ID: 344203
Cookbook: browseurl.jbs
Time: 09:07:54
Date: 26/01/2021
Version: 31.0.0 Emerald

Table of Contents

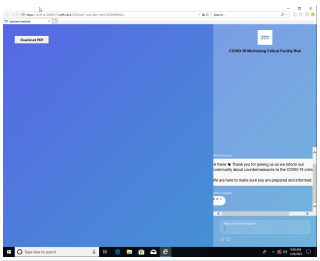
Analysis Report https://tinyurl.com/Uptime-Covid19

Overview

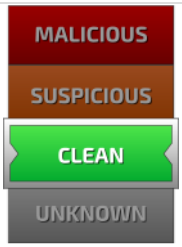
General Information

Sample URL:	http://https://tinyurl.com/Uptime-Covid19
Analysis ID:	344203

Most interesting Screenshot:



Detection

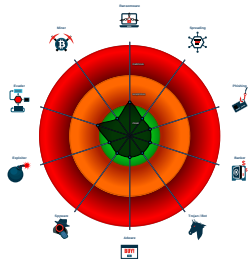


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 4952 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4720 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4952 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - AcroRd32.exe (PID: 6604 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\COVID-19_v4.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
    - AcroRd32.exe (PID: 6680 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\COVID-19_v4.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
    - RdrCEF.exe (PID: 7036 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
      - RdrCEF.exe (PID: 6204 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1704,5597326268629714092,5294744840436624648,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=11483793060652442055 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=11483793060652442055 --renderer-client-id=2 --mojo-platform-channel-handle=1716 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
      - RdrCEF.exe (PID: 1328 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1704,5597326268629714092,5294744840436624648,131072 --disable-features=VizDisplayCompositor --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --lang=en-US --gpu-preference s=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=18152290393966851700 --mojo-platform-channel-handle=1736 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
      - RdrCEF.exe (PID: 5804 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1704,5597326268629714092,5294744840436624648,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=16145082219574015218 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=16145082219574015218 --renderer-client-id=4 --mojo-platform-channel-handle=1848 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
      - RdrCEF.exe (PID: 1012 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1704,5597326268629714092,5294744840436624648,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=6472226303739352892 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=6472226303739352892 --renderer-client-id=5 --mojo-platform-channel-handle=2180 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
- **cleanup**

Malware Configuration

No configs have been found

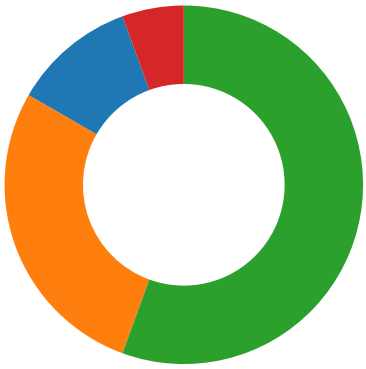
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



- Compliance
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection

Click to jump to signature section

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

Compliance:

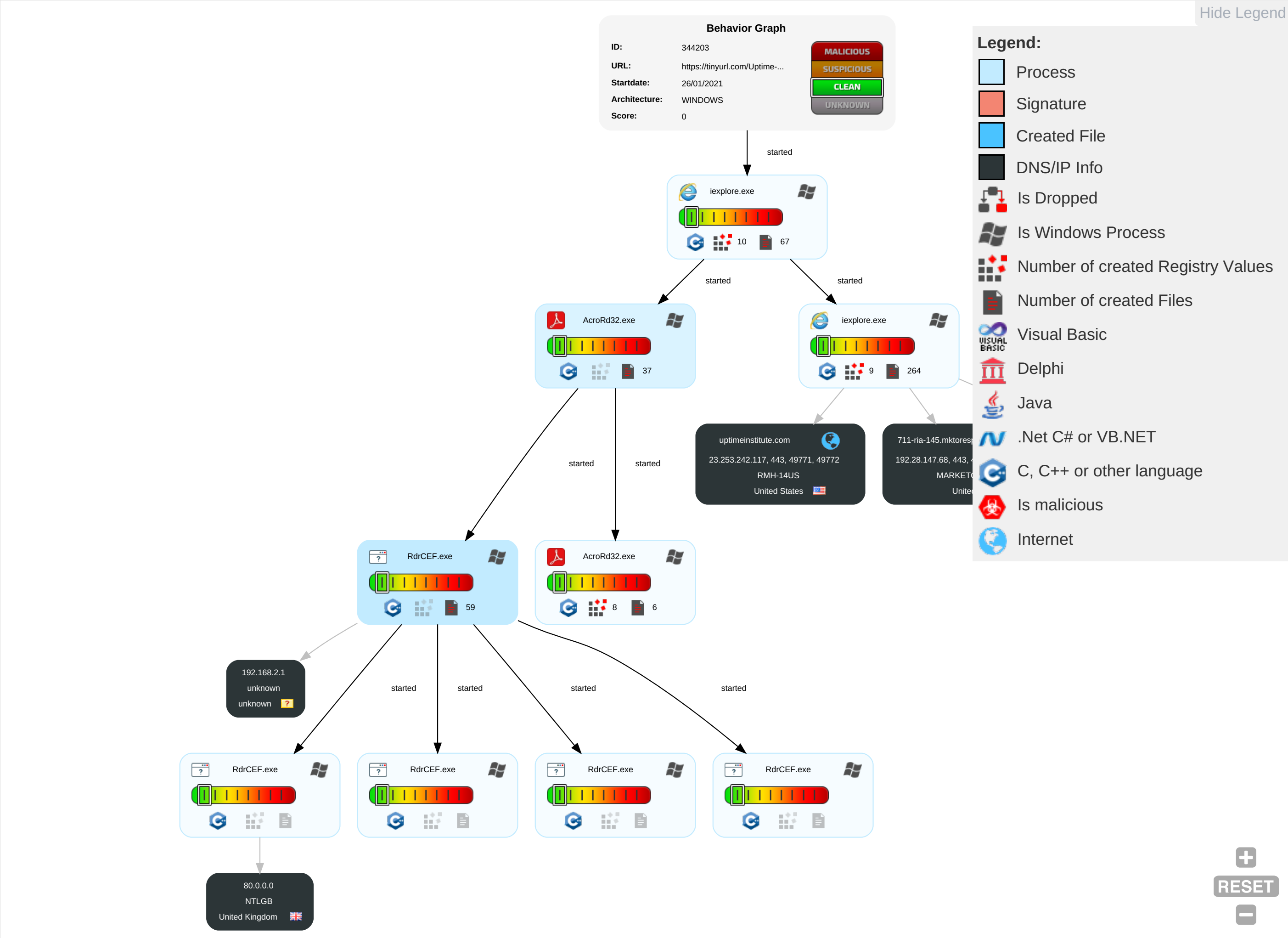
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impac
Valid Accounts	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	Modif Syste Partiti
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	Devic Lockc
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	Delet Devic Data

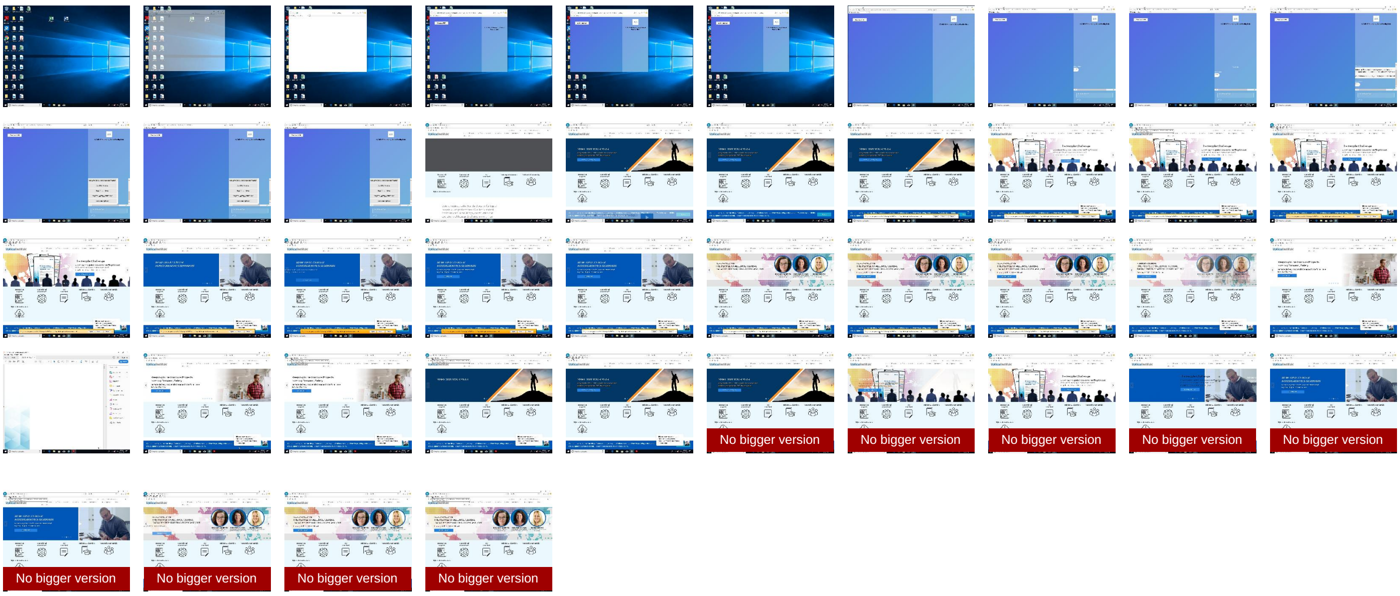
Behavior Graph

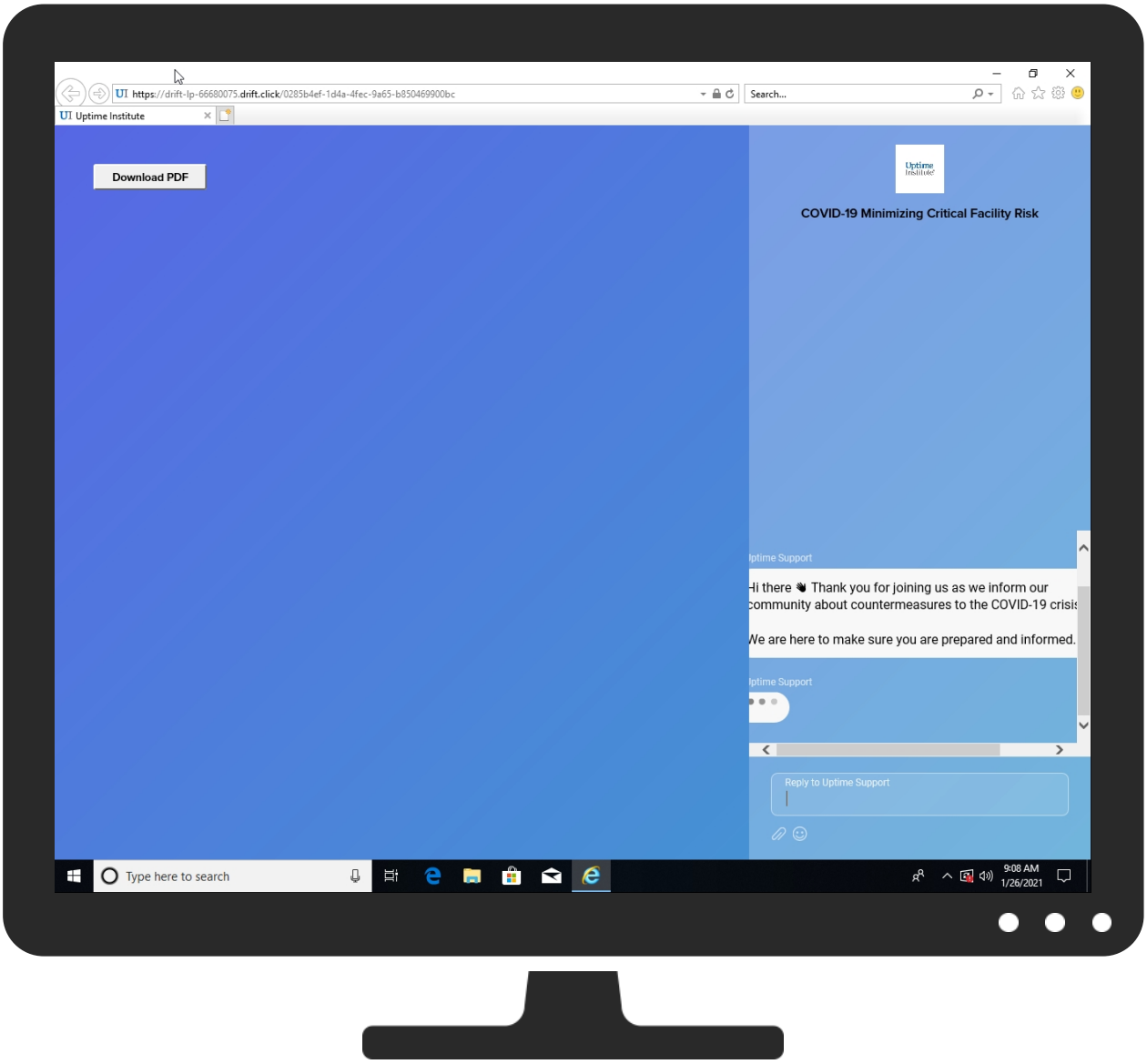


Screenshots

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://tinyurl.com/Uptime-Covid19	0%	Virustotal		Browse
http://https://tinyurl.com/Uptime-Covid19	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
dualstack.com.imgix.map.fastly.net	0%	Virustotal		Browse
drift-lp-66680075.drift.click	0%	Virustotal		Browse
embeds.driftcdn.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://bnjmnt4n.now.sh/	0%	Avira URL Cloud	safe	
http://cameronspear.com/blog/bootstrap-dropdown-on-hover-plugin/	0%	Avira URL Cloud	safe	
http://https://uptimeinstitut075.drift.click/0285b4ef-1d4a-4fec-9a65-b850469900bc	0%	Avira URL Cloud	safe	
http://https://raw.githubusercontent.com/stefanpenner/es6-promise/master/LICENSE	0%	Avira URL Cloud	safe	
http://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://www.marksimonson.comProxima	0%	Avira URL Cloud	safe	
http://https://uptimeinstitute.cRoot	0%	Avira URL Cloud	safe	
http://labs.skinkers.com/touchSwipe/	0%	URL Reputation	safe	
http://labs.skinkers.com/touchSwipe/	0%	URL Reputation	safe	
http://labs.skinkers.com/touchSwipe/	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	Avira URL Cloud	safe	
http://ejohn.org/	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://www.missioncriticalmagazine.com/articles/93441-predictions	0%	Avira URL Cloud	safe	
http://https://drift-lp-66680075.drift.click/0285b4ef-1d4a-4fec-9a65-b850469900bcRoot	0%	Avira URL Cloud	safe	
http://https://www.digitalcreed.in/mumbai-power-failure-datacenters/	0%	Avira URL Cloud	safe	
http://brm.io/jquery-match-height/	0%	URL Reputation	safe	
http://brm.io/jquery-match-height/	0%	URL Reputation	safe	
http://brm.io/jquery-match-height/	0%	URL Reputation	safe	
http://vodkabears.github.io/vide/	0%	Avira URL Cloud	safe	
http://daneden.me/animate	0%	URL Reputation	safe	
http://daneden.me/animate	0%	URL Reputation	safe	
http://daneden.me/animate	0%	URL Reputation	safe	
http://https://mths.be/mit	0%	URL Reputation	safe	
http://https://mths.be/mit	0%	URL Reputation	safe	
http://https://mths.be/mit	0%	URL Reputation	safe	
http://https://coronavirustechhandbook.com/%E2%80%AC)	0%	Avira URL Cloud	safe	
http://https://mths.be/platform	0%	URL Reputation	safe	
http://https://mths.be/platform	0%	URL Reputation	safe	
http://https://mths.be/platform	0%	URL Reputation	safe	
http://www.joelambert.co.uk/flux	0%	Avira URL Cloud	safe	
http://https://drift-lp-e.com/t.click/0285b4ef-1d4a-4fec-9a65-b850469900bcRoot	0%	Avira URL Cloud	safe	
http://https://drift-lp-66680075.drift.click/0285b4ef-1d4a-4fec-9a65-b850469900bc)	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
alb-event-1454785217.us-east-1.elb.amazonaws.com	18.205.49.143	true	false		high
afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com	54.147.21.139	true	false		high
ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com	54.84.154.238	true	false		high
d2201ucog3v8ee.cloudfront.net	13.226.159.87	true	false		high
dl7g9llrghqi1.cloudfront.net	13.224.94.49	true	false		high
a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com	54.85.240.191	true	false		high
scontent.xx.fbcdn.net	185.60.216.19	true	false		high
okt.to	34.200.97.200	true	false		high
s3.amazonaws.com	52.216.137.118	true	false		high
s3-1-w.amazonaws.com	52.216.26.196	true	false		high
prod-east-stats-tap-alb-627711272.us-east-1.elb.amazonaws.com	52.0.1.164	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
dualstack.com.imgix.map.fastly.net	151.101.14.208	true	false	• 0%, Virustotal, Browse	unknown
d21prwqavi0i2.cloudfront.net	13.224.94.89	true	false		high
prod-east-pipedream-alb-988701200.us-east-1.elb.amazonaws.com	35.173.77.57	true	false		high
tinyurl.com	104.20.139.65	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
drift-lp-66680075.drift.click	52.20.141.124	true	false	• 0%, Virustotal, Browse	unknown
stats.l.doubleclick.net	108.177.15.154	true	false		high
a4d6c1c8368a911ea98860aeb4e6dc37-182063218.us-east-1.elb.amazonaws.com	34.198.102.54	true	false		high
targeting.api.drift.com	100.24.186.63	true	false		high
uptimeinstitute.com	23.253.242.117	true	false		high
embeds.driftcdn.com	13.224.94.26	true	false	• 0%, Virustotal, Browse	unknown
711-ria-145.mktoresp.com	192.28.147.68	true	false		unknown
www.google.co.uk	172.217.22.227	true	false		unknown
pop-efr5.mix.linkedin.com	185.63.145.5	true	false		high
fast.wistia.com	unknown	unknown	false		high
presence.api.drift.com	unknown	unknown	false		high
metrics.api.drift.com	unknown	unknown	false		high
embedwistia-a.akamaihd.net	unknown	unknown	false		high
file2.api.drift.com	unknown	unknown	false		high
static.oktopost.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
js.driftt.com	unknown	unknown	false		high
customer.api.drift.com	unknown	unknown	false		high
event.api.drift.com	unknown	unknown	false		high
107326-26.chat.api.drift.com	unknown	unknown	false		high
fg8vvsvnieiv3ej16jby.litix.io	unknown	unknown	false		unknown
distillery.wistia.com	unknown	unknown	false		high
conversation.api.drift.com	unknown	unknown	false		high
messaging.api.drift.com	unknown	unknown	false		high
www.linkedin.com	unknown	unknown	false		high
cdn.leadmanagerfx.com	unknown	unknown	false		unknown
connect.facebook.net	unknown	unknown	false		high
px.ads.linkedin.com	unknown	unknown	false		high
munchkin.marketo.net	unknown	unknown	false		unknown
drift-prod-file-uploads.s3.amazonaws.com	unknown	unknown	false		high
snap.licdn.com	unknown	unknown	false		high
pipedream.wistia.com	unknown	unknown	false		high
driftt.imgix.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://drift-lp-66680075.drift.click/0285b4ef-1d4a-4fec-9a65-b850469900bc	false		unknown

