CET	35.190.63.234	443	192.168.2.3	49756	CN=events.apester.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Oct 20 07:39:18 CEST 2020 Thu Mar 17 17:40:46 CET 2016	Mon Jan 18 06:39:18 CET 2021 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 22, 2020 06:12:08.928565025 CET	35.190.63.234	443	192.168.2.3	49757	CN=events.apester.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Oct 20 07:39:18 CEST 2020 Thu Mar 17 17:40:46 CET 2016	Mon Jan 18 06:39:18 CET 2021 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Nov 22, 2020 06:12:09.081449032 CET	172.67.156.77	443	192.168.2.3	49760	CN=searchiq.co, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jul 02 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Fri Jul 02 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 22, 2020 06:12:09.105983019 CET	172.67.156.77	443	192.168.2.3	49761	CN=searchiq.co, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jul 02 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Fri Jul 02 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 22, 2020 06:12:09.197608948 CET	23.111.11.71	443	192.168.2.3	49765	CN=*.omappapi.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Mon Mar 16 17:48:27 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Wed Mar 16 17:48:27 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 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
Nov 22, 2020 06:12:09.198219061 CET	23.111.11.71	443	192.168.2.3	49764	CN=*.omappapi.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Mon Mar 16 17:48:27 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Wed Mar 16 17:48:27 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Nov 22, 2020 06:12:09.241817951 CET	172.67.156.77	443	192.168.2.3	49768	CN=searchiq.co, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jul 02 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Fri Jul 02 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 22, 2020 06:12:09.242363930 CET	172.67.156.77	443	192.168.2.3	49769	CN=searchiq.co, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jul 02 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Fri Jul 02 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 22, 2020 06:12:09.401140928 CET	104.18.53.245	443	192.168.2.3	49771	CN=searchiq.co, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jul 02 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Fri Jul 02 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 22, 2020 06:12:09.402446032 CET	104.18.53.245	443	192.168.2.3	49770	CN=searchiq.co, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jul 02 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Fri Jul 02 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 22, 2020 06:12:09.507849932 CET	13.224.102.94	443	192.168.2.3	49774	CN=api.opmnstr.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 09 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 09 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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=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		
Nov 22, 2020 06:12:09.511323929 CET	13.224.102.94	443	192.168.2.3	49775	CN=api.opmnstr.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 09 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 09 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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Nov 22, 2020 06:12:09.748271942 CET	45.61.136.49	443	192.168.2.3	49772	CN=sync.audiencepixel.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Sep 06 07:16:02 CEST 2020 Thu Mar 17 17:40:46 CET 2016	Sat Dec 05 06:16:02 CET 2020 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Nov 22, 2020 06:12:09.750237942 CET	45.61.136.49	443	192.168.2.3	49773	CN=sync.audiencepixel.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Sep 06 07:16:02 CEST 2020 Thu Mar 17 17:40:46 CET 2016	Sat Dec 05 06:16:02 CET 2020 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Nov 22, 2020 06:12:09.883539915 CET	192.0.76.3	443	192.168.2.3	49777	CN=*.wp.com 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 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Tue Jul 05 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031 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=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		
Nov 22, 2020 06:12:09.889218092 CET	192.0.76.3	443	192.168.2.3	49778	CN=*.wp.com 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 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Tue Jul 05 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031 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=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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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		
Nov 22, 2020 06:12:10.424612045 CET	35.186.220.219	443	192.168.2.3	49779	CN=renderer.apester.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Oct 26 02:56:42 CET 2020 Thu Mar 17 17:40:46 CET 2016	Sun Jan 24 02:56:42 CET 2021 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Nov 22, 2020 06:12:10.425523996 CET	35.186.220.219	443	192.168.2.3	49780	CN=renderer.apester.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Oct 26 02:56:42 CET 2020 Thu Mar 17 17:40:46 CET 2016	Sun Jan 24 02:56:42 CET 2021 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Nov 22, 2020 06:12:10.447633982 CET	172.217.23.130	443	192.168.2.3	49782	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Nov 03 08:33:42 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Jan 26 08:33:42 CET 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Code Manipulations

Statistics

Behavior

- iexplore.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 4952 Parent PID: 792

General

Start time:	06:12:04
Start date:	22/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff67c8c0000
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: 5640 Parent PID: 4952

General

Start time:	06:12:05
Start date:	22/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4952 CREDAT:17410 /prefetch:2
Imagebase:	0x910000
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

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

Analysis Process: iexplore.exe PID: 7896 Parent PID: 4952

General

Start time:	06:12:55
Start date:	22/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4952 CREDAT:82962 /prefetch:2
Imagebase:	0x910000
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

Analysis Process: iexplore.exe PID: 8024 Parent PID: 4952

General

Start time:	06:12:58
Start date:	22/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4952 CREDAT:17424 /prefetch:2
Imagebase:	0x910000
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

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

Analysis Process: iexplore.exe PID: 8152 Parent PID: 4952

General

Start time:	06:13:01
Start date:	22/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4952 CREDAT:82970 /prefetch:2
Imagebase:	0x910000
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

Disassembly