URLs from Memory and Binaries

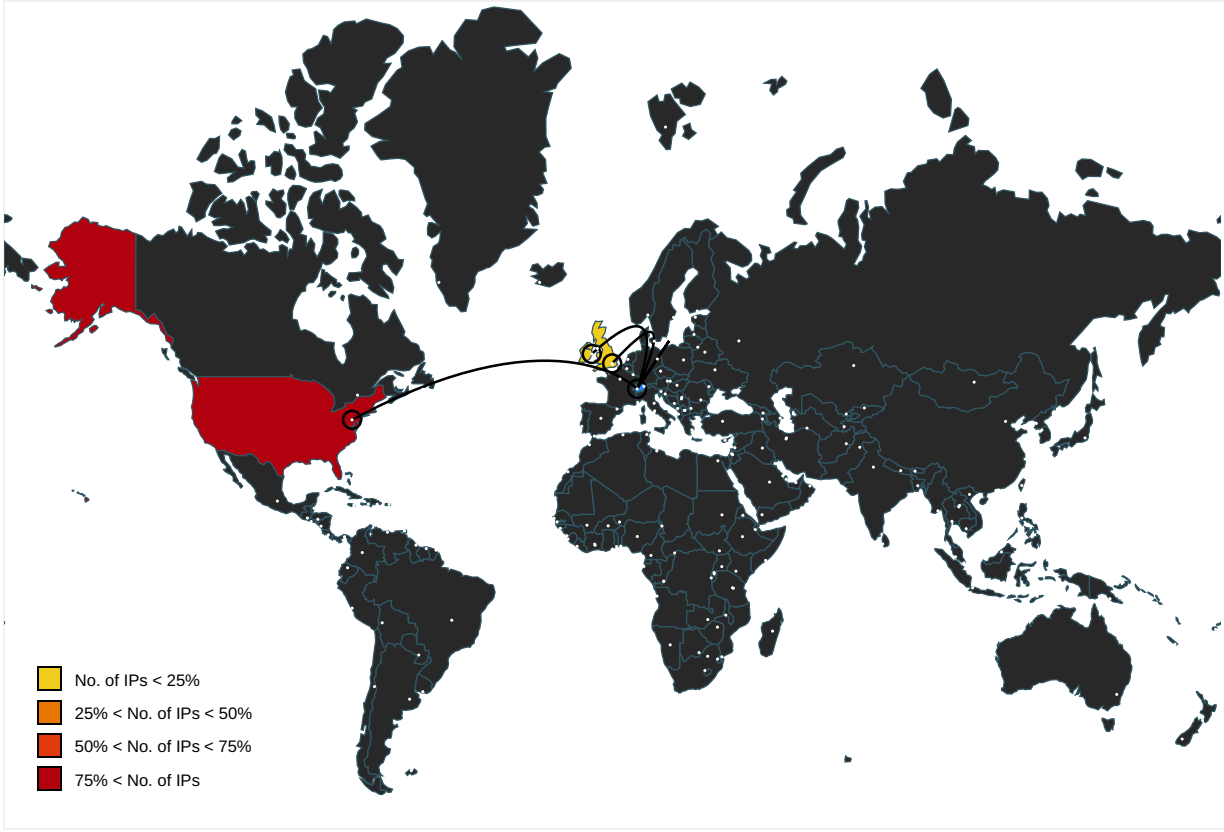
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://osvaldas.info/drop-down-navigation-responsive-and-touch-friendly	main[1].js.2.dr	false		high
http://https://ru.uptimeinstitute.com/	DK8VEZ04.htm.2.dr	false		high
http://https://js.driftt.com/v1-include/	0285b4ef-1d4a-4fec-9a65-b850469900bc[1].htm.2.dr	false		high
http://fontawesome.io	fontawesome-webfont[1].eot.2.dr, font-awesome.min[1].css.2.dr	false		high
http://https://www.osha.gov/SLTC/covid-19/controlprevention.html#health)	COVID-19_v4[1].pdf.2.dr	false		high
http://www.opensource.org/licenses/MIT)	d5329677e6dd65ffc03192ef1cf31c48[1].js.2.dr	false		high
http://https://bnjmnt4n.now.sh/	m4f3yi9k9dbi[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://insidetrack.uptimeinstitute.com/member/collection/show/27960)	COVID-19_v4[1].pdf.2.dr	false		high
http://github.com/rstacruz/jquery.transit	d5329677e6dd65ffc03192ef1cf31c48[1].js.2.dr	false		high
http://https://uptimeinstitute.com/education/course-details/advanced-seminars	DK8VEZ04.htm.2.dr	false		high
http://https://uptimeinstitute.com/t.click/0285b4ef-1d4a-4fec-9a65-b850469900bcZ	~DFF84D0E94BA24769C.TMP.1.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/normalize/3.0.3/normalize.min.css	index[1].htm.2.dr	false		high
http://https://www.linkedin.com/company/uptime-institute/)	COVID-19_v4[1].pdf.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://uptimeinstitute.com/component/search/?id=1519&Itemid=101&format=opensearch	DK8VEZ04.htm.2.dr	false		high
http://cameronspear.com/blog/bootstrap-dropdown-on-hover-plugin/	bootstrap-hover-dropdown[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://px.ads.linkedin.com/collect?	insight.min[1].js.2.dr	false		high
http://https://uptimeinstitut075.drift.click/0285b4ef-1d4a-4fec-9a65-b850469900bc	{22E7D53B-5FF9-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://www.opensource.org/licenses/mit-license.php	d5329677e6dd65ffc03192ef1cf31c48[1].js.2.dr	false		high
http://https://raw.githubusercontent.com/stefanpenner/es6-promise/master/LICENSE	vendors-widget-8f96283c571fdb07659e[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://api.jquery.com/jQuery.cssHooks/)	d5329677e6dd65ffc03192ef1cf31c48[1].js.2.dr	false		high
http://https://www.datacenterdynamics.com/en/opinions/thunder-lightning-or-rain/	DK8VEZ04.htm.2.dr	false		high
http://https://caniuse.com/#search=webp	popover[1].js.2.dr	false		high
http://code.jquery.com/jquery-1.6.4.js	popover[1].js.2.dr	false		high
http://getbootstrap.com/javascript/#tooltip	sppagebuilder[1].js.2.dr	false		high
http://https://connect.facebook.net/en_US/fbevents.js	DK8VEZ04.htm.2.dr	false		high
http://www.gnu.org/licenses/gpl-2.0.html	sppagebuilder[1].js.2.dr, pagebuilder[1].css.2.dr, jcemediabox[1].js.2.dr	false		high
http://www.videolan.org/x264.html	4e036e6e141330cf88cc4402a61e3db52123c795[1].dat.2.dr	false		high
http://getbootstrap.com)	bootstrap.min[1].js.2.dr	false	• Avira URL Cloud: safe	low
http://https://github.com/krux/postscribe/blob/master/LICENSE.	gtm[1].js.2.dr	false		high
http://https://uptimeinstitute.com/media/nextend/cache/image/static/77daa3621ab63c2664627229d1a726b9.jpg	DK8VEZ04.htm.2.dr	false		high
http://www.marksimonson.comProxima	proxima-nova-semibold[1].otf.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.yootheme.com/license)	spotlight[1].js.2.dr	false		high
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.2.dr	false		high
http://jquery.com/)	d5329677e6dd65ffc03192ef1cf31c48[1].js.2.dr	false		high
http://https://file2.api.drift.com/drift-prod-file-uploads/889c%2F889c981fd965d1400b1535b0557c725e/COVID19%	0285b4ef-1d4a-4fec-9a65-b850469900bc[1].htm.2.dr	false		high
http://goo.gl/nK90K	d5329677e6dd65ffc03192ef1cf31c48[1].js.2.dr	false		high
http://https://insidetrack.uptimeinstitute.com	DK8VEZ04.htm.2.dr	false		high
http://https://uptimeinstitute.cRoot	{22E7D53B-5FF9-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/nickpettit/glide	animate.min[1].css.2.dr	false		high
http://https://embed-ssl.wistia.com/deliveries/c7702482e79cb95b283fc1efb7f1a99c7c9169b4.bin	nkiia6prcu[1].js.2.dr	false		high
http://https://file2.api.drift.com/download/drift-prod-file-uploads/2dd4%2F2dd4a6b5a75b5a801fa24c140180767f	0285b4ef-1d4a-4fec-9a65-b850469900bc[1].htm.2.dr	false		high
http://https://embed-ssl.wistia.com/deliveries/4e036e6e141330cf88cc4402a61e3db52123c795.bin	nkiia6prcu[1].js.2.dr	false		high
http://https://embed-ssl.wistia.com/flash/embed_player_v2.0.swf?2017-04-20	nkiia6prcu[1].js.2.dr	false		high
http://https://embed-ssl.wistia.com/deliveries/44abfc80e3f2688c2dbae317df9605466f8b7fe1.bin	nkiia6prcu[1].js.2.dr	false		high
http://labs.skinkers.com/touchSwipe/	d5329677e6dd65ffc03192ef1cf31c48[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://embed-ssl.wistia.com/deliveries/047d5c34ecef8e7e3578f3c6777d21ce81277c14.bin	nkiia6prcu[1].js.2.dr	false		high
http://dimsemenov.com/plugins/magnific-popup/	jquery.magnific-popup.min[1].js.2.dr	false		high
http://www.modernizr.com/)	sppagebuilder[1].js.2.dr	false		high
http://https://uptimeinstitute.com/images/favicon.ico~	imagestore.dat.2.dr	false		high
http://https://uptimeinstitute.com/media/nextend/cache/js/static/d5329677e6dd65ffc03192ef1cf31c48.js	DK8VEZ04.htm.2.dr	false		high
http://remysharp.com/2009/01/26/element-in-view-event-plugin/	sppagebuilder[1].js.2.dr	false		high
http://https://cct.google/taggy/agent.js	gtm[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.joomlacontenteditor.net	jcemediabox[1].js.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://ejohn.org/	d5329677e6dd65ffc03192ef1cf31c48[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://getbootstrap.com/javascript/#tabs	sppagebuilder[1].js.2.dr	false		high
http://https://twitter.com/uptimeinstitute	DK8VEZ04.htm.2.dr	false		high
http://https://file2.api.drift.com/download/drift-prod-file-uploads/5196%2F5196981c981726679226106175 87ce7e	0285b4ef-1d4a-4fec-9a65-b850469900bc[1].htm.2.dr	false		high
http://https://developers.marketo.com/MunchkinLicense.pdf	munchkin[1].js.2.dr	false		high
http://https://www.google.%/ads/ga-audiences	analytics[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://uptimeinstitute.com/t.click/0285b4ef-1d4a-4fec-9a65-b850469900bc469900bc	~DFF84D0E94BA24769C.TMP.1.dr	false		high
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	sppagebuilder[1].js.2.dr	false		high
http://https://developer.mozilla.org/en/CSS/CSS_transitions#Properties_that_can_be_animated	d5329677e6dd65ffc03192ef1cf31c48[1].js.2.dr	false		high
http://https://www.missioncriticalmagazine.com/articles/93441-predictions	DK8VEZ04.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.cdc.gov/coronavirus/2019-nCoV/index.html)	COVID-19_v4[1].pdf.2.dr	false		high
http://https://journal.uptimeinstitute.com	DK8VEZ04.htm.2.dr	false		high
http://https://uptimeinstitute.com/t.click/0285b4ef-1d4a-4fec-9a65-b850469900bc	~DFF84D0E94BA24769C.TMP.1.dr	false		high
http://www.joomshaper.com	sppagebuilder[1].js.2.dr, pagebuilder[1].css.2.dr	false		high
http://https://drift-lp-66680075.drift.click/0285b4ef-1d4a-4fec-9a65-b850469900bcRoot	{22E7D53B-5FF9-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://uptimeinstitute.com/media/nextend/cache/image/static/48afb8ca794f3b445e3dff4a8890c3a3.jpg	DK8VEZ04.htm.2.dr	false		high
http://https://insidetrack.uptimeinstitute.com/member/dashboard/member)	COVID-19_v4[1].pdf.2.dr	false		high
http://https://uptimeinstitute.com/privacy-policy	DK8VEZ04.htm.2.dr	false		high
http://plugins.jquery.com/project/touchSwipe	d5329677e6dd65ffc03192ef1cf31c48[1].js.2.dr	false		high
http://https://www.digitalcreed.in/mumbai-power-failure-datacenters/	DK8VEZ04.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://github.com/zuk/jquery.inview/	sppagebuilder[1].js.2.dr	false		high
http://https://github.com/mattbryson/TouchSwipe-Jquery-Plugin	d5329677e6dd65ffc03192ef1cf31c48[1].js.2.dr	false		high
http://getbootstrap.com/javascript/#collapse	sppagebuilder[1].js.2.dr	false		high
http://brm.io/jquery-match-height/	matchheight[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://datacenter.uptimeinstitute.com/2021-staffing-report.html	DK8VEZ04.htm.2.dr	false		high
http://https://www.datacenterdynamics.com/en/opinions/climate-change-skepticism-data-center/	DK8VEZ04.htm.2.dr	false		high
http://getbootstrap.com/javascript/#transitions	sppagebuilder[1].js.2.dr	false		high
http://https://github.com/joelhy)	d5329677e6dd65ffc03192ef1cf31c48[1].js.2.dr	false		high
http://vodkabears.github.io/vide/	sppagebuilder[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://uptimeinstitute.com/ui-intelligence)	COVID-19_v4[1].pdf.2.dr	false		high
http://daneden.me/animate	animate.min[1].css.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://mths.be/mit	m4f3yi9k9dbi[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://modernizr.com/download/#-fontface-backgroundsize-borderimage-borderradius-boxshadow-flexbox-h	modernizr[1].js.2.dr	false		high
http://https://js.driftt.com/deploy/assets/index.html	~DFF84D0E94BA24769C.TMP.1.dr	false		high
http://https://drift-lp-66680075.drift.click/0285b4ef-1d4a-4fec-9a65-b850469900bc	~DFF84D0E94BA24769C.TMP.1.dr	false		unknown
http://https://coronavirustechhandbook.com/%E2%80%AC)	COVID-19_v4[1].pdf.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://mths.be/platform	m4f3yi9k9dbi[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.joelambert.co.uk/flux	d5329677e6dd65ffc03192ef1cf31c48[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://embed-ssl.wistia.com/deliveries/97976ebd7d9da4aeda87dd23de414403ae22021c.bin	nkiia6prcu[1].js.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://drift-lp-e.com/t.click/0285b4ef-1d4a-4fec-9a65-b850469900bcRoot	{22E7D53B-5FF9-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://blog.alexmaccaw.com/css-transitions	sppagebuilder[1].js.2.dr	false		high
http://https://github.com/pixelcog/parallax.js/blob/master/LICENSE)	parallax.min[1].js.2.dr	false		high
http://https://drift-lp-66680075.drift.click/0285b4ef-1d4a-4fec-9a65-b850469900bc)	COVID-19_v4[1].pdf.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://embed-ssl.wistia.com/deliveries/df52710d015b2d5dd19fde48151d963f66a7d206.bin	nkiia6prcu[1].js.2.dr	false		high
http://https://github.com/CWSpear/bootstrap-hover-dropdown/issues/55	bootstrap-hover-dropdown[1].js.2.dr	false		high
http://davidwalsh.name/detecting-google-chrome-javascript	d5329677e6dd65ffc03192ef1cf31c48[1].js.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.177.15.154	unknown	United States		15169	GOOGLEUS	false
54.84.154.238	unknown	United States		14618	AMAZON-AESUS	false
34.198.102.54	unknown	United States		14618	AMAZON-AESUS	false
50.16.7.188	unknown	United States		14618	AMAZON-AESUS	false
54.147.21.139	unknown	United States		14618	AMAZON-AESUS	false
192.28.147.68	unknown	United States		53580	MARKETOUS	false
52.216.137.118	unknown	United States		16509	AMAZON-02US	false
23.253.242.117	unknown	United States		33070	RMH-14US	false
52.20.141.124	unknown	United States		14618	AMAZON-AESUS	false
52.216.26.196	unknown	United States		16509	AMAZON-02US	false
52.0.1.164	unknown	United States		14618	AMAZON-AESUS	false
80.0.0.0	unknown	United Kingdom		5089	NTLGB	false
18.205.49.143	unknown	United States		14618	AMAZON-AESUS	false
35.173.77.57	unknown	United States		14618	AMAZON-AESUS	false
34.200.97.200	unknown	United States		14618	AMAZON-AESUS	false
185.63.145.5	unknown	United States		14413	LINKEDINUS	false
104.20.139.65	unknown	United States		13335	CLOUDFLARENETUS	false
13.224.94.26	unknown	United States		16509	AMAZON-02US	false
54.85.240.191	unknown	United States		14618	AMAZON-AESUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.224.94.49	unknown	United States		16509	AMAZON-02US	false
185.60.216.19	unknown	Ireland		32934	FACEBOOKUS	false
151.101.14.208	unknown	United States		54113	FASTLYUS	false
100.24.186.63	unknown	United States		14618	AMAZON-AESUS	false
13.224.94.89	unknown	United States		16509	AMAZON-02US	false
13.226.159.87	unknown	United States		16509	AMAZON-02US	false
172.217.22.227	unknown	United States		15169	GOOGLEUS	false
104.16.19.94	unknown	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344203
Start date:	26.01.2021
Start time:	09:07:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://tinyurl.com/Uptime-Covid19
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:	32
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:	clean0.win@17/265@34/28
EGA Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://uptimeinstitute.com/ • Browsing link: https://file2.api.drift.com/download/drift-prod-file-uploads/5196%2F5196981c98172667922610617587ce7e/COVID-19_v4.pdf?mimeType=application%2Fpdf

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.83.120.32, 13.88.21.125, 216.58.207.136, 216.58.207.142, 172.217.23.68, 172.217.23.74, 216.58.207.131, 40.88.32.150, 104.42.151.234, 151.101.2.110, 151.101.66.110, 151.101.130.110, 151.101.194.110, 92.122.144.104, 2.21.60.250, 13.107.42.14, 152.199.19.161, 95.101.22.211, 95.101.22.235, 92.122.144.200, 72.247.178.8, 72.247.178.11, 40.126.31.139, 40.126.31.141, 40.126.31.8, 20.190.159.138, 40.126.31.143, 40.126.31.4, 40.126.31.6, 20.190.159.134, 51.104.139.180, 95.101.22.216, 95.101.22.224, 92.122.146.26, 23.55.110.54, 23.55.110.79, 20.54.26.129, 51.104.144.132 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, a168.g2.akamai.net, arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, e10776.b.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, acroipm2.adobe.com, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, l-0005.l-msedge.net, login.live.com, a122.dscd.akamai.net, audownload.windowsupdate.nsatc.net, www.google.com, dualstack.f4.shared.global.fastly.net, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, www.google-analytics.com, fonts.googleapis.com, fs.microsoft.com, acroipm2.adobe.com.edgesuite.net, ris-prod.trafficmanager.net, www.tm.a.prd.aadg.akadns.net, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, blobcollector.events.data.trafficmanager.net, cs9.wpc.v0cdn.net, au.download.windowsupdate.com.edgesuite.net, e4578.dscb.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wildcard.marketo.net.edgekey.net, arc.msn.com, e9706.dscg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, www.googletagmanager.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www-linkedin-com.l-0005.l-msedge.net, www-google-analytics.l.google.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, www-googletagmanager.l.google.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, login.msa.msidentity.com, armmf.adobe.com, wildcard.licdn.com.edgekey.net, go.microsoft.com.edgekey.net, embedwistia-a.akamaihd.net.edgesuite.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:09:57	API Interceptor	7x Sleep call for process: RdrCEF.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\05349744be1ad4ad_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	410
Entropy (8bit):	5.604035508344572
Encrypted:	false
SSDEEP:	6:men9YOFLvEWdM9Qxi7Z+P41TK6tJHen9YOFLvEWdM9QyNKi7Z+P41TK6ti:vDRM9JZiEfEDRM9x7ZiE
MD5:	93469E98C0CAA2CE750B44AB686DC1C8
SHA1:	B1A3D7BD9E0A64A87607D194AF5DBFADDFC44414
SHA-256:	3D4598616CD0F4FC1E4729806D7CF88BD5836F1DE35B2F814286C8093D9C2BF7
SHA-512:	3D22B4AF19327DDBCFC101121F8525FE9C20160539BE4FEBF3E8B44DF51C2A767B851A6FC8BEE480D2E8B5CB691CA5B21A744C0E52B8D82DCCBC1D179F955 47
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .....g./....."#.D.e.=...A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo..... _G.A.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ...A.g./....."#.D.PV?...A....d.{v.^.G...d.W.:...P..k%..A..Eo..... .A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	522
Entropy (8bit):	5.579414688513426
Encrypted:	false
SSDEEP:	6:mi9NqEYOFLvEk3oyZF8Be7Ywcr1TK6tDi9NqEYOFLvEkuPUF8Be7Ywcr1TK6tyiB:V9zXDF9PQs9zOPUF9PQr9zIRF9PQ
MD5:	E8FBF6B025F3FE74B4E1A3C53658DA47
SHA1:	6EE1601F9EB2DAABDA30DA09249FFC4AE0D24562
SHA-256:	CB3AB405EE002D95ECF00575F523329D0412890E25611255457D651C79DF07CC
SHA-512:	EFA0F772632156D42F4BF057941BEB21EE3C7F610EDE8FB774368826B59C25D82BF646F2AC790124B42D724244172F464BA88EFE4DDEDC5C5EBFAE6E64F08D2 F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0	
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .lt4.g./....."#.D.4.:...A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....=.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .....g./....."#.D.+.=...A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....t..<.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ... .g./....."#.D/..>...A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	492
Entropy (8bit):	5.597685159372404
Encrypted:	false
SSDEEP:	12:DyeRVFAFjVFAFcW/G0lUo6j9yeRVFAFjVFAF2flUo6j9:tB4v4c4G0SBTB4v4WSB
MD5:	44B03FB89CE5B3CA32A111168FCF871D
SHA1:	CD592870DC47BD8DDB9D0339A253E9F420095488
SHA-256:	895C904F5786EC12582EFDCC622CB4B2640FB04B9B845FF4A53F4B60E5737F24
SHA-512:	FD2A73FC2ADB1C0279B490FD20CEB48AF7439B38CEF553AECA2E253663F28E3920C0A59F07172155F0164EDC1A01778738EFFCABD6A3D7DAEFB47DEFACD718E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js .....g./....."#.Do-.=...A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....%[.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ...?.g./....."#.D>#I?...A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....} .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0ace9ee3d914a5c0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.633750191297938
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5RsqVll26wHiWulHyA1TK6t:IbRkiDl/wCWuss
MD5:	E454ABF93A4648BE6728648B56049D84
SHA1:	97B83A93A42358DD804DA381C79ED28F6A6C3530
SHA-256:	7830AE29FA441456B6108D03DDD199A16F5F292D5816C716D3AECD83C57B99D4
SHA-512:	80317A4D44E4FD5BA7F14B706E836028B88E7C3021CCC2BCBC118232161027B32741376558946B5846C0314571EFF116CCA50FAD60DA671B2A187EA0E585BA42
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js .....g./....."#.D..L>...A..8 P..a...R..Y....7.@..2Dm{..A..Eo.....A..Eo.....7}Y.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.549774243016546
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVuKa67VVyh9PT41TK6t6H:pyixRueZV41TE
MD5:	63A4920224DE697D85859FB534D70306
SHA1:	C2684F3B706160E39DC4DCB6BFDC481979BFE17D
SHA-256:	B0E9D1B1A7726F255CBE7E49487B99159CDE0609E3222B42B7631DBC3CB781D3
SHA-512:	3C5E0172E6D0769F01FA7A1E504494B6BBA7594AFC447A4B4F2260CB29338034E2F155E15E4C130DD4456DF8859FF186BB1061CB1CCF77B30B09BF01AB4692B1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ...?.g./....."#.D..I?...Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo.....G.8.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.559671877146129
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
SSDEEP:	6:mvYOFLvEWdhwjQHoqB22NLZIl6P41TK6tLy9:0RhkzMLZCc
MD5:	8320AE47B85EB000CB711C42B70EA0CB
SHA1:	58AA3949043F4AE2E93101AF9C909F1EB0CD2F9F
SHA-256:	77C20B3FDCA1C9EE813A6E388212D19319BF4F5B37880243EB36046E9AC540E1
SHA-512:	223C0D69FEBC2CC4F74DD6C79C05303501B5A1D929AA7B35DD31D6ACBAF487C90E2E65B3BCBF56D702667D9DF59464DA4831168E1E39043C178CAA3B0493D 25
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ..I7.g./....."#.D...?...A.].>....uUf..N...k.....c..l.A..Eo.....A ..Eo.....c.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	209
Entropy (8bit):	5.51420094053031
Encrypted:	false
SSDEEP:	3:m+lZd8RzYOCGLvHkWBGKuKjXKX7KoQRA/KVdKLuV73KVtwEwcyxMtv9EWm1TK5kS:mJYOFLvEWdGQRQOdQg56g1TK6tIt
MD5:	E011E29BA386906F620BF7EC7CE0DF22
SHA1:	FA1DE105D0E94802E78CC5230526AFCBF489D711
SHA-256:	553211D5F2760171F0F02DC03DD103E942F30C48E2C2A5EC28371DF44C501E2C
SHA-512:	7A2091550C6D59E87F07BD016B7BD2AB152199B619EE6A8FE48ACC1C4F777334B281A7AB4A2EC96540A211A9FFC33F8B915DF8F8A0555991B2DF14D0DC527C6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ..DA.g./....."#.D.*J?...A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo .....9.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2a426f11fd8ebe18_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	537
Entropy (8bit):	5.603383907465128
Encrypted:	false
SSDEEP:	12:Z5MyMuR/ENE/J5MtUMuR/El5MdgwMuR/E:ZSruR/E6JSnuR/ElSduuR/E
MD5:	9F75D12D6E3367B720A9D1C8332CE882
SHA1:	2F9A16D2E6C76966D00586E9BF16FA754EFF6F1C
SHA-256:	41FC795D21A1DFFBBA487013F260FD53AAFED2AED394208335F6A878F61E4FDE
SHA-512:	874751E62E8EE2DC5153FCCD409323663F25F75772EF7F98786243C38F2120F1F0A3D9AB69D6C724E89803985D3429ECDB49C145AAC8C78C85D8F5BFF57156CI
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ...4.g./....."#.D(H.:...A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....q.....0\r..m.....3.... <lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .%D..g./....."#.D.D.=...A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....9.....0\r..m.....3....<lb.. ._keyhttps://rna-resource.acrobat.com/base_uris.js ... .g./....."#.D.>...A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....Z+.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.472568413518983
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtuiSvHMby0zBUKSAA1TK6tC1:pRPSEbek
MD5:	963BC71458D24404B2F70B5D06A1A511
SHA1:	8A95BEFA900DE9AC1454DA1995143C51A6AC6A44
SHA-256:	FAB30D9B31C76DB18D5315E6A697115E8EF8AD56C9E9AA9FD68AB22BE6D81911
SHA-512:	91EE2C5AA1E001D6BB7C4CC46B97C15932E002C9FF8E677F9C4472C0776B6E83A9279CF831D4F969A4E313416BC0288F07DF96816404AE29A0A249049EE51F0I
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js .c.B.g./....."#.D.tJ?...AQ..E.=....=h`t..t..3%A.F$..w..A..Eo..... .....A..Eo.....a.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	531
Entropy (8bit):	5.526908802181351
Encrypted:	false
SSDEEP:	12:KkXxKMSCvxwvtUlekXxKMSCv5vtUlaokXxKMSCvVVvtUl:KkXxiCJcWekXxiC5WRkXxiCd9W
MD5:	E8B08267483FCF063C1CF54AAD8D0E5E
SHA1:	A3B6272EF85FF11B0061218AD269B837EC1F6EAA
SHA-256:	EBB2624B59ED96A478490D3FEA7D1C654A8B15D1E938922225DE164D37F37270
SHA-512:	491D3A67D03D1E890F1D51C6567365D4E60BBCF8716826BDA75C0CD4B3781FFB99E042840F6CC2786AED9A80CA2950051F03B1938465AAA537346EFE99405DE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ...4.g./....."#.D.A.:...A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....0\r..m.....1.....5... ._keyhttps://rna-resource.acrobat.com/plugins.js ..A..g./....."#.D.=.=...A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....t.....0\r..m.....1.....5..._keyhttps://rna-resource.acrobat.com/plugins.js .b. .g./....."#.D^..>...A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....X.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	374
Entropy (8bit):	5.60193898526398
Encrypted:	false
SSDEEP:	6:mkl9YOFLvEWsfOLL+dWGJyM+VY1TK6t6l2kl9YOFLvEWsfOLpnDyM+VY1TK6t:5h6OLL+8dkCh6OLpyk
MD5:	416C347A520B6885FBDF9BC42718FD6D
SHA1:	9BEABA18F3D27B698946DD715C74947E9EBB49BE
SHA-256:	ED78FD44C9726DAB22C3265A6A38041281EB325578CDDFBC988347D96DFA2F38
SHA-512:	9C3260C11CC556A4C33F7A735F1A92A24FA8504C6D24BC13657CC565B05B374B872E8E839EBD5C792BA6F2F64FB34B7833CFA426937A164639C5CCC095650261
Malicious:	false
Reputation:	low
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ..V..g./....."#.D...=...A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....Y.....0\r..m.....;.. .I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ..j2.g./....."#.D...>...A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	488
Entropy (8bit):	5.630680371378419
Encrypted:	false
SSDEEP:	12:URVFAFjVFAFtwSeKaTLnlRVFAFjVFAF+kj1wSeKaTLn:UB4v4twzXLnlB4v431wzXLn
MD5:	04810FF3A275701468CA66781962B26C
SHA1:	3F652C9658A0ACC93FE7436B0B3D565F83BB9150
SHA-256:	8BC2EE9368A50F8BC36165FF77EFE57E29E6D242100495A3F2C97CF27FA8FC53
SHA-512:	B856B463A1D70FD8E487D775FCB6DFA3780F967615ECBE442C0166DDF534A9A92B11DC562810B2A2D55791AF51895F254FA2AF31EE578672516FD180C2DAB62
Malicious:	false
Reputation:	low
Preview:	0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js ..V..g./....."#.DQ..>...A.....H...{...2. ./.k`..r4.C. .A..Eo.....A..Eo.....0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js .d=A.g./....."#.D..X?...A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....*.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.489987671334711
Encrypted:	false
SSDEEP:	3:m+lx4F08RzYOCGLvHkWBGKuKjXKGBIEGdevA/KPWFvfzw2hxuArpYFm1TK5ktCNl:ms2VYOFLvEWdvBIEGdeXu1T511TK6te
MD5:	99D65572264FDBAFA5570D6B82283F51
SHA1:	83E17EFA86F89243DC798F5641A40CA481B6C133
SHA-256:	C236878A52BDE6BE43DAAB76DB457C10B883BA1637320CC761A43566781A9973
SHA-512:	D9A3C3643653B61B663CE0F3A939FB24868BA9E517597BBFCFA61DFB38D979AB7C040A4E02B97724444E72801998C413FA48F925043CF72FD931DD2C0C9FC8D

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .:.?.g./....."#.D.<H?...A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo .....M.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.637960236514771
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQaCs4B7OhKlvA1TK6t:RbR16xCs4BJk
MD5:	33EF62F61C1B399489FA373A87D4E2D4
SHA1:	034260A8283039604B242469815BE04F126B81E5
SHA-256:	C9706FCE97D766793613A7BCA3F933FCBC36D1A555FCCA47396A82651905945E
SHA-512:	FCE199036DB36808F46A143B499EA477DFA42FB8AEF9E7586B581FE8EEAE4C75571683B552AEFE2E25943379E0918E4F0B7EDFB5458A5A761610877CEC770092
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ..17.g./....."#.D...?...A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....z.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.5503279552961295
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVuKU2SQdFt1TK6t:B2geRHRQ/U2S0
MD5:	7A5209578F2B1A3CB2F91A61D34721F8
SHA1:	8D01C701789DCEA6102ED896C718449490E8D6BF
SHA-256:	ECB8E714D7268093A1E19ED20D8AEFC4F71EE3F1F0E16D9C1A35CB0EC7CCC169
SHA-512:	813DF176621273EE9163C3F3E2FD5E1EF87B6D3EAAB0B168A5572C125BF9E4491C471C323F51261DB00E67EE8E99C2730162588143DCC9E107A9D177B06A9745
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ..?.g./....."#.D.1H?...A@..{o]...9o|..qY....T....{..u.b..A..Eo..... .....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	412
Entropy (8bit):	5.622249445019874
Encrypted:	false
SSDEEP:	6:mzyEYOFLvEWdrIOQYvMyt1S/1TK6tKMzyEYOFLvEWdrIOQYd5t1S/1TK6t5:WyeRlbvRt1wwEyeRlhd5t1w3
MD5:	D22ED59E344335CDCF1CD0C2883DEF1E
SHA1:	7241A35A059D660BEA80578ECC2A786C8DD1FB50
SHA-256:	393B2AD6B511338059383558E72F9C3316E76F7A5CF1B989F832786F59FFE27E
SHA-512:	F56D8169A1BEDBB177C4C1EBDDEF18BE37D8DC67217DECA5E3AC40F8739823FF03E5CA0FA47D95426BFF438CD20D93C516F95161D04070C2D5523448B88CC AF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..1..g./....."#.D.!.=...A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.... ...w.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...3.g./....."#.Di5.>...A.t\a.....x5.'OuE.C..@.....x..A..Eo..... .....A..Eo.....@x9.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.521553208259348

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0	
Encrypted:	false
SSDEEP:	6:mnYOFLvEWdhwyuv94Zh+rqwK+41TK6td:wRhYGyGwK+Ej
MD5:	3B1D43CB60F40BB9B9D692E808839F31
SHA1:	D69452ABF78945794EB8B065DC295CBE239D3C72
SHA-256:	DD4F54BAC1EAB9B030359F4DE6D0707CB3EF9A47AA55FB16CFF63FFF38F5D911
SHA-512:	3ECDD56F1DED7D020D5507A4FF2DAB79AD6DDC18BEAAD34F20AB20E000DBCBE110C590FDFD9CC0D4AD210E62CBAD08AEBDB3220976F2C1EF782DA011D35 83908
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ..-7.g./....."#.De..?...A.....7...o..a=.98I.....(3.$G.A..Eo..... ...A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	460
Entropy (8bit):	5.601879849557567
Encrypted:	false
SSDEEP:	6:mYXYOFLvEWdrROk/RJbu2WwfO441TK6t8HeYXYOFLvEWdrROk/RJbu1ofO441TKE:/RrROk/hVfLECXRrROk/xfLEt
MD5:	833B3889FAF3C853D1458E2B16294F23
SHA1:	47B555594CD0A1332677BEE23A65E06439A063BF
SHA-256:	C89656C9ADC24581BD19E5849E4FC2A71E0F69D7209248712234C2E4434B73FB
SHA-512:	190101FD85E0113C5BCAAA07A88CDB3A73EFF85CFFB16B51115B82714D02D3164230BCB81C28F76591195E9D4A0119A917AB6D0C82B0BD6697008F18771889D9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .[...g./....."#.D...=...A..~..rw.+[....!.)?..f.U..(=.=.A..Eo..... .....A..Eo.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .V.3.g./....."#.D...>...A..~..rw.+ [....!.)?..f.U..(=.=.A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.623704669983878
Encrypted:	false
SSDEEP:	6:mmDEYOFLvEWXIkYiS1QPLr1TK6t3sr+mDEYOFLvEWXIDQynS1QPLr1TK6t:xqT+xCPLn9KZqTiQJCPLn
MD5:	6C65BF6D1A081D7170DE48A0BA0EDF16
SHA1:	017298BB0AAA2EEFA50BE909E95CD6F7AD079A84
SHA-256:	7BC6CD74737110BA57960C83A2127A5B54D0A7E786A917C5251415274EC21B7B
SHA-512:	F123EC7ED84FBAAA248DCE34656521693968B9BBCADE998F3C757DBEA18124219516EDC541E3C2DCD16B0BE66D850E88257582352A9111C186DA34E0B33DB5 2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .},..g./....."#.DK..=...A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....BIN.....0\r..m.....:. ...f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ..U2.g./....."#.D*..>...A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....R.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	414
Entropy (8bit):	5.632279580937359
Encrypted:	false
SSDEEP:	6:m52YOFLvEWdMAujC9QhAsEJ41TK6t8/E52YOFLvEWdMAuZbLsEJ41TK6tH:zRMkmAsDSBRM3sDd
MD5:	5DE139AA3BB59070BD8DD57EBA240865
SHA1:	DD4043E212D8CB8B498CF892BAA874F593A78BFF
SHA-256:	3ABBCB30240003EDE2A320859AA88D51FB39B20F936AD076AC4FA6BC6467B820
SHA-512:	1102E9FBE94B04813F0B19353C62191DDF2E0B9542A2D5491363E7A25D81787D3D1BA169948346572F36ADC65A3D9C3D966A7948C4DBA4E99424B1F1C131DF84
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0	
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .~...g./....."#.Dn..=...A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....:.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ...?.g./....."#.D.iH?...A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....P.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	420
Entropy (8bit):	5.582362659972082
Encrypted:	false
SSDEEP:	6:mYilPYOFLvEWd8CAdAuw2Fong1TK6tQYilPYOFLvEWd8CAdAu0V89zY2Fong1TK+:6lJRV2FoMSlJRZk02FoM
MD5:	1F7DA103B9C99A1836220D78012DF192
SHA1:	CC88EE2FA4F3A0D2DD54F98D4C86F5B980E17FB0
SHA-256:	9AE43B0B08B3F26DEA67DBADDE11D225C5BCA0C8FE4565F6D75B086BEF87DE4E
SHA-512:	31660227B9688A1439A77327A4758C425AD44674125265DF39FFAB79B7A94BFA55B6E80A703A055ED040E554C7F2412F640BC9B4BAE27253BE49ADDEF423C284
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .i...g./....."#.D...=...Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....5.....0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ...?.g./....."#.D0.I?...Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....,zjH.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	446
Entropy (8bit):	5.595023783217551
Encrypted:	false
SSDEEP:	6:mY8nYOFLvEWdrROk/Ius9YVPOe16wG1TK6tiJY8nYOFLvEWdrROk/IuVwiPOe16v:F8hRrROk/e9YV2e2n8hRrROk/Ii2e2X
MD5:	602404B6EE699F7793EA83B52E0811DA
SHA1:	A297C8961BDA4E3EFDCD1BC6B08DAADF9AA47F15
SHA-256:	05118A8A5D5A83491C4FF7E7436633E09E229BB23C7DBE4DE784A21E19D55E28
SHA-512:	E1BD48443EDE0E04F84E9B5B3222BABC9E5F3941460702775704451E79199C44B1BE28875466385B1CED7ADA27DCD74197CA3FFB5112F270E02A5B573FE7778D
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .F...g./....."#.D...=...A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....-|).....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ...3.g./....."#.Db..>...A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....%L&/.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	426
Entropy (8bit):	5.650297518300655
Encrypted:	false
SSDEEP:	6:mLrnYOFLvEWdrIoJUQzPLqirNJIi1TK6tJeLrnYOFLvEWdrIoJUQGrNJIi1TK6tR:ehRc4L/rNJIC3GhRcXrNJIC
MD5:	EF51A486D8B4D692154AAD6CD6039902
SHA1:	185F08D644ED7FAD0CAA8A5C95FDD577E2F6C7D4
SHA-256:	CCA6AB437D4002B5EBF02002DE6790D2AC70EDE6C60C528642A4EED7705FED69
SHA-512:	DCB28120D2023E59BC3335DFB3A16D1620DFCF7067008E8F3E2356E017E0E2953DD5E928C5D133C98CDAB55EC599C3ADC1CA9653022B43AE8BBFD484654A97B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .kf..g./....."#.D;T.=...A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....W.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ...3.g./....."#.D.`.>...A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....YM3.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	416

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0	
Entropy (8bit):	5.614959206803588
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhu3qZLzgm2d/1TK6td/l2OEYOFLvEWdrIhu8efpZLzgm2d/1TK+:0RNeReb/KRm4Re
MD5:	450F4A81859CC00076ED0E71FCAA086B
SHA1:	7AA75C27E5F5CED0FEE1D442A1C221B12B515BF6
SHA-256:	C81EC43E32298A915947C05A689E98F21D395BE3ED0A62EF6FF9427BA672F337
SHA-512:	2C44D0FB5240CC2FF9D0F02A1747E335F28FD98EE1227CAD3CB133B676810FA6DB4B2CA10B9CD41BEDC256718C99F62E1228045E0EA0A8C6292FFDA1AE13AE9C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .8...g./....."#.DG..=...AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....j.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .BH3.g./....."#.D...>...AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....WVO.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	564
Entropy (8bit):	5.63170160530403
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1KuF2kx56uvp1TK6tUAElVYOFLvEW1KS/2kx56uvp1TK6tdP9/Ef:6JJKun+JJKGjP9/YJJKJd8
MD5:	4D908FECCAEF144D945ABEEC0DC57B82
SHA1:	47E52DF40A24B7217A1727677DEE66834C22C238
SHA-256:	575BCAAA5B4AFA8CF4AB3449E6D5E0B845C529DE15F2B1317557378B756BF21A
SHA-512:	102D8F60FB55512E9D5FA005DFB59AFC83F28DCC513B954818B5C2776F22DF765ACA5EFD5EEAE83E8814A5F93E20A0218B4B925F6EE836EE25884F94C697F85
Malicious:	false
Reputation:	low
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .B.7.g./....."#.DuV.:...Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....].h.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .....g./....."#.DE.=...Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....\.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...%.g./....."#.D...>...Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....vu.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.597687260428077
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvuDsaHD7ihUDLYtmOZn1TK6tI:xRBJAsoDcFZLu
MD5:	CCC82D0CD2ACDCCC26FD44E949802CD3
SHA1:	0449693EF3F5C211F04C9EFAF593E7C3526FA8EB
SHA-256:	141B6AF49E26216CF3C123FA7377A1A1FD14F2DFEFFC1575353C1ABB2441773E
SHA-512:	99D2D819C03C133173EC1ABF30E497AE39DEA6084D6675353CDD77B8782EA5EC0C1DAACD81F177136F8A4F0D5338CAE7970AB47AAA7544A69283182255EE27A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ...?.g./....."#.DjPH?...A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....,.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	633
Entropy (8bit):	5.615776146892911
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp7NWFH9aVPu1TK6t448sRPYOFLvEWIa7zp771aVPu1TK6tEHm:BPHCFH9acFPH11acCZPH59U12ac
MD5:	623B551CCE83CB2719DBE2A2FE90925E
SHA1:	175373AA584A9A923DC33E774AC3D785CE593B71
SHA-256:	0BE40C9B65509EA810C9D203796911A4FB224C09D2B6536C2F2B55A6D5B01EB1
SHA-512:	7BF2720ACA1DFFF3239C9E07842B2B96C33BAB1EC39752B73BF946A838A7242788D568CC03F75B09CF228DE8DD3BA6780A1F072B1DBDE000E160EADDB9167E6
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0	
Reputation:	low
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .}.4.g./....."#.D.t.:...A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....*.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .tF..g./....."#.DPn.=...A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....h.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ... .g./....."#.D..>...A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....0.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.563960851854798
Encrypted:	false
SSDEEP:	6:mKPYOFLvEWdENU9QTg+k9JwiM3Y1TK6ts:bJRT9J9er0a
MD5:	8EC2A03814242B4C96F7FED899962003
SHA1:	43934E24ADB155F68D817554A7F8A3DFF18D04C4
SHA-256:	42AD359C54C40045A549A284074EE6A631539E78B8E72AD363A1458EB4AE1802
SHA-512:	3F565442F183EB80BE556B2DD9CE62AFC391BDB23EE10727D6DD2C9919A0F7EEF794ACCDA58AC356F2656092CBFD68FD0A2D9E72BFD79652601085D206BEF5C2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ..47.g./....."#.D...?...A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo.....Dh.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	modified
Size (bytes):	208
Entropy (8bit):	5.54473008262403
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQ9x2ljBRCh/41TK6tFk:XRc9EwDi/EM
MD5:	E9893DF44EA25B33292FEFFD61FC8F91
SHA1:	9CCDE6A6526D9859F0CB86D9C2F52EE616DBDB2D
SHA-256:	7F2FE5521F57EEE183DE3BB85B7570B244F682065BC9A707F13ABCE99CE58681
SHA-512:	BA5AF54BDBABF470CDB72F1DC35EE8791B5B46A24AD55FC3317E6285CFFF7F01FC3AA48FEAD4327364FE79D82369525263587C074BA27C04A4697F457066B3A5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .6@A.g./....."#.D..^?...APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.....A..Eo.....A.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.588729506706953
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhudjCoW8dAuVULlF4r1TK6t:bs6xRkibCoBAu2LlF4n
MD5:	2F896D5C46426BAB032B15C22BA0CB30
SHA1:	DF207C3BFDD4054A1AE17EB795215069066AB089
SHA-256:	7767FF14E9CD804107AB7552C12140525F0D2B1D1349421E44C0D343DA3285D3
SHA-512:	473BA5EA0EB203789C8E2313792146F9B6F567C358C8D01F078F7E36F8B2AAD76FF27CB8D5E7A92030629D8F0366AD0B6C9BEB536EA33E0F75943775BF029E08
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .....g./....."#.D...=...A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....H.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	215

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0	
Entropy (8bit):	5.493748412121961
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFvS+ZD9kiVCcu1isLK5m1TK5ktoCl:mhYOFLvEWd/aFuo+XN941TK6tx
MD5:	AD2245EC147F8582F359D5CE9003AB02
SHA1:	5C244924736FA155143532F25FBC5C27BDA87F77
SHA-256:	9EDBD432D4512CD9473A6319271FC998F529C98D2C61588FEF032030A2D219ED
SHA-512:	EF8DCCACC0CBA0EC96CE8285BFED3365F7BE241EB7EEBFE419B33D9312E7CE88FEE794EAA16765387E6315BE789D5C92BD850220F8F0D91820DF5A507C880 2F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js .Y,C.g./....."#.D..J?...A...a.f.m.i.o.p..3U5....^...I.A..Eo.....A ..Eo.....^.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.489372831135057
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQt+7xaGXoBMqVd3G4K41TK6taN:2DRuRHNDYB9Vd2kYN
MD5:	4680DB88142A75A05D7E05E693EEB6B7
SHA1:	93C6F5F0D99D891DFDEECB86B3E7388145EC144C
SHA-256:	D8CADF5E9F191911C5F11EABC57A33C70FB71EB2175D7C1973C431833550A3A6
SHA-512:	527E73B0876EE83F444A6EAAA521704CC62C9D13F46C1B4F89A27F400A0403A0D486E8C11DB7A97BB805DEB7C50CF250E2614167DB27B711B5F003217733E836
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ..nB.g./....."#.D.\J?...A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.. ...../.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.607826076163463
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9QDvMOuA424r1TK6tLMkqYOFLvEWd8CAd9QM+KwG1OuA424rt:+RQkMBrnx8RQBnBrnJ/
MD5:	4F3C372B5CC0FE323ECC28BE0197F79E
SHA1:	93BAD2263C4046AAB5D22EB10F3C743AFD815B84
SHA-256:	8B6F73B1BF742A76C5D3FBCB36D757FF2738F42E5E793725F2FFA1F84DEB4BC1
SHA-512:	EBB459FBA1020039AA8A8AC5D218AB275FDB756A5B8E289DD25C62B71BB4E685CB231E83B3949439638A7CADBBF5D22F7E497E9ECC67AD01C315CA0487C89E 60
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...gT...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .....g./....."#.D.U.>...A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo... .....0\r..m.....P...gT...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ..IB.g./....."#.D.!_?...A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo..... .....A..Eo.....C.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.519596472614944
Encrypted:	false
SSDEEP:	3:m+lS5Etla8RzYOCGLvHkWBGKuKjXKVRNUp/KPWFvBTmvD9wIbg2iHio/Mm1TK5kP:moXXYOFLvEWdENUAuYJyC8n1TK6tD9
MD5:	11249E571232CCAE4DA6CA60BB76496D
SHA1:	167A7BFCCDB772E0875475B1A43174B607074DB3
SHA-256:	F576C2F17A7E4BC989C7D8A41A779CF031D1D245E41B2BBA0E4D2E6D76FE6420
SHA-512:	1AFC171A6BCEEC9A6CF7F2A08819B8B90A73031965D73EC5102C178081E89DCCCCE1ED000FBED6A0BF5A47208824C1956076E6878D418336172D190937A52F1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0	
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ..{6.g./....."#.D?n.?...A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....Z.{l.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	442
Entropy (8bit):	5.630631250868618
Encrypted:	false
SSDEEP:	6:mQZYOFLvEWdrROk/VQpTCo22hksLmB41TK6tOQZYOFLvEWdrROk/VQJW1olhdSS9:nRrROk/VGO7XNm5RrROk/VaDluSNm
MD5:	767CBAA7953E41F1E5CB0C66D35E162C
SHA1:	E12628441AD6CE0E605D79D0CFFCA815CF83D5F5
SHA-256:	35FF5F16569617A623299A89A8AD9A561E03CDE5FA97B8458062D846F3079CF2
SHA-512:	EB40C681A1AFE9C892CF375D5F31AAB6D63C686086BBDC9DEF116C0CC4FDF8487C58FCF08CC40B585F6A3046CB2BEF63CE6E8D58FD2E1EFCA6393B11C38A2A3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....].....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .....g./....."#.DMe.=...A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....>.....0\r..m.....].....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ...3.g./....."#.D.~.>...A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....+.w.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.562705778281698
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWuKwHkyjAdm9741TK6t:qxRctHkyjAdu7E
MD5:	85EE38470D4391F096E8782719CB8FC7
SHA1:	8F2090E2D78C3B11288465BCAE3F5C96C88445F1
SHA-256:	6B1C54E68727FB27B0E38D2F0AD418152B8F4571277469CA7AC676ECDD5F8EA3
SHA-512:	78770E1A2DCC1B3449C5D3423D90507C1F8CC1C2D0F302C3F4141C7288C031EC793BB7ADC5FFDB4AC2A19389C654BA07116E0ED213B9175CDAC1C937C9C40F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ...?.g./....."#.D.AI?...A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....8..5.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.530408987750352
Encrypted:	false
SSDEEP:	3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFvZbp6shoq+Nem1TK5ktabt:mMOYOFLvEWdwAPVulJn1TK6t
MD5:	70C9F5346465435D233F7F4ACBF12BE4
SHA1:	C3409F9BCF53B2F0CC24D0B96E712B39E4284B68
SHA-256:	9A38489255D9FD7D7FADA1FE557E913616141070698FA8481FB8B700FFE09F81
SHA-512:	B4B1E7324AD8F12DF6CE4A8618BE455627DC302A22A032A1547584587697785 85FFB442776E8BFECAD05B1480C195F416D58DF3022B4273A4A2F9C1F6E2FA4F3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L....Ey...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ..w6.g./....."#.DeQ.?...A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo.....o.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.61456007677364
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0	
SSDEEP:	6:m3PXYOFLvEWdBJvYQrtl799zhcsBXIh1TK6tm:mxRBJQi99DB0
MD5:	B01570280C69515B5223E2632855AE3F
SHA1:	F14AB6ECA6F0FA0D2D8FBEF579C7B6244BD0CD6E
SHA-256:	478C87AFF717B0B9020F72450077B0DA7888D4FA65ED4E111EBBEC29C5850803
SHA-512:	FBAF5408722062ABB28D54C0E16EEF9C3719363540A689DE20474B8B8601A0457C47E8BFFE8588F5572C1BFC11A2790DF0BEE90BD3CE853A5342F92E11DA147
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ..GA.g./....."#.D..U?...A...k..`..N3.... ..d..$[....{.A..Eo.....A..E o.....^.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	456
Entropy (8bit):	5.56367882422481
Encrypted:	false
SSDEEP:	6:msPYOFLvEWdrROk/RJUQD0jHMc3Me/1TK6tosPYOFLvEWdrROk/RJUQtk7fc3Mee:3RrROk/sFMcjRrROk/s+kcfy
MD5:	CA577A68C8FFE40EA07680A36A19C88B
SHA1:	731EE0FE9B6E76C97BC7C17748F5DAB5D10EFB6F
SHA-256:	3472AD44ED4D1ECE712A852FE8A523891A9B76E0D19502F0B315B69DA8405CD3
SHA-512:	34FF6D689DF36D65027E46CDEF486B4F84CC9AF88C2B754A6B9CD6F7E187B40A35EB21616B6FB770034B169DE1E8838E4651A8196CEBAAA9E608D6C3CFC293 9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .....g./....."#.D.\.=...A.....9Q].8O.z....=..:.N.{....N{.A..Eo..... .....A..Eo.....yp.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .=.3.g./....."#.D...>...A..... 9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	2016
Entropy (8bit):	5.3247325061810065
Encrypted:	false
SSDEEP:	24:Mfg1zZFufGMisp6r6C9QPwh/p04ALMk6pqa+utmWKwEWn:h1zZ4+dsp6bh/ph0P6pZmyVn
MD5:	C03505BE9786C96E6DA30B093E10D1D8
SHA1:	35F673CCB869369FC5541CB8F8A9EA0B6CBD062A
SHA-256:	B228E562FFB923E5EB6C21BCFE312D1FA50DF452726ABB3A0092950D781EE787
SHA-512:	27A5042B4CFF359DACC687E41083990E6B81EFA657C8413F4227651616FD9D37DA0004F5C4C21B5C9946BCA4ABBEEB067EC8AB5C85F21643049A733497D9CA0
Malicious:	false
Reputation:	low
Preview:	....h...oy retne....'.....'.....;.y~A..z.B_./.....*...z.B_./.....oB*.8.B_./.....#...(...A_./.....k7A..z.B_./.....D.4..z.B_./.....[.i..%..z.B_./.....<...W..J.8.B_./ .....,+..._.#.z.B_./.....J..j....z.B_./.....6<|....8.B_./.....A?.2:...z.B_./.....+.{..'.z.B_./.....*)....J:.z.B_./.....2q....z.B_./.....P....V.z.B_./.....+.U.!..V.z.B_./..... .....P[. q.z.B_./.....!...0.o.z.B_./.....u\]..q.z.B_./.....z.B_./.....*.....z.B_./.....o..k...z.B_./.....^.~..z..z.B_./.....o..z.B_./.....Gy.'.h..z.B_./.....F..=z;..z. B_./.....3....z.B_./.....v...q...8.B_./.....C..M.....A_./.....a.....8.B_./.....~.,.4>..z.B_./.....&.S.....z.B_./.....@..x..z.B_./.....=....m...z.B_./.....;/....z.B_./..... .....q..z.B_./.....MV3...z.B_./.....:..N.A...z.B_./.....B_./.....ID.oy retne

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	292
Entropy (8bit):	5.203992416425946
Encrypted:	false
SSDEEP:	6:mJLH+q2PWXp+N2nKuAl9OmbnIFUtpqzcZmwPqFVNVkwOWXp+N2nKuAl9OmbjLJ:6r+vaHAahFUtpqzc/PqFVNV5fHAaSJ
MD5:	920D6BE1913D1FEEBF3A18F9EAE4D171
SHA1:	442E5FB1FA54BE04780EB65C45DE03B815EEAA1C
SHA-256:	FBE53B828021FE6E94B167D6F754CD36144FCD3FA55ACF82D97B6F48F55D3DB9
SHA-512:	E2F4F35B8033BDF700E4759DF2889140518BB1A8926E72795C1190EAF01E394BF912073323C9DF93CC2C20FF3FB619532AF52A5AC09305C1163780BA99280DCA
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG	
Preview:	2021/01/26-09:10:04.156 1bdc Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/01/26-09:10:04.157 1bdc Recovering log #3.2021/01/26-09:10:04.158 1bdc Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	917504
Entropy (8bit):	0.007775583823103001
Encrypted:	false
SSDEEP:	24:TGEXiXKGEXiXKGEXiXJ88hMXiXN8hMXiXTg8hMXiXTg8hMXiXT:TGEiaGEiaGEiCsMi9sMiDgsMiDgsMiD
MD5:	CFB315BC46FE90003DA8EBD9F4B3ADCC
SHA1:	D2CE24C0F4BC5B05A24FBE51370821160EAADF1B
SHA-256:	551AED495E031A34FDA7CD305771663B585FFAD758EFFBD8EE8B2EFE35E6DE8B
SHA-512:	D6C2C4979825630A8348BA0786A5F83020D3DF098FA6142E6237CBB61F92BBACC6012E045B8E681463F6D31ADB1985539A1AE93A255B22F7B99625A8B284612B
Malicious:	false
Reputation:	low
Preview:	VLnk.....?.....Tq.>..j..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210126170958Z-265.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 117 x -152 x 32
Category:	dropped
Size (bytes):	71190
Entropy (8bit):	2.814460721183318
Encrypted:	false
SSDEEP:	1536:fJsCfiGv/n0/KcypczcsY3ajBdcn1ga4YrUKWi:xungf3Rya4YPX
MD5:	B85D43F0E677338BDE874282E04F4E86
SHA1:	79834231C0763AD659B37EB504265C90B9B394C9
SHA-256:	F5C6324235C798836B12E1366543D0A9674491EE39F20DE61385BF3549C9BB7B
SHA-512:	051F5CF79F71E16CAC819C9A18E2DF56D17CBFF39B459C8AFE1CFC5A7A58541A576B91BF10302558305D353E44FD0BFDD263579DFFE26D306266EBB43CD1D10
Malicious:	false
Reputation:	low
Preview:	BM.....6...(...u...h..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3024000
Category:	modified
Size (bytes):	32768
Entropy (8bit):	3.3859947904115377
Encrypted:	false
SSDEEP:	96:iR49IVXEBodRBkQMOhFVCsL49IVXEBodRBkRjMOhAVCs749IVXEBodRBkljMOhh3:iGedRBsedRBSedRBledRBj
MD5:	9EA128D5B7D7E5CAD7DD7142702F983C
SHA1:	CC1B392F3CC65569B01C3F5B2EA6EB28D5F04020
SHA-256:	BA162ABA5A82D92D5121B6AAA0E3773303DC9E5F728E3CC2D2DD139D0F937353
SHA-512:	608EB496EF87A85DDD21A690A60E9DE30E680AC6AE2375CB37B5AACA9CA05FBC12D386CACEEE27CEF0B34D25EE6E7481B7709811CCCF68A0A7CB641E35FFB0A4
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....$.....1.....T...U.1.D..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	
Category:	dropped
Size (bytes):	34928
Entropy (8bit):	3.200442249881825
Encrypted:	false
SSDEEP:	96:x7OhFVCPC949IVXEBodRBkVMOhFVCswLR49IVXEBodRBkLjMOhAVCsQd49IVXEBc:xGiedRB3LGedRB8CedRBnyedRBt
MD5:	116790D0FD9101D82E420B384ADB71E6
SHA1:	5F4EF42290463F09112B158583CFEBF393816E4E
SHA-256:	736C1B3634D49C0B5555EC15FAD23BC4289B3E5A455C073CCA23F35DF437B224
SHA-512:	8100A257966B14AE44601447F8140AF620061B5E4EF052672147FA919B595CAD003E6BD3BDA5ECB84B93D3D835C504894868F207F595BB37D0ED2A43C2A38D95
Malicious:	false
Reputation:	low
Preview:	.....'..... .....X.. .h...y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\AS0DF7C1\drift-lp-66680075.drift[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):	18692
Entropy (8bit):	4.955879949952378
Encrypted:	false
SSDEEP:	96:pRnRKnRKfnRKfRKf6hRKf6PRKf6PRKf6WARKf6WRKf6W0RKf6W0OZRKf6W0ORRKN:k
MD5:	1147D54B3929586AA320D77C9020D59A
SHA1:	46659C24CF73530329109021453AE943EF9F7E48
SHA-256:	CEC758FA94AE0FB2FBF5F93756058FA27F2E8C542F6E251A890D87C8B7FEA63B
SHA-512:	02CC9DE109471BE84EB79E6599CAC32502FADD76087357EA167CF7084ED7E9455667685FD29B082265ADD2B9B5E6D9D4EADE40F9012C8A2A2FA4572369B03CE 1
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root><item name="Drift.Targeting.firstVisit" value="1611680931" ltime="3949957856" htime="30864389" /></root><root><item name="Drift.Targeting.firstVisit" value="1611680931" ltime="3949957856" htime="30864389" /><item name="testKey" value="testKey" ltime="3949957856" htime="30864389" /></root><root><item name="Drift.Targeting.firstVisit" value="1611680931" ltime="3949957856" htime="30864389" /><item name="Drift.Targeting.lastVisit" value="1611680931" ltime="3949957856" htime="30864389" /><item name="testKey" value="testKey" ltime="3949957856" htime="30864389" /></root><root><item name="Drift.Targeting.firstVisit" value="1611680931" ltime="3949957856" htime="30864389" /><item name="Drift.Targeting.lastVisit" value="1611680931" ltime="3949957856" htime="30864389" /><item name="Drift.Targeting.currentPageViewStarted" value="1611680931" ltime="3949957856" htime="30864389" /><item name="testKey" value="testKey" ltime="3949957856" htime="30864389" /></root><root><i

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\JN2WT4O2\uptimeinstitute[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):	28778
Entropy (8bit):	5.123590926347279
Encrypted:	false
SSDEEP:	192:yyrR6GDRzImBByB511BBBvqKqKy0gmt/6+mtZ:yyrR6GDRzImBByB511BBBvqKqKFhW
MD5:	D5EBBA29A98225885C3238C37EB22D65
SHA1:	7E1616CEF8295D340288D845D4F8D5846AFE6A6E
SHA-256:	796FE63AA8016CEF22C30160B2ECE492E224C2BD3EED93042D82A65C0D3E8217
SHA-512:	8CA918EBA80816F4367A92B72036421C881F66DDBE6699F479C19E44986B4BA08C1B1B30F2B94F6135906858FC23107BBEA44AECB5CD4A373EB56C0C0B28EB6 E
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root></root><root><item name="undefined" value="null" ltime="4121337856" htime="30864389" /></root><root><item name="undefined" value="null" ltime="4121337856" htime="30864389" /><item name="loglevel" value="WARN" ltime="4143807856" htime="30864389" /></root><root><item name="undefined" value="null" ltime="4121337856" htime="30864389" /><item name="loglevel" value="WARN" ltime="4143807856" htime="30864389" /><item name="wistia" value="{"__distillery":"bd47369_3f054f44-c4b6-4fa8-b2d5-f4208891cec8-4864b8c72-54e409052dee-e117"}" ltime="4149887856" htime="30864389" /></root><root><item name="undefined" value="null" ltime="4121337856" htime="30864389" /><item name="loglevel" value="WARN" ltime="4143807856" htime="30864389" /><item name="wistia" value="{"__distillery":"bd47369_3f054f44-c4b6-4fa8-b2d5-f4208891cec8-4864b8c72-54e409052dee-e117"}" ltime="4149887856" htime="30864389" /><item name="Drift.Targeting.firstVisit" value

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{22E7D539-5FF9-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	36440

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{22E7D539-5FF9-11EB-90E4-ECF4BB862DED}.dat	
Entropy (8bit):	1.9013615430635444
Encrypted:	false
SSDEEP:	96:r9Z6Zr2V9WqYtqnfqVRMqYqMqtfq8Mrq9qQU:r9Z6Zr2V9W3tlfERM9V+fFMrwo
MD5:	7B0278839A74103AA42F110D8C7CA95F
SHA1:	070CC336C05DAE8D7EDD894D9F4D3A076A2D7C23
SHA-256:	B1CA6AC5D4714AAE0B7D2374D494E71BD01DE9E8DDEB24A2F4FCF345C506D484
SHA-512:	8614741627283F38CA6D034C9A4150BF70B9A35E01D24CC514A5B4112592FB26822C54F992D00361E2E77402DF13F29ECA7C6D93F5969F26415035A164045CFA
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\{22E7D53B-5FF9-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	51416
Entropy (8bit):	2.333982761750789
Encrypted:	false
SSDEEP:	384:rGyIoYh0Lgm6m35brAlAeA53TbrAlAeAGc3/z702oPGKHLEAlAbA6nXiAKHLcAlj:/XBr2x43r2xi3Lw26a286O2j
MD5:	86BBE8810019FF2737433C41298C3AD4
SHA1:	970235D5EA5838FC4EDED84E50E0776E3C5D8871
SHA-256:	BDCDAFFE3CB2AAE29225406B12030FD80B9F2008F334369D1793D3BA276C498D
SHA-512:	BA154690FD2CC3A4DD1D16F4F7F331303B3A51708AF11163C7A986AC3F592A9132388CAA670DAE2606D5A2F3508C4D8A33DDD37701BD7629F897FAD4B0DB64AC
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\{2B3A2F45-5FF9-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5654185895784114
Encrypted:	false
SSDEEP:	48:IwhGcprAGwpap7G4pQIuGrapbSxrGQpKjG7HpRasTGIpG:rXZIQpd6IgBSxFAyTa4A
MD5:	BFECD5754593AB19BC0FE1E5C75F71A9
SHA1:	65C912B934511D49BE71AB4249C5AF9473443EEB
SHA-256:	008912392E54304B718C366343D78447315E66A5A397FA17F9ADF3CA2C49F8BE
SHA-512:	460477F92F0A2B59EFD2E32C0EAA2E1D9669FAADC14ACC9AD12889804B468624440BD6DD345C46FA1DAB636503DEE78D4959C60B1F88520CFC3F4713CE2185C
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

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:	dropped
Size (bytes):	1766
Entropy (8bit):	3.7524706973000375
Encrypted:	false
SSDEEP:	24:uwD7SRgLkTGi3H/ogfQOT4nZJJJJi6sw5AVb:uwD7SRLwtOT4ni
MD5:	A81C19D710EE0F12C8F99888080D7086
SHA1:	225370C170610C5FB8D714306C6BEEF92A6744BC
SHA-256:	FB309FE6A0F4B550516A05F19CC596DE352D900E8873B1B43EE5FDBF3A4A0B37

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
SHA-512:	26EA5A5A94D9375614CE3308A49980DE9D330667FDE286041DA84BE2CE2D9D85C2E3468B573B3D6A7723AEC2D22B554A1DD235FDA4A6C8DEF26355D6182A9E7
Malicious:	false
Reputation:	low
Preview:	E.h.t.t.p.s.:./.w.w.w...g.o.o.g.l.e...c.o.m./.s.2./.f.a.v.i.c.o.n.s.?.d.o.m.a.i.n.=.h.t.t.p.s.:./.u.p.t.i.m.e.i.n.s.t.i.t.u.t.e...c.o.m.6....PNG.....IHDR.....a....sBIT....|.d.....IDAT8.c`.....~.....".Z....'=oW.....[[.....bV.g..?.....P.....*.....P.....Gd%L...ad.....Qd{ !.....Jo``..gxx.....k[...|70.0~.i.t.>....,=0"....P.pmK.....2.06....W.G.]MM.....BMc1.....IEND.B`.....L.`.....L.`.....h.t.t.p.s.:./.u.p.t.i.m.e.i.n.s.t.i.t.u.t.e...c.o.m./.i.m.a.g.e.s./.f.a.v.i.c.o.n...i.c.o.~..... .h.....(..... .... ..... [VV.[VV.[VV.[VV.[VV.....\...\..\...\...\.@.\.`.\..\.....[VV.[VV.[VV`.....\.`.\...\.....\.@.\

C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\mms\RUUXANB4\4e036e6e141330cf88cc4402a61e3db52123c795[1].dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ISO Media, MP4 Base Media v1 [IS0 14496-12:2003]
Category:	dropped
Size (bytes):	917504
Entropy (8bit):	7.682180435487432
Encrypted:	false
SSDEEP:	24576:vkLikZauDH15ffIYQsdfNrn2TXaOQsevVtu:liRuDV5ffmsd9nSXKfu
MD5:	80A90A7D22FA4269B4BA95D8B6DABF6A
SHA1:	0FF8CB4FFD25F90B694A6C3126A91D7FBBBD5C1C
SHA-256:	CBF414EB673B0389274431B816FFFC7247315A6D87760568DD3EC7015737652F
SHA-512:	3347F6475D0D028C8B841A1E28C40077C085B80C00A03FC9F13E0AA8347566CD31AC87A2FAF7157C5BBBA0C086111EBBB4B36044EDD5A2E401C8D28BEFBC5DE5
Malicious:	false
Reputation:	low
Preview:	... ftypisom....isomiso2avc1mp41...#moov...lmvhd.....@.....%trak...\tkhd.....^.....@.....$edts....elst.....^.....mdia... mdhd.....<.....-hdlr.....vide.....VideoHandler....Hminf....vmhd.....$dinf....dref.....url .....stbl....stsd.....avc1.....H...H.....2avcC.d.....gd....@..~.....<..1....h.8.....stts.....v.....stss.....,.....[.....i.....w.....+.....9.....G.....U.....c.....q.....%.....3.....A.....O.....].....k.....t.ctts.....

C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\mms\UR4L0N6Q\52284660f7abf8538f64d3f7b857f505[1].dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	0.4169828839481698
Encrypted:	false
SSDEEP:	192:rRQJ5G7RsKIUBde7QgCVUJAXv9hmz2wf:ryjG99naCVUJAXTmH
MD5:	4131F7592D7A56F6B0FB1CD230A72FDD
SHA1:	47ABCEC34E24014E2284C5BA6105029EC54ADD3E
SHA-256:	C2A0FC254BA404D549FA1AF561A4D54C58F2F1D2D09260F8EEB543E3B3FFC162
SHA-512:	E2F5903B288D6F779DE9D98158EAA51A63FF07768BA5624A2EDEE2BADDA9F83270AFB71A9BC60F3F7DA28534794DB4D4E02002534E6BBE7FE7731388866F60D5
Malicious:	false
Reputation:	low
Preview:	.....".....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\4a3c1161b81f906ccb7e41df6b548811[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	311
Entropy (8bit):	4.275710046886378
Encrypted:	false
SSDEEP:	6:tI9mc4slcLRMjDdCdqLcZJ2dqLczkdF5dFJFHFpLzKQJAt8:t4yLRMjJCdqldqaUFDFDLzW+
MD5:	4A3C1161B81F906CCB7E41DF6B548811
SHA1:	D598E9F435D6C5ACE9AAD0D2387E61836C42D2E0
SHA-256:	AC11A69407AEAAC27F7C75939B4A14A5F58B380E3EACF4C4CDDCC0973B52AE7D
SHA-512:	314F3708EAEA83D0C1EB2373E0AB499CCC406BCA446672AB0C56BD8B8352E693F808F3A24175E00DF049D105379A4C02533757296580031DE9D6019A4A5CEAB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://js.driftt.com/deploy/assets/static/images/4a3c1161b81f906ccb7e41df6b548811.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\4a3c1161b81f906ccb7e41df6b548811[1].svg	
Preview:	<svg xmlns="http://www.w3.org/2000/svg" viewBox="-389.8 299 18.8 18.8"><path d="M-385.3 316.2c-.8.8-2.1.8-3 0-.8-.8-.8-2.1 0-3l4.4-4.4-4.4-4.4c-.8-.8-.8-2.1 0-3 .8-.8 2.1-.8 3 0l4.4 4.4 4.4-4.4c.8-.8 2.1-.8 3 0 .8.8.8 2.1 0 3l-4.4 4.4 4.4 4.4c.8.8.8 2.1 0 3-.8.8-2.1.8-3 0l-4.4-4.4-4.4 4.4z" fill="#FFF"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\COVID-19_v4.pdf.xh95llp.partial	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PDF document, version 1.4
Category:	modified
Size (bytes):	493819
Entropy (8bit):	7.250711517967212
Encrypted:	false
SSDEEP:	6144:isuj94oJG5XN1VjG0Yg/y1Xy0LM1yYq9Bl92/:5ujyow5d1tYOy1CMMKz
MD5:	5196981C98172667922610617587CE7E
SHA1:	AB1CEC38D09E16639780AEA57B5712367122DB9E
SHA-256:	CCAA6475522D0CED583D5BCCD5D7EE2FC2751EBEBA689F88FAF19017AF631B1C
SHA-512:	60ECAB01566CBB63355A6605E24FB74F50E6F6A27C31585EF484A758B28F1765F5748D2BA4D742DAEB278FABB5F5026884CBDBBBEBCEA02ECE61C011E50F609B
Malicious:	false
Reputation:	low
Preview:	%PDF-1.4.%.....141 0 obj.<</Linearized 1/L 493819/O 144/E 351380/N 18/T 490878/H [8336 1604]>>.endobj. ..xref..141 402..0000000016 00000 n..0000009940 00000 n..0000010085 00000 n..0000010121 00000 n..0000014944 00000 n..0000014993 00000 n..0000015042 00000 n..0000015091 00000 n..0000015141 00000 n. .0000015191 00000 n..0000015242 00000 n..0000015293 00000 n..0000015343 00000 n..0000015393 00000 n..0000015442 00000 n..0000015491 00000 n..0000015540 00000 n..0000015590 00000 n..0000015641 00000 n..0000015691 00000 n..0000015741 00000 n..0000015791 00000 n..0000015842 00000 n..0000015892 00000 n. .0000015941 00000 n..0000015992 00000 n..0000016042 00000 n..0000016092 00000 n..0000016142 00000 n..0000016256 00000 n..0000016306 00000 n..0000016356 00000 n..0000016405 00000 n..0000016456 00000 n..0000016507 00000 n..0000016558 00000 n..0000016608 00000 n..0000016658 00000 n..0000016708 00000 n. .0000016758 00000 n..0000016807 00000 n..0000016858 00000 n..0000016908 00000 n..000001695

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\COVID-19_v4.pdf.xh95llp.partial:Zone.Identifier	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:gAWY3n:qY3n
MD5:	FBCCF14D504B7B2DBCB5A5BDA75BD93B
SHA1:	D59FC84CDD5217C6CF74785703655F78DA6B582B
SHA-256:	EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913
SHA-512:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443E8
Malicious:	false
Reputation:	low
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\COVID-19_v4.pdf:Zone.Identifier	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	very short file (no magic)
Category:	modified
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:W:W
MD5:	ECCBC87E4B5CE2FE28308FD9F2A7BAF3
SHA1:	77DE68DAECD823BABBB58EDB1C8E14D7106E83BB
SHA-256:	4E07408562BEDB8B60CE05C1DECFE3AD16B72230967DE01F640B7E4729B49FCE
SHA-512:	3BAFBF08882A2D10133093A1B8433F50563B93C14ACD05B79028EB1D1279902724145098065199450142 3A66C276AE26C43B739BC65C4E16B10C3AF6C202AEBB
Malicious:	false
Reputation:	low
Preview:	3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\KFOmCnqEu92Fr1Mu4mxM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20268, version 1.1
Category:	downloaded
Size (bytes):	20268

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\KFOmCnqEu92Fr1Mu4mxM[1].woff	
Entropy (8bit):	7.970212610239314
Encrypted:	false
SSDEEP:	384:LyfRPUY1e32pJd75q1DzPjsnouCrZsZtetWFNFfIP0clWvdzNcrm:uJPb1em3dSPjKrZYtWntk0wvdzh
MD5:	60FA3C0614B8FB2F394FA29944C21540
SHA1:	42C8AE79841C592A26633F10EE9A26C75BCF9273
SHA-256:	C1DC87F99C7FF228806117D58F085C6C573057FA237228081802B7D8D3CF7684
SHA-512:	C921362A52F3187224849EB566E297E48842D121E88C33449A5C6C1193FD4842BBD3EF181D770ADE9707011EB6F4078947B8165FAD51C72C17F43B592439FFF4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v20/KFOmCnqEu92Fr1Mu4mxM.woff
Preview:	wOFF.....O,.....P.....GDEF.....G...d....GPOS.....GSUB.....'.....r.OS/2.....P...`t...cmap...$.....W.cvt .....T...T+...fpgm...p...5....w.`.gasp..... ....glyf.....;Q..ID..&0hdmx..H....n..... ..head..Hx...6...6.j.zhhea..H.....$....hmtx..H....t.....Xdloca..KD.....BC%.maxp..M0... ... .(..name..MP.....t.U9.post..N ..... .m.dprep.. N4.....l.f..x...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R...A.J.x.l..h.a.....l.m.6.1+.X....i...y....&....._.63..5....2>...x|D...ct.Kx..H@b.3..l..#u.....L.*.....^.*.4.....rP..{.* .....Q....JT.:Xu>..T./>...oq.....~..@.....lq../.... ..#..".&.8.H$..r...J)..jj...&..f.=.9..N9.....'F..8.4.....m...m...m.m..n..&.X..}....S.|.....n.....PHaE...J*...4..MjJ.*..nW)..rn3'/.....ks5zY 5c...Mgg.5..p..rR{c...p..t\.8.c=..p...X.(.....7....=.....!...H .....(.0...(.q.JT?.b..z].'T...m..vNi.....t....:P.R..H....t.....&?.:.j.51+.S."j.SK'I.^....}S.i.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\MessageSlider-76521ac1662a2f2c2def[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	4386
Entropy (8bit):	5.736875603030061
Encrypted:	false
SSDEEP:	96:MGhcncLTKjS6EFxNx5mLj5HoZV0ada4OST:MoDLTKmRFxN+Lj5HoH0w/T
MD5:	0069E1EA5B8CA98B0CE75B0F81C6DCE8
SHA1:	9AA425DBA7F7E2B70A5778B489DDDB388429D054
SHA-256:	8D785A96303735282967B9F97F1364D94163E8FF1E80EA6B2F95372142BB604F
SHA-512:	B1CB7793BCD6740A57AABB50624EB1A61EA0DF0068CE53F7029B7A24C3E425BEBCA841DC06CCBA1D592A84CD0810FC608125A48F8E99C7E66311DC12725463 D2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://js.driftt.com/deploy/assets/assets/MessageSlider-76521ac1662a2f2c2def.css
Preview:	._23adWK3Uprf4Ktba9B88ed{display:table-cell;overflow:hidden;min-width:24px;height:24px;font-size:12px;font-weight:700;border-radius:100%;border:3px solid #fff;text- align:center;vertical-align:middle;background-color:#ff001f;color:#fff;background-clip:padding-box}..-zOcMNdFsi7uCebRFihg7,._3GvcBFnnOqEvAbpxb4K9_,.AsmHNMwa 8V6JFxwzpR6dG,.j8lkf_ta2sl2WMvjiqiaK{display:-ms-flexbox;display:flex}.AsmHNMwa8V6JFxwzpR6dG{position:fixed;bottom:0;right:0;width:400px;height:400px;-ms-flex- pack:end;justify-content:flex-end;-ms-flex-align:end;align-items:flex-end}._3GvcBFnnOqEvAbpxb4K9_{position:relative;padding:.75rem;-ms-flex-direction:row-reverse;flex- direction:row-reverse;-ms-flex-pack:start;justify-content:flex-start;-ms-flex-align:end;align-items:flex-end}._3GvcBFnnOqEvAbpxb4K9_ ._2zlCNz6GWncyQ9b6a9K hmX,._3GvcBFnnOqEvAbpxb4K9_ .j8lkf_ta2sl2WMvjiqiaK{z-index:2}._3GvcBFnnOqEvAbpxb4K9_ .j8lkf_ta2sl2WMvjiqiaK{margin-left:.75rem;position:relative;border- radius:.3125rem;box-shadow:0 2px 6px 0 rgba(0,0,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\MessageSlider-f3bd3611b35b24047f7d[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	15645
Entropy (8bit):	5.385950848023877
Encrypted:	false
SSDEEP:	192:YTeBHVzR/8/ccoe5ksgnhLPhuDZd6Bd9WHKkEQ7nW/Z2GU:qeN8DQLoDj6pPWPR
MD5:	F3BD3611B35B24047F7DC8373FC6D076
SHA1:	DFB8E39AEE9BD7A7F40694CA59E2FD4E23496817
SHA-256:	411869F45029FD59C7972A0D74A64EDE1C699EFB67D6D6829B5899C96FA40117
SHA-512:	A962A48CC36C0ACAD4BE24FC2F1D9528B224E76B3615E7F7E1EA9DD827B56FA03AB6D50B3961DEBB0D7572589FC2FB6007E4BE0F2FB1E73FE4D18C3624E820 02
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://js.driftt.com/deploy/assets/assets/MessageSlider-f3bd3611b35b24047f7d.js
Preview:	(window.driftWebpackJsonp=window.driftWebpackJsonp||[]).push([[9],{1536:function(e,t,n){"use strict";n.r(t),function(e){var a=n(26),r=n.n(a),s=n(50),i=n.n(s),o=n(161),c=n .n(o),l=n(149),u=n.n(l),p=n(207),d=n.n(p),m=n(206),h=n.n(m),f=n(205),v=n.n(f),g=n(15),b=n(61),T=n(256),y=n(3),C=n(9),_=n(638),l=n(1675),w=n(1753),k=n(1752),E=n(1625),O=n(79),P=n(59),S=n(5),N=n(7),A=n(34),M=n(24),j=n(32),R=n(23),B=n(1553),D=n(60),W=n(11),L=n(97),x=n(12),z=n(150),U=n(43),H=n(196),q=n(162),F=n(2 77),G=n(114),Y=function(t){var n=t.attachmentCount,a=t.messagePreview,r=t.maxLength;if("string"==typeof a){var s=a.length>r?a.trim().slice(0,r)+"...":a.trim();if(s)return e .createElement("span",null,s)}return n>0?e.createElement(w.a,{count:n}):e.createElement("span",null,e.createElement("em",null,"No preview"))};Y.propTypes={messa gePreview:g.PropTypes.string,attachmentCount:g.PropTypes.number,maxLength:g.PropTypes.number},Y.defaultProps={attachmentCount:0,maxLength:100};var J=f unction(t){function n(){var e,t,a,s,o=

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\S6u9w4BMUTPHh6UVSwiPHw[1].woff	
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.@"l$.J...#.FwFa...]..G....C#.v.2.....>.....hiY..Q...JD:K-& j,...Y... ...E.SQY.-a).a..... XG..O.(5.....S.~L.l.>.....{..R..m7.....=..eL7=..G?.,.....q....$.`....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\S6u9w4BMUTPHh7USSwiPHw[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 30024, version 1.1
Category:	downloaded
Size (bytes):	30024
Entropy (8bit):	7.98341417708702
Encrypted:	false
SSDEEP:	768:Bxk6hFMXBOJ5Wuln1Hczrm+CwYHAtP9BN6abu5oHhDxht4JwhJzcja7:BxSBOJ5DlnqbCwSAtPHnNHmwhJzcja7
MD5:	656963C4BEB814E754E38478FCAA0439
SHA1:	B316CB67F50354A2B934C51E7EB86D003F4E9E39
SHA-256:	0BD12C73F8DBABEAB3E723111D08140CDDED5C22BA6AFACA174373A72A819DA2
SHA-512:	72EF110C286D22F2D8EA0C790704DBC236E9BE81D939C4A039A59C9612D1E61989168163E475C1439A6E93A097AEF9761A42A7983062BCE36FE60253ECD5294E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/lato/v17/S6u9w4BMUTPHh7USSwiPHw.woff
Preview:	wOFF.....uH.....GPOS.....z.4..GSUB...x...S...p.:.|OS/2.....[...`x._.VDMX...(.....s.z.cmap...X.....cvt .....fpgm.....s.Y.7gasp.....''..glyf... ...S....P....hdmx..c....6.....A.head..m....6...6.O..hhea..n.....$.i.>hmtx..n$.....vkh`.loca..p8.....2..maxp..q.... ... .name..r....;....<.RNpost..sX.....EW..Dprep..t...\...r_ .78x.T..l 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.!!.^xX7..=.....{X=.h.aRE.u...y...+4.6vW[.B.....D0 .55..&..ug.5...r(.h.Q9..r..W.!.[.0;..G.....H[..P.G)G.....m..c....}....'=\p.''..dL^.W..>qf.e.y...v...$lq_...%G....{.#.STw`.G.<.....j9e.OG..N...!.(4.L...EW../...C{.Z.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.....$...whmtx..h.....v}.O7loca..j.....9maxp..l.... ... ....name..l....8....:.TApost..n.....EW..xprep..o....K...K....x.T..l Q.EO....m.m.m;X...Fl..? us..p.$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.!!.^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...-..I(.>..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\blank[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 100 x 100
Category:	downloaded
Size (bytes):	1214
Entropy (8bit):	6.925737607348584

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\blank[1].gif	
Encrypted:	false
SSDEEP:	24:xaI1hiyWwjx82lY2T3oVkK53yJ3VmA2LOsj8GY8a9AH:CuNn2kwJ3AAeOsYL8aAH
MD5:	FBDC4ED9A1E2EE4917A265306927BCF1
SHA1:	6D177725D8230DF0457E72004080F712E26FE624
SHA-256:	A78759EA185FD0FA42CA9BE1FC5BCA4D3167A2836DC6C85E479A19DBF57FE2C2
SHA-512:	E529A409048C78837F0D6A6EB77450070EEECC7915D81C45970915F3BBE92BFDAF9056580BB84C14B21C499D04A73945EECD0AD33C61942C5D28DAF06CC7C4D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fast.wistia.com/assets/images/blank.gif
Preview:	GIF89ad.d.....!..XMP DataXMP<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c067 79.157747, 2015/03/30-23:40:42 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CC 2015 (Macintosh)" xmpMM:InstanceID="xmp.iid:B06C130C478A11E6B3E8D67655718D4D" xmpMM:DocumentID="xmp.did:B06C130D478A11E6B3E8D67655718D4D"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:492A1D7F478811E6B3E8D67655718D4D" stRef:documentID="xmp.did:492A1D80478811E6B3E8D67655718D4D"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.....~}|{zyxwvutsrqponmlkjihgfedcba`_^]\[ZYXWVUTSRQPONML

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bootstrap.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	121200
Entropy (8bit):	5.098234288513285
Encrypted:	false
SSDEEP:	768:Vy3Gxw/Vc/QWfJxtQOIuiHlq5mzI4X8OAduFKbv2ctg2Bd8JP7ecQVvH1FS:nw/aTfIuiHlq5mN8lDbNmPbh
MD5:	A3FCACC7DB44CDC3DA744A6747CBF5D0
SHA1:	4ABFA5315DAB8C7B69729651ADB40DECD5A4728B
SHA-256:	4192EC7C351F57F6CC845570C162A063245AD97E56F82B39572F8D5358B5FD5D
SHA-512:	6CC97C314CAF3242ADB3444B6B89527FD7F7232BFC3351F0E002219BA1DFCA73FD550E7EFF87AE6D48AE72C09F37306089848FDA9AE73326BAAA16B7F678371
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://uptimeinstitute.com/templates/flex/css/bootstrap.min.css
Preview:	/*!. * Bootstrap v3.3.7 (http://getbootstrap.com). * Copyright 2011-2016 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). *//*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */html{font-family:sans-serif;-webkit-text-size-adjust:100%;-ms-text-size-adjust:100%}body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background-color:transparent}a:active,a:hover{outline:0}abbr[title]{border-bottom:1px dotted}b,strong{font-weight:700}dfn{font-style:italic}h1{margin:.67em 0;font-size:2em}mark{color:#000;background:#ff0}small{font-size:80%}sub,sup{position:relative;font-size:75%;line-height:0;vertical-align:baseline}sup{top:-.5em}sub{bottom:-.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:1em 40px}hr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\c7702482e79cb95b283fc1efb7f1a99c7c9169b4[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 640x360, frames 3
Category:	downloaded
Size (bytes):	82922
Entropy (8bit):	7.95661370974671
Encrypted:	false
SSDEEP:	1536:efNHZVELXT84cN9q/puLWVJF339Z6yTZg3hMfHOhwDhOR26YPVgSsHQv8:MHW439q/puL8v3f6cemfiwDhORWPwHr
MD5:	0B394B4EA14016E06278894362FDDB5C
SHA1:	17E03AA63777A8F36578D8F18524E179C3B6513C
SHA-256:	FFE8729A7D79E90F1719C2ACEB2BDA61156989E0E54A7434D715E71C3541C2B9
SHA-512:	EE9BE5EA389E3D1777D16E0AB1226DCCE29E77983AD8C1C79C5C8BD5C134BC71C6D96ABB3F3E1AB0FFA99D4F66D3C9676B30BB4DBB440B38C6847511E4EA3FC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://embedwistia-a.akamaihd.net/deliveries/c7702482e79cb95b283fc1efb7f1a99c7c9169b4.jpg?image_crop_resized=640x360
Preview:	......JFIF.....C.....C.....h...."...}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..L.OE9.rib.P7/<..sD...:..G.}...ZL..\|..@..T....h..(/..@*..[...4.>.....h....V...}...Q..84.g.hO!s.J.4.F.?.IL....j.....w..?t..Uf.Wl.t.i.).0....k....c....,.Yw.....8.v.3.O9V.;.g.q3.k...-..x&...p.....P.5...\.U.....;V...0.9.....5H..W.z.3.<...[.....Z.[S#1'..+...a6.+!..HB>O=.'xs.E....R..p.....&\.j...<$_.W...T...k6....W.>.^rNi...9c....z.P5..r..Ik..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\c7702482e79cb95b283fc1efb7f1a99c7c9169b4[2].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 1280x720, frames 3
Category:	downloaded
Size (bytes):	231167

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\c7702482e79cb95b283fc1efb7f1a99c7c9169b4[2].jpg	
Entropy (8bit):	7.969520025862345
Encrypted:	false
SSDEEP:	6144:StBweOp41u51/zdeeCFmKy+VVV5OKZ4XiGvz0e:StBruLBeBNy6VMKZ4yMzn
MD5:	09FA7FDAF43451E1A7D1F1A9C4B9716E
SHA1:	2C39FB04EF0E8C7AC60C172ABF0ED69167818488
SHA-256:	3C0A1476EF889F721E657C27E4C33A32AB3E6CEE9EAD212FC73E60B0AAD0196E
SHA-512:	B433C5EFBCC5F142605B6B6A0FEAC23F7C2485BA99340D438CCB0DC0A56592132563AF49DDF97FE75C28574B2D50BF96EB56EB577828B6491CE306B340A0387
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://embedwistia-a.akamaihd.net/deliveries/c7702482e79cb95b283fc1efb7f1a99c7c9169b4.jpg?image_crop_resized=1280x720
Preview:	.....JFIF.....C.....C.....".....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..F{wv.q..Lh$C.\..u.....w<.k ....;.R.@~a.H....?.Y... R.g?*.Pi....gO_..".T.....PdS..v.sC)S.V.7..sQKn...@...0(P@..6.S@.w ..%H.4.RNELT.....B..*.....X`.Q=...t.,.....9|.t...#.Z7-.*2..(.A...5.Q..4..NN.:..< %..W..@.*.(Q.L.....#M..X..s.]I...V|....Q..%d#D0v.O.....c.QO.,.1p...Vo.[.....J..qL..:....Qu...^.Z.;...X.M&...DR!..z...J.....I.....fj.....Z.0..q...s[.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\cookieconsent.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	3938
Entropy (8bit):	4.810660944554395
Encrypted:	false
SSDEEP:	48:u00LI2I/YPuYLOWjQ0cN7xjXndM78JtdnJZtTJwIjDPZw4zK4cg64cAK4cgD4cp:5kRWYbOiGdTt7ZflBHRaq
MD5:	4AFFDA653D65484BF6983822FA6ADB23
SHA1:	225DF1E9345D47CF62A552B7E6720BE1E759B49B
SHA-256:	456AB1A71507ED91ABAE14C9D08FAFFB373A7BC711A66E44341B7B8B7BB72AB4
SHA-512:	B099A8733858188D4E901DF45B4C8243DD64AAD621B1035A552BC5FC58DAE2F23A91FF06C4A517F7E44D17B3CB9667773F9E8C15081EE907FDF10FA3EA218E5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.0.3/cookieconsent.min.css
Preview:	.cc-window{opacity:1;transition:opacity 1s ease}.cc-window.cc-invisible{opacity:0}.cc-animate.cc-revoke{transition:transform 1s ease}.cc-animate.cc-revoke.cc-top{transform:translateY(-2em)}.cc-animate.cc-revoke.cc-bottom{transform:translateY(2em)}.cc-animate.cc-revoke.cc-active.cc-bottom,.cc-animate.cc-revoke.cc-active.cc-top,.cc-revoke:hover{transform:translateY(0)}.cc-grower{max-height:0;overflow:hidden;transition:max-height 1s}..cc-link,.cc-revoke:hover{text-decoration:underline}.cc-revoke,.cc-window{position:fixed;overflow:hidden;box-sizing:border-box;font-family:Helvetica,Calibri,Arial,sans-serif;font-size:16px;line-height:1.5em;display:-ms-flexbox;display:flex;-ms-flex-wrap:nowrap;flex-wrap:nowrap;z-index:9999}.cc-window.cc-static{position:static}.cc-window.cc-floating{padding:2em;max-width:24em;-ms-flex-direction:column;flex-direction:column}.cc-window.cc-banner{padding:1em 1.8em;width:100%;-ms-flex-direction:row;flex-direction:row}.cc-revoke{padding:.5em}.cc-header{font-size:18

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\cookieconsent.min[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):	19802
Entropy (8bit):	5.21863639193455
Encrypted:	false
SSDEEP:	384:sne5yGafGZwprGryKfxNQUDIg7jmhILuWFRv0eVdHPyZ7fxS0QoyZ+2mRwjO0dpJ:sGaf6wZKLzdLueRv0zZ7fxSlcRA5dQfY
MD5:	F2BC0804920974CDB94FECA2936B668C
SHA1:	253B288316EE7BB62B0BC755D7834B14B265F18C
SHA-256:	AF4C6683814AA527CAF53BDE3D021E6AAFE00833B45F2DEAD043C87ED7864674
SHA-512:	08ED1DF4DDE697A224F0FDE61B2EA3D56C792969D6CF29D06E244969984CDF614FF7D2919D3ECEFA134D1869EE564B718DE605539C67F4A7DBEDCD77DB09D2B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.0.3/cookieconsent.min.js
Preview:	!function(e){if(!e.hasInitialised){var t={escapeRegExp:function(e){return e.replace(/[\-\[\]\/\{\}\(\)*\+\?\.\\\^\$|]/g,"\\$&")},hasClass:function(e,t){var i=" ";return 1===e.nodeType&&(i+e.className+i).replace(/[\n\t]/g,i).indexOf(i+t+i)>=0},addClass:function(e,t){e.className+=" "+t},removeClass:function(e,t){var i=new RegExp("\\b"+this.escapeRegExp(t)+"\\b");e.className=e.className.replace(i,"")},interpolateString:function(e,t){var i=/{{([a-z][a-z0-9\-_]*)}}/gi;return e.replace(i,function(e){return t(arguments[1])||""})},getCookie:function(e){var t="; "+document.cookie,i=t.split("; "+e+"=");return 2!=i.length?void 0:i.pop().split(";").shift()},setCookie:function(e,t,i,n,o){var s=new Date;s.setDate(s.getDate()+(i||365));var r=[e+"="+t,"expires="+s.toUTCString(),"path="+(o||"/")];n&&r.push("domain="+n),document.cookie=r.join(";")},deepExtend:function(e,t){for(var i in t)t.hasOwnProperty(i)&&(i in e&&this.isPlainObject(e[i])&&this.isPlainObject(t[i])?this.deepExtend(e[i],t[i]):e[i]=t[

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:	downloaded
Size (bytes):	208

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\css[1].css	
Entropy (8bit):	5.24520196411175
Encrypted:	false
SSDEEP:	6:0IFFlMcC5+56ZRWHTizlpdAxawTdTmuNin:jF/EO6ZRoT6pixawTNmuY
MD5:	7FB85CAC150CA937798AE5B1067CD37C
SHA1:	135FB90710B0D35DFDE21EC7435A18115EA07855
SHA-256:	436CE6DA77B85F44967DA69ED53CE908B908F73AEE0243AEF7EE3BA650A225E0
SHA-512:	B0C53A0410200010A206A73E5C5A3A29E9CB00EAEB614E746150F8CA216F27938E8A26D3741D07ED08CB0D70CE5D46F08BF15E97213D02AA100702C7652C98E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Roboto+Slab
Preview:	@font-face {. font-family: 'Roboto Slab';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/robotoslab/v12/BngbUXZYTXPIvIBgJJSb6s3BzlRRfKOFbvjojISmb2Rl.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\css[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	181
Entropy (8bit):	5.166918428964377
Encrypted:	false
SSDEEP:	3:0SYWFFWIIYClWWdsRI5XwDKLRIHDfFRWdFTfqzrZqcdvXuR4Uunkcoq/VL5JYARY:0IFFlRds+56ZRWHTizlpdvXuRZnq/jJY
MD5:	D02DA02257788D95CE46A069389B9ED3
SHA1:	960A1211B3881115E1261C19F40B56CA8349BAAA
SHA-256:	7C04DA9E7C92F747AC8D24AA8BEBEA9059741355C9D8996CFB247AD5097CCA26
SHA-512:	CE6FFAF1A802C6EE844E7B94D0FE1C142F811B82A70036ADA716B0D345A4E77F1994F428B93568B6947F6A5ABD8D50D33B294520F5EE6542C39995057BB5B937
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Overpass
Preview:	@font-face {. font-family: 'Overpass';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/overpass/v5/qFdH35WCmI96Ajtm81GlU90.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\font-awesome.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	31000
Entropy (8bit):	4.746143404849733
Encrypted:	false
SSDEEP:	384:wHu5yWeTUKW+KlkJ5de2UYDyVfwYUas2l8yQ/8dwmaU8G:wwlr+Klk3Yi+fwYUf2l8yQ/e9vf
MD5:	269550530CC127B6AA5A35925A7DE6CE
SHA1:	512C7D79033E3028A9BE61B540CF1A6870C896F8
SHA-256:	799AEB25CC0373FDEE0E1B1DB7AD6C2F6A0E058DFADAA3379689F583213190BD
SHA-512:	49F4E24E55FA924FAA8AD7DEBE5FFB2E26D439E25696DF6B6F20E7F766B50EA58EC3DBD61B6305A1ACACD2C80E6E659ACCEE4140F885B9C9E71008E9001FBF4B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://uptimeinstitute.com/templates/flex/css/font-awesome.min.css
Preview:	/*!. * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome. * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License). */@font-face{font-family:'FontAwesome';src:url('../fonts/fontawesome-webfont.eot?v=4.7.0');src:url('../fonts/fontawesome-webfont.eot?#iefix&v=4.7.0') format('embedded-opentype'),url('../fonts/fontawesome-webfont.woff2?v=4.7.0') format('woff2'),url('../fonts/fontawesome-webfont.woff?v=4.7.0') format('woff'),url('../fonts/fontawesome-webfont.ttf?v=4.7.0') format('truetype'),url('../fonts/fontawesome-webfont.svg?v=4.7.0#fontawesomeregular') format('svg');font-weight:normal;font-style:normal}.fa{display:inline-block;font:normal normal normal 14px/1 FontAwesome;font-size:inherit;text-rendering:auto;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}.fa-lg{font-size:1.33333333em;line-height:.75em;vertical-align:-15%}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-fw{width:1.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\gtm[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	112978
Entropy (8bit):	5.547188435231018
Encrypted:	false
SSDEEP:	1536:2F+UTXOOVX+HYEG0oI6vDGC7Xz1Ltp3YHa+CquP7T1z9dwKP1/4hgEhJHTg0AipF:1UTXtVOHe0q17htd8uTpi6J+
MD5:	FF50EE83703D709E1A038840F9ED2C83
SHA1:	14F1CEEC1E2840B7806772901B34E57F07CAF489

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\gtm[1].js	
SHA-256:	0C8A9618C4982E0F6D395936C36850B0608F29DDD86A1A2AD1AC5E523CDFFF82
SHA-512:	D65954C491FF29C2FD0DD0BAF8A2E26FF748069068F0A9988E1387934A058C69D02B025C0FA807AB68CE3A296A8822543577B98C84DBF8245D3A3BF475151820
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.googletagmanager.com/gtm.js?id=GTM-WPMZ556
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(w,g){w[g]=w[g]||{};w[g].e=function(s){return eval(s);};})(window,'google_tag_manager');(function(){..var data = {."resource": {. "version":"8",. . "macros":[{. "function":"__e". },{. "function":"__gas",. "vtp_cookieDomain":"auto",. "vtp_doubleClick":false,. "vtp_setTrackerName":false,. "vtp_useDebugVersion":false,. "vtp_fieldsToSet":["list",["map","fieldName","allowLinker","value","true"],["map","fieldName","cookieDomain","value","auto"]],. "vtp_useHashAutoLink":false,. "vtp_decorateFormsAutoLink":false,. "vtp_enableLinkId":false,. "vtp_enableEcommerce":false,. "vtp_trackingId":"UA-24440320-1",. "vtp_enableRecaptchaOption":false,. "vtp_enableTransportUrl":false,. "vtp_enableUaRlsa":false,. "vtp_enableUseInternalVersion":false. },{. "function":"__v",. "vtp_setDefaultValue":false,. "vtp_dataLayerVersion":2,. "vtp_name":

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\icon-Hybrid-Infrastructure[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 300 x 300, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	3960
Entropy (8bit):	7.359525831816714
Encrypted:	false
SSDEEP:	96:VhPLxhHk/iHmdzfRAQohXYnF8tPRpxZH8:3xhPHm9WhXNtXxa
MD5:	4179D59C52AC74F2C1514A34D79B3E0A
SHA1:	4326F2C3B4AAA5DBB9F2477C95D6EB5E545BF4C5
SHA-256:	CCC7CA5CCD5E57EFC51AE6E1928F002D3DBF9ECC6CEF46CA4B5EA8D0CFEC27B3
SHA-512:	FA09650F362B21D260833AFB1B785F5C0B90485CB48F607C1D44C1F980847245DE57AD6391631CEEA29046C1C722B9A36B8AFBD9B5854617E13760C51A4BB169
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://uptimeinstitute.com/images/Icons/icon-Hybrid-Infrastructure.png
Preview:	.PNG........IHDR...,...,.....N.~G....PLTE...#. # #. |<......tRNS..,Ux............nC.#^.... D..K...y(....$.[.7...~.=..0......sphq.......d..c..j<.L...!..o..}\.H.....%V.F.m.>.aN"z.{...-.'W.|....:/r..BT..8...?......;..tGi.b.....Ylvu.@&M.X4........J)S*.Pf.I.1....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\icon-Research-Reports[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 300 x 300, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	4629
Entropy (8bit):	7.468697223645627
Encrypted:	false
SSDEEP:	96:Oo9XoN33eX5DkRPAxr00gy1XUXo5sORKN+:dtOaxrfgyJ5hIN+
MD5:	FDF118D4EEF73F1CAD902EADD7EA803D
SHA1:	DF9F5092058E68B2F925CB56E4514FA08457D3E9
SHA-256:	B77E792AB36EE060AE3E1338F854A251AD32A8E5526037AECCE402C55681C9F6
SHA-512:	9E0CBDAC61BD217CA4517CCE34872D6D48FFF9407BEDC63157F802D1752F9B41CC3277D56B04BC863F57A641011E8523168A2CFB954E37E99027AE1EE7D6B1 E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://uptimeinstitute.com/images/Icons/icon-Research-Reports.png
Preview:	.PNG........IHDR...,...,.....N.~G....PLTE...#. # #. J[.!....tRNS...`.p.0 Pgz...|jV6..H....R.#w...3.m....)...<-.@7................F.q....%...J........9.....:."..B..i5!x[.c..2N....1].....bn..$T*LDW........8.E.t......Q;....G...a>..X....K..y...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\icon-Tier-Standard[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 300 x 300, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	2771
Entropy (8bit):	7.063332217438764
Encrypted:	false
SSDEEP:	48:2yVqmVSUfUSvy7Hnm5gDE62y+25cOH4KBVMs:2uqmVSGUSq7ZDEG+25TYcVMs
MD5:	EDA994FB8F2620CA6EDEE2DDB6A07491
SHA1:	F6B4C0513775E44B239CBCD521BCECA58A5FFB85
SHA-256:	4D46B91440881815DA1624A6C76731BF9E734D23845B003BC0E390E1010602A0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\icon-Tier-Standard[1].png	
SHA-512:	A3B4D1678B3D5F70229ED18CC2716E76CD7056759395C6C9EAF6D43FC397D22CBBBE6806840A889193C96B8EC485F2D79391EB74BAD8C290EFB673F1D2D086 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://uptimeinstitute.com/images/Icons/icon-Tier-Standard.png
Preview:	.PNG........IHDR...,...,.....N.~G....PLTE...#. ...t....tRNS."|....s.......Z..Fr.[.B...!.y.`b}..........t.... ..../..@...+...C..j.......f..7>PO0.D4........d....#...m, <.W.gx3.n.Jp......$.-..M.o..'Q.....ie..8.....N.A...VH...c..q...~6)=.T.Y...:E.^kz.w.h%.(.....L.....&v.5..u*UA.....IDATx...QEA...E.......k8.`wo&)!.............O.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\init[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.8731406795131336
Encrypted:	false
SSDEEP:	3:xORi:xn
MD5:	1424EB76249899D757E4D168341A50DC
SHA1:	42101E71440ABD46C8112A96D4D5C0DD445120CE
SHA-256:	16F1EFA415BFDD7ABCF8FDD76CC05AE6FA66FFDFDC730368ECEA89ECFE5C3A12
SHA-512:	271F3DFD54E2B14E6CEA6A45E09A9F1BCF1A3BFB19A7F66821C20D558A7FF7F3423EB25EEBF2391CCF36A9762DA22EB609017169BF34F7BFF562D61D1F7AD0 3
Malicious:	false
Reputation:	low
Preview:	POST, OPTIONS

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jcemediabox[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):	5922
Entropy (8bit):	4.826765436498545
Encrypted:	false
SSDEEP:	96:j0u8xqRyKY4v1NJfgR9u7UVvqSMD6UUdrdjHDsFhx8:Qx5K4zVvqS8px8
MD5:	F3FAB02A79DA2632C80C3BB4674AA40D
SHA1:	098855B7A2D60B522A131880188B71C1EC5FE729
SHA-256:	4FC216ED242CF1759EA9A3FD18DE4CE4E610E6642A1406301D7DFB4DAE062F46
SHA-512:	C60DAFD67D6BF703D91FA7229C5F6DB4A987624F87372BDED7030652C46C909F9C1D3DF9A228A172C4A86448780E65772545CEBD965E40DA222EEECAB6B07D 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://uptimeinstitute.com/plugins/system/jcemediabox/css/jcemediabox.css?1d12bb5a40100bbd1841bfc0e498ce7b
Preview:	@media print{a.jcepopup span.jcemediabox-zoom-image{background:0 0!important}}.jcepopup.hide,.jcepopup.noshow{display:none}#jcemediabox-popup-body,#jcemediabox-popup-container,#jcemediabox-popup-content,#jcemediabox-popup-iframe,#jcemediabox-popup-img,#jcemediabox-popup-loader,#jcemediabox-popup-object,#jcemediabox-popup-overlay,#jcemediabox-popup-page{left:0;top:0;margin:0;padding:0;border:0;outline:0;font-size:100%;vertical-align:baseline;background:0 0;height:100%;width:100%}#jcemediabox-popup-body,#jcemediabox-popup-container,#jcemediabox-popup-content,#jcemediabox-popup-overlay{box-sizing:content-box}#jcemediabox-popup-page{position:fixed!important;z-index:10000}#jcemediabox-popup-page.scrolling{position:absolute!important}#jcemediabox-popup-overlay{position:absolute;cursor:pointer}#jcemediabox-popup-frame{position:relative;overflow:visible;height:100%;z-index:10001;cursor:pointer}#jcemediabox-popup-body{position:relative;overflow:visible;margin:0 auto;width:300px;height:300px;z-i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\js[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	100691
Entropy (8bit):	5.5227171275940234
Encrypted:	false
SSDEEP:	1536:JvTXOSCVX+HYEG0oI6vDGu7Xz1Ltp32mTiBHm+Zx8hzDsvDv5SqO77T1z9dwKP1h:JvTXkVOHO0qh7htg0QQOOPpS+
MD5:	24C6E75E80AA986CE01F1C02BA9EAC0C
SHA1:	79D35960C6F0B703D1CF1E1263B9DC96480F6C3F
SHA-256:	E7F52BC3075FEF832CBCFE0BB03F6D1870B68A5BE1C62C15025981515FF54AF0
SHA-512:	B01B7AC29A270257EDA63E94173AF6DFE39D3394DBCE73B0573D9824DA06FAB710481829F17BBAB10687491AFA3B02A531023AB1375D6E15D67D214ACF27846
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\js[1].js	
IE Cache URL:	http://https://www.googletagmanager.com/gtag/js?id=UA-24440320-1
Preview:	// Copyright 2012 Google Inc. All rights reserved..(function(){..var data = {."resource": {. "version":"1",. . "macros":[{. "function":"__e". },{. "function":"__cid". }],. "tags":[{. "function":"__rep",. "once_per_event":true,. "vtp_containerId":["macro",1],. "tag_id":1. }],. "predicates":[{. "function":"_eq",. "arg0":["macro",0],. "arg1":"gtm.js". }],. "rules":[. [["if",0],["add",0]]].},."runtime":[].....};./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var aa,ba=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}},da=function(a){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return b?b.call(a):{next:ba(a)}},ea="function"==typeof Object.create?Object.create:function(a){var b=function(){};b.prototype=a;return new b},fa;.if("function"==typeof Object.setPrototypeOf)fa=Object.setPrototypeOf;else{var ha;a:{var ka={a:!0},la={};t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\logo-sq-Digital-Realty_330x330[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 330x330, frames 3
Category:	downloaded
Size (bytes):	6766
Entropy (8bit):	7.596719246502099
Encrypted:	false
SSDEEP:	192:p1ZDdhQlm1Fr8Eu77IICxDlrhP+CPiMuui/fk3JsYQ:RDh1FrC8uzLHlofuJsx
MD5:	85FA5AEE86BCD9CD86D25847284FACC5
SHA1:	E78ACD421B7558B8322CCA53F2CA6B222B3CEF46
SHA-256:	CF932A1FE2DD7797878EE13A39C0D490FDFF0272AD487D5B1FA7945F8F9C40DB
SHA-512:	8029B2949D9AF4DEE6B8E403821FB4E4F3384237058124D12FE610E61E0E4CE8C6EABFE2CE5E60F1B183E4439E9A7434D017EAC5AECA7A349D3CA29BF9D4508 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://uptimeinstitute.com/images/logo-client-carousel/logo-sq-Digital-Realty_330x330.jpg
Preview:	......JFIF.....J.J..... .....|./.....kp-"..X.....c..y.f..{.. ....?....Y.mv.....?...V/.....4.8gl./.....i.p..|..7.....v.~3.*.....Y.....@....>.....w.z.....*.....Lc..1J..h.....g1.....>....z...;t'+d...C..y.. ...Y...s.F.B.....-..vo.N..*.....Jhx=.{..W..j.....=..e.... ..5}...Z..>.....g.h.V?.....,.....g.X.....g..\.....}....h.....yu.....%e .....G..^f..[W....uUl.}..De<.i.L..6..c...l..Q.,...,..r.S5._...m.wU*.J.h_@..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\logo-sq-ING_330x330[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 330x330, frames 3
Category:	downloaded
Size (bytes):	9600
Entropy (8bit):	7.757755414235998
Encrypted:	false
SSDEEP:	192:CJgiCXa7HP922qnYJOcdJa+B5NRnVrbCsGV4TyA1Vvm0iOUp6:fiCXAP9uYldJa+T7n1bZpTyEvmnZp6
MD5:	20C94C0614E242402B4DF8B2E683C394
SHA1:	4EEAE7BC253D4246AD8E68ACD30AAB94A6CC486A
SHA-256:	3FFC165D6F7D4F9F8B3624A1C808A170F078B507B3F2B749569E63B381CC66B7
SHA-512:	D27FB8742ECB83F3C8597BC2FCE5CAE450FC3D9D798371F23C8470E6B4C4AB160B3B975A773D9A73C47519521381426D73FEF6A59FCB0C835DBB4697192533 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://uptimeinstitute.com/images/logo-client-carousel/logo-sq-ING_330x330.jpg
Preview:	......JFIF.....J.J..... .....Q.....u..$...T..G^..N.^.....R..d....5.Z.<9..o..Kf...wE!...O2._.sW.oU....Z..P..N...v2.)...!.....;>.J..<%.O...@.....0..oF..~zN..S..R..v.5..l...../.=k;9[.tN) .....N...$..N..i.x.x...<..o.....f..L....4p..?....>{..5...&..Q.<~mu.....E\c..6@}.....qZ.#.....=3.<... C.....|.+M$A..)....7...N.....(.h..... .....1.....4s.r.).2.c8.2..A.x.....e.....U..;W...c..3...\..^d.]-=z.v./2=.iC....c..m[Ik.A.&.;.=tt ..tQo....Xy..2....[j.....=tt.kY..Eg..-<...0|..,|...D...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\logo-sq-Orange-330x330[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 330x330, frames 3
Category:	downloaded
Size (bytes):	9771
Entropy (8bit):	7.791221325714216
Encrypted:	false
SSDEEP:	192:7yiWEDmOgkXqHTbYq000L++Q6ih61LMNuRMMMMMMOJeildEabJPUIACQcuy0:2yDbjMTbYq000L++Q6k6SOMMMMMMGeii
MD5:	70068F84E781C1532908E60D088691FE
SHA1:	2A28E3B5D31D49808A6AFBBD7F15A9C9B4E4B745
SHA-256:	40662A14CE5F0AB466580A78C47FC2157A4B85828C38E761BC2398A7E39F1C01
SHA-512:	0E6009998480376013 58A4B8D7880ECF1ECB03B3A73A184E50414DC9876A1F249407D92BB5B7E04EB44920F6CC229C280FB03BF6B3A9E6A565650C3526808229
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://uptimeinstitute.com/images/logo-client-carousel/logo-sq-Orange-330x330.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\logo-sq-Orange-330x330[1].jpg	
Preview:	......JFIF.....J.J.....H.....,.....(.g.....7. .....&p.....x...,.....(.g.....7. .....&p.....x...,.....(.g.....7. .....&p.....x...,.....(.g.....7. .....&p.....x...,.....(.g.....'.|.x..&p....~.j.....L.o....h>..t.....pU.4/...!>.tW.....A3..7..O.Zh.V=.Ms<...>.WD.[6um.....z..&p.m.<f.-.....<JO.Y.?..n.<gq..}.....L.u[w\.=...u..r.~.O.....~q..?..q.Rs.7. .....L.V)Ka..}w....d.)>...6.....hn.....&p.7..1.v..g.....l....e..y.E..\9....$7. .....Q...1P..&p....X.|\g..x..+>..x.....<...|yx.90.....-t.:,.....3.....n.....-..:,.....3.....n.....-..:,.....3.....n.....-..:,.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\logo-sq-PayPal_330x330[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 330x330, frames 3
Category:	downloaded
Size (bytes):	11149
Entropy (8bit):	7.842861856394662
Encrypted:	false
SSDEEP:	192:mIxcP8xv9vGa7ozfwR26qsaSLy9EQPZ8GcrX5wVA902AavJMTgDM79lU6A:mImyvGaEsR26U+xKAO2ZJMTsG9lU6A
MD5:	8D54B0F1442276F86482FDD50476A8B1
SHA1:	68B83E7E8BC80E7E5A4C6591CC7D81F900527B7E
SHA-256:	DD8EE98DD43101A48CC64848A09A9D65FE4355CCAF4B753A3017637F580901A4
SHA-512:	F984943480C135429323085588848F29D776F3BFB9CDCECFFA2EDEADDEF26790FA2B3A05FC20CAF209D5E57F3688D078467174E22FDB6F451D6CD04E2E976F8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://uptimeinstitute.com/images/logo-client-carousel/logo-sq-PayPal_330x330.jpg
Preview:	......JFIF.....J.J..... .....c....IE..K%8.....g.....?e.Z...S..a...-..P.....@?{.zx.....(..c&.o...q4.yc..{.....*....2O.O....._0l.,..o@..T.a.?rv..C.m.....I..r.h.a....y.?.c".:.....C.....&,.....OG...v@....\.u...d....[.D..fZP....=?e/... ...5..I...m.....,.&.@....h.#.I.....w.1....87.G6l...Vg(..J.....s....Z0.....q.8.:..N.=.z..-. ....[...:m<.].....#6*.(_...R4.Q.L.J>..q.v|>.....,.Tb}.Wu8.lb.s4~o.4K..a...dfm$..y..U.b..)O-~}.m+.-,!Zl..W....F0.."..Mf1...P.g.....J9o.\;."E.'.....ob.b*....{..Sfw.>c..^5...{..j.....~....t{.-o\.....O..... ...}..9.....4.<.....gc....7@.YN...\Y.. .....8x..*.....n.....G.....}c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\logo-sq-Salesforce_330x330[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 330x330, frames 3
Category:	downloaded
Size (bytes):	10634
Entropy (8bit):	7.8194212005585335
Encrypted:	false
SSDEEP:	192:hdddPM4EO6nvcZtDTe/EqkzP/pSrn1/GpyjMpLwKpRACJGvj:DddUa6nkLqEqWBSUpyIpkER/JGvj
MD5:	A31B85B83072BD92CB8673713D9B9A45
SHA1:	769B25B18243B444D589334A334298E31C820C33
SHA-256:	02029169CDC273C185D0A5C3E669CB32AF619409E64D2AE7000AA11AEA20A93A
SHA-512:	AB9E01D18CBCFBE9B0F0E644A17D5A50923F2B9F374463859ECFE9F6370155958BCCD809C6BA8C425E62D9DB5899BD59D9887330685E8A7AF5B9B0EF0FC534 3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://uptimeinstitute.com/images/logo-client-carousel/logo-sq-Salesforce_330x330.jpg
Preview:	......JFIF.....J.J..... _.\.....tc...Nm.n.....}.....*.;.....(....^..N}..._.{l.`..|....=...n.l`.>.@...f...&V.....e`.....-...q`.....`....?7....6.5$..;..\.%.H..s...(.....X.2.'...].@....L...!.....K.`...,....U..Y1.....,hT...@f....r..~.....7).eZ..L..&..Y>.....OR.%.....p..gP.....5#L.....^..`.r.Jl..a....i...2.....x..Q....;u._.....E.H.p.n ...v....48^t.....Ml.....~@..n..../ .....@..x.....N7...ZF.....~..f..... .....?.....H.....1..kiH.5>....W`..5y0..@..Az..D.....t.....=.....N...>su.....y..._...../...L..`>#....0.....e.-...(.F.B..... ....._fl..h.#....3...\;D..mOq.....5..=..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\logo-sq-TD_SHIELD_330x330[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 330x330, frames 3
Category:	downloaded
Size (bytes):	8592
Entropy (8bit):	7.7711357190070505
Encrypted:	false
SSDEEP:	192:69hIUyifKlcLksYYYqZ48mHVVpt1p3c0RqwoOuLS7eO:69uyzYYYq28Mbj1psYqwojM
MD5:	ED4BEEEF93A8DE13F4A2229DD576192E
SHA1:	E8D86BB569CF127B8FC4722C78FC6CAF7AC52225
SHA-256:	028EC32BF670D4A1058BCECD4BC5358A65B498FEAC5A69C8ECD041C5946CD850
SHA-512:	79D092DB3929A2EE937A548ADD55846A70268FB8CC43732688E290B28EB80C57815BD1E23DEB41BB340FF7545D649FDD2532538FABF79046748DFD6CC6A2C0C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://uptimeinstitute.com/images/logo-client-carousel/logo-sq-TD_SHIELD_330x330.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\logo-sq-TD_SHIELD_330x330[1].jpg	
Preview:	......JFIF.....J.J..... ......" ....M..o.....Yw. .. ....e.f.....z.....]..o.....Yw... ...@...>TF...e.f....`..|Tu|.]..o.=k....;.{...!B.....Ahiq.C.W.=C...,.....;....x.{.8..s7.K...7..N.!..t....u_.S..e.f.... ...<...hy.^.E.z....'z...:`.r.Ay.?8.]..o....B. P.....j.l.Yw... .w..-C.....U.EsQe.f.... ...<...^va..%.z....'z...:`.r.A..%yA.]..o....B.P.....\.....Aj.0x9w.(..s:.....7..N.!..t.....E./,.2.....Aj.0y.X.g...:..]..o....B.P.....@3|@..B.Z.K..... p.Yw... ..}...}.....@3|@.....7.....,.....@3|@.....{\.t.....z.....].....kx.v.....g`....Z....p....kx.v..D..s. p...kx.v..V.....pZ.....p}.<...r....;.....a..v^.....g`

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\main-8cc258245c33f3963e1a[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):	35033
Entropy (8bit):	5.303407906465342
Encrypted:	false
SSDEEP:	384:UnmzO9odgFHKS3IN+FCdLKJtr/HiBitZKMHIhmV1INHu1ycGKTyrW7IyJuylvk7T:UgO9owqSqbdLQo8yDpKtlMFwIA3fa
MD5:	8824FBE6EE8C0F99975716C5A3325F96
SHA1:	210FADEA0C41182A2DC4B339F1125643A31A2175
SHA-256:	C72F0BFAC1F9D6F6A61D6368238EF45B15DA5DA53BC7243C848DD5E1E0434373
SHA-512:	E51D995BA3754E917EDD479B52C982DD6155E02BFD82F64D88518F12CA400125A38CE17725444D2C5ED24A6066D234297BC33373B7ACA2823BA960BCBF448CE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://drift-lp-66680075.drift.click/_next/static/chunks/main-8cc258245c33f3963e1a.js
Preview:	_N_E=(window.webpackJsonp_N_E=window.webpackJsonp_N_E||[]).push([[2],{0:function(t,e,n){n("fpCY"),t.exports=n("BMP1")},"0sNQ":function(t,e){"trimStart"in String .prototype||(String.prototype.trimStart=String.prototype.trimLeft),"trimEnd"in String.prototype||(String.prototype.trimEnd=String.prototype.trimRight),"description"in Sym bol.prototype||Object.defineProperty(Symbol.prototype,"description",{get:function(){return/\((.+)\)/.exec(this)[1]}}),Array.prototype.flat||(Array.prototype.flat=function(t,e){retu rn e=this.concat.apply([],this),t>1&&e.some(Array.isArray)?e.flat(t-1):e},Array.prototype.flatMap=function(t,e){return this.map(t,e).flat()}),Promise.prototype.finally||(Promise.prototype.finally=function(t){if("function"!=typeof t)return this.then(t,t);var e=this.constructor||Promise;return this.then((function(n){return e.resolve(t()).then((functi on(){return n})))},(function(n){return e.resolve(t()).then((function(){throw n}))}))}},"1zPn":function(t,e,n){"use strict";var r=n("JB68"),

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\main[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	15727
Entropy (8bit):	5.142240193270684
Encrypted:	false
SSDEEP:	192:fyPAoqG/4sV7n7kk+qq+zkeiO9PTOp6pxBQ9Hb250zNI2YJDSy+mulUnmPiEa2y2:fiqa77n7rgEk4xMb2505jBmzV7DLRj
MD5:	E68A080991D754ABA55F6D936BEAB0C8
SHA1:	4D687277D15F34C9EA23F3308FFD261458204DEB
SHA-256:	D47A6A9D73B3D0F8DECA4E4516480CE9FCFECC342C1999346038097D8C66FC8A
SHA-512:	B904FE7CF926E7074B861E0B489AC0B8479A2660936C292682BBA6FAA710973B1EBA80CF25DC8B96FEECCAE586C8A320DA6FAD121C97A8EF8F48F48F1986B68 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://uptimeinstitute.com/templates/flex/js/main.js
Preview:	/**. * Flex. * Template Name - Flex 2.5.2. * @author Aplikko http://www.aplikko.com. * @copyright Copyright (c) 2017 Aplikko. * @license http://www.gnu.org/licenses/gpl-2 .0.html GNU/GPLv2 or later.*//../* Parallax */.(function($){'use strict';var $window=$(window);var windowHeight=$window.height();$window.resize(function(){window Height=$window.height()});$.fn.parallax=function(xpos,speedFactor,outerHeight){var $this=$(this);var getHeight;var firstTop;var paddingTop=0;$this.each(function(){firstTo p=$this.offset().top});if(outerHeight){getHeight=function(jqo){return jqo.outerHeight(!0)}}else{getHeight=function(jqo){return jqo.height()}}if(arguments.length<1||xpos== =null)xpos="50%";if(arguments.length<2||speedFactor===null)speedFactor=0.1;if(arguments.length<3||outerHeight===null)outerHeight=!0;function update(){var pos=$w indow.scrollTop();$this.each(function(){var $element=$(this);var top=$element.offset().top;var height=getHeight($element);if(top+height<pos||top>pos+windowHeight) {return}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\mediaelement-and-player[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	86415
Entropy (8bit):	5.21628935717835
Encrypted:	false
SSDEEP:	768:+cxI9UGkAKCOlqdyo+Gj7H6Rdc9/mNotkxWGU2phBsKK40Lg757fYib2bi+uWab+:+cOCGkAKCOlqdyo+Gj7aRdc9/gw2pxq
MD5:	9FA8F59A0F47F2037D60DA99A31E3593
SHA1:	9ED96F5485564164699F3BDFC40A0CE198F63F93
SHA-256:	6929F335C538DE45301C8FBC86E50ABD7021BD61543C33130B83D288F4CA875E
SHA-512:	343217982B4BC2E60FB5D9A07E055538D65AD657748394856B039D8538A746B60AFFFD80E3412BBC3F7A175C306713CB1A21DE8C6035B617536B0D5F4C649DA6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://uptimeinstitute.com/media/widgetkit/widgets/mediaplayer/mediaelement/mediaelement-and-player.js?wkv=1.4.9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\mediaelement-and-player[1].js	
Preview:	var mejs=mejs||{};mejs.version="2.13.2";mejs.meIndex=0;mejs.plugins={silverlight:[{version:[3,0],types:["video/mp4","video/m4v","video/mov","video/wmv","audio/wma","audio/m4a","audio/mp3","audio/wav","audio/mpeg"]}],flash:[{version:[9,0,124],types:["video/mp4","video/m4v","video/mov","video/flv","video/rtmp","video/x-flv","audio/flv","audio/x-flv","audio/mp3","audio/m4a","audio/mpeg","video/youtube","video/x-youtube"]}],youtube:[{version:null,types:["video/youtube","video/x-youtube","audio/youtube","audio/x-youtube"]}],vimeo:[{version:null,types:["video/vimeo","video/x-vimeo"]}]};mejs.Utility={encodeUrl:function(url){return encodeURIComponent(url)},escapeHTML:function(s){return s.toString().split("&").join("&").split("<").join("<").split("").join(""")},absolutizeUrl:function(url){var el=document.createElement("div");el.innerHTML='x';return el.firstChild.href},getScriptPath:function(scriptNames){var i=0,j,codePath="",testname="",slashP

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\memnYaGs126MiZpBA-UFUKW-U9hIIqU[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23868, version 1.1
Category:	downloaded
Size (bytes):	23868
Entropy (8bit):	7.979638985615689
Encrypted:	false
SSDEEP:	384:a9YHfFZFePSGOLmI/WzYJb0u5XG2pyuLku5UtnK4yj1CPVkasY8C/EU0a6k:N/F2s7uY2q22pyptjVkasvCcjzk
MD5:	AEFF9F0AF1A6193B84B19ECA87EA4880
SHA1:	EF93A075CEFCF2A9ADB8C5F47F6E4073070B9210
SHA-256:	A97D00D68E7A6805D042116D737E92690809443E87F08085FCA52F78C6FABCCF
SHA-512:	D57FD22A73F5BDE931CEA3BFA8F2ED0D66B46EF108CDF8A800DF184505A53101E2CFFF8F221C6E78EDA813B04073675A5BF8946A71E68D2270DD329AB4BA281
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKW-U9hIIqU.woff
Preview:	wOFF.....]<.....GDEF.....6...:.z..GPOS.....GSUB.....$5"OS/2...X...]...`..!.cmap.....6.....cvt .....o.....fpgm...`.....s.ugasp.....#glyf...Fp..pn....head..O....6...6....hhea..O....#...$....hmtx..O....4...`l.=`loca..S.....2_\BFmaxp..V0... ... .]..name..VP.....8Gtpost..WL.....y. .prep..\ .....@..R.x.c`d``.a..&.v..F..FFWFW ....$=...d.c%..fl.....]r.2.....x.U....P.E.}.....5.\A.kX..k..\.....v.c.1.p...X8../....n.C...\.%...Z..u...\.p.}.1\....z.#.....)..KB8.~.9...]]...Rg.~.1xT.jH.....3.....x.%..@0...?.%.N.OJ.s&pJ...:[h-.a.{..(|....nw-..7...).L...'...T.M7..bz..~.)b.....\.....x....]Q...o.....6..qm...~.....g..3..s. J..*.4o...>(.....|.76g;N.Ln....uFQM=..<6o.O.....m.M.#...T..bE..4...M..29-..r.j..5.....a...3....s.ge..y-sH1.....&.c.r.jR[....k.p*s.Tx. .h@_.>...Z.==....n.^.....k....`.....^...us\/..us]]...rM]}/.{.=.....R..Q.(.7.%.....Bx..<.0.F8. .G..Y.u...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\memnYaGs126MiZpBA-UFUKWiUNhIIqU[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23408, version 1.1
Category:	downloaded
Size (bytes):	23408
Entropy (8bit):	7.978409043250865
Encrypted:	false
SSDEEP:	384:j08SX8c0+xc6rxYT9FQkeKX1QG2BP2KFlVuaMYtsKqe3a9MMzjF5aSP2ZW0a6HZ:8Xf0++OqTTQgSFBP/lV+YOKKjMzHZ
MD5:	D7E0C8F45B667E66E0FA94D77D6B2F11
SHA1:	4A5442D59539782926397E807BA97441C55D66D1
SHA-256:	F461846EBDE06B126199AB1B219003C99009D9A40CAFDC0D3ABF86565B62E3E8
SHA-512:	E38C6D197138F9868A6B52E9BF463A3CBEF615CEDEDD78DDA54F385FE437C626699FCD75F66009AA8D83CF3E124F1BB1940A1896DDA5CF14C3AA99AB98AAC82
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKWiUNhIIqU.woff
Preview:	wOFF.....[p.....T.....GDEF.....6...:.z..GPOS.....GSUB.....$5"OS/2...X...]...`....cmap.....6.....cvt .....b.....g.ifpgm...T.....s.ugasp.....glyf...E...pBEN$Zhead..N....6...6..{.hhea..N<...#...$....hmtx..N`.....`..PSloca..Q.....2Il,+maxp..T.... ... .*..name..T.....)/C.post..U.....y. .prep..Z.....x.c`d``.a..&.v..F..FFWFW ....$=...d.c%..fl.....]r.2.....x.U....P.E.}.....5.\A.kX..k..\.....v.c.1.p...X8../....n.C...\.%...Z..u...\.p.}.1\....z.#.....)..KB8.~.9...]]...Rg.~.1xT.jH.....3.....x.c`f9.....u..1...<.f.....A.(.....@`.....//..?....^..... 9.8.m@J....}.....x....]Q...o.....6..qm...~.....g..3..s. J..*.4o...>(.....|.76g;N.Ln....uFQM=..<6o.O.....m.M.#...T..bE..4...M..29-..r.j..5.....a...3....s.ge..y-sH1.....&.c.r.jR[....k.p*s.Tx. .h@_.>...Z.==....n.^.....k....`.....^...us\/..us]]...rM]}/.{.=.....R..Q.(.7.%.....Bx..<.0.F8. .G..Y.u...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\normalize.min[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):	1934
Entropy (8bit):	4.98338924175476
Encrypted:	false
SSDEEP:	24:BiLOQK04tXKTPJmyOk7S+ftxdtAXREbVO8o03PtpxVo7YgVsTQ/WYqlrmufpc+To:MB7ZSm70P0/tpxoCi6lrJRc+t9ZeTdn
MD5:	350564E02A1F081BB16171BF2C9A10A4
SHA1:	B70F77268B43925D62AB6354A9B377CBF0BFB475
SHA-256:	FCEF96BD3D8479BD51214EA2308B44862E719474C22C78361E02E6546156C96F
SHA-512:	3A3AADED8A57A9833AFFF01D32112B577A2DDFCAD880617940B244C31EF385EB232FD56A7E15A2473FDD58ADB686C9FDE91373D022E5F39FA98353F40667E05
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/normalize/3.0.3/normalize.min.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\normalize.min[1].css	
Preview:	/*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */html{font-family:sans-serif;-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background-color:transparent}a:active,a:hover{outline:0}abbr[title]{border-bottom:1px dotted}b,strong{font-weight:bold}dfn{font-style:italic}h1{font-size:2em;margin:.67em 0}mark{background:#ff0;color:#000}small{font-size:80%}sub,sup{font-size:75%;line-height:0;position:relative;vertical-align:baseline}sup{top:-0.5em}sub{bottom:-0.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:1em 40px}hr{box-sizing:content-box;height:0}pre{overflow:auto}code,kbd,pre,samp{font-family:monospace,monospace;font-size:1em}button,input,optgroup,select,textarea{color:inheri

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\oktrk[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):	9198
Entropy (8bit):	5.272951187413071
Encrypted:	false
SSDEEP:	192:QFJs4kmsKUQxqojFo2k7anTCgjEKDqUxT6+U/:UJrkmsKUwFo2k2nTCgjtli
MD5:	57315C24D6FEC75C4D46A8CC3FA6E0D5
SHA1:	58900450D7F3F70CF32421E034C39C9D2BBB0A2E
SHA-256:	09016600A13DD4825B72516765A8DA53D1AB896F7582C4619D014E8EE147EA84
SHA-512:	5F8D9C1EED2F3C01D1F3017F1F86761592E3BB6C8F65FF7F140D3CB249C9DE153544AE4A919400542894A04595C2EB74756766569242570F4906848470C6B9CC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.oktopost.com/oktrk.js
Preview:	!function(){"use strict";var o,i,a,t,u,r,s,B,l,c={domain:"okt.to",paths:{convert:"/c",ping:"/ping",lead:"/ping/form"}},f=window.OktopostTrackerObject||"_oktrk",e=window[f].q||[],d=[];t="oktrkCallback_",a=function(o){var a=this,i=o.debug,l=function(){return t+Math.floor(1e3*Math.random()+1)},c=function(t,e){if("function"==typeof e||i.isDebugSet()){var n,r,o=function(){for(var t=l();void 0!==window[f][t];)t=l();return t}();n=o,r=e,window[f][n]=function(t){window[f][n]=void 0,delete window[f][n],i.debug(t),"function"==typeof r&&r(t)},t.callback=f+"."+o}};a.getCacheBuster=function(){return(new Date).getTime().toString()},a.getArrayFromHtmlCollection=function(t){var e,n=[];for(e=0;e<t.length;e++)n.push(t[e]);return n},a.isInArray=function(t,e){return-1!==a.indexInArray(t,e)},a.indexInArray=function(t,e){var n;for(n=t.length-1;0<=n;n--)if(t[n]===e)return n;return-1},a.getQueryParam=function(t){var e,n="";for(e in t)t.hasOwnProperty(e)&&(n=n+"&"+encodeURIComponent(e)+"="+encodeURIComponent(t[

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\pagebuilder[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	546
Entropy (8bit):	5.08387312088776
Encrypted:	false
SSDEEP:	6:URCgVMzVyp4yaSEIVyi4tSHuga5GGGh1SwcLia/elyNAFFBWtIcLia/iruwiYtIw:Uk3UaJgoGGD1n1qpi21shhw1kCL
MD5:	6A8E91C24B3BAE3F8AB32A1C6DF9B4EC
SHA1:	98769EE6832D88DB5B85864B495E3433BB78B82B
SHA-256:	9BA8AE1B40AC5E3DF95BB58BBDE96ACF18F61A63CAB13F58216CE7D666A0D748
SHA-512:	108075DB35A7CF474B612E0D45DDD035B06CD40C1211F7B171C36DB5C6A64CC266BD812B9DB9B95E0059C66971ACD25896D3229DF1557CE2EA746AD1C524B30
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://uptimeinstitute.com/plugins/system/helix3/assets/css/pagebuilder.css
Preview:	/**.* @package Helix3 Framework.* @author JoomShaper http://www.joomshaper.com.* @copyright Copyright (c) 2010 - 2016 JoomShaper.* @license http://www.gnu.org/licenses/gpl-2.0.html GNU/GPLv2 or Later.*/...sppb-row-container {. margin-right: auto;. margin-left: auto;. padding-left: 15px;. padding-right: 15px;.}.@media (min-width: 768px) {. .sppb-row-container {. width: 750px;. }.}.@media (min-width: 992px) {. .sppb-row-container {. width: 970px;. }.}.@media (min-width: 1200px) {. .sppb-row-container {. width: 1170px;. }.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\permaclosed[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	68
Entropy (8bit):	4.625316929997097
Encrypted:	false
SSDEEP:	3:YGKyNMvhdYc0WopJQAW/DZ:YGKuMvhdYYopzo
MD5:	F267542F8C80B7078E5EB19F8A070E6C
SHA1:	EDD62ED14499971041A29171BD9CD6182D3A0792
SHA-256:	5F255F3C49DD47038D0D222CC15CC982015528BCE5A305B104FDB43E5509B41E
SHA-512:	9CC1A7D5E5520A6FFB997F5AE3457128D31D4B68DF46AD3B4BF5A8629AF0716EFFE14B155A62B16EB51CF7AE2084062BD567CF60F8BA45F862E1629BBED1F0E7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://conversation.api.drift.com/conversations/2970831152/permaclosed

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\permaclosed[1].json	
Preview:	{"conversationId":2970831152,"messageText":null,"sentMessage":false}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\permaclosed[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	18
Entropy (8bit):	3.614369445886757
Encrypted:	false
SSDEEP:	3:PYg9q1Ri:PN9n
MD5:	CC7FD95A87EA3721CE1853BF3C4DD75E
SHA1:	7F687F7881ADF0FC407378D375A61B8F198C0912
SHA-256:	0F06A4C8D34690D4E42C81F232A5BDFE9FCBDE8A54B5CCD0609A313E90DA0879
SHA-512:	FD6C456B1A52743D3A1A599C6B453D2DE6C06246DBC60031C4079E4D2EFAD8D64C942C65C9244519669A46545757A990088CFE170A22EDCA1C4876561224DE8
Malicious:	false
Reputation:	low
Preview:	HEAD, GET, OPTIONS

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\polyfills-294c424039b0467de929[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):	92179
Entropy (8bit):	5.333518460749562
Encrypted:	false
SSDEEP:	1536:xCNdC7dSD/v3h5q6+zX/9AZ7w9hoxiMfPk:k0kz+zVbpN
MD5:	BC95CCE33231C5A860C265AF46179D68
SHA1:	F7C92F472259185B0BCA3EAD3F848418E5F5ACD9
SHA-256:	8FD56030FF403AD9BEDBC1BCEEDB951BA2FE1E95801AEAF2DC4F34556E03C2C6
SHA-512:	2B51B295E8E14524D84175C95F068E75068E656D2756584EB56624234AC23B9E944B6DABAA0E150A539409784211831B001EF5603F22C221F95EF42F380A6368
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://drift-lp-66680075.drift.click/_next/static/chunks/polyfills-294c424039b0467de929.js
Preview:	_N_E=(window.webpackJsonp_N_E=window.webpackJsonp_N_E||[]).push([[8],{Ri3X:function(t,e,r){(function(t){!function(){var e="undefined"!=typeof globalThis?globalThis:"undefined"!=typeof window?window:"undefined"!=typeof t?t:"undefined"!=typeof self?self:{};function r(t,e){return t(e={exports:{}},e.exports),e.exports}var n=function(t){return t&&t.Math==Math&&t},o=n("object"==typeof globalThis&&globalThis)||n("object"==typeof window&&window)||n("object"==typeof self&&self)||n("object"==typeof e&&e)||Function("return this")(),i=function(t){try{return!!t()}catch(t){return!0}},a=!i((function(){return 7!=Object.defineProperty({},1,{get:function(){return 7}})[1]})),u={}.propertyIsEnumerable,s=Object.getOwnPropertyDescriptor,c={f:s&&!u.call({1:2},1)?function(t){var e=s(this,t);return!!e&&e.enumerable}:u},f=function(t,e){return{enumerable:!(1&t),configurable:!(2&t),writable:!(4&t),value:e}},l={}.toString,h=function(t){return l.call(t).slice(8,-1)},p="".split,d=i((function(){return!Object("z").pro

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\preset4[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	assembler source, ASCII text
Category:	downloaded
Size (bytes):	48715
Entropy (8bit):	5.0405092600544394
Encrypted:	false
SSDEEP:	768:MRXvICvav+vsuvRHvsxvR0T+kpICpfp6pXpsapvjMhGHZyc8URTuQ1rLGfLBQE8:M1hGHZyCl
MD5:	2C2ACAD69B23B7280FD2ECE9CB125372
SHA1:	559896F8ED8C8E40D718B60A9D13FD3829B8804F
SHA-256:	4D722FC55B9FB3C27821AC6C04173B35DAE66CE4E03AF600F72CE7766573CB06
SHA-512:	4FC2F485ED1A1C3A358788316B37AB240EA245402537E3B0FF24A7CA65F5894DF902DBEBE01199104E8F0562644B04AD5D03940A03EE329452AABCF185C6D8D6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://uptimeinstitute.com/templates/flex/css/presets/preset4.css
Preview:	.major_color_bckg-100 {. background-color: #428bca;.}..major_color_bckg-90 {. background-color: rgba(66,139,202,0.9);.}..major_color_bckg-80 {. background-color: rgba(66,139,202,0.8);.}..major_color_bckg-70 {. background-color: rgba(66,139,202,0.7);.}..major_color_bckg-60 {. background-color: rgba(66,139,202,0.6);.}..major_color_bckg-50 {. background-color: rgba(66,139,202,0.5);.}..major_color_bckg-40 {. background-color: rgba(66,139,202,0.4);.}..major_color_bckg-30 {. background-color: rgba(66,139,202,0.3);.}..major_color_bckg-20 {. background-color: rgba(66,139,202,0.2);.}..major_color_bckg-10 {. background-color: rgba(66,139,202,0.1);.}..black_bckg-90 {. background-color: rgba(0,0,0,0.9);.}..black_bckg-80 {. background-color: rgba(0,0,0,0.8);.}..black_bckg-70 {. background-color: rgba(0,0,0,0.7);.}..black_bckg-60 {. background-color: rgba(0,0,0,0.6);.}..black_bckg-50 {. background-color: rgba(0,0,0,0.5);.}..black_bckg-40 {. background-color: rgba(0,0,0,0.4);.}..black

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\read[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\read[1].txt	
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.8731406795131336
Encrypted:	false
SSDEEP:	3:xORi:xn
MD5:	1424EB76249899D757E4D168341A50DC
SHA1:	42101E71440ABD46C8112A96D4D5C0DD445120CE
SHA-256:	16F1EFA415BFDD7ABCF8FDD76CC05AE6FA66FFDFDC730368ECEA89ECFE5C3A12
SHA-512:	271F3DFD54E2B14E6CEA6A45E09A9F1BCF1A3BFB19A7F66821C20D558A7FF7F3423EB25EEBF2391CCF36A9762DA22EB609017169BF34F7BFF562D61D1F7AD0 3
Malicious:	false
Reputation:	low
Preview:	POST, OPTIONS

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\read[2].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.8731406795131336
Encrypted:	false
SSDEEP:	3:xORi:xn
MD5:	1424EB76249899D757E4D168341A50DC
SHA1:	42101E71440ABD46C8112A96D4D5C0DD445120CE
SHA-256:	16F1EFA415BFDD7ABCF8FDD76CC05AE6FA66FFDFDC730368ECEA89ECFE5C3A12
SHA-512:	271F3DFD54E2B14E6CEA6A45E09A9F1BCF1A3BFB19A7F66821C20D558A7FF7F3423EB25EEBF2391CCF36A9762DA22EB609017169BF34F7BFF562D61D1F7AD0 3
Malicious:	false
Reputation:	low
Preview:	POST, OPTIONS

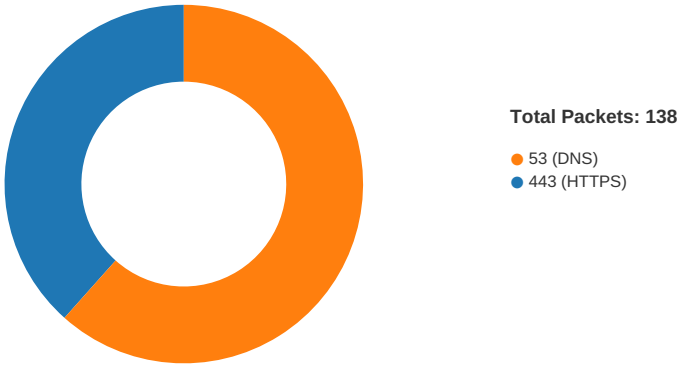
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\slick[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	6412
Entropy (8bit):	5.317054044235682
Encrypted:	false
SSDEEP:	192:YBX0NVRWY6FYgP9onNz+I2Rn4kA+UVKpuFLWmdFG+:+zs1+3RzuFpFr
MD5:	8D633FE842A23904BB2B60CC2EDE30A3
SHA1:	E9A56B95A7C7C7C9858A97C1092E41916E7CA13B
SHA-256:	33BDE17D3ED87824C30A6D1B31347D7751EA2E6C340C8163F278A2F53B38F8E1
SHA-512:	D340DFBB18DC97E3EDA05662F7D6D5A7A79107AEE058804FE527F9E0CF0E1C65CB182F9BC6FED8FC35DC153E5094C6386003A0D7B74F700D53613F5C90CE51 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://uptimeinstitute.com/templates/flex/sppagebuilder/addons/slick_carousel/assets/css/slick.css
Preview:	/* Slick */...slick-slider {. position: relative;. margin: 0 auto;. display: block;. -moz-box-sizing: border-box;. box-sizing: border-box;. -webkit-user-select: none;. -moz-user-select: none;. -ms-user-select: none;. user-select: none;. -webkit-touch-callout: none;. -khtml-user-select: none;. -ms-touch-action: pan-y;. touch-action: pan-y;. -webkit-tap-highlight-color: transparent;.}..slick-list {. position: relative;. display: block;. overflow: hidden;. margin: 0;. padding: 0;.}..slick-list:focus {. outline: none;.}..slick-list.dragging {. cursor: pointer;. cursor: hand;.}..slick-slider .slick-track,..slick-slider .slick-list {. -webkit-transform: translate3d(0, 0, 0);. -moz-transform: translate3d(0, 0, 0);. -ms-transform: translate3d(0, 0, 0);. -o-transform: translate3d(0, 0, 0);. transform: translate3d(0, 0, 0);.}..slick-track {. position: relative;. top: 0;. left: 0;. display: block;.}..slic

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 09:08:42.650126934 CET	49706	443	192.168.2.3	104.20.139.65
Jan 26, 2021 09:08:42.650253057 CET	49707	443	192.168.2.3	104.20.139.65
Jan 26, 2021 09:08:42.690006971 CET	443	49706	104.20.139.65	192.168.2.3
Jan 26, 2021 09:08:42.690149069 CET	49706	443	192.168.2.3	104.20.139.65
Jan 26, 2021 09:08:42.690486908 CET	443	49707	104.20.139.65	192.168.2.3
Jan 26, 2021 09:08:42.690644979 CET	49707	443	192.168.2.3	104.20.139.65
Jan 26, 2021 09:08:42.700220108 CET	49706	443	192.168.2.3	104.20.139.65
Jan 26, 2021 09:08:42.700750113 CET	49707	443	192.168.2.3	104.20.139.65
Jan 26, 2021 09:08:42.740125895 CET	443	49706	104.20.139.65	192.168.2.3
Jan 26, 2021 09:08:42.740719080 CET	443	49707	104.20.139.65	192.168.2.3
Jan 26, 2021 09:08:42.741710901 CET	443	49706	104.20.139.65	192.168.2.3
Jan 26, 2021 09:08:42.741729975 CET	443	49706	104.20.139.65	192.168.2.3
Jan 26, 2021 09:08:42.741832972 CET	49706	443	192.168.2.3	104.20.139.65
Jan 26, 2021 09:08:42.742301941 CET	443	49707	104.20.139.65	192.168.2.3
Jan 26, 2021 09:08:42.742332935 CET	443	49707	104.20.139.65	192.168.2.3
Jan 26, 2021 09:08:42.742458105 CET	49707	443	192.168.2.3	104.20.139.65
Jan 26, 2021 09:08:42.742503881 CET	49707	443	192.168.2.3	104.20.139.65
Jan 26, 2021 09:08:42.783171892 CET	49706	443	192.168.2.3	104.20.139.65
Jan 26, 2021 09:08:42.783359051 CET	49707	443	192.168.2.3	104.20.139.65
Jan 26, 2021 09:08:42.788645983 CET	49706	443	192.168.2.3	104.20.139.65
Jan 26, 2021 09:08:42.788837910 CET	49706	443	192.168.2.3	104.20.139.65
Jan 26, 2021 09:08:42.788866997 CET	49707	443	192.168.2.3	104.20.139.65
Jan 26, 2021 09:08:42.823025942 CET	443	49706	104.20.139.65	192.168.2.3
Jan 26, 2021 09:08:42.823271036 CET	443	49706	104.20.139.65	192.168.2.3
Jan 26, 2021 09:08:42.823286057 CET	443	49706	104.20.139.65	192.168.2.3
Jan 26, 2021 09:08:42.823295116 CET	443	49707	104.20.139.65	192.168.2.3
Jan 26, 2021 09:08:42.823482037 CET	49706	443	192.168.2.3	104.20.139.65
Jan 26, 2021 09:08:42.823792934 CET	443	49707	104.20.139.65	192.168.2.3
Jan 26, 2021 09:08:42.823812962 CET	443	49707	104.20.139.65	192.168.2.3
Jan 26, 2021 09:08:42.823957920 CET	49707	443	192.168.2.3	104.20.139.65
Jan 26, 2021 09:08:42.825129986 CET	49706	443	192.168.2.3	104.20.139.65
Jan 26, 2021 09:08:42.825784922 CET	49707	443	192.168.2.3	104.20.139.65
Jan 26, 2021 09:08:42.828567982 CET	443	49706	104.20.139.65	192.168.2.3
Jan 26, 2021 09:08:42.828583956 CET	443	49706	104.20.139.65	192.168.2.3
Jan 26, 2021 09:08:42.828756094 CET	443	49707	104.20.139.65	192.168.2.3
Jan 26, 2021 09:08:42.829164028 CET	443	49706	104.20.139.65	192.168.2.3
Jan 26, 2021 09:08:42.829262018 CET	49706	443	192.168.2.3	104.20.139.65
Jan 26, 2021 09:08:42.829349995 CET	443	49707	104.20.139.65	192.168.2.3
Jan 26, 2021 09:08:42.829488039 CET	49707	443	192.168.2.3	104.20.139.65
Jan 26, 2021 09:08:42.906764984 CET	443	49706	104.20.139.65	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 09:08:42.908588886 CET	443	49707	104.20.139.65	192.168.2.3
Jan 26, 2021 09:08:45.195575953 CET	443	49706	104.20.139.65	192.168.2.3
Jan 26, 2021 09:08:45.195620060 CET	443	49706	104.20.139.65	192.168.2.3
Jan 26, 2021 09:08:45.195646048 CET	443	49706	104.20.139.65	192.168.2.3
Jan 26, 2021 09:08:45.195683956 CET	443	49706	104.20.139.65	192.168.2.3
Jan 26, 2021 09:08:45.195693016 CET	49706	443	192.168.2.3	104.20.139.65
Jan 26, 2021 09:08:45.195760012 CET	49706	443	192.168.2.3	104.20.139.65
Jan 26, 2021 09:08:45.195804119 CET	49706	443	192.168.2.3	104.20.139.65
Jan 26, 2021 09:08:45.286698103 CET	49709	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.287997007 CET	49710	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.412605047 CET	443	49709	52.20.141.124	192.168.2.3
Jan 26, 2021 09:08:45.412740946 CET	49709	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.413326979 CET	49709	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.413881063 CET	443	49710	52.20.141.124	192.168.2.3
Jan 26, 2021 09:08:45.414021015 CET	49710	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.414499044 CET	49710	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.539007902 CET	443	49709	52.20.141.124	192.168.2.3
Jan 26, 2021 09:08:45.539949894 CET	443	49709	52.20.141.124	192.168.2.3
Jan 26, 2021 09:08:45.539995909 CET	443	49709	52.20.141.124	192.168.2.3
Jan 26, 2021 09:08:45.540038109 CET	443	49709	52.20.141.124	192.168.2.3
Jan 26, 2021 09:08:45.540075064 CET	443	49709	52.20.141.124	192.168.2.3
Jan 26, 2021 09:08:45.540119886 CET	49709	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.540230036 CET	49709	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.540256977 CET	443	49710	52.20.141.124	192.168.2.3
Jan 26, 2021 09:08:45.541107893 CET	443	49710	52.20.141.124	192.168.2.3
Jan 26, 2021 09:08:45.541147947 CET	443	49710	52.20.141.124	192.168.2.3
Jan 26, 2021 09:08:45.541183949 CET	443	49710	52.20.141.124	192.168.2.3
Jan 26, 2021 09:08:45.541229963 CET	443	49710	52.20.141.124	192.168.2.3
Jan 26, 2021 09:08:45.541282892 CET	49710	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.541347027 CET	49710	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.541363955 CET	49710	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.557085991 CET	49709	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.557399035 CET	49710	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.558043957 CET	49709	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.558156967 CET	49710	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.558269978 CET	49709	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.726944923 CET	443	49709	52.20.141.124	192.168.2.3
Jan 26, 2021 09:08:45.797343969 CET	443	49709	52.20.141.124	192.168.2.3
Jan 26, 2021 09:08:45.797416925 CET	49709	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.797422886 CET	443	49709	52.20.141.124	192.168.2.3
Jan 26, 2021 09:08:45.797466993 CET	443	49709	52.20.141.124	192.168.2.3
Jan 26, 2021 09:08:45.797483921 CET	49709	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.797527075 CET	49709	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.797755003 CET	443	49709	52.20.141.124	192.168.2.3
Jan 26, 2021 09:08:45.797781944 CET	443	49709	52.20.141.124	192.168.2.3
Jan 26, 2021 09:08:45.797812939 CET	49709	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.797835112 CET	49709	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.885519028 CET	49710	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.923053980 CET	443	49709	52.20.141.124	192.168.2.3
Jan 26, 2021 09:08:45.923099041 CET	443	49709	52.20.141.124	192.168.2.3
Jan 26, 2021 09:08:45.923127890 CET	49709	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.923135042 CET	443	49709	52.20.141.124	192.168.2.3
Jan 26, 2021 09:08:45.923157930 CET	49709	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.923190117 CET	49709	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.923877954 CET	49709	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.958966970 CET	443	49710	52.20.141.124	192.168.2.3
Jan 26, 2021 09:08:45.959112883 CET	49710	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.974648952 CET	49709	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.993490934 CET	49709	443	192.168.2.3	52.20.141.124
Jan 26, 2021 09:08:45.993657112 CET	49709	443	192.168.2.3	52.20.141.124

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 09:08:41.494119883 CET	64938	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:41.551755905 CET	53	64938	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:42.579144955 CET	60152	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:42.635427952 CET	53	60152	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:44.160881996 CET	57544	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:44.209203959 CET	53	57544	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:45.215749979 CET	55984	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:45.283195019 CET	53	55984	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:45.413853884 CET	64185	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:45.461869955 CET	53	64185	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:45.983625889 CET	65110	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:45.998668909 CET	58361	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:46.041501999 CET	53	65110	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:46.062695026 CET	53	58361	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:46.070867062 CET	63492	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:46.132272959 CET	53	63492	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:46.157196999 CET	60831	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:46.221060038 CET	53	60831	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:46.352556944 CET	60100	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:46.411896944 CET	53	60100	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:46.451111078 CET	53195	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:46.509356022 CET	53	53195	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:46.747767925 CET	50141	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:46.807012081 CET	53	50141	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:47.000236988 CET	53023	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:47.007801056 CET	49563	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:47.048119068 CET	53	53023	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:47.064057112 CET	53	49563	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:49.930422068 CET	51352	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:49.978301048 CET	53	51352	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:50.043304920 CET	59349	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:50.101975918 CET	53	59349	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:50.197149992 CET	57084	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:50.253371954 CET	53	57084	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:51.036478996 CET	58823	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:51.095171928 CET	53	58823	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:52.042665958 CET	57568	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:52.085402966 CET	50540	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:52.107099056 CET	53	57568	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:52.144540071 CET	53	50540	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:52.146502018 CET	54366	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:52.202893019 CET	53	54366	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:52.781517982 CET	53034	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:52.786108971 CET	57762	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:52.801110983 CET	55435	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:52.811182976 CET	50713	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:52.839504004 CET	53	53034	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:52.846508026 CET	53	57762	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:52.857244015 CET	53	55435	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:52.870352983 CET	53	50713	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:53.609977961 CET	56132	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:53.660851002 CET	53	56132	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:54.646363974 CET	58987	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:54.708287954 CET	53	58987	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:54.845717907 CET	56579	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:54.905486107 CET	53	56579	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:55.623410940 CET	60633	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:55.682986975 CET	53	60633	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:59.129395962 CET	61292	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:59.185915947 CET	53	61292	8.8.8.8	192.168.2.3
Jan 26, 2021 09:08:59.477699995 CET	63619	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:08:59.534230947 CET	53	63619	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:00.860697031 CET	64938	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:00.908988953 CET	53	64938	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 09:09:04.905579090 CET	61946	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:04.956680059 CET	53	61946	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:05.009303093 CET	64910	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:05.068783998 CET	53	64910	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:06.432008982 CET	52123	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:06.492196083 CET	53	52123	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:08.145958900 CET	56130	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:08.196830988 CET	53	56130	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:08.359271049 CET	56338	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:08.417073011 CET	53	56338	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:08.431246042 CET	59420	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:08.438011885 CET	58784	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:08.497862101 CET	53	58784	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:08.499927998 CET	53	59420	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:09.049443960 CET	63978	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:09.107965946 CET	53	63978	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:09.406824112 CET	62938	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:09.414330006 CET	55708	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:09.457529068 CET	53	62938	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:09.483545065 CET	53	55708	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:09.731781006 CET	56803	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:09.762049913 CET	57145	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:09.780036926 CET	53	56803	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:09.810674906 CET	53	57145	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:10.377356052 CET	55359	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:10.518666983 CET	58306	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:10.524118900 CET	53	55359	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:10.581808090 CET	53	58306	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:12.637202024 CET	64124	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:12.693648100 CET	53	64124	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:12.774436951 CET	49361	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:12.822525024 CET	53	49361	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:13.133934021 CET	63150	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:13.192095995 CET	53	63150	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:13.693092108 CET	64124	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:13.740940094 CET	53	64124	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:13.820363045 CET	49361	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:13.876615047 CET	53	49361	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:14.062340975 CET	53279	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:14.123425961 CET	53	53279	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:14.696069956 CET	64124	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:14.752749920 CET	53	64124	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:14.847429991 CET	49361	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:14.903825045 CET	53	49361	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:15.966713905 CET	56881	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:16.014547110 CET	53	56881	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:16.700128078 CET	64124	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:16.757600069 CET	53	64124	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:16.854809999 CET	49361	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:16.904268980 CET	53	49361	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:17.788582087 CET	53642	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:17.845344067 CET	53	53642	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:19.579773903 CET	55667	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:19.630659103 CET	53	55667	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:20.906287909 CET	64124	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:20.962675095 CET	53	64124	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:21.318764925 CET	49361	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:21.366823912 CET	53	49361	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:21.374914885 CET	54833	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:21.422909975 CET	53	54833	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:22.386173010 CET	62476	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:22.434295893 CET	53	62476	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:23.923084974 CET	49705	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:23.971126080 CET	53	49705	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 09:09:25.332473040 CET	61477	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:25.383481026 CET	53	61477	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:25.627716064 CET	61633	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:25.694638014 CET	53	61633	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:26.312925100 CET	55949	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:26.373943090 CET	53	55949	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:26.569775105 CET	57601	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:26.620788097 CET	53	57601	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:26.912378073 CET	49342	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:26.963196039 CET	53	49342	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:44.634438992 CET	56253	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:44.695096016 CET	53	56253	8.8.8.8	192.168.2.3
Jan 26, 2021 09:09:59.876040936 CET	49667	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:09:59.934710026 CET	53	49667	8.8.8.8	192.168.2.3
Jan 26, 2021 09:10:03.748498917 CET	55439	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:10:03.806440115 CET	53	55439	8.8.8.8	192.168.2.3
Jan 26, 2021 09:10:03.887788057 CET	57069	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:10:03.948180914 CET	53	57069	8.8.8.8	192.168.2.3
Jan 26, 2021 09:10:04.763708115 CET	55439	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:10:04.822688103 CET	53	55439	8.8.8.8	192.168.2.3
Jan 26, 2021 09:10:04.926632881 CET	57069	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:10:04.988225937 CET	53	57069	8.8.8.8	192.168.2.3
Jan 26, 2021 09:10:06.124723911 CET	55439	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:10:06.124798059 CET	57069	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:10:06.182928085 CET	53	55439	8.8.8.8	192.168.2.3
Jan 26, 2021 09:10:06.183942080 CET	53	57069	8.8.8.8	192.168.2.3
Jan 26, 2021 09:10:08.145387888 CET	57069	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:10:08.145459890 CET	55439	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:10:08.202447891 CET	53	55439	8.8.8.8	192.168.2.3
Jan 26, 2021 09:10:08.205065966 CET	53	57069	8.8.8.8	192.168.2.3
Jan 26, 2021 09:10:12.275455952 CET	55439	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:10:12.275526047 CET	57069	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:10:12.332443953 CET	53	55439	8.8.8.8	192.168.2.3
Jan 26, 2021 09:10:12.337264061 CET	53	57069	8.8.8.8	192.168.2.3
Jan 26, 2021 09:10:28.935844898 CET	57659	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:10:28.999878883 CET	53	57659	8.8.8.8	192.168.2.3
Jan 26, 2021 09:10:31.738666058 CET	54717	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:10:31.796360970 CET	53	54717	8.8.8.8	192.168.2.3
Jan 26, 2021 09:11:01.711750031 CET	63975	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:11:01.759866953 CET	53	63975	8.8.8.8	192.168.2.3
Jan 26, 2021 09:11:02.789902925 CET	56639	53	192.168.2.3	8.8.8.8
Jan 26, 2021 09:11:02.849078894 CET	53	56639	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 26, 2021 09:08:42.579144955 CET	192.168.2.3	8.8.8.8	0xd707	Standard query (0)	tinyurl.com	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:45.215749979 CET	192.168.2.3	8.8.8.8	0x8803	Standard query (0)	drift-lp-66680075.drift.click	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:45.983625889 CET	192.168.2.3	8.8.8.8	0x5631	Standard query (0)	file2.api.drift.com	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:46.070867062 CET	192.168.2.3	8.8.8.8	0x7e43	Standard query (0)	js.driftt.com	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:46.157196999 CET	192.168.2.3	8.8.8.8	0x4b4e	Standard query (0)	s3.amazonaws.com	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:46.451111078 CET	192.168.2.3	8.8.8.8	0xf6fd	Standard query (0)	drift-prod-file-uploads.s3.amazonaws.com	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:46.747767925 CET	192.168.2.3	8.8.8.8	0x74e1	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:47.007801056 CET	192.168.2.3	8.8.8.8	0xe3f1	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:49.930422068 CET	192.168.2.3	8.8.8.8	0xe591	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 26, 2021 09:08:51.036478996 CET	192.168.2.3	8.8.8.8	0x19e	Standard query (0)	embeds.driftcdn.com	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.042665958 CET	192.168.2.3	8.8.8.8	0x967f	Standard query (0)	customer.api.drift.com	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.085402966 CET	192.168.2.3	8.8.8.8	0x207d	Standard query (0)	metrics.api.drift.com	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.781517982 CET	192.168.2.3	8.8.8.8	0x48bf	Standard query (0)	event.api.drift.com	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.786108971 CET	192.168.2.3	8.8.8.8	0x2a3c	Standard query (0)	107326-26.chat.api.drift.com	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.801110983 CET	192.168.2.3	8.8.8.8	0x3e9f	Standard query (0)	targeting.api.drift.com	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.811182976 CET	192.168.2.3	8.8.8.8	0x1f37	Standard query (0)	presence.api.drift.com	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:54.646363974 CET	192.168.2.3	8.8.8.8	0x7acb	Standard query (0)	messaging.api.drift.com	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:54.845717907 CET	192.168.2.3	8.8.8.8	0x40f	Standard query (0)	driftt.imgix.net	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:55.623410940 CET	192.168.2.3	8.8.8.8	0x701	Standard query (0)	conversation.api.drift.com	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:05.009303093 CET	192.168.2.3	8.8.8.8	0x462d	Standard query (0)	uptimeinstitute.com	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:06.432008982 CET	192.168.2.3	8.8.8.8	0x3765	Standard query (0)	fast.wistia.com	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:08.359271049 CET	192.168.2.3	8.8.8.8	0x1053	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:08.431246042 CET	192.168.2.3	8.8.8.8	0x5942	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:08.438011885 CET	192.168.2.3	8.8.8.8	0x24ea	Standard query (0)	static.oktopost.com	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:09.049443960 CET	192.168.2.3	8.8.8.8	0xa98e	Standard query (0)	okt.to	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:09.406824112 CET	192.168.2.3	8.8.8.8	0x12ca	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:09.414330006 CET	192.168.2.3	8.8.8.8	0x3335	Standard query (0)	munchkin.marketo.net	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:09.731781006 CET	192.168.2.3	8.8.8.8	0x84e4	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:10.377356052 CET	192.168.2.3	8.8.8.8	0xc573	Standard query (0)	711-ria-145.mktoresp.com	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:10.518666983 CET	192.168.2.3	8.8.8.8	0x7f3b	Standard query (0)	cdn.leadmanagerfx.com	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:13.133934021 CET	192.168.2.3	8.8.8.8	0x13b8	Standard query (0)	embedwistia-a.akamaihd.net	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:17.788582087 CET	192.168.2.3	8.8.8.8	0xb67a	Standard query (0)	distillery.wistia.com	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:21.374914885 CET	192.168.2.3	8.8.8.8	0x50c6	Standard query (0)	pipedream.wistia.com	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:59.876040936 CET	192.168.2.3	8.8.8.8	0x3d54	Standard query (0)	fg8vvsvnieiv3ej16jby.litix.io	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2021 09:08:42.635427952 CET	8.8.8.8	192.168.2.3	0xd707	No error (0)	tinyurl.com		104.20.139.65	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:42.635427952 CET	8.8.8.8	192.168.2.3	0xd707	No error (0)	tinyurl.com		172.67.1.225	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:42.635427952 CET	8.8.8.8	192.168.2.3	0xd707	No error (0)	tinyurl.com		104.20.138.65	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:45.283195019 CET	8.8.8.8	192.168.2.3	0x8803	No error (0)	drift-lp-66680075.drift.click		52.20.141.124	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:45.283195019 CET	8.8.8.8	192.168.2.3	0x8803	No error (0)	drift-lp-66680075.drift.click		34.225.101.196	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:46.041501999 CET	8.8.8.8	192.168.2.3	0x5631	No error (0)	file2.api.drift.com	istio.api.drift.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2021 09:08:46.041501999 CET	8.8.8.8	192.168.2.3	0x5631	No error (0)	istio.api.drift.com	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 09:08:46.041501999 CET	8.8.8.8	192.168.2.3	0x5631	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		54.147.21.139	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:46.041501999 CET	8.8.8.8	192.168.2.3	0x5631	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		3.94.218.138	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:46.041501999 CET	8.8.8.8	192.168.2.3	0x5631	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		34.193.113.164	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:46.041501999 CET	8.8.8.8	192.168.2.3	0x5631	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		50.16.7.188	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:46.132272959 CET	8.8.8.8	192.168.2.3	0x7e43	No error (0)	js.driftt.com	dl7g9llrghqi1.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 09:08:46.132272959 CET	8.8.8.8	192.168.2.3	0x7e43	No error (0)	dl7g9llrghqi1.cloudfront.net		13.224.94.49	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:46.132272959 CET	8.8.8.8	192.168.2.3	0x7e43	No error (0)	dl7g9llrghqi1.cloudfront.net		13.224.94.39	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:46.132272959 CET	8.8.8.8	192.168.2.3	0x7e43	No error (0)	dl7g9llrghqi1.cloudfront.net		13.224.94.122	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:46.132272959 CET	8.8.8.8	192.168.2.3	0x7e43	No error (0)	dl7g9llrghqi1.cloudfront.net		13.224.94.64	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:46.221060038 CET	8.8.8.8	192.168.2.3	0x4b4e	No error (0)	s3.amazonaws.com		52.216.137.118	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:46.509356022 CET	8.8.8.8	192.168.2.3	0xf6fd	No error (0)	drift-prod-file-uploads.s3.amazonaws.com	s3-1-w.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 09:08:46.509356022 CET	8.8.8.8	192.168.2.3	0xf6fd	No error (0)	s3-1-w.amazonaws.com		52.216.26.196	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:46.807012081 CET	8.8.8.8	192.168.2.3	0x74e1	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 09:08:46.807012081 CET	8.8.8.8	192.168.2.3	0x74e1	No error (0)	stats.l.doubleclick.net		108.177.15.154	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:46.807012081 CET	8.8.8.8	192.168.2.3	0x74e1	No error (0)	stats.l.doubleclick.net		108.177.15.157	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:46.807012081 CET	8.8.8.8	192.168.2.3	0x74e1	No error (0)	stats.l.doubleclick.net		108.177.15.155	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:46.807012081 CET	8.8.8.8	192.168.2.3	0x74e1	No error (0)	stats.l.doubleclick.net		108.177.15.156	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:47.064057112 CET	8.8.8.8	192.168.2.3	0xe3f1	No error (0)	www.google.co.uk		172.217.22.227	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:49.978301048 CET	8.8.8.8	192.168.2.3	0xe591	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2021 09:08:49.978301048 CET	8.8.8.8	192.168.2.3	0xe591	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:51.095171928 CET	8.8.8.8	192.168.2.3	0x19e	No error (0)	embeds.driftcdn.com		13.224.94.26	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:51.095171928 CET	8.8.8.8	192.168.2.3	0x19e	No error (0)	embeds.driftcdn.com		13.224.94.55	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:51.095171928 CET	8.8.8.8	192.168.2.3	0x19e	No error (0)	embeds.driftcdn.com		13.224.94.77	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:51.095171928 CET	8.8.8.8	192.168.2.3	0x19e	No error (0)	embeds.driftcdn.com		13.224.94.52	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.107099056 CET	8.8.8.8	192.168.2.3	0x967f	No error (0)	customer.api.drift.com	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 09:08:52.107099056 CET	8.8.8.8	192.168.2.3	0x967f	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		54.147.21.139	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.107099056 CET	8.8.8.8	192.168.2.3	0x967f	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		3.94.218.138	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.107099056 CET	8.8.8.8	192.168.2.3	0x967f	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		34.193.113.164	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.107099056 CET	8.8.8.8	192.168.2.3	0x967f	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		50.16.7.188	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.144540071 CET	8.8.8.8	192.168.2.3	0x207d	No error (0)	metrics.api.drift.com	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 09:08:52.144540071 CET	8.8.8.8	192.168.2.3	0x207d	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		50.16.7.188	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.144540071 CET	8.8.8.8	192.168.2.3	0x207d	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		3.94.218.138	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.144540071 CET	8.8.8.8	192.168.2.3	0x207d	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		34.193.113.164	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2021 09:08:52.144540071 CET	8.8.8.8	192.168.2.3	0x207d	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		54.147.21.139	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.839504004 CET	8.8.8.8	192.168.2.3	0x48bf	No error (0)	event.api.drift.com	alb-event-1454785217.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 09:08:52.839504004 CET	8.8.8.8	192.168.2.3	0x48bf	No error (0)	alb-event-1454785217.us-east-1.elb.amazonaws.com		18.205.49.143	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.839504004 CET	8.8.8.8	192.168.2.3	0x48bf	No error (0)	alb-event-1454785217.us-east-1.elb.amazonaws.com		18.204.181.250	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.846508026 CET	8.8.8.8	192.168.2.3	0x2a3c	No error (0)	107326-26.chat.api.drift.com	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 09:08:52.846508026 CET	8.8.8.8	192.168.2.3	0x2a3c	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		54.84.154.238	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.846508026 CET	8.8.8.8	192.168.2.3	0x2a3c	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		52.206.124.92	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.846508026 CET	8.8.8.8	192.168.2.3	0x2a3c	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		3.223.88.48	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.846508026 CET	8.8.8.8	192.168.2.3	0x2a3c	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		52.73.109.12	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.846508026 CET	8.8.8.8	192.168.2.3	0x2a3c	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		54.205.123.19	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.846508026 CET	8.8.8.8	192.168.2.3	0x2a3c	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		54.163.54.133	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.846508026 CET	8.8.8.8	192.168.2.3	0x2a3c	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		54.145.60.167	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.846508026 CET	8.8.8.8	192.168.2.3	0x2a3c	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		3.220.170.252	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.857244015 CET	8.8.8.8	192.168.2.3	0x3e9f	No error (0)	targeting.api.drift.com		100.24.186.63	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.857244015 CET	8.8.8.8	192.168.2.3	0x3e9f	No error (0)	targeting.api.drift.com		34.204.215.213	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.870352983 CET	8.8.8.8	192.168.2.3	0x1f37	No error (0)	presence.api.drift.com	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2021 09:08:52.870352983 CET	8.8.8.8	192.168.2.3	0x1f37	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		54.85.240.191	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.870352983 CET	8.8.8.8	192.168.2.3	0x1f37	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		54.173.95.250	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.870352983 CET	8.8.8.8	192.168.2.3	0x1f37	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		35.174.210.7	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:52.870352983 CET	8.8.8.8	192.168.2.3	0x1f37	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		52.0.218.127	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:54.708287954 CET	8.8.8.8	192.168.2.3	0x7acb	No error (0)	messaging.api.drift.com	istio.api.drift.com		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 09:08:54.708287954 CET	8.8.8.8	192.168.2.3	0x7acb	No error (0)	istio.api.drift.com	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 09:08:54.708287954 CET	8.8.8.8	192.168.2.3	0x7acb	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		54.147.21.139	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:54.708287954 CET	8.8.8.8	192.168.2.3	0x7acb	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		3.94.218.138	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:54.708287954 CET	8.8.8.8	192.168.2.3	0x7acb	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		34.193.113.164	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:54.708287954 CET	8.8.8.8	192.168.2.3	0x7acb	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		50.16.7.188	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:54.905486107 CET	8.8.8.8	192.168.2.3	0x40f	No error (0)	driftt.imgix.net	dualstack.com.imgix.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 09:08:54.905486107 CET	8.8.8.8	192.168.2.3	0x40f	No error (0)	dualstack.com.imgix.map.fastly.net		151.101.14.208	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:55.682986975 CET	8.8.8.8	192.168.2.3	0x701	No error (0)	conversation.api.drift.com	istio.api.drift.com		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 09:08:55.682986975 CET	8.8.8.8	192.168.2.3	0x701	No error (0)	istio.api.drift.com	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2021 09:08:55.682986975 CET	8.8.8.8	192.168.2.3	0x701	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		50.16.7.188	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:55.682986975 CET	8.8.8.8	192.168.2.3	0x701	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		3.94.218.138	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:55.682986975 CET	8.8.8.8	192.168.2.3	0x701	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		34.193.113.164	A (IP address)	IN (0x0001)
Jan 26, 2021 09:08:55.682986975 CET	8.8.8.8	192.168.2.3	0x701	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		54.147.21.139	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:05.068783998 CET	8.8.8.8	192.168.2.3	0x462d	No error (0)	uptimeinstitute.com		23.253.242.117	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:06.492196083 CET	8.8.8.8	192.168.2.3	0x3765	No error (0)	fast.wistia.com	dualstack.f4.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 09:09:08.417073011 CET	8.8.8.8	192.168.2.3	0x1053	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 09:09:08.417073011 CET	8.8.8.8	192.168.2.3	0x1053	No error (0)	scontent.xx.fbcdn.net		185.60.216.19	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:08.497862101 CET	8.8.8.8	192.168.2.3	0x24ea	No error (0)	static.oktopost.com	d21prwqavi0i2.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 09:09:08.497862101 CET	8.8.8.8	192.168.2.3	0x24ea	No error (0)	d21prwqavi0i2.cloudfront.net		13.224.94.89	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:08.497862101 CET	8.8.8.8	192.168.2.3	0x24ea	No error (0)	d21prwqavi0i2.cloudfront.net		13.224.94.6	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:08.497862101 CET	8.8.8.8	192.168.2.3	0x24ea	No error (0)	d21prwqavi0i2.cloudfront.net		13.224.94.121	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:08.497862101 CET	8.8.8.8	192.168.2.3	0x24ea	No error (0)	d21prwqavi0i2.cloudfront.net		13.224.94.86	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:08.499927998 CET	8.8.8.8	192.168.2.3	0x5942	No error (0)	snap.licdn.com	wildcard.licdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 09:09:09.107965946 CET	8.8.8.8	192.168.2.3	0xa98e	No error (0)	okt.to		34.200.97.200	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:09.107965946 CET	8.8.8.8	192.168.2.3	0xa98e	No error (0)	okt.to		52.20.195.32	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:09.107965946 CET	8.8.8.8	192.168.2.3	0xa98e	No error (0)	okt.to		23.22.90.252	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:09.457529068 CET	8.8.8.8	192.168.2.3	0x12ca	No error (0)	px.ads.linkedin.com	mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 09:09:09.457529068 CET	8.8.8.8	192.168.2.3	0x12ca	No error (0)	mix.linkedin.com	pop-efr5.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 09:09:09.457529068 CET	8.8.8.8	192.168.2.3	0x12ca	No error (0)	pop-efr5.mix.linkedin.com		185.63.145.5	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2021 09:09:09.483545065 CET	8.8.8.8	192.168.2.3	0x3335	No error (0)	munchkin.marketo.net	wildcard.marketo.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 09:09:09.780036926 CET	8.8.8.8	192.168.2.3	0x84e4	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 09:09:10.524118900 CET	8.8.8.8	192.168.2.3	0xc573	No error (0)	711-ria-145.mktoresp.com		192.28.147.68	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:10.581808090 CET	8.8.8.8	192.168.2.3	0x7f3b	No error (0)	cdn.leadmanagerfx.com	d2201ucog3v8ee.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 09:09:10.581808090 CET	8.8.8.8	192.168.2.3	0x7f3b	No error (0)	d2201ucog3v8ee.cloudfront.net		13.226.159.87	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:10.581808090 CET	8.8.8.8	192.168.2.3	0x7f3b	No error (0)	d2201ucog3v8ee.cloudfront.net		13.226.159.69	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:10.581808090 CET	8.8.8.8	192.168.2.3	0x7f3b	No error (0)	d2201ucog3v8ee.cloudfront.net		13.226.159.85	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:10.581808090 CET	8.8.8.8	192.168.2.3	0x7f3b	No error (0)	d2201ucog3v8ee.cloudfront.net		13.226.159.105	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:13.192095995 CET	8.8.8.8	192.168.2.3	0x13b8	No error (0)	embedwistia-a.akamaihd.net	embedwistia-a.akamaihd.net.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 09:09:17.845344067 CET	8.8.8.8	192.168.2.3	0xb67a	No error (0)	distillery.wistia.com	prod-east-stats-tap-alb-627711272.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 09:09:17.845344067 CET	8.8.8.8	192.168.2.3	0xb67a	No error (0)	prod-east-stats-tap-alb-627711272.us-east-1.elb.amazonaws.com		52.0.1.164	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:17.845344067 CET	8.8.8.8	192.168.2.3	0xb67a	No error (0)	prod-east-stats-tap-alb-627711272.us-east-1.elb.amazonaws.com		54.209.247.25	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:21.422909975 CET	8.8.8.8	192.168.2.3	0x50c6	No error (0)	pipedream.wistia.com	prod-east-pipedream-alb-988701200.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 09:09:21.422909975 CET	8.8.8.8	192.168.2.3	0x50c6	No error (0)	prod-east-pipedream-alb-988701200.us-east-1.elb.amazonaws.com		35.173.77.57	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:21.422909975 CET	8.8.8.8	192.168.2.3	0x50c6	No error (0)	prod-east-pipedream-alb-988701200.us-east-1.elb.amazonaws.com		34.205.237.238	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:26.373943090 CET	8.8.8.8	192.168.2.3	0x44bb	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 09:09:59.934710026 CET	8.8.8.8	192.168.2.3	0x3d54	No error (0)	fg8vvsvnieiv3ej16jby.litix.io	a4d6c1c8368a911ea98860aeb4e6dc37-182063218.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 09:09:59.934710026 CET	8.8.8.8	192.168.2.3	0x3d54	No error (0)	a4d6c1c8368a911ea98860aeb4e6dc37-182063218.us-east-1.elb.amazonaws.com		34.198.102.54	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:59.934710026 CET	8.8.8.8	192.168.2.3	0x3d54	No error (0)	a4d6c1c8368a911ea98860aeb4e6dc37-182063218.us-east-1.elb.amazonaws.com		52.5.78.18	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:59.934710026 CET	8.8.8.8	192.168.2.3	0x3d54	No error (0)	a4d6c1c8368a911ea98860aeb4e6dc37-182063218.us-east-1.elb.amazonaws.com		23.23.196.21	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2021 09:09:59.934710026 CET	8.8.8.8	192.168.2.3	0x3d54	No error (0)	a4d6c1c8368a911ea98860aeb4e6dc37-182063218.us-east-1.elb.amazonaws.com		3.210.75.230	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:59.934710026 CET	8.8.8.8	192.168.2.3	0x3d54	No error (0)	a4d6c1c8368a911ea98860aeb4e6dc37-182063218.us-east-1.elb.amazonaws.com		52.204.236.206	A (IP address)	IN (0x0001)
Jan 26, 2021 09:09:59.934710026 CET	8.8.8.8	192.168.2.3	0x3d54	No error (0)	a4d6c1c8368a911ea98860aeb4e6dc37-182063218.us-east-1.elb.amazonaws.com		52.20.19.138	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 26, 2021 09:08:42.741729975 CET	104.20.139.65	443	192.168.2.3	49706	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	Mon Aug 03 02:00:00 CEST 2020	Tue Aug 03 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
							Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 26, 2021 09:08:42.742332935 CET	104.20.139.65	443	192.168.2.3	49707	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	Mon Aug 03 02:00:00 CEST 2020	Tue Aug 03 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
							Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 26, 2021 09:08:45.540075064 CET	52.20.141.124	443	192.168.2.3	49709	CN=*.drift.click 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 Jul 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	Mon Aug 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 26, 2021 09:08:45.541229963 CET	52.20.141.124	443	192.168.2.3	49710	CN=*.drift.click 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 Jul 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	Mon Aug 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		
Jan 26, 2021 09:08:46.249170065 CET	13.224.94.49	443	192.168.2.3	49716	CN=drift.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	Mon Sep 21 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	Sat Oct 23 02:00:00 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		
Jan 26, 2021 09:08:46.249528885 CET	13.224.94.49	443	192.168.2.3	49717	CN=drift.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	Mon Sep 21 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	Sat Oct 23 02:00:00 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		
Jan 26, 2021 09:08:46.300985098 CET	54.147.21.139	443	192.168.2.3	49712	CN=drift.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	Mon Sep 21 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	Sat Oct 23 02:00:00 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 26, 2021 09:08:46.301240921 CET	54.147.21.139	443	192.168.2.3	49713	CN=drift.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	Mon Sep 21 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	Sat Oct 23 02:00:00 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		
Jan 26, 2021 09:08:46.476593018 CET	52.216.137.118	443	192.168.2.3	49719	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Jan 26, 2021 09:08:46.477309942 CET	52.216.137.118	443	192.168.2.3	49718	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Jan 26, 2021 09:08:46.764389038 CET	52.216.26.196	443	192.168.2.3	49722	CN=*.s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Nov 09 01:00:00 CET 2019 Tue Dec 08 13:05:07 CET 2015	Fri Mar 12 13:00:00 CET 2021 Sat May 10 14:00:00 CEST 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=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 26, 2021 09:08:46.764501095 CET	52.216.26.196	443	192.168.2.3	49723	CN=*.s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Nov 09 01:00:00 CET 2019 Tue Dec 08 13:05:07 CET 2015	Fri Mar 12 13:00:00 CET 2021 Sat May 10 14:00:00 CEST 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=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Jan 26, 2021 09:08:46.918705940 CET	108.177.15.154	443	192.168.2.3	49724	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 Jan 05 13:07:00 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 30 14:06:59 CEST 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		
Jan 26, 2021 09:08:46.919924021 CET	108.177.15.154	443	192.168.2.3	49725	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 Jan 05 13:07:00 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 30 14:06:59 CEST 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		
Jan 26, 2021 09:08:47.166835070 CET	172.217.22.227	443	192.168.2.3	49728	CN=www.google.co.uk, 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 Jan 05 13:11:42 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 30 14:11:41 CEST 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		
Jan 26, 2021 09:08:47.170423031 CET	172.217.22.227	443	192.168.2.3	49729	CN=www.google.co.uk, 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 Jan 05 13:11:42 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 30 14:11:41 CEST 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 26, 2021 09:08:50.097316980 CET	104.16.19.94	443	192.168.2.3	49731	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020	Thu Oct 21 01:59:59 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		
Jan 26, 2021 09:08:50.101944923 CET	104.16.19.94	443	192.168.2.3	49730	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020	Thu Oct 21 01:59:59 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		
Jan 26, 2021 09:08:51.191514969 CET	13.224.94.26	443	192.168.2.3	49739	CN=*.driftcdn.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	Fri Apr 10 02:00:00 CEST 2020	Mon May 10 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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 26, 2021 09:08:51.191647053 CET	13.224.94.26	443	192.168.2.3	49738	CN=*.driftcdn.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	Fri Apr 10 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	Mon May 10 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		
Jan 26, 2021 09:08:52.410562038 CET	54.147.21.139	443	192.168.2.3	49741	CN=drift.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	Mon Sep 21 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	Sat Oct 23 02:00:00 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 26, 2021 09:08:52.410618067 CET	54.147.21.139	443	192.168.2.3	49740	CN=drift.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	Mon Sep 21 02:00:00 CEST 2020	Sat Oct 23 02:00:00 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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 26, 2021 09:08:52.438029051 CET	50.16.7.188	443	192.168.2.3	49743	CN=drift.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	Mon Sep 21 02:00:00 CEST 2020	Sat Oct 23 02:00:00 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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 26, 2021 09:08:52.447784901 CET	50.16.7.188	443	192.168.2.3	49742	CN=drift.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	Mon Sep 21 02:00:00 CEST 2020	Sat Oct 23 02:00:00 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
							Thu Oct 22 02:00:00 CEST 2015	Mon Dec 31 02:00:00 CET 2037		
							Mon May 25 14:00:00 CEST 2015	Wed Jun 28 19:39:16 CEST 2034		
							Wed Sep 02 02:00:00 CEST 2009			
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 26, 2021 09:08:53.095879078 CET	18.205.49.143	443	192.168.2.3	49747	CN=drift.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	Mon Sep 21 02:00:00 CEST 2020	Sat Oct 23 02:00:00 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
							Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
							Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
							Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 26, 2021 09:08:53.097853899 CET	18.205.49.143	443	192.168.2.3	49746	CN=drift.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	Mon Sep 21 02:00:00 CEST 2020	Sat Oct 23 02:00:00 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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 26, 2021 09:08:53.101490021 CET	54.84.154.238	443	192.168.2.3	49748	CN=wschat.api.drift.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	Mon Apr 13 02:00:00 CEST 2020	Thu May 13 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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 26, 2021 09:08:53.102281094 CET	54.84.154.238	443	192.168.2.3	49749	CN=wschat.api.drift.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	Mon Apr 13 02:00:00 CEST 2020	Thu May 13 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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 26, 2021 09:08:53.112883091 CET	100.24.186.63	443	192.168.2.3	49750	CN=drift.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	Mon Sep 21 02:00:00 CEST 2020	Sat Oct 23 02:00:00 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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 26, 2021 09:08:53.113327026 CET	100.24.186.63	443	192.168.2.3	49751	CN=drift.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	Mon Sep 21 02:00:00 CEST 2020	Sat Oct 23 02:00:00 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
							Thu Oct 22 02:00:00 CEST 2015	Mon Dec 31 02:00:00 CET 2037		
							Mon May 25 14:00:00 CEST 2015	Wed Jun 28 19:39:16 CEST 2034		
							Wed Sep 02 02:00:00 CEST 2009			
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 26, 2021 09:08:53.125847101 CET	54.85.240.191	443	192.168.2.3	49752	CN=drift.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	Mon Sep 21 02:00:00 CEST 2020	Sat Oct 23 02:00:00 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
							Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
							Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
							Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 26, 2021 09:08:53.126060009 CET	54.85.240.191	443	192.168.2.3	49753	CN=drift.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	Mon Sep 21 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	Sat Oct 23 02:00:00 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		
Jan 26, 2021 09:08:54.998475075 CET	54.147.21.139	443	192.168.2.3	49758	CN=drift.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	Mon Sep 21 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	Sat Oct 23 02:00:00 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 26, 2021 09:08:55.007375956 CET	151.101.14.208	443	192.168.2.3	49759	CN=imgix.map.fastly.net, O="Fastly, Inc.", L=San Francisco, ST=California, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Thu Aug 06 18:29:48 CEST 2020 Wed Aug 19 02:00:00 CEST 2015	Sat Aug 07 18:29:48 CEST 2021 Tue Aug 19 02:00:00 CEST 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=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		
Jan 26, 2021 09:08:55.007811069 CET	151.101.14.208	443	192.168.2.3	49760	CN=imgix.map.fastly.net, O="Fastly, Inc.", L=San Francisco, ST=California, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Thu Aug 06 18:29:48 CEST 2020 Wed Aug 19 02:00:00 CEST 2015	Sat Aug 07 18:29:48 CEST 2021 Tue Aug 19 02:00:00 CEST 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=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		
Jan 26, 2021 09:08:55.085608006 CET	54.147.21.139	443	192.168.2.3	49757	CN=drift.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	Mon Sep 21 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	Sat Oct 23 02:00:00 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 26, 2021 09:08:55.950161934 CET	50.16.7.188	443	192.168.2.3	49761	CN=drift.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	Mon Sep 21 02:00:00 CEST 2020	Sat Oct 23 02:00:00 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
							Thu Oct 22 02:00:00 CEST 2015	Mon Oct 19 02:00:00 CEST 2025		
							Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
							Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 26, 2021 09:08:55.950366974 CET	50.16.7.188	443	192.168.2.3	49762	CN=drift.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	Mon Sep 21 02:00:00 CEST 2020	Sat Oct 23 02:00:00 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
							Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
							Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
							Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 26, 2021 09:09:05.442320108 CET	23.253.242.117	443	192.168.2.3	49771	CN=*.uptimeinstitute.com CN=Thawte RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Thawte RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Oct 07 02:00:00 CEST 2020 Mon Nov 06 13:23:52 CET 2017	Fri Nov 05 13:00:00 CET 2021 Sat Nov 06 13:23:52 CET 2027	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=Thawte RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:52 CET 2017	Sat Nov 06 13:23:52 CET 2027		
Jan 26, 2021 09:09:05.450968027 CET	23.253.242.117	443	192.168.2.3	49772	CN=*.uptimeinstitute.com CN=Thawte RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Thawte RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Oct 07 02:00:00 CEST 2020 Mon Nov 06 13:23:52 CET 2017	Fri Nov 05 13:00:00 CET 2021 Sat Nov 06 13:23:52 CET 2027	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=Thawte RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:52 CET 2017	Sat Nov 06 13:23:52 CET 2027		
Jan 26, 2021 09:09:08.502051115 CET	185.60.216.19	443	192.168.2.3	49780	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Dec 22 01:00:00 CET 2020 Tue Oct 22 14:00:00 CEST 2013	Mon Mar 22 00:59:59 CET 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jan 26, 2021 09:09:08.502167940 CET	185.60.216.19	443	192.168.2.3	49781	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Dec 22 01:00:00 CET 2020 Tue Oct 22 14:00:00 CEST 2013	Mon Mar 22 00:59:59 CET 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jan 26, 2021 09:09:08.608450890 CET	13.224.94.89	443	192.168.2.3	49782	CN=*.oktopost.com, OU=PremiumSSL Wildcard, O=Oktopost Technologies Ltd, STREET=Tuval 34 St., L=Ramat Gan, OID.2.5.4.17=5252244, C=IL CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE	Sun Sep 22 02:00:00 CEST 2019 Fri Nov 02 01:00:00 CET 2018 Tue May 30 12:48:38 CEST 2000	Tue Sep 28 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 Sat May 30 12:48:38 CEST 2020	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 Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE	Tue May 30 12:48:38 CEST 2000	Sat May 30 12:48:38 CEST 2020		
Jan 26, 2021 09:09:08.608582020 CET	13.224.94.89	443	192.168.2.3	49783	CN=*.oktopost.com, OU=PremiumSSL Wildcard, O=Oktopost Technologies Ltd, STREET=Tuval 34 St., L=Ramat Gan, OID.2.5.4.17=5252244, C=IL CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE	Sun Sep 22 02:00:00 CEST 2019 Fri Nov 02 01:00:00 CET 2018 Tue May 30 12:48:38 CEST 2000	Tue Sep 28 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 Sat May 30 12:48:38 CEST 2020	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 Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE	Tue May 30 12:48:38 CEST 2000	Sat May 30 12:48:38 CEST 2020		
Jan 26, 2021 09:09:09.365544081 CET	34.200.97.200	443	192.168.2.3	49787	CN=okt.to CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 13:53:07 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Apr 20 14:53:07 CEST 2021 Wed Sep 29 21:21:40 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=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Jan 26, 2021 09:09:09.366450071 CET	34.200.97.200	443	192.168.2.3	49786	CN=okt.to CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 13:53:07 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Apr 20 14:53:07 CEST 2021 Wed Sep 29 21:21:40 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=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Jan 26, 2021 09:09:09.556226015 CET	185.63.145.5	443	192.168.2.3	49789	CN=px.ads.linkedin.com, O=LinkedIn Corporation, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jan 06 01:00:00 CET 2021 Wed Sep 23 02:00:00 CEST 2020	Tue Jul 06 01:59:59 CEST 2021 Mon Sep 23 01:59:59 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 26, 2021 09:09:09.556624889 CET	185.63.145.5	443	192.168.2.3	49790	CN=px.ads.linkedin.com, O=LinkedIn Corporation, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jan 06 01:00:00 CET 2021 Wed Sep 23 02:00:00 CEST 2020	Tue Jul 06 01:59:59 CEST 2021 Mon Sep 23 01:59:59 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
Jan 26, 2021 09:09:10.679522991 CET	13.226.159.87	443	192.168.2.3	49799	CN=cdn.leadmanagerfx.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 Dec 17 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sun Jan 16 00:59:59 CET 2022 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		
Jan 26, 2021 09:09:10.683008909 CET	13.226.159.87	443	192.168.2.3	49800	CN=cdn.leadmanagerfx.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 Dec 17 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sun Jan 16 00:59:59 CET 2022 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		
Jan 26, 2021 09:09:11.174937010 CET	192.28.147.68	443	192.168.2.3	49798	CN=*.mktoresp.com, OU=IT, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jan 17 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jan 21 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jan 26, 2021 09:09:11.226326942 CET	192.28.147.68	443	192.168.2.3	49797	CN=*.mktoresp.com, OU=IT, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jan 17 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jan 21 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jan 26, 2021 09:09:16.488635063 CET	52.216.26.196	443	192.168.2.3	49807	CN=*.s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Nov 09 01:00:00 CET 2019 Tue Dec 08 13:05:07 CET 2015	Fri Mar 12 13:00:00 CET 2021 Sat May 10 14:00:00 CEST 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=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Jan 26, 2021 09:09:16.488807917 CET	52.216.26.196	443	192.168.2.3	49808	CN=*.s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Nov 09 01:00:00 CET 2019 Tue Dec 08 13:05:07 CET 2015	Fri Mar 12 13:00:00 CET 2021 Sat May 10 14:00:00 CEST 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

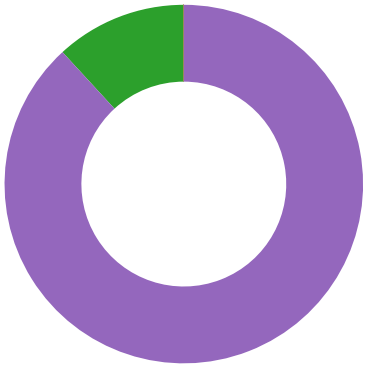
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Jan 26, 2021 09:09:18.202301979 CET	52.0.1.164	443	192.168.2.3	49810	CN=*.wistia.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Thu Apr 30 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sun May 30 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	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		
Jan 26, 2021 09:09:21.690042973 CET	35.173.77.57	443	192.168.2.3	49812	CN=*.wistia.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Thu Apr 30 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sun May 30 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 26, 2021 09:10:00.299360991 CET	34.198.102.54	443	192.168.2.3	49822	CN=*.litix.io CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Nov 27 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Dec 27 00:59:59 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	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		
Jan 26, 2021 09:10:00.300256014 CET	34.198.102.54	443	192.168.2.3	49823	CN=*.litix.io CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Nov 27 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Dec 27 00:59:59 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	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		

Code Manipulations

Statistics

Behavior



System Behavior

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

General

Start time:	09:08:40
Start date:	26/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff72e030000
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: 4720 Parent PID: 4952

General

Start time:	09:08:41
Start date:	26/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4952 CREDAT:17410 /prefetch:2
Imagebase:	0xab0000
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: AcroRd32.exe PID: 6604 Parent PID: 4952

General

Start time:	09:09:46
Start date:	26/01/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\COVID-19_v4.pdf'
Imagebase:	0x10b0000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx	read data or list directory | read attributes | write attributes | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	10E65C3	CreateDirectoryExW
C:\Users\user\AppData\Local\Temp\acrocef_low	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	110AE05	CreateDirectoryW
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	success or wait	1	10FEA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210126170958Z-265.bmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	10FEA85	NtCreateFile
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11783C8	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11783C8	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11783C8	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11783C8	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11783C8	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11783C8	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R39qmbb_1hzfywr_55k.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	10FEA85	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	3	10FEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R15hnkdj_1hzfyws_55k.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	10FEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1d9rcbm_1hzfywt_55k.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	10FEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rdl8qex_1hzfywu_55k.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	10FEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rhpisg8_1hzfywv_55k.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	10FEA85	NtCreateFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\System\Acrobatbrokerserverdispatchercpp789	success or wait	1	10FCF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	10FD41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	10FD41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0\cPathInfo	success or wait	1	10FD41D	NtCreateKey

Analysis Process: AcroRd32.exe PID: 6680 Parent PID: 6604

General

Start time:	09:09:48
Start date:	26/01/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\COVID-19_v4.pdf'
Imagebase:	0x10b0000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: RdrCEF.exe PID: 7036 Parent PID: 6604

General

Start time:	09:09:57
Start date:	26/01/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043
Imagebase:	0x10f0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
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	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	success or wait	3	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	3	11E59E2	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	1	11F83E5	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	29	11F8447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	161	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	3	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	6	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	3	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	18	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	3	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	6	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	3	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	success or wait	11	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	end of file	3	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	1622	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	3	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	29	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	success or wait	6	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	end of file	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	4	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	success or wait	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	end of file	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	success or wait	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	end of file	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	success or wait	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	end of file	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	success or wait	4	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	end of file	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	success or wait	2	11E59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	end of file	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	success or wait	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	success or wait	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	end of file	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	success or wait	12	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	end of file	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	success or wait	12	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	end of file	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	success or wait	27	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	end of file	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	success or wait	30	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	end of file	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	success or wait	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	success or wait	44	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	success or wait	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	end of file	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	28	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	30	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	end of file	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	success or wait	10	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	end of file	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	10	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	10	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	success or wait	10	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	end of file	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	120	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	142	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	end of file	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	success or wait	134	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	end of file	2	11E59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	24	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	success or wait	97	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	16	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	success or wait	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	3	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	success or wait	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	success or wait	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	success or wait	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	success or wait	3	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	success or wait	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	success or wait	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	success or wait	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	4	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	success or wait	85	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	success or wait	4	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	success or wait	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	success or wait	1	11E59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	success or wait	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	success or wait	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	success or wait	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	success or wait	7	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	success or wait	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	success or wait	159	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	success or wait	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	success or wait	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	success or wait	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	success or wait	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	success or wait	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	success or wait	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	success or wait	2	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	success or wait	75	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	success or wait	6	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	success or wait	15	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	success or wait	5	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	end of file	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js	unknown	4096	success or wait	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js	unknown	4096	end of file	1	11E59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	success or wait	1	11E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	end of file	1	11E59E2	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	4	unknown	1	11F83E5	ReadFile

Analysis Process: RdrCEF.exe PID: 6204 Parent PID: 7036

General

Start time:	09:09:59
Start date:	26/01/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1704,5597326268629714092,5294744840436624648,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=11483793060652442055 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=11483793060652442055 --renderer-client-id=2 --mojo-platform-channel-handle=1716 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x10f0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: RdrCEF.exe PID: 1328 Parent PID: 7036

General

Start time:	09:10:02
Start date:	26/01/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1704,5597326268629714092,5294744840436624648,131072 --disable-features=VizDisplayCompositor --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --lang=en-US --gpu-preferences=KAAAAAAAAACAAwABAQAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=1815229039396685170 0 --mojo-platform-channel-handle=1736 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0x10f0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: RdrCEF.exe PID: 5804 Parent PID: 7036

General

Start time:	09:10:04
Start date:	26/01/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1704,5597326268629714092,5294744840436624648,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=16145082219574015218 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=16145082219574015218 --renderer-client-id=4 --mojo-platform-channel-handle=1848 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x10f0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: RdrCEF.exe PID: 1012 Parent PID: 7036

General

Start time:	09:10:10
Start date:	26/01/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1704,5597326268629714092,5294744840436624648,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=6472226303739352892 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=6472226303739352892 --renderer-client-id=5 --mojo-platform-channel-handle=2180 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x7ff7488e0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis