ID: 379346
Cookbook: browseurl.jbs
Time: 20:50:29
Date: 31/03/2021
Version: 31.0.0 Emerald

Table of Contents

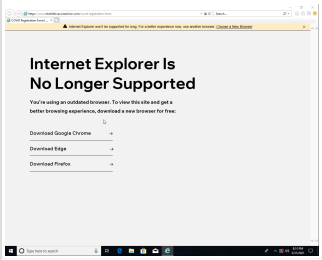
Analysis Report https://www.foothillsvaccineclinic.com/…

Overview

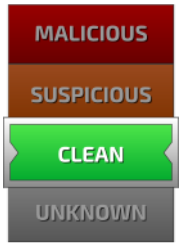
General Information

Sample URL:	http://https://www.foothillsvaccineclinic.com/covid-registration-form
Analysis ID:	379346
Infos:	

Most interesting Screenshot:



Detection

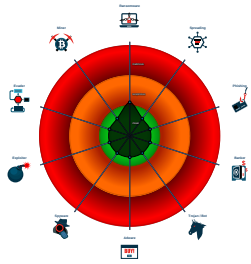


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5620 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5556 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5620 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6664 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5620 CREDAT:82966 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

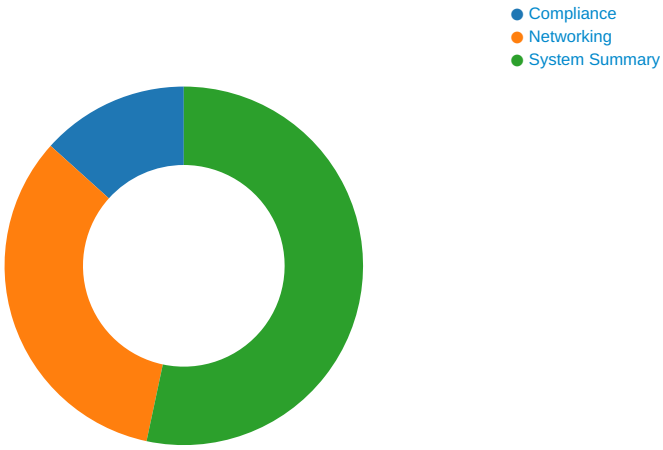
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



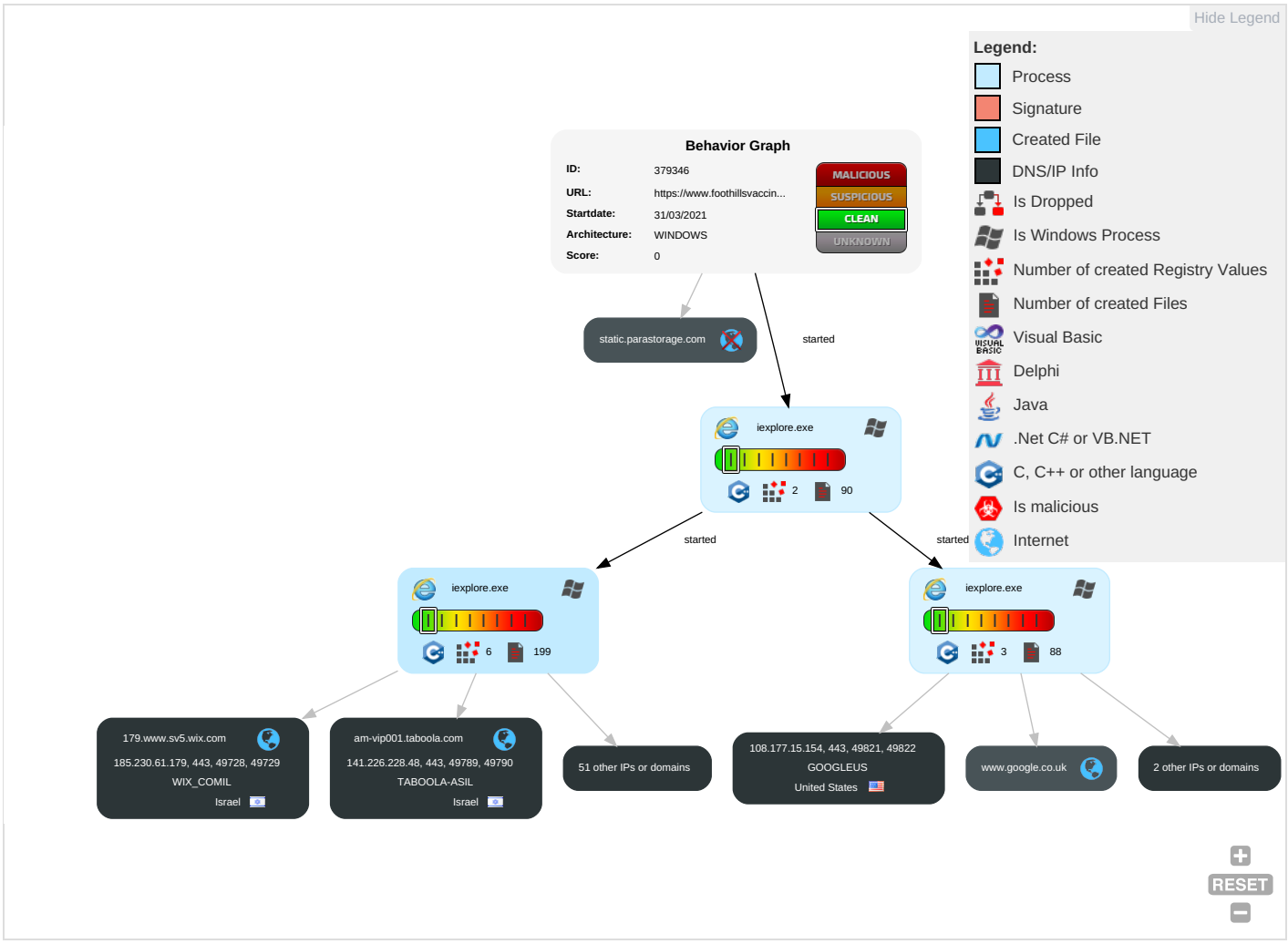
Click to jump to signature section

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	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

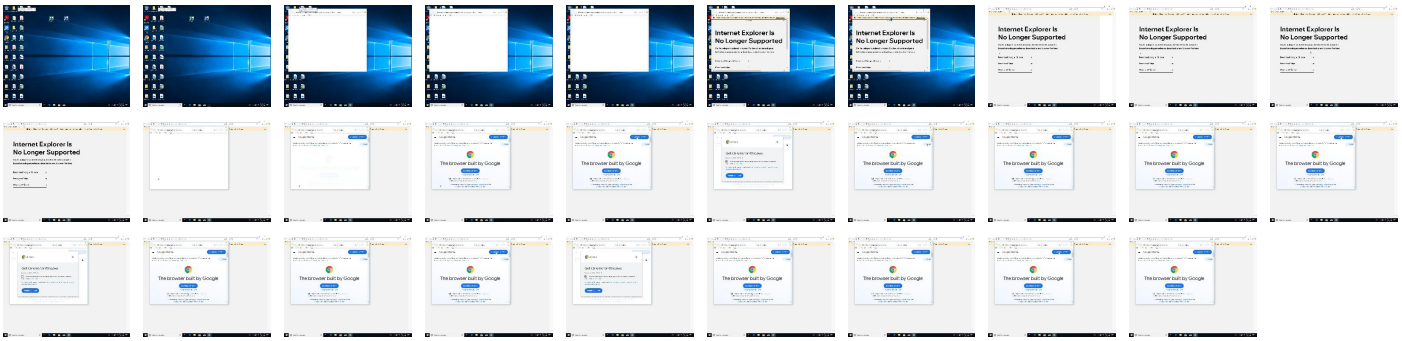
Behavior Graph

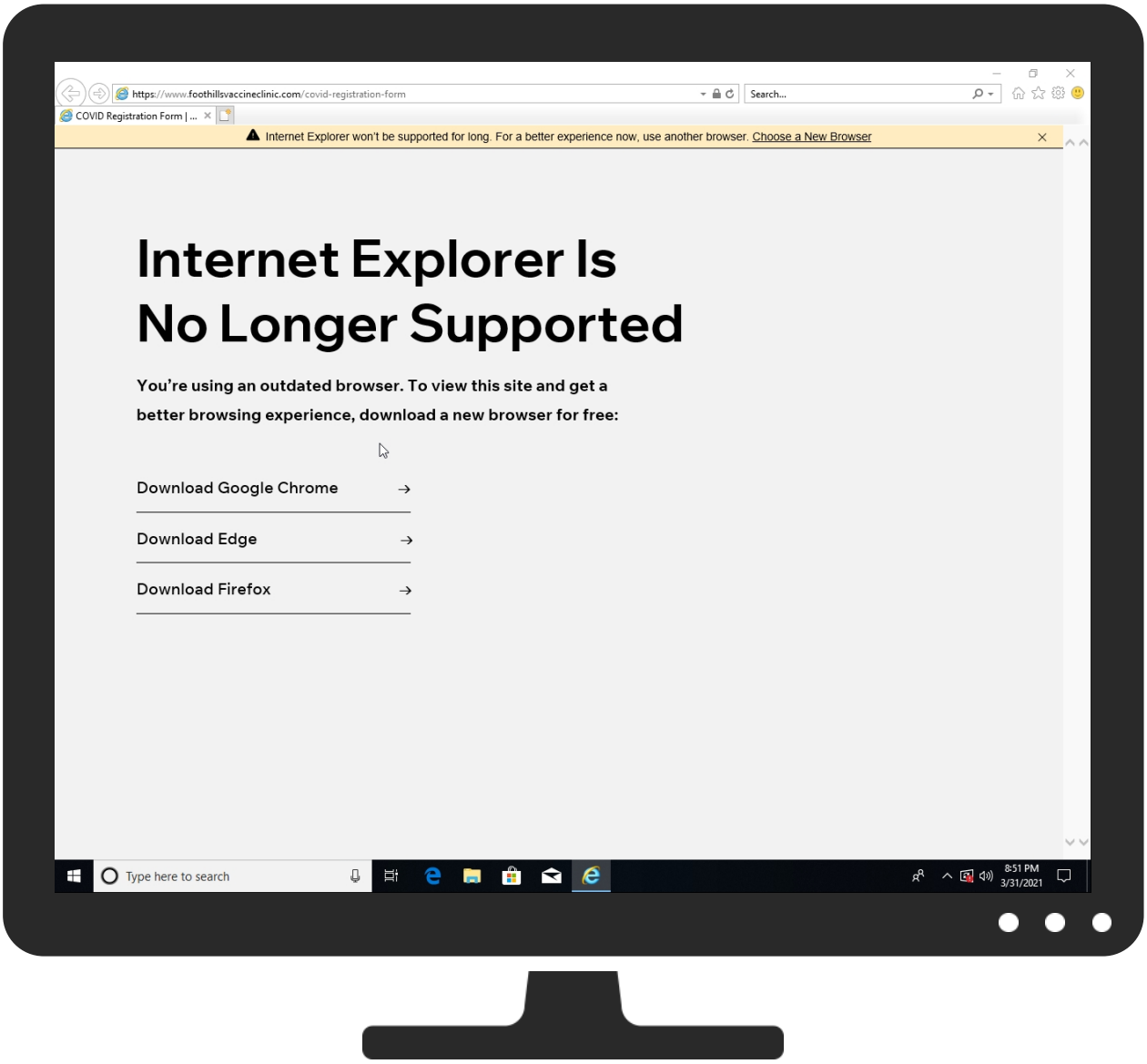


Screenshots

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://www.foothillsvaccineclinic.com/covid-registration-form	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
browser.sentry-cdn.com	0%	Virustotal		Browse
tls13.taboola.map.fastly.net	0%	Virustotal		Browse
td-balancer-euw2-6-109.wixdns.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://polymer.github.io/AUTHORS.txt	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://www.foothillsvaccineclinic.com/covid-registration-formaccineclinic.com/covid-registration-fo	0%	Avira URL Cloud	safe	
http://https://www.foothillsvaccineclinic.com	0%	Avira URL Cloud	safe	
http://https://chromeenterprise.google/	0%	Avira URL Cloud	safe	
http://https://about.google/	0%	URL Reputation	safe	
http://https://about.google/	0%	URL Reputation	safe	
http://https://about.google/	0%	URL Reputation	safe	
http://https://www.optimantra.com/optimus/patient/patientaccess/servicesall?pid=UENVaHY2UFg4RXdMVmlTUzIzQXh	0%	Avira URL Cloud	safe	
http://polymer.github.io/PATENTS.txt	0%	Avira URL Cloud	safe	
http://https://browser.sentry-cdn.com/5.21.4/bundle.min.js	0%	Avira URL Cloud	safe	
http://https://browser.sentry-cdn.com/4.6.2/bundle.min.js	0%	URL Reputation	safe	
http://https://browser.sentry-cdn.com/4.6.2/bundle.min.js	0%	URL Reputation	safe	
http://https://browser.sentry-cdn.com/4.6.2/bundle.min.js	0%	URL Reputation	safe	
http://https://www.foothillsvaccineclinic.com/	0%	Avira URL Cloud	safe	
http://polymer.github.io/CONTRIBUTORS.txt	0%	Avira URL Cloud	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
star-mini.c10r.facebook.com	185.60.216.35	true	false		high
dart.l.doubleclick.net	216.58.215.230	true	false		high
pagead46.l.doubleclick.net	172.217.168.34	true	false		high
browser.sentry-cdn.com	151.101.194.217	true	false	• 0%, Virustotal, Browse	unknown
tls13.taboola.map.fastly.net	151.101.1.44	true	false	• 0%, Virustotal, Browse	unknown
stats.l.doubleclick.net	108.177.15.155	true	false		high
td-balancer-euw2-6-109.wixdns.net	35.246.6.109	true	false	• 0%, Virustotal, Browse	unknown
gcp.media-router.wixstatic.com	34.102.176.152	true	false		high
pop-eda6.mix.linkedin.com	108.174.11.69	true	false		high
179.www.sv5.wix.com	185.230.61.179	true	false		high
obs.cheqzone.com	54.83.110.109	true	false		unknown
fast.fonts.com	104.17.70.188	true	false		high
scontent.xx.fbcdn.net	185.60.216.19	true	false		high
googleads.g.doubleclick.net	172.217.168.66	true	false		high
www.google.co.uk	216.58.215.227	true	false		unknown
polyfill.io	151.101.130.109	true	false		high
td-username-euw2-6-109.wix.com	35.246.6.109	true	false		high
atlas.c10r.facebook.com	185.60.216.6	true	false		high
bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com	34.202.131.150	true	false		high
cheqzone2.b-cdn.net	89.187.165.193	true	false		high
www.google.ch	172.217.168.67	true	false		high
am-vip001.taboola.com	141.226.228.48	true	false		high
4382365.fls.doubleclick.net	unknown	unknown	false		high
en.wix.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
2542116.fls.doubleclick.net	unknown	unknown	false		high
ob.cheqzone.com	unknown	unknown	false		unknown
www.foothillsvaccineclinic.com	unknown	unknown	false		unknown
trc-events.taboola.com	unknown	unknown	false		high
static.parastorage.com	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
siteassets.parastorage.com	unknown	unknown	false		high
static.wixstatic.com	unknown	unknown	false		high
cx.atdmt.com	unknown	unknown	false		high
www.linkedin.com	unknown	unknown	false		high
adservice.google.ch	unknown	unknown	false		high
trc.taboola.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
connect.facebook.net	unknown	unknown	false		high
px.ads.linkedin.com	unknown	unknown	false		high
frog.wix.com	unknown	unknown	false		high
snap.licdn.com	unknown	unknown	false		high
s.pinimg.com	unknown	unknown	false		high
cdn.taboola.com	unknown	unknown	false		high
www.wix.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.foothillsvaccineclinic.com/covid-registration-form	false		unknown

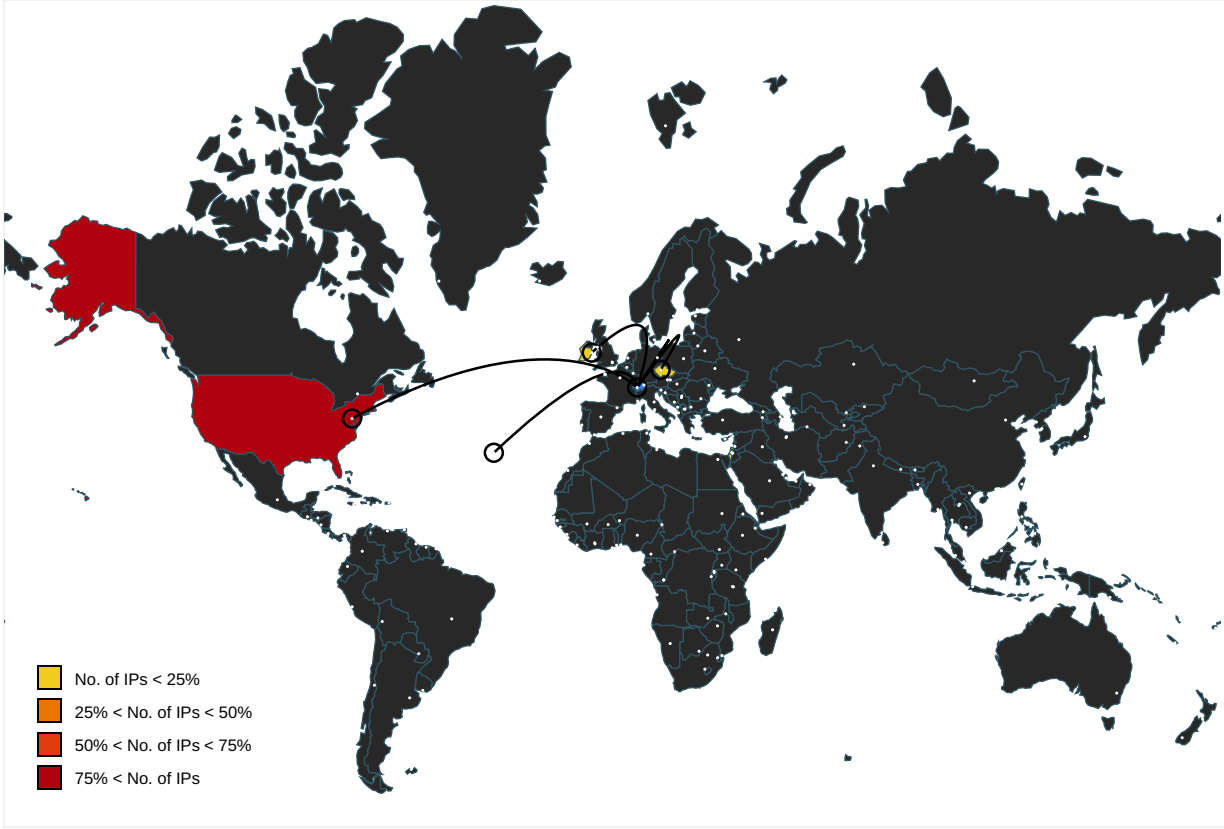
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://static.parastorage.com/services/wix-thunderbolt/dist/platform.5b826978.chunk.min.js	covid-registration-form[1].htm.2.dr	false		high
http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/v7/helvetic	internet-explorer[1].htm.2.dr	false		high
http://https://static.parastorage.com/services/wix-thunderbolt/dist/platform.5b826978.chunk.min.js.map	platform.5b826978.chunk.min[1].js.2.dr	false		high
http://https://github.com/zloirock/core-js	minified[1].js.2.dr	false		high
http://https://static.parastorage.com/services/wix-thunderbolt/dist/ooiTpaSharedConfig.886a4044.chunk.min.j	covid-registration-form[1].htm.2.dr, ooiTpaSharedConfig.886a4044.chunk.min[1].js.2.dr	false		high
http://https://static.parastorage.com/services/wix-thunderbolt/dist/main.c9d8a82e.chunk.min.js.map	main.c9d8a82e.chunk.min[1].js.2.dr	false		high
http://https://blog.google/products/chrome/	chrome[1].htm.18.dr	false		high
http://https://static.parastorage.com/services/wix-thunderbolt/dist/page-features.087592ee.chunk.min.js.map	page-features.087592ee.chunk.min[1].js.2.dr	false		high
http://https://px.ads.linkedin.com/collect?	insight.min[1].js.2.dr	false		high
http://polymer.github.io/AUTHORS.txt	bolt-custom-elements.min[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com	chrome[1].htm.18.dr	false		high
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=2542116;cat=chrom0;ord=1088143482153;	~DFF1E8BD5DBDDFE99F.TMP.1.dr	false		high
http://https://static.parastorage.com/services/wix-thunderbolt/dist/vendor-react-dom.7455c905.chunk.min.js.	vendor-react-dom.7455c905.chunk.min[1].js.2.dr	false		high
http://www.wix.com/blog	internet-explorer[1].htm.2.dr	false		high
http://https://static.parastorage.com/services/wix-thunderbolt/dist/bi-common.inline.8c2ead74.chunk.min.js.	covid-registration-form[1].htm.2.dr	false		high
http://scrollmagic.io	animation.gsap.min[1].js.18.dr	false		high
http://https://static.parastorage.com/services/editor-elements/dist/FiveGridLine_SolidLine.539a3d84.chunk.m	covid-registration-form[1].htm.2.dr, FiveGridLine_SolidLine.539a3d84.chunk.min[1].js.2.dr	false		high
http://img.youtube.com/vi/CakiQCH5ZY0/mqdefault.jpg"	bolt-main-prod-old[1].js.2.dr	false		high
http://https://www.foothillsvaccineclinic.com/covid-registration-formaccineclinic.com/covid-registration-fo	{81439702-929D-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://static.parastorage.com/services/editor-elements/dist/bootstrap-components-classic.4e8d8bbf.c	bootstrap-components-classic.4e8d8bbf.chunk.min[1].js.2.dr, covid-registration-form[1].htm.2.dr	false		high
http://https://static.parastorage.com/services/wix-thunderbolt/dist/activePopup.1e06371f.chunk.min.js	covid-registration-form[1].htm.2.dr	false		high
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.2.dr	false		high
http://https://www.foothillsvaccineclinic.com	covid-registration-form[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://https://bugs.chromium.org/p/v8/issues/detail?id=4118	wixui.Captcha.chunk[1].js.2.dr	false		high
http://https://static.parastorage.com/services/wix-thunderbolt/dist/tpaCommons.5946c45b.chunk.min.js.map	tpaCommons.5946c45b.chunk.min[1].js.2.dr	false		high
http://https://chromium.googlesource.com/chromium/src/	chrome[1].htm.18.dr	false		high
http://https://static.parastorage.com/services/wix-thunderbolt/dist/windowMessageRegister.inline.62dd41f7.c	covid-registration-form[1].htm.2.dr	false		high
http://https://chromeenterprise.google/	chrome[1].htm.18.dr	false	• Avira URL Cloud: safe	unknown
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/1006927621/?random	f[1].txt0.2.dr	false		high
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=2542116;cat=chrom0;ord=4025465958136;	~DFF1E8BD5DBDDFE99F.TMP.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://static.parastorage.com/services/wix-ui-santa/1.1559.0/	viewerComponentService.bundle[1].js.2.dr, dataRefs.bundle.min[1].js.2.dr	false		high
http://https://about.google/	chrome[1].htm.18.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.optimantra.com/optimus/patient/patientaccess/servicesall?pid=UENVaHY2UFg4RXdMVmlTUzIzQXh	covid-registration-form[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://polymer.github.io/PATENTS.txt	bolt-custom-elements.min[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://investors.wix.com/	internet-explorer[1].htm.2.dr	false		high
http://https://static.parastorage.com/unpkg/requirejs-bolt	internet-explorer[1].htm.2.dr	false		high
http://dev.wix.com/	internet-explorer[1].htm.2.dr	false		high
http://https://browser.sentry-cdn.com/5.21.4/bundle.min.js	covid-registration-form[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.wix.com/jobs/main	internet-explorer[1].htm.2.dr	false		high
http://https://greensock.com/standard-license	gsap.min[1].js.2.dr	false		high
http://rock.mit-license.org	minified[1].js.2.dr	false		high
http://https://github.com/madrobby/zepto/blob/master/src/detect.js#files	imageClientApi[1].js.2.dr	false		high
http://https://static.parastorage.com/services/wix-thunderbolt/dist/protectedPages.c3173846.chunk.min.js.ma	protectedPages.c3173846.chunk.min[1].js.2.dr	false		high
http://https://static.wixstatic.com/media/311dce_77ca1007cf83485da0b7e16ffb9735ac~mv2.png	internet-explorer[1].htm.2.dr	false		high
http://https://static.parastorage.com/services/wix-thunderbolt/dist/ooi.751f312e.chunk.min.js.map	ooi.751f312e.chunk.min[1].js.2.dr	false		high
http://https://npms.io/search?q=ponyfill.	lodash.min[1].js.2.dr	false		high
http://https://static.parastorage.com/services/editor-elements/dist/DocumentMedia.73dfebf3.chunk.min.js.map	DocumentMedia.73dfebf3.chunk.min[1].js.2.dr	false		high
http://https://browser.sentry-cdn.com/4.6.2/bundle.min.js	internet-explorer[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://static.parastorage.com/services/wix-thunderbolt/dist/page-features.087592ee.chunk.min.js	covid-registration-form[1].htm.2.dr	false		high
http://static.wixstatic.com/media/bc001baa4397444f809fa5f147c28a9e.jpg	bolt-main-prod-old[1].js.2.dr	false		high
http://https://static.parastorage.com/services/wix-bolt/1.7107.0/bolt-main/app/main-r.min.js	internet-explorer[1].htm.2.dr	false		high
http://https://tools.ietf.org/html/rfc7230#section-3.2	fetch.umd[1].js.2.dr	false		high
http://www.amazon.com/	msapplication.xml.1.dr	false		high
http://https://www.foothillsvaccineclinic.com/	covid-registration-form[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://static.parastorage.com/services/wix-thunderbolt/dist/pageTransitions.be89e7bb.chunk.min.js	covid-registration-form[1].htm.2.dr	false		high
http://https://static.parastorage.com/unpkg/whatwg-fetch	internet-explorer[1].htm.2.dr	false		high
http://https://static.parastorage.com/services/editor-elements/dist/MeshGroup.132daa54.chunk.min.js.map	MeshGroup.132daa54.chunk.min[1].js.2.dr	false		high
http://www.twitter.com/	msapplication.xml5.1.dr	false		high
http://https://static.parastorage.com/services/wix-thunderbolt/dist/externals-registry.inline.e8e6f495.chun	covid-registration-form[1].htm.2.dr	false		high
http://https://static.parastorage.com/services/wix-thunderbolt/dist/bi.inline.3becbef1.chunk.min.js	covid-registration-form[1].htm.2.dr	false		high
http://https://static.parastorage.com/services/wix-thunderbolt/dist/tpaCommons.5946c45b.chunk.min.js	covid-registration-form[1].htm.2.dr	false		high
http://schema.org	chrome[1].htm.18.dr	false		high
http://https://s.pinimg.com/ct/core.js	gtm[1].js.2.dr	false		high
http://img.youtube.com/vi/CakiQCH5ZY0/mqdefault.jpg	bolt-main-prod-old[1].js.2.dr	false		high
http://https://static.parastorage.com/services/editor-elements/dist/Container_RectangleArea.d3c310c8.chunk.	Container_RectangleArea.d3c310c8.chunk.min[1].js.2.dr, covid-registration-form[1].htm.2.dr	false		high
http://https://github.com/madrobby/zepto/blob/master/MIT-LICENSE	imageClientApi[1].js.2.dr	false		high
http://https://www.google.ch/pagead/1p-user-list/642100862/?random	f[2].txt.2.dr	false		high
http://static.wixstatic.com/media/139571a1212e4d3d8074041626ba3ed6.jpg"	bolt-main-prod-old[1].js.2.dr	false		high
http://https://github.com/getsentry/sentry-javascript	bundle.min[1].js.2.dr	false		high
http://https://2542116.fls.doubleclick.net	chrome[1].htm.18.dr	false		high
http://polymer.github.io/CONTRIBUTORS.txt	bolt-custom-elements.min[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://static.parastorage.com/services/wix-thunderbolt/dist/vendor-react.inline.98bfcadc.chunk.min.	covid-registration-form[1].htm.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://static.doubleclick.net	chrome[1].htm.18.dr	false		high
http://https://static.parastorage.com/services/editor-elements/dist/MeshGroup.132daa54.chunk.min.js	covid-registration-form[1].htm.2.dr	false		high
http://https://www.foothillsvaccineclinic.com/covid-registration-form	covid-registration-form[1].htm.2.dr, ~DF8500B3B48B442132.TMP.1.dr	false		unknown
http://https://static.parastorage.com/services/editor-elements/dist/bootstrap-components-common.b37b13ef.ch	covid-registration-form[1].htm.2.dr, bootstrap-components-common.b37b13ef.chunk.min[1].js.2.dr	false		high
http://https://siteassets.parastorage.com/pages/singlePage/viewerViewModeJson	internet-explorer[1].htm.2.dr	false		high
http://https://schema.org/WebPage	chrome[1].htm.18.dr	false		high
http://www.nytimes.com/	msapplication.xml3.1.dr	false		high
http://webfonts.fonts.com	internet-explorer[1].htm.2.dr, helvetica[1].css.2.dr	false		high
http://https://static.parastorage.com/services/santa/1.1518.0	internet-explorer[1].htm.2.dr	false		high
http://https://static.parastorage.com/services/wix-thunderbolt/dist/dynamicPages.ea31d9ca.chunk.min.js	covid-registration-form[1].htm.2.dr	false		high
http://https://reactjs.org/docs/error-decoder.html?invariant=	react.production.min[1].js.2.dr, react-dom.production.min[1].js.2.dr	false		high
http://https://googleads.g.doubleclick.net	chrome[1].htm.18.dr	false		high
http://https://static.parastorage.com/services/santa-members-viewer-app/1.744.0/app.bundle.min.js	covid-registration-form[1].htm.2.dr	false		high
http://https://static.parastorage.com/client/pfavico.ico~	imagestore.dat.2.dr	false		high
http://https://static.parastorage.com/services/wix-thunderbolt/dist/dynamicPages.ea31d9ca.chunk.min.js.map	dynamicPages.ea31d9ca.chunk.min[1].js.2.dr	false		high
http://https://developer.chrome.com/webstore/?hl=en	chrome[1].htm.18.dr	false		high
http://https://static.parastorage.com/services/editor-elements/dist/DropDownMenu_OverlineMenuButtonSkin.b9e	covid-registration-form[1].htm.2.dr	false		high
http://https://static.parastorage.com/services/wix-thunderbolt/dist/vendor-react-dom.7455c905.chunk.min.js	covid-registration-form[1].htm.2.dr	false		high
http://static.wixstatic.com/media/d967ba93f0314c78924edc8a8c8cfa15.jpg	bolt-main-prod-old[1].js.2.dr	false		high
http://https://bugs.chromium.org/p/v8/issues/detail?id=3056	wixui.Captcha.chunk[1].js.2.dr	false		high
http://https://static.parastorage.com/services/wix-thunderbolt/dist/platformPubsub.5f1d9daf.chunk.min.js.ma	platformPubsub.5f1d9daf.chunk.min[1].js.2.dr	false		high
http://https://static.parastorage.com/services/wix-thunderbolt/dist/tpa.f6e17687.chunk.min.js.map	tpa.f6e17687.chunk.min[1].js.2.dr	false		high
http://www.wikipedia.com/	msapplication.xml6.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://static.parastorage.com/services/wix-thunderbolt/dist/wix-code-sdk-providers.3a33b93f.chunk.m	covid-registration-form[1].htm.2.dr	false		high
http://https://static.parastorage.com/services/tag-manager-client/1.282.0/siteTags.bundle.min.js	internet-explorer[1].htm.2.dr	false		high
http://https://static.parastorage.com/services/wix-perf-measure/1.401.0/wix-perf-measure.bundle.min.js	internet-explorer[1].htm.2.dr, covid-registration-form[1].htm.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
108.177.15.155	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
54.83.110.109	obs.cheqzone.com	United States		14618	AMAZON-AESUS	false
216.58.215.230	dart.l.doubleclick.net	United States		15169	GOOGLEUS	false
172.217.168.67	www.google.ch	United States		15169	GOOGLEUS	false
35.246.6.109	td-balancer-euw2-6-109.wixdns.net	United States		15169	GOOGLEUS	false
151.101.194.217	browser.sentry-cdn.com	United States		54113	FASTLYUS	false
172.217.168.66	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
141.226.228.48	am-vip001.taboola.com	Israel		200478	TABOOLA-ASIL	false
104.17.70.188	fast.fonts.com	United States		13335	CLOUDFLARENETUS	false
108.174.11.69	pop-eda6.mix.linkedin.com	United States		14413	LINKEDINUS	false
185.60.216.6	atlas.c10r.facebook.com	Ireland		32934	FACEBOOKUS	false
185.230.61.179	179.www.sv5.wix.com	Israel		58182	WIX_COMIL	false
151.101.130.109	polyfill.io	United States		54113	FASTLYUS	false
185.60.216.35	star-mini.c10r.facebook.com	Ireland		32934	FACEBOOKUS	false
151.101.1.44	tls13.taboola.map.fastly.net	United States		54113	FASTLYUS	false
185.60.216.19	scontent.xx.fbcdn.net	Ireland		32934	FACEBOOKUS	false
89.187.165.193	cheqzone2.b-cdn.net	Czech Republic		60068	CDN77GB	false
34.102.176.152	gcp.media-router.wixstatic.com	United States		15169	GOOGLEUS	false
34.202.131.150	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	379346
Start date:	31.03.2021

Start time:	20:50:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://www.foothillsvaccineclinic.com/covid-registration-form
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:	28
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@5/227@34/20
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.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): 23.54.113.53, 13.64.90.137, 52.147.198.201, 40.88.32.150, 104.43.193.48, 88.221.62.148, 151.101.2.49, 151.101.66.49, 151.101.130.49, 151.101.194.49, 13.88.21.125, 172.217.168.8, 172.217.168.14, 204.79.197.200, 13.107.21.200, 172.217.168.2, 23.211.4.189, 23.57.82.43, 172.217.168.68, 172.217.168.34, 13.107.42.14, 20.82.210.154, 152.199.19.161, 23.57.80.111, 92.122.213.247, 92.122.213.194, 216.58.215.227, 172.217.168.74, 2.20.142.210, 2.20.142.209, 216.58.212.174, 216.58.212.131, 216.58.215.238, 20.54.26.129, 2.17.179.193, 20.50.102.62 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, cdn.onenote.net.edgekey.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, 2-01-37d2-0006.cdx.cedexis.net, l-0005.l-msedge.net, audownload.windowsupdate.nsatc.net, www.google.com, watson.telemetry.microsoft.com, www.gstatic.com, au-bg-shim.trafficmanager.net, www.google-analytics.com, fonts.googleapis.com, n2.shared.global.fastly.net, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, e1553.dspg.akamaiedge.net, cs9.wpc.v0cdn.net, tools.google.com, au.download.windowsupdate.com.edgesuite.net, www.googleadservices.com, e6449.dsca.akamaiedge.net, store-images.s-microsoft.com-c.edgekey.net, adservice.google.com, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e9706.dscg.akamaiedge.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, go.microsoft.com, www.googletagmanager.com, bat.bing.com, arc.trafficmanager.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, cdn.onenote.net, www-linkedin-com.l-0005.l-msedge.net, skypedataprdcolwus17.cloudapp.net, www-google-analytics.l.google.com, ie9comview.vo.msecnd.net, fonts.gstatic.com, www-googletagmanager.l.google.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, bat-bing-com.a-0001.a-msedge.net, s.pinimg.com.edgekey.net, wildcard.licdn.com.edgekey.net, go.microsoft.com.edgekey.net, tools.l.google.com, skypedataprdcolwus15.cloudapp.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\O4AKH200\www.wix[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):	39521
Entropy (8bit):	5.403197498265254
Encrypted:	false
SSDEEP:	768:QHHHHmHm59m5Sm5ym5Em5ym5ym5ym5ym5ym5fbm5fQm5fQm5f5m5f5m5fHm5fHmO:QHHHHmHm59m5Sm5ym5Em5ym5ym5ym5yW
MD5:	B2685A29BD0B9B5A8A5304A1F63E160E
SHA1:	0C0FAAB41744EA41D4C283D82CEA7E5B1F62A804
SHA-256:	6E08AA84F8405B0589D44A3FF26E062D32D6D88FF4DAEEF8AA601CF5C61AD1A0
SHA-512:	19466CE4C33673284ED7AA1B70E22446997A2BDAC8189583C3117DB1C7BB2EEFECBADB605EEA276479A95C0544E17CD6772B668EA18B908077372E5963DFCB(3
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="fedops.logger.sessionId" value="d901f1c9-2473-40fc-889d-d024d8574641" ltime="1203775216" htime="30877354" /></root><root> <item name="fedops.logger.sessionId" value="d901f1c9-2473-40fc-889d-d024d8574641" ltime="1203775216" htime="30877354" /></root><root><item name="fed ops.logger.sessionId" value="d901f1c9-2473-40fc-889d-d024d8574641" ltime="1203775216" htime="30877354" /></root><root><item name="fedops.logger.sessionId" value="d901f1c9-2473-40fc-889d-d024d8574641" ltime="1203775216" htime="30877354" /></root><root><item name="fedops.logger.sessionId" value="d901f1c9-2473-4 0fc-889d-d024d8574641" ltime="1203775216" htime="30877354" /><item name="wixSessionTS" value="1617249082613" ltime="1209275216" htime="30877354" /></r oot><root><item name="fedops.logger.sessionId" value="d901f1c9-2473-40fc-889d-d024d8574641" ltime="1203775216" htime="30877354" /><item name="wixSessi onTS" value="1617249082613" ltime="1209275216" htime="30877354" /><item name="_uetsid" val

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\TETS29UR\www.google[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aK1r0aKb:JFK1rFKb
MD5:	132294CA22370B52822C17DCB5BE3AF6
SHA1:	DD26B82638AD38AD471F7621A9EB79FED448A71C
SHA-256:	451ABBE0AEFC000F49967DABF8D42344D146429F03C8C8D4AE5E33FF9963CF77
SHA-512:	6D5808CAD199A785C82763C68F0AE1F4938C304B46B70529EA26B3D300EF9430AD496C688D95D01588576B3A577001D62245D98137FD5CD825AD62E17D36F15C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\TETS29UR\www.google[1].xml	
Preview:	<root></root><root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{81439700-929D-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	60616
Entropy (8bit):	2.135887280604929
Encrypted:	false
SSDEEP:	192:rTZsZ22H6WHQtHmfHAxMHwHoHkfHCYsrHxHIgWHAHTHosHwWHHHiBHBOW:rVMN5U8JQIqERegzxHnSh
MD5:	16BEEAAF53E7B8E147469ADAED767BF4
SHA1:	999E2DD3650A5F908CF0BFAF3F85B82DDEDBC251
SHA-256:	A446B596A3260955DCF9435908339AB365080EFE234DD8E84692089301DE4099
SHA-512:	5B77F966FFC3CF848017B5AA60FA5AE47FE2AD1D5A5C570F7102BCDFC423FE21D191825D525B9BEEA6209E15E64D93AA4B8201C5D8A21F9E787931191B35902
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\{81439702-929D-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	31062
Entropy (8bit):	1.749622202977041
Encrypted:	false
SSDEEP:	48:IwGGcpr3GwpaiG4pQWGrapbSYGQpBV4GHHpcVuTGUp8VZGzYpmVNTGopumHN5quq:raZhQS6YBSgjZ2EWZMRPpUX10YUMr
MD5:	9976B0B864E4B278FC1AEFCCA8C16467
SHA1:	3D6827A8F2322C956A73EB5E0C1F92FAECCE223B
SHA-256:	837420F5B64C6690044D1F2EF3A6783E2C5D939430F50E6D3AD8FD6286B7E644
SHA-512:	26DDEC82A447A851E16CF31C381EF58D04EBDAD9690402998DC4DAFFA5776D94856B742C27AEE0F3054702BA1382644332D3F0F0E24FB45FA9783D718388B49
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\{87CD21D5-929D-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5847576905485456
Encrypted:	false
SSDEEP:	48:IwnGcpr0Gwpa+G4pQeGrapbSvGQpKNG7HpRSTGIpX2LGApm:rNZMQ+6QBS5AsTGFGg
MD5:	C1EE974BBCE7E3E6B4F0A35975B115BE
SHA1:	93AF01822175C19D8A654AD181C19DCFF8244D8F
SHA-256:	659A146E2C683059C3053F2FAA8517A8E064827C36482556377981F9C6AB85D6
SHA-512:	435C6BBF3914A946D3F51D7910C52FCB6D17D27B836F6E600CCCBCB42BA38A0FB702EA2DA0F45308EA8A8DDD3B091CF89CC2024A943354F9033C0449243FF64
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\{9CBCF508-929D-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9CBCF508-929D-11EB-90E4-ECF4BB862DED}.dat	
Size (bytes):	80250
Entropy (8bit):	2.9296103959798696
Encrypted:	false
SSDEEP:	192:rUZvQQ6ak9jW2HWBM0AfPTfK66sGcGtG6fMlTfKX6sGcGax7F1E26fMgkm6sGcG0:rEo7zZt2atjn+ry2+Bb+6+Ah+O+Gb+s
MD5:	B597DD820F3F0ABA8B218BBDE2BE3BBA
SHA1:	4BA8423E92860AB2AE4C5759A497B56FF997CDDF
SHA-256:	7ED8582FA18C0A09BB92E876652A996D6CC3BB0F095A4A9A3BD0DBF6712D5F62
SHA-512:	0E84B9D7BA893B66336454455644FEDAABB0381C6BD3E75E2FBCFDBA838CF12A036B80497E99A74DF1B63235536ABAD3E37D044E21ACE99A0BAC6CEF4A52FE60
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\{9CBCF509-929D-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5660787980136541
Encrypted:	false
SSDEEP:	48:IwVGcpr0GwpahG4pQVGrapbS59GQpKvBG7HpR2TGIpG:rLZMQz6FBS5HAvwTCA
MD5:	BB4591000DA84060C6B29C38D32BD554
SHA1:	1AF74E02FFAF38729A99D0E3F291F11B516077C5
SHA-256:	151A1C0CEC76E4C65E0CB836DA2F94F8AAB6578071030D9335BB1E3F5A907DF8
SHA-512:	3D63B11C4C41D6AC3C9FD7B85055E1FF5EFF4259683592741390DBB7F9A00E08AA381806CA0D916340EB39AA8BA4D7A73D2C5DED53E94143986675F534DD775
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.098031466882481
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEAX4nWimI002EtM3MHdNMNxOEAGDnWimI00ObVbkEtMb:2d6NxOJX4SZHKd6NxOJGDSZ76b
MD5:	B4C5A351A717F00B20D14C451FA9D761
SHA1:	46DC6602AA182B9443A54F14B2C68A1E31AEA645
SHA-256:	A2AA50AFF676FCF872A2E566F8B13C64405F49052313835E83EBD0EC1B8A3DA8
SHA-512:	B4C156CBAB4749EDEF1895A3112CE974ED644C87E9A54C75912B684EF5AE3F61875562011B0A6C7BEF9F94F9EBF12EE66AEA9BA69B3AC1462A8887A629245CDC
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x5930f0ab,0x01d726aa</date><accdate>0x5930f0ab,0x01d726aa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x5930f0ab,0x01d726aa</date><accdate>0x59335302,0x01d726aa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.13640209870431
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kbnWimI002EtM3MHdNMNxe2kbnWimI00Obkak6EtMb:2d6NxrmSZHKd6NxrmSZ7Aa7b
MD5:	1F98DAAD2349E79A9F8294D8DA689769
SHA1:	B243720DCDE1FF2B2DDA4570D068DB4DE00D4939

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
SHA-256:	8255AD5F056B8529E194091058CC59CAF6095D30E742A4FE7085C610DA0FE3AE
SHA-512:	05011103962F9D6FA237623BABF79C12E773B348409375F81A9F5FCF978162365A1A203F464E3E8629D2C2862AD10AA185BD9CED8CC6A9410C3975617438FD19
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x5916b6d7,0x01d726aa</date><accdate>0x5916b6d7,0x01d726aa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x5916b6d7,0x01d726aa</date><accdate>0x5916b6d7,0x01d726aa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.128556244941621
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLjrDnWimI002EtM3MHdNMNxvLjrDnWimI00ObmZEtMb:2d6NxvnrDSZHKd6NxvnrDSZ7mb
MD5:	CCEEB3F3C2BC0DF2090628EA29C243CD
SHA1:	A4A3E5ADB93D03A94B14395F82E82192D3D93FCA
SHA-256:	490198D125F16E224BA5769AB28748C7B7FF69FB30C58CF44634872102C31A9B
SHA-512:	BF1E699317989C872A008D9160000472994F8EC54F9EE7888DB7D42944DB086C1E4EE5A67704CA716A87561F6E750A13D7F8FFA47FE0ED64D4B4F9D0E8A9540B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x59335302,0x01d726aa</date><accdate>0x59335302,0x01d726aa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x59335302,0x01d726aa</date><accdate>0x59335302,0x01d726aa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.110292108008223
Encrypted:	false
SSDEEP:	12:TMHdNMNxicUDnWimI002EtM3MHdNMNxicUDnWimI00Obd5EtMb:2d6NxlUDSZHKd6NxlUDSZ7Jjb
MD5:	C41FA819DE6B7A392528F5F008673537
SHA1:	A78BA9C6A5387D8CB74FF1ADD01E4211AC4DBB4D
SHA-256:	E13B622B76E2E625D6875A89D81E485E36107077CAD8D2017FD59BF4B56A539A
SHA-512:	E9D271E0989D43E2D5D9744D8F58CB71C234BCD0CE7DFE4EC217FB67BD087F496D19C51CFF3C4A85C5A3DFD16C8E0D738244E86187E4F5E83D588FDBBA8FD5F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x5929ca11,0x01d726aa</date><accdate>0x5929ca11,0x01d726aa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x5929ca11,0x01d726aa</date><accdate>0x5929ca11,0x01d726aa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.155127946165807
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwNVwV4nWimI002EtM3MHdNMNxhGwNVwV4nWimI00Ob8K075EtMb:2d6NxQeVwV4SZHKd6NxQeVwV4SZ7YKa/
MD5:	6715EBF8DF6FAF9D7754F22257EDC4A6
SHA1:	69816385C779F0DB6FBE24FA96E190F37F6453C2
SHA-256:	A32E0E3DE87ADBF36B6391290C6D7C799A5E176AB3570C059A433207AC599857
SHA-512:	4546377CE44874D3D163058224E6E5E23233A530B4C2CD4B29AB527EB0733D5A7A29454DCD1C64C765C6EDE4C26B47C8F79E492C0E94C8D227E0E41AACA8CE0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x5935b559,0x01d726aa</date><accdate>0x5935b559,0x01d726aa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x5935b559,0x01d726aa</date><accdate>0x5935b559,0x01d726aa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.093079171865968
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nAX4nWimI002EtM3MHdNMNx0nAX4nWimI00ObxEtMb:2d6Nx0AX4SZHKd6Nx0AX4SZ7nb
MD5:	B791BB5984FA0481ED4FC57B84C68072
SHA1:	1B250337FCFBEABB9E77345F4FB5AF9AA329E090
SHA-256:	3C3B897E97D9A48F050DEE9EC7DAD5AB50B68E84E1C8E3EADDA5A55F7D6D3FBA
SHA-512:	BDD4AD0BB7D8DF3D5EFD5B74BF2FEDCD64F25971F74E5903040BB08F9183AA04AE46630C4EE0BD0E9B6AD053643DC08E95AE27B737D41CE9F586E1002CC714C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x5930f0ab,0x01d726aa</date><accdate>0x5930f0ab,0x01d726aa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x5930f0ab,0x01d726aa</date><accdate>0x5930f0ab,0x01d726aa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.163299577893242
Encrypted:	false
SSDEEP:	12:TMHdNMNxxjnWimI002EtM3MHdNMNxx84nWimI00Ob6Kq5EtMb:2d6NxtSZHKd6Nx+4SZ7ob
MD5:	04D7977DC666B962C88FF723B76F7EA8
SHA1:	C5353264E6136F3663DD80A03794111A3D5D2138
SHA-256:	FB37DE8C2087DC9B0E66C6E46BE8EF0FCD7299C9BE2BCB1213D6CF6CC9CA6E79
SHA-512:	8BC6A396ECE58496EE463B4F16649C494AC9CCAD55B4889548D99FD85EFF7F3DD231D2F9192BEC1D215CFFBB823C48612CDB1DC5A421C01397D61509F55252F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x592e8e4b,0x01d726aa</date><accdate>0x592e8e4b,0x01d726aa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x592e8e4b,0x01d726aa</date><accdate>0x5930f0ab,0x01d726aa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.150366838141872
Encrypted:	false
SSDEEP:	12:TMHdNMNxcbplnWimI002EtM3MHdNMNxcbKDnWimI00ObVEtMb:2d6Nx2SZHKd6Nx3DSZ7Db
MD5:	83AD2B9F0C2D1A99D2414AED1EFE46C3
SHA1:	0AD131669D90391CA8C4E883BF2162E844246207
SHA-256:	7DD7A8FDC0ED9C07FC3DC15239DAFB5C4B8E29BFFB32290448A0BA1BCAEB87E9
SHA-512:	BA493FE4CBDC25AD88D5A60FAA6EFD988880B572E6C1E31D7581AF08B7AF95908B0EC0561E8912E96E015DB979A82ED8160EF0CB118215C7F79BA71BAD4BF350
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x5927674f,0x01d726aa</date><accdate>0x5927674f,0x01d726aa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x5927674f,0x01d726aa</date><accdate>0x5929ca11,0x01d726aa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.095963314918083
Encrypted:	false
SSDEEP:	12:TMHdNMNxfncUDnWimI002EtM3MHdNMNxfncUDnWimI00Obe5EtMb:2d6NxUUDSZHKd6NxUUDSZ7ijb
MD5:	736BBB2C65A85EAFC70FB3E08DFF4F75
SHA1:	AC30E4B57AD952A113B88E1783A86D8434A215EF
SHA-256:	43BA4E6822F2F07932EE101C5F3403BBA3B4BE08385B1288BC01CB5A075BB5AE
SHA-512:	02932313BB303744170F9C37582D7B230CD3673526F0AE950F2892438C92C96A5A69F76D5FC272BE6A91A7DF2E672D7BBD84B2D17E49589B33048F1B7F65A0F1
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x5929ca11,0x01d726aa</date><accdate>0x5929ca11,0x01d726aa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x5929ca11,0x01d726aa</date><accdate>0x5929ca11,0x01d726aa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	889
Entropy (8bit):	7.104607793265337
Encrypted:	false
SSDEEP:	12:15uDGZbVl+KkDbMRv/7//76PcVAcDDx6UK9QEVJoOfJG4KH/TLWRNAfk0YndDe3f:1wDGTjfx77DDxtK9jfAH/3WRmoDWOXw
MD5:	EEFCE1C985430D9BEACB98C54D6ABC21
SHA1:	A9300DC0D4E1E3DA705A5636EE2A5B7CD5E94BA2
SHA-256:	9C676D1A8D3A3F5603D48FD611B30A15F856462CD5A0C7078D4E12657550000B
SHA-512:	DADB7B6A9278477F52B4DF978AA27A3C642F028890BD2EA884CD8EA1775AEC320E67054E8E76E77CBD4182E3BB4ED00EEFE1A98294412BABD7D3B1C3050C4145
Malicious:	false
Reputation:	low
Preview:	F.h.t.t.p.s.:././.w.w.w...g.o.o.g.l.e...c.o.m./.c.h.r.o.m.e./.s.t.a.t.i.c./.i.m.a.g.e.s./.f.a.v.i.c.o.n.s./.f.a.v.i.c.o.n.-.1.6.x.1.6...p.n.g.....PNG.....IHDR.....(-.S...YPLTE...z.Q.K..A..[.RK.I>.PD..A..\..a..A..a.K@..[..@..[..@.SH..Z._.WL..@.qQ.PC..A.L@..\.l;.Ul..B.fl..A.PC-.P..E.SH..@..X..=.PC.VJ..A!.f..@.VJ.OA.<.QE.YN..@/.e..?T.L.<.RF.WK..B..[.MAK....^l..".d..a.QE.RF.h;F.....>.v..u.~s.J=..;e..[..q..c..H.....?.ud.t.m..k.si.yd?.V.[n.W..V..T.`T..S#.Qz.LlqL.G.SG.RE..D.PC..A..@.P?.:..s....9tRNS..%.....{i=;1)$.....RPFE?8#..../.....IDAT..=..r.Q.D..@H.....2.{W.@...w...`..<M.....y.n....xq.m.l..... ,..0...4U .f[.s..k..htN...3*..;..W0.....|`..+..'Iz~.[.F...3..Q...G.U..E.#!..$&]4Q.9."..~..i.v.X$..}'....X....o.A.K .K<Q.".8...N+.....w7.v...0.tc....A.)XbJ.....IEND.B`.....dCe`....dCe`....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1001175813[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	modified
Size (bytes):	42
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEy:1QEoy
MD5:	D89746888DA2D9510B64A9F031EAECD5
SHA1:	D5FCEB6532643D0D84FFE09C40C481ECDF59E15A
SHA-256:	EF1955AE757C8B966C83248350331BD3A30F658CED11F387F8EBF05AB3368629
SHA-512:	D5DA26B5D496EDB0221DF1A4057A8B0285D15592A8F8DC7016A294DF37ED335F3FDE6A2252962E0DF38B62847F8B771463A0124EF3F84299F262ED9D9D3CEE4
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\26b8484e-52e3-44ac-b958-865809934ebb[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\26b8484e-52e3-44ac-b958-865809934ebb[1].woff	
File Type:	Web Open Font Format, TrueType, length 48908, version 1.0
Category:	downloaded
Size (bytes):	48908
Entropy (8bit):	**7.9908769597228275**
Encrypted:	**true**
SSDEEP:	768:2noxWxiIDP1D007rQc2v/5eRPz2S76YGQ3AmzfwSqwSmBHPch7vsqazs6/B40fB8:2n5Q0CZe12S76YGQwmzIhmivsqaAcBF8
MD5:	B1C2C4A57ABC248FA5B015E5DD93000C
SHA1:	E287387E70687D521E839DF86F38CFF3F1D71301
SHA-256:	4D18B41D696C25E7E1A9372398C555C52162D9C995552E792ECDC054274CC8F2
SHA-512:	4769393B4D3A6DB167AC9FEAABFBA27D55056415D3F039A5F14FE3142B49B06A4636379D1E738D1B97C5072E095DE7955799136229D8D7FB273C58014957C0FC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/Helvetica/v2/26b8484e-52e3-44ac-b958-865809934ebb.woff
Preview:	wOFF.....Z.....L.....GPOS.....1,...;GSUB... .....N./.<OS/2...,...S...`h5|.VDMX.....|....o.w.cmap.....#.<.cvt .."....X.....:..fpgm.."".....6...gasp..'p.....'glyf.. '...}.....*c.head.....6...6...hhea...<...!...$.M.6hmtx...`..._....Z.T.loca.....W.....4maxp..... ... .[.dname...8.....3.post..... ...2prep.....x....T...~w.f.....[D^."*"/.....]...p .5....&..L.Q.q$..:hX...+.....#C.....uP....[...8:.c.s.l.....W_}.....}.(...b9$...x.m.d.o....~...!^.1.Z..W.^\|W...O...~L...7fX...p..<.:q..3.:S{2.7S.2.?S.$x..;.Ho..`.C.v.....v..N'.7..o...X..Y.* D...5.x..L.L...y.S.y..g.g....m.m.....{.w..!...{7y...o.....o.o..!_.o.....f.,.|......./.?._.....?..@.@.....'.....`.`.....].....C.BcB.B.C....=.Z.....*.....*..B.P2..7.7....;.{. {.....G.....w.?...FZD.G.....e.HAdUdC.$.v.N..g.3.....Y...r.:_G..p.c.gt@thtdt\tbtZtVt~ta....-.].d.x...=.hm.W.}.%Y...Y=.FfM..=<.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\4UaGrENHsxJlGDuGo1OIlI3K[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 82300, version 1.1
Category:	downloaded
Size (bytes):	82300
Entropy (8bit):	**7.993868899885629**
Encrypted:	**true**
SSDEEP:	1536:nG4K6l+BuoexS2Sv1TEThLUb2AQ3i/U7sCV30lbRS5NA7UFloGIN46:nGxkBxS2YEThIb2v3iIsCV2H7UFl9Z6
MD5:	78F084CD32CB85327C04655BD20D7135
SHA1:	BA8CD3AC9F80EC121C20A4423987BE8B3A706D55
SHA-256:	DC662D2DD599D356BAF970A6AE9AACB4477FCC84E39159FE4B49ED82D2ACB4B7
SHA-512:	06CF2D6AD91ABF5B8DF8AC54D4345E6560A43C59D013B2170454BA00FBF255B1D5060BD89F34640E0DFFBCB6323B7C4A94AEBEE9A4125286997E17E3606BB5D 0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/googlesans/v27/4UaGrENHsxJlGDuGo1OIlI3K.woff
Preview:	wOFF.....A|.....GDEF.....<e.e.GPOS...D..;.....Qr.'GSUB..=\...<..#X....OS/2..O....U...`kr[.cmap..O.....@Y..Dcvt ..V....y.....fpgm..V.....uo..gasp..^ H.....glyf..^T...a..x..head.....6...6..'.hhea..... ...$.0..hmtx.....H.v4loca.."....&O..^maxp..+.... ... .name..+....e...m...+post...D.....*N....prep..@....p..... ..x.U..F.q... s.G.....jiZ ...DCB...H...BO....ao.....{.^.....lb>..zCz.....O...i..k.....$9-S.m.$..S<. .x.|...}..e.V2Z..g4\p..{.5.....~[}_.X}^.#.`..S..U.T.....;... {....!...._../.....?."-=x..Y.p...}.z.$... ....f4.*.w..9.J.033...'.0.p.....^.....:.T...AS.;...^.l.m...@..jD;...h{.C...'....9c.. ...a..(.7v(BY.1Q.rT.{.{'T.....34A.B?.gE..B.*Q5...C0....c...Y?.....+~\...IR`.'.4)B...(.R....7..0...w.>>. ..O.....w.x^Xi.r..:...p8R#..."....t-..p[.]..-..v..E.K..5..=y8.. ..9...p._.{.;.3a..,c...6..mw;..5|...5..78.S.&.)v.gr6.p..s!.q1.p9..j.....:Yg.....I.`.m.=c..{...9*..Ud..d.Rp|....LI.'\)Y%Y...].O..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\50ac1699-f3d2-47b6-878f-67a368a17c41[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22537, version 1.0
Category:	downloaded
Size (bytes):	22537
Entropy (8bit):	7.980046807695369
Encrypted:	false
SSDEEP:	384:7jtnrP2HkbVPlywA397tSeRHNm/gWsatewLC6/q7LJxtL42eHa3NmQNxF:7jhrmUyj3rNIth1q7Nxt824dQ3F
MD5:	AFC80FD38B63916E55B3434D6DC50AA8
SHA1:	A93E6A628D615ECC4A03268D615B2C7339BB82CA
SHA-256:	8E1FB2C958070695B9633261993A47CDAC70A25EB9C321EA0DC7207036D5140D
SHA-512:	AC516CEB938F721E006D05A3E712E6142A0F086EA71A44CA00187A48C183DF7B4B3EEBF9811C8FE9840CB6D345E445DD9A5A3E892B3BBE9DDF7A670161A3B8 A8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/Helvetica/v2/50ac1699-f3d2-47b6-878f-67a368a17c41.woff
Preview:	wOFF.....X.....Rt.....GPOS...l...^.....HOS/2.....T...`e...VDMX... ...V....r8y.cmap...x...m...../cvt .....K.....fpgm...4.....,...gasp.....glyf.....9;..\n W...head..G....6...6.z}whhea..G<... ...$.>..hmtx..G\.....loca..IX...b.....+~.maxp..K.... ... ...Mname..K.....!=..$post..Q..... ...2prep..Q.....y..x...OO.Q...Li.RhE...4..`HHJ ..4FME..R..7F.....}....1..u#&.j.BM ...v...;t..x..uD.....w.....&....-}.s...E....&u8{..T.|..T:..\R'f....W..]..|....B...,j...kS.....Y.,...cm...].T....^OU!.iD)..r..4.1MjZ+Z.=j...S...0k..v.z.+...u...1p7.]]J.....Xf....B.uPm..frK.d..1?.....h.}_6.u.e...h...-.!..g].%....2(y.....7.L..k.".su.>|.....d~...^...Y.^.b..-se..X....uu.x..~..N.M#.....y...&.2.`.N....m.kA....s...A..0.$k..5.....i..0.....q.>.. ..g..}...7..*.....L...=.....j;V..jtY..V#.t.1..t...i.b.;.19j.....i.....t.Dt.t.*h.5.....u...;.....Jh..KT^.~..2*oAD.....+..G.....x.c`a.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\7041360063881691[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\704136006388169[1].js	
Category:	downloaded
Size (bytes):	249005
Entropy (8bit):	5.478861089638576
Encrypted:	false
SSDEEP:	6144:Rk1HWCSntDV/H4K3V/H486EPjQHWuH3Hpn:f6EM
MD5:	EAD7F77461BA4AD1540065627593F0AB
SHA1:	72E4D31E93C7B6621CA0CBB9379D6B7500BB91FB
SHA-256:	7632EBA773406DA1C4E7AF50E61F6063A23F1242A051BFDBCE0DC535B7ABCB26
SHA-512:	92E06E13FB0E8D4C6F284674C8147083980B8846FBB2BA88B50586C7B2621A3DCA6961B1B1EF709DBBACE95A9F3458923EAAEAC5BBF96A372D4FA28D8662080 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://connect.facebook.net/signals/config/704136006388169?v=2.9.33&r=stable
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ScrollMagic.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	18500
Entropy (8bit):	5.288803063564337
Encrypted:	false
SSDEEP:	384:CEKmt3JtBOgr3CSEVbMtClyCJ4qelm2JDX6r:jv395bO+t7e4qEJDM
MD5:	955ABE8CF2E241745BEE38B92BEBC76C
SHA1:	414B13E1866A94EAEF2643A5167381BBE2AA7699
SHA-256:	09756F2D963931CD3831E019D7DFC7A71DC6EC0E02ED4CF6232C46E3B40A9909
SHA-512:	0A8289AE94A67E9262ADBE1198E622B78B01F031713A0C808854EE91A3C2101E3003C61586A7D4B05D5666531B8B5A51DCC8BB53AF5D29FD34C36C17BFEBED5 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/external_hosted/scrollmagic/ScrollMagic.min.js
Preview:	/** @license ScrollMagic v2.0.6 | (c) 2018 Jan Paepke (@janpaepke) | license & info: http://scrollmagic.io. *. * Copyright (c) 2018 Jan Paepke. *. * Permission is hereby granted, free of charge, to any person obtaining a copy. * of this software and associated documentation files (the "Software"), to deal. * in the Software without restriction, including without limitation the rights. * to use, copy, modify, merge, publish, distribute, sublicense, and/or sell. * copies of the Software, and to permit persons to whom the Software is. * furnished to do so, subject to the following conditions:. *. * The above copyright notice and this permission notice shall be included in. * all copies or subst antial portions of the Software.. *. * THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR. * IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,. * FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE. * AUTHORS OR COPYRIGHT HOLDERS

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\WixMadeforText_W_BdIt[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 28692, version 1.13107
Category:	downloaded
Size (bytes):	28692
Entropy (8bit):	7.984015162753741
Encrypted:	false
SSDEEP:	384:0xmMzIjVGNHUnD6SundIUZ9mIqA3b/zdaijMACAE9MVYlJMp2PXO9T9BVzdcAkQO:PWggdIUZw4na1z/TPXmVSAnZFG
MD5:	9557403059EA8B62EF946E44250971FA
SHA1:	F5D7EA5B2DDE5D291490E7AF03DD72E70114299B
SHA-256:	0871C5BF40DA6C907DFD85E3803AC0A950029E66BA1C970B7F4BD5F713541B59
SHA-512:	AF18FEA8D59897ED48B46477A1A4DC8969280302EC3717C284BC671BBB89BF3C93BC1DB8EBD996254FEC392D86FE8D489D3E32EF8B81B0DE537146E7533713 0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/WixMadefor/v2/WixMadeforText_W_BdIt.woff
Preview:	wOFF.....p.....33.....GDEF..]....."."!GPOS..]....x..H.....GSUB..l.....fOS/2.....\...`....cmap...h.....X..:.cvt .....$..Afpgm...x.....0.6gasp..\.....glyf... T..H[..u....Khead.....6...6.D..hhea.....$...$.g..hmtx...X.....h..-*loca.....w....i.K.maxp..... ... .9..name..[...,....DCnEpost..\..... ...@prep...$.....Q.T.....33...._.<..... .....O...X...../.a.....x.%...Q.....Q.t7.....-t.{.....e..S..O.>...s...;.].^..R.\./..0..O.s..F.|.....Zx....4Y..oR.m.m..m.m.m..jjfz..|'y.... o.K....UP%.x&.Gk++...*V...:.....^W.j...#.J.TI?.....J..n*..f.g?iWo.?.....U....Q7...R.3..V.[..y|f[..vL.d[.W....F..%.W..t..i...mMn.h.m.....{#.....:.."z/...z..nhn...^.....q.Do.zS.....7. .....9U..ir..L.PW?R.|+M..U.>...q[.v..I.}.....a.....+..H..Sb.....#.Ym._...29G.a#.....%|..%..w.Z.lU<e?..N.1..<j.....[.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\WixMadeforText_W_It[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 27412, version 1.13107
Category:	downloaded
Size (bytes):	27412
Entropy (8bit):	7.982891923389201
Encrypted:	false
SSDEEP:	768:ap6knzmw/hRKu7qDk7lddf2H7jE/MnEzqD2NSXTiheFG:aYJw/Hlxf7Mn5SNi4z
MD5:	8E17780BCDC9E29BFDF2B5EC643E7B3B
SHA1:	CFBB4904DAF466D0AD0864DC43249C30866E7285
SHA-256:	507BC6DAB5FCF62276BFEE3155DDF6083AE9EBB54729FB56040A60DEE9C705B3
SHA-512:	ABA09CC85AAC3F2096A98FEFBDCA5DF572D718A553AC2F2918945E788901D87D0244A15E01CA417945A2E02BB10D6813CF390A83168662747FEB701B39C9222
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/WixMadefor/v2/WixMadeforText_W_It.woff
Preview:	wOFF.....k.....33.....GDEF..Z....."."!GPOS..[d.....Dn....GSUB..g.....fOS/2.....[...`....cmap...H.....X..:.cvt ...0.....+...fpgm...X.....0.6gasp..Z..... ...glyf...h..F+..u.....head.....6...6.}..hhea.....#...$...+hmtx...X.....h.jGRloca.....z....."S..maxp..... .. ....name..Y.....?.k.post..Z..... ...@prep.....,.....33.[.._.<..... .....x.c`d``.....,{._0\f@.....O...R...../.a...1.....x.%.....@...'.H.$xc..:..... l.(h....Z...../.:RL.f.T-.....@..U....e..]....9..(....1...x.....J..oW~.m.m.m.m.mc...d.y .s.SIW.z.'d...wx.p>.C..EW.A..@...Cc....3..YF.b.....~...t3.....'.QN..0.....+.Hj...".Vj %.[.yH..3v..S].5.!Tg....7..F ...q..x.f\^.`\~..1.0myR.qQ...z.U..RM.Tg...@..~.F..|....[B...D.:.F_[.. mB.`....!.%(.h JXk.....~.iH'.P...ul4..3)J.N.#3.{...e.....#M.....z.DFh.M..H./..6....v....P..Z...9.+.N..... .....".:...a.J..... .P..cU..8*.....^..O(.C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\activityi;src=2542116;type=2542116;cat=chrom0;ord=832802698175;gtm=2wg3o0;~oref=https___www.google[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	368
Entropy (8bit):	5.44280429578039
Encrypted:	false
SSDEEP:	6:hn8FQiowadCc4svmzw9xUpCX96v6OqPbRmEH7fuUo1xidiVzj0Mo:hnMQbwuOaxyCkv4AEH7GXfisVP0N
MD5:	155279A0BFCAE230EFFA498F6CEBC1D2
SHA1:	06D7309F67AE3A3C00F40AAD9F37B15D52BCC520
SHA-256:	F1150117502CDDBC6566148E3F562FAA13F69E9AC1521AE3BD25587F85C8D2E7
SHA-512:	DAE69E55489CBFD338FFD229D4AEBD26D19DBEEB1C9E0CD0C5999BF0A62DDD52240AF814E5A0BCC371C925437234E7CD9E93FC4E9EB99B7F874C7170C6D8 F31
Malicious:	false
Reputation:	low
IE Cache URL:	http:// https://2542116.fls.doubleclick.net/activityi;src=2542116;type=2542116;cat=chrom0;ord=832802698175;gtm=2wg3o0;~oref=https%3A%2F%2Fwww.google.com%2Fintl% 2Fen%2Fchrome%2F?
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"><html><head><title></title></head><body style="b ackground-color: transparent"></body></html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\animation.gsap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2411
Entropy (8bit):	5.443885333865454
Encrypted:	false
SSDEEP:	48:T9CwjsCJ9lDEtsQQMQHWs5G7Jo3oAFzSHrcTXwhKF1baz0vwCQ5biBz5bhLr24:T9djrgtYMQHqEoc9e54DLy4
MD5:	FBC6FD5E2FC6409C75F602320CB5909E
SHA1:	A37D2D19425526B6F9DC1873525AFB437CEFE25F
SHA-256:	ECA64F6A9419A07B0638C88AC89F7B1C7B8D6F16865291DF6F668D200064A233
SHA-512:	1092F44A35A17423AE8F70D554B5204B8A0FFE41355706567B09469D42D60F6A174434DA921D8A21B73EF6862B6FC8D6EAD14FF2B85A373AD4E5B090C39C5801
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/external_hosted/scrollmagic/animation.gsap.min.js
Preview:	/** @license ScrollMagic v2.0.6 | (c) 2018 Jan Paepke (@janpaepke) | license & info: http://scrollmagic.io. *. * Copyright (c) 2018 Jan Paepke. *. * Permission is hereby granted, free of charge, to any person obtaining a copy. * of this software and associated documentation files (the "Software"), to deal. * in the Software without restriction, including without limitation the rights. * to use, copy, modify, merge, publish, distribute, sublicense, and/or sell. * copies of the Software, and to permit persons to whom the Software is. * furnished to do so, subject to the following conditions:. *. * The above copyright notice and this permission notice shall be included in. * all copies or substantial portions of the Software.. *. * THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR. * IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,. * FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE. * AUTHORS OR COPYRIGHT HOLDERS

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\animations-vendors.3ce71584.chunk.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	213372
Entropy (8bit):	5.308008187653904
Encrypted:	false
SSDEEP:	6144:Kp6AbyGVvuvWP/f/K27ZsCrnvPdYDgdp/YMwuaN4uOV2Jrkm:Kp668WP/rVBk4uOEtkm
MD5:	061426BB972AFBE1135CA30CCAFE0787
SHA1:	7B667A67FB0C0C1527F19C7873066C547DBEEB87
SHA-256:	532B59397CCFBE42140127241BD0082250589F221AC8CE237DBB04F8E6F8D139
SHA-512:	6490EABF6859745AFEDEF7E4500BC97B9C5EF527B74B5F343266BA18C69C2EEA6FCE538F96F470F13FFCB0826836FE717D5A6F94AE2F859AD922D8CE0A9A598 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-thunderbolt/dist/animations-vendors.3ce71584.chunk.min.js
Preview:	(window.webpackJsonp__wix_thunderbolt_app=window.webpackJsonp__wix_thunderbolt_app||[]).push([[21],{394:function(e,t,n){"use strict";function r(e,t){var n=Objec t.keys(e);if(Object.getOwnPropertySymbols){var r=Object.getOwnPropertySymbols(e);t&&(r=r.filter((function(t){return Object.getOwnPropertyDescriptor(e,t).enumera ble}))),n.push.apply(n,r)}return n}function i(e){for(var t=1;t<arguments.length;t++){var n=null!=arguments[t]?arguments[t]:{};t%2?r(Object(n),!0).forEach((function(t){a(e ,t,n[t])})):Object.getOwnPropertyDescriptors?Object.defineProperties(e,Object.getOwnPropertyDescriptors(n)):r(Object(n)).forEach((function(t){Object.defineProper rty(e,t,Object.getOwnPropertyDescriptor(n,t))}))}return e}function a(e,t,n){return t in e?Object.defineProperty(e,t,{value:n,enumerable:!0,configurable:!0,writable:!0}):e [t]=n,e}function o(e){return e*Math.PI/180}var s={normal:function(e,t){return e/t.maxTravelHeight},legacy_in:function(e,t){var n=t.maxTravelHeight,r=t.travelLastFold,i=t. travelFirs

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\black-history-month-themes[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1000 x 610, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	87138
Entropy (8bit):	7.979760110192943
Encrypted:	false
SSDEEP:	1536:oDX4MgLMjhCPWsE+wnchq68X4m+0fuW1yid4sRmx6NIPelA3Zeh9DCxf:oDIFiXtlncuXa0WW1zdDD+P0Keh9DCd
MD5:	6EF63947E7D5589589D608DDD33F8439
SHA1:	07930D2057D6D572D2D40123A883A4A07F44DD44
SHA-256:	086DB3480EE29F29F997891787C74361844CBE9013D626DE892ECAD7A598C6C5
SHA-512:	CF88110B8D2969DEE946342DC3A08C8E4DE99ECEE38876641D122B46D6F82D1A43C3648758B483FD2819BB573C48B7DF29CDDE4350A22A34FC04DBC4C061B7 4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/chrome/static/images/homepage/black-history-month-themes.png
Preview:	.PNG........IHDR.....b.....c!.....PLTE....=..;...6S....h...*.....>.1.gNt.....;.....+.....C.....?.1.e,U.459.R.=.u.A..J..D.9V..B..N..:.:.~3S..I..q..F.&N.-Q.?Y..S.!K.....C..S..6. .E.E].0a.A7/.Y.'Z.9g.@T.5O./M.:R.SZ.Z].%^.Na.LX.An.FV.R|..G.)K.Cc.#I.a`.Hu.9^./X.+d....9....2j.'R....Jm.!p.....M.....Ge..{...G.Z..p..jc.!x...Sw.`m.lq.L..;q.ug....Tj.Bz..g....`~..C. ..V.....j.....".."..a.....{v..G..E....w.....1Y.`..;a..E....x..o..).....Yk.:r...,..5...k.-..Ih.p..x.....*.|...v.....&Q.....Pv.....I..v{..<.....;U.....w.~.....b..T..*F....c|...~...'P..*&..... e.z$Aj..i..8u.....A.....t.....,{X....}.F.....^.....)C.....m..UW.}.....6..EZ.LNO#qC....|{..YqK...k..^`c...nnq...M|.K_.!k.....k0Ig`W..mD..I_.....tRNS.....T._.....^... .Q.IDATx..?..@...".$...M|.....p.%...]..ED*8..8..\ p.q.)....]..m.x'.O.K...<...%m.,..!.....YR\....s))..9..iz...r..._.%D~..._....YB.Z.)..E.@.d.q.9)...6....."

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bolt-custom-elements.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	113551
Entropy (8bit):	5.351401537580938
Encrypted:	false
SSDEEP:	1536:QOEzTf4tlH+4VgN8/jd4TPrMsFhb7hKR2lW003UevfilY:TifhhY5QX
MD5:	5FB06CADBF497C26972AF94E2F529397
SHA1:	DAAEDC1CC9A0C9863C19DF9ADEC7FECC51C81FE5
SHA-256:	9366C382B51C6458C73CF5E88A51455726C3F4D4D23E3CC6EA56DDA1A9E77710
SHA-512:	6D8AA904420961D2AC6CCC4467BAB77A126AE9F23A9F6C046B908B64DEDB562E419A113C4108C2BB1C5D49D0665C7B6A0523442DB5BAA9E83702A8182438A36 B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7107.0/bolt-main/app/bolt-custom-elements.min.js
Preview:	var customElementsPackage=function(e){var t={};function n(r){if(t[r])return t[r].exports;var i=t[r]={i:r,l:!1,exports:{}};return e[r].call(i.exports,i,i.exports,n),i.l=!0,i.exports}return n.m=e,n.c=t,n.d=function(e,t,r){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:r})},n.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object .defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},n.t=function(e,t){if(1&t&&(e=n(e)),8&t)return e;if(4&t&&"object"= =typeof e&&e&&e.__esModule)return e;var r=Object.create(null);if(n.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var i in e) n.d(r,i,function(t){return e[t]}.bind(null,i));return r},n.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};return n.d(t,"a",t),t},n.o=function (e,t){return Object.prototype.hasOwnProperty.call(e,t)},n.p="",n(n.s=1)}([function(e,t,n){e.exports=function(e){var t={};function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bolt-main-prod-old[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	2012259
Entropy (8bit):	5.618038706308556
Encrypted:	false
SSDEEP:	49152:SNnVRSefooi1GQrTMbMdMl8yoDXrK1nP2Uf4dB3v3SjEba8XViEyN:JOQQMdM6AP2Uf4dB3v3SjEba8XViEyN
MD5:	EBBA1C527B51C9CDC591DBFC35310CA1
SHA1:	9CB9AC53C2CB7DCA2D8201DA83616F8810363C75
SHA-256:	26DD368DFA87FB4F597969B4E89D46977CCF102879FF796E388FEA8A62B77232
SHA-512:	A7611C2511EA56C2A1228FC07D29143003A0149949AA8580579A50FAAAC2B49AC921CAC818068C2E4C9C19BA20787223EC85DF4513A6A02C5F51D7BC3DBAF45
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7107.0/bolt-main/app/bolt-main-prod-old.js
Preview:	define(["lodash","coreUtilsLib","react","prop-types","warmupUtils","zepto","react-dom","santa-components","coreUtils","tpaComponents","color","thirdPartyAnalytics","create-react-class","layout-utils","layout","wix-dom-sanitizer","data-capsule","galleriesCommon","bolt-components"],function(e,t,n,r,a,o,i,s,u,l,c,p,d,f,g,m,v,y,h){return function(e){var t={};function n(r){if(t[r])return t[r].exports;var a=t[r]={i:r,l:!1,exports:{}};return e[r].call(a.exports,a,a.exports,n),a.l=!0,a.exports}return n.m=e,n.c=t,n.d=function(e,t,r){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:r})},n.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},n.t=function(e,t){if(1&t&&(e=n(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var r=Object.create(null);if(n.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var a in e)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bolt-main-r.init[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	338852
Entropy (8bit):	5.446294168118535
Encrypted:	false
SSDEEP:	3072:Ucwt+ywr9a6+s7BDIMCPS31NOjR/M84hV4HhDSo2wDZDtiu8eYEmss2fPjM:NwtsDISa7r8OVPjM
MD5:	8E2ADD131D5E8CE3B79E71E3A7BDDD6D
SHA1:	CBCDDA54B860DF21C1384FBF0489FE794BCF8279
SHA-256:	58A65336D59C4ABB3CEBBAAE49EE37E0FB489EAF5C3653CC5F20F7149CC25A2F
SHA-512:	597B191A08BDF820F71F3A180B466754DA71CC5BA8FF5ACC1DC7DA38984EDEC9F2770EBEE2486C04BF7C060BF2E44949D8F5560032236E9EE123ACA8C68B29E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7107.0/bolt-main/app/bolt-main-r.init.js
Preview:	(this.webpackJsonp=this.webpackJsonp||[]).push([[4],{220:function(e,n,r){"use strict";e.exports={prefersReducedMotion:function(e){return!(!(e=e||("undefined"!=typeof window?window:void 0))||!e.matchMedia)&&e.matchMedia("(prefers-reduced-motion: reduce)").matches}},221:function(e,n,r){"use strict";function t(e,n){return function(e){if(Array.isArray(e))return e}(e)||function(e,n){var r=[],t=!0,o=!1,a=void 0;try{for(var i,s=e[Symbol.iterator]();!(t=(i=s.next()).done)&&(r.push(i.value),!n||r.length!==n);t=!0);}catch(e){o=!0,a=e}finally{try{t||null==s.return||s.return()}finally{if(o)throw a}}return r}(e,n)||function(){throw new TypeError("Invalid attempt to destructure non-iterable instance")}()}var o=r(54);e.exports={getContextId:function(e){var n=e.mainRootId,r=e.innerRoute,t=e.tpaInnerRoute,a=e.lang,i=e.platformGoToEditorCounter,s=e.pagesVersion;return[n,r,t,a,o.uniqueId("context"),i,s].join("$$")},getMainRootIdFromContextId:function(e){return t(e.split("$$"),1)[0]}}},222:function(e,n,r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bt[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	3.0950611313667666
Encrypted:	false
SSDEEP:	3:CUMllRPQEsJ9pse:Gl3QEsJLse
MD5:	AD4B0F606E0F8465BC4C4C170B37E1A3
SHA1:	50B30FD5F87C85FE5CBA2635CB83316CA71250D7
SHA-256:	CF4724B2F736ED1A0AE6BC28F1EAD963D9CD2C1FD87B6EF32E7799FC1C5C8BDA
SHA-512:	EBFE0C0DF4BCC167D5CB6EBDD379F9083DF62BEF63A23818E1C6ADF0F64B65467EA58B7CD4D03CF0A1B1A2B07FB7B969BF35F25F1F8538CC65CF3EEBDF8A910
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....L..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bundle.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	72170

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bundle.min[1].js	
Entropy (8bit):	5.291418439127055
Encrypted:	false
SSDEEP:	768:ugT7CZ2ilPNNqNb61qY8ZQUWxikVdotBhhS+ly6Rv5//g7lhH4HfSzO0BTPUQ3j4:jT7+NkbvLF5/AlhH4sKP
MD5:	E2A262292E08E10807A052B02C5951E9
SHA1:	21769E4CBA828D2225D4247D1B14D550C77954E3
SHA-256:	635B050935D2360B9D5FD1F7E7FA3C6B949A14809518AF434C0F31F3AF393046
SHA-512:	587FB55A5BE7621B407EE2554E69CD34A2F9A1685AA53EF76A2D48C36526DB46B774ED2DB17331F7B49F2B2C83FFC62961F69AB8E4EC17DC7779A92808AC305A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://browser.sentry-cdn.com/4.6.2/bundle.min.js
Preview:	/*! @sentry/browser 4.6.2 (1c1b0715) | https://github.com/getsentry/sentry-javascript */.var Sentry=function(t){"use strict";var e=function(t,n){return(e=Object.setPrototypeOf||{__proto__:[]}instanceof Array&&function(t,e){t.__proto__=e}||function(t,e){for(var n in e)e.hasOwnProperty(n)&&(t[n]=e[n])})(t,n)};function n(t,n){function r(){this.constructor=t}e(t,n),t.prototype=null===n?Object.create(n):(r.prototype=n.prototype,new r)}var r,o,i=function(){return(i=Object.assign||function(t){for(var e,n=1,r=arguments.length;n<r;n++)for(var o in e=arguments[n])Object.prototype.hasOwnProperty.call(e,o)&&(t[o]=e[o]);return t}).apply(this,arguments)};function s(t,e,n,r){return new(n||(n=Promise))(function(o,i){function s(t){try{u(r.next(t))}catch(t){i(t)}}function a(t){try{u(r.throw(t))}catch(t){i(t)}}function u(t){t.done?o(t.value):new n(function(e){e(t.value)}).then(s,a)}u((r=r.apply(t,e||[])).next())})}function a(t,e){var n,r,o,i,s={label:0,sent:function(){if(1&o[0])throw o[1];return o[1]},tr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bundle.min[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	65304
Entropy (8bit):	5.220447655902976
Encrypted:	false
SSDEEP:	768:5thPgk5Zi8QLtFJ0+nMACXn3nVWa062vjg4/aBkaAYPiIZRSfWRV0lspnFAz6QCs:pa0CUXgvjg4/UkaAYPigRLnkCdEhs0L
MD5:	CA197586ED80A7767CC602668C7B18BE
SHA1:	4C529C1C294D362DE3CC90CAF487FFEEA8827F56
SHA-256:	D58AE5786D8A1FECE18908C69B138536CB2FC61A5507ACFC2A7107A2D31F10DD
SHA-512:	C857991615F1D1662F275648F757DC80BC8D13C6166C97ECAA121EA290211182D88CF6E1DBD443C313DEE20BC3A3238B01CF2D0908DB106080C32BC37E8D950
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/unpkg/@wix/santa-bundle@1.1061.0/dist/bundle.min.js
Preview:	/** MobX - (c) Michel Weststrate 2015, 2016 - MIT Licensed */..!function(e){if("object"==typeof exports&&"undefined"!=typeof module)module.exports=e();else if("function"==typeof define&&define.amd)define("prop-types",[],e);else{var t;t="undefined"!=typeof window?window:"undefined"!=typeof global?global:"undefined"!=typeof self?self:this,t.PropTypes=e()}}(function(){return function e(t,n,r){function o(a,s){if(!n[a]){if(!t[a]){var u="function"==typeof require&&require;if(!s&&u)return u(a,!0);if(i)return i(a,!0);var c=new Error("Cannot find module '"+a+"'");throw c.code="MODULE_NOT_FOUND",c}var l=n[a]={exports:{}};t[a][0].call(l.exports,function(e){var n=t[a][1][e];return o(n||e)},l,l.exports,e,t,n,r)}return n[a].exports}for(var i="function"==typeof require&&require,a=0;a<r.length;a++)o(r[a]);return o}({1:[function(e,t){"use strict";var n=e(4),r=e(5),o=e(3);t.exports=function(){function e(e,t,n,i,a,s){s!==o&&r(!1,"Calling PropTypes validators directly is not supported by the `prop-types`

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\chrome-logo[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	5828
Entropy (8bit):	5.292681906113015
Encrypted:	false
SSDEEP:	96:+4JqrKfS5c6qyc/7lRy9dvNK60ALhVxeHRI:HvJ4rHi
MD5:	C365DFBEBEFF9E8606BDF3E3B3AECBCA
SHA1:	4CF31EC373CFE7D1E3A03CF21AC11D38B888F9C3
SHA-256:	610FFD583BAF9476A6AAB758F9C3B76A5C8EBB8A7B2446B7EFCA0B26A97D761D
SHA-512:	70FA9071CEFA580844B41CAF796894CB7CC2ABF2B7E8990B62BA3D09C7975503587DE3787C6B864940DD1318BBD583C9ECA6356C497AD97DBF85F22B8A77EB1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/chrome/static/images/chrome-logo.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="48" height="48" viewBox="0 0 192 192"><defs><circle id="a" cx="96" cy="96" r="88"/></defs><clipPath id="b"><use xlink:href="#a" overflow="visible"/></clipPath><g clip-path="url(#b)"><path fill="#DB4437" d="M21.97 8v108h39.39L96 56h88V8z"/><linearGradient id="c" gradientUnits="userSpaceOnUse" x1="29.337" y1="75.021" x2="81.837" y2="44.354"><stop offset="0" stop-color="#a52714" stop-opacity=".6"/><stop offset=".66" stop-color="#a52714" stop-opacity="0"/></linearGradient><path fill="url(#c)" d="M21.97 8v108h39.39L96 56h88V8z"/></g><path clip-path="url(#b)" fill="url(#b)" fill="#3E2723" fill-opacity=".15" d="M62.31 115.65L22.48 47.34l-.58 1 39.54 67.8z"/><g clip-path="url(#b)"><path fill="#0F9D58" d="M8 184h83.77l38.88-38.88V116H61.36L8 24.48z"/><linearGradient id="d" gradientUnits="userSpaceOnUse" x1="110.872" y1="164.495" x2="52.538" y2="130.329"><stop offset="0" stop-color="#055524" stop-opacity=".4"/><stop offse

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\components.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\components.min[1].js	
Category:	downloaded
Size (bytes):	107479
Entropy (8bit):	5.178995573339264
Encrypted:	false
SSDEEP:	1536:k4EbwKaraPyj+TxNWfpgnFBUo6vBmKF9C8tT1IG54m6C/WbNZ+:a2CrWf+gHdD/kO
MD5:	7BF7C826161717F8C6627668F5FDB821
SHA1:	1FD2F26F71B4C5EA61EAB45FD040268A17FB43BA
SHA-256:	85D887A648E6CE1B8743222102CD3401B443BDDF871725FBABA86276FAF0A2D0
SHA-512:	47DFE9E5667675D704CCF37794AA541AD940BB125856D3F8832452474332E868DDD0D1586FF0EE7968062C3CDDADFB268B162303C9715CCD192F7CFFB6726B7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7107.0/node_modules/wix-santa/dist/packages-bin/components/components.min.js
Preview:	define("components",["lodash","coreUtils","santa-components","componentsCore","prop-types","skins","reactDOM","zepto","santa-core-utils","create-react-class","image-client-api","textCommon","backgroundCommon","santa-animations","galleriesCommon","displayer","imageZoom","comboBoxInput"],(function(e,t,i,n,s,a,o,r,p,l,c,d,u,h,m,g,y,f){return function(e){var t={};function i(n){if(t[n])return t[n].exports;var s=t[n]={i:n,l:!1,exports:{}};return e[n].call(s.exports,s,s.exports,i),s.l=!0,s.exports}return i.m=e,i.c=t,i.d=function(e,t,n){i.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:n})},i.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},i.t=function(e,t){if(1&t&&(e=i(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var n=Object.create(null);if(i.r(n),Object.defineProperty(n,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\coreUtils.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	116660
Entropy (8bit):	5.352158808373356
Encrypted:	false
SSDEEP:	3072:3Svggjht6Jf0Cd6SKB3YHZn7Svu6NtDYRWq:EBouNtMP
MD5:	7B872A8AE7CCFCD7DC98408080E04B31
SHA1:	2D968A176EF5A479E5DA90E80ED02A49EAE02861
SHA-256:	BBDCF4CD2965B75F0491C66C54DD8DF12C0287788684EC0833F1346047952528
SHA-512:	5AC1483EEB8ED230B1AA0B2CF283329E477FEA61CF06E3F2E759A49F2BDA174818633A21ED6D7DCC926BB26101C5A7B500E3C416A2ABAA6985BECC87CECE2563
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7107.0/node_modules/wix-santa/dist/packages-bin/coreUtils/coreUtils.min.js
Preview:	define("coreUtils",["lodash","warmupUtils","santa-core-utils","warmupUtilsLib","color","thirdPartyAnalytics","xss","data-capsule","mobileLayoutUtils"],(function(e,t,n,o,r,a,i,s,c){return function(e){var t={};function n(o){if(t[o])return t[o].exports;var r=t[o]={i:o,l:!1,exports:{}};return e[o].call(r.exports,r,r.exports,n),r.l=!0,r.exports}return n.m=e,n.c=t,n.d=function(e,t,o){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:o})},n.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},n.t=function(e,t){if(1&t&&(e=n(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var o=Object.create(null);if(n.r(o),Object.defineProperty(o,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var r in e)n.d(o,r,function(t){return e[t]}.bind(null,r));return o},n.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};retu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\coreUtils[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	106440
Entropy (8bit):	5.514423242622045
Encrypted:	false
SSDEEP:	1536:/kEG2CvhaFfvXms/fMYNMlVF2pNPakN0IF/U2yCSE3N78Ly+BQ5:/0hef5rPFN5U2yCSlQ5
MD5:	C5855B89AA2BAA5A7DC2601B6D79A246
SHA1:	CA7BDB490EB7F016092CD1DF5FACBEDA78E90B8F
SHA-256:	9762EB531AF491063EEFFED6A53E265BF0DC434CD97D8947841507EE9856598E
SHA-512:	600FE2751F95998371DB89AF562B2F37876AB36C1B558456B2DB6E31002464E40E2E701D95670B6C0B621FF985888D1DDA909EB46ACBF9B4CB3E1D47DF2C367
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/unpkg/@wix/santa-core-utils@1.2697.0/dist/coreUtils.js
Preview:	!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t(require("lodash"),require("zepto"),require("warmupUtilsLib")):"function"==typeof define&&define.amd?define(["lodash","zepto","warmupUtilsLib"],t):"object"==typeof exports?exports.coreUtils=t(require("lodash"),require("zepto"),require("warmupUtilsLib")):e.coreUtils=t(e.lodash,e.zepto,e.warmupUtilsLib)}(this,(function(e,t,n){return function(e){var t={};function n(r){if(t[r])return t[r].exports;var o=t[r]={i:r,l:!1,exports:{}};return e[r].call(o.exports,o,o.exports,n),o.l=!0,o.exports}return n.m=e,n.c=t,n.d=function(e,t,r){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:r})},n.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},n.t=function(e,t){if(1&t&&(e=n(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var r=Object.create(null);if(n.r(r),Object.defineProperty

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\dynamicPages.ea31d9ca.chunk.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\dynamicPages.ea31d9ca.chunk.min[1].js	
Category:	downloaded
Size (bytes):	3831
Entropy (8bit):	5.281180025971212
Encrypted:	false
SSDEEP:	48:lDrvaqXyuBXMRwmSvGeO+EUitKs+aSeLM8Pix3sUjWqr6mYBwFqhF6MVPTnDelyE:HuR4vZxSLSeURj6wM1sRRiA1qqVhC
MD5:	245B266A0D84FF98C84D3147009629BD
SHA1:	D7C857C19B07C249173250A3AB2FA8108939021B
SHA-256:	0169501B24183C6A42DC3AB2284FB2C68182307D2BA0902FA5B76FF0C7C6AF9E
SHA-512:	C208F84DB0762D3DB0C856D6ACB80BB60DD667176643EB04A21DEE38F99F1695CF20240914B002E5CC9040E6E8496F4BF9FA11EDFCEE57C687E8450869DE7DC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-thunderbolt/dist/dynamicPages.ea31d9ca.chunk.min.js
Preview:	(window.webpackJsonp__wix_thunderbolt_app=window.webpackJsonp__wix_thunderbolt_app||[]).push([[47],{303:function(e,t,r){"use strict";r.r(t),r.d(t,"site",(function(){return R})),r.d(t,"DynamicPagesResponseHandlerSymbol",(function(){return d.a}));var n,a=r(0),o=r(27),i=r(4),c=r(367),u=r(368),s=r(23),d=r(207),l="__403__dp",p="__404__dp",f="__500__dp",b="__uknown_error__dp",h=function(e){return e.replace("./","").split("/")},v=function(e){return h(e)[0]},O=function(e,t){var r=t.result,n=r.page,o=r.data,i=r.head,c=r.tpaInnerRoute,u=r.publicData;return Object(a.a)(Object(a.a)({},e),{pageId:n,dynamicRouteData:{pageData:o,pageHeadData:i,publicData:u,tpaInnerRoute:c}})};!function(e){e.PAGES="pages",e.SITEMAP="sitemap"}(n||(n={}));var g=function(e,t,r,n,a){var o=e.optionsData.bodyData,i=o.routerPrefix,c=o.config,u=o.pageRoles,s=function(e){return"/"+h(e).slice(1).join("/")}(t),d=""+n+i+s+r;return JSON.stringify({routerPrefix:i,routerSuffix:s,fullUrl:d,config:c,pageRoles:u,requestInfo:{formFactor

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\frame-listener.bundle.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	12492
Entropy (8bit):	5.160419543755334
Encrypted:	false
SSDEEP:	192:3yEiy5RPrtX3wF++ATgkStaO3umwutHnvlAg6fyvumWUpx2PO+lAg68JD2kD63:3yQQFVQmwckf9mJQPe852T3
MD5:	D829108208F1EB9B9BC884C5E6C43A54
SHA1:	05A79B7F0738CFD2F2FE3C6CEBDBD0A7702EB44C
SHA-256:	22EE05C11B27143CF6474926408154A2723EC321249FAF6684BACA657F64B723
SHA-512:	51646E8E2B5557949EB5A77B10092ABA6E8575C17E696477CDEFF012687E857E9D01B5BD33E511892EFCB8292DB3781323C1CD7440CB9E41C82F8B298A849A1E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/unpkg/data-capsule@1.0.83/dist/statics/frame-listener.bundle.min.js
Preview:	!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==typeof define&&define.amd?define("data-capsule",[],t):"object"==typeof exports?exports["data-capsule"]=t():e["data-capsule"]=t()}("undefined"!=typeof self?self:this,function(){return function(e){function t(n){if(r[n])return r[n].exports;var o=r[n]={i:n,l:!1,exports:{}};return e[n].call(o.exports,o,o.exports,t),o.l=!0,o.exports}var r={};return t.m=e,t.c=r,t.d=function(e,r,n){t.o(e,r)||Object.defineProperty(e,r,{configurable:!1,enumerable:!0,get:n})},t.n=function(e){var r=e&&e.__esModule?function(){return e.default}:function(){return e};return t.d(r,"a",r),r},t.o=function(e,t){return Objec t.prototype.hasOwnProperty.call(e,t)},t.p="",t.p="undefined"!=typeof window&&window.__STATICS_BASE_URL__||t.p,t(t.s=54)}({0:function(e,t,r){"use strict";function n(e,t){if(!(e instanceof t))throw new TypeError("Cannot call a class as a function")}var o=function(){function e(e,t){for(var r=0;r<t.length;r++){va

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\gsap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	57826
Entropy (8bit):	5.336045925794379
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\gsap.min[1].js	
SSDEEP:	768:N1JsoGPTyHRUxrSOdlWfT2OlUFi2rLei2YCv0BiDTTW9t9gE0aZC3n5N:NDFGlrSGlWTCPb9b+
MD5:	663FD753CAE2B462CF8ED119C3F991AB
SHA1:	06A63BC0EC823880B5420C23071E3C3C0582C11A
SHA-256:	732117AC92A33B760D9290A33F1541762EE9449DC417EA249B5A0DF50738AD16
SHA-512:	D11607AA8380466A71344C3E7ACC4D1D768FA17594DFAB300BC6B90609A77B164D98E8437B00AF2913568AD262C1FE34A3C254B20F37D54BBF71120DEEC09D2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/unpkg/@wix/santa-external-modules@1.644.0/tweenmax-plugins/3.1.1-transition-phase/gsap.min.js
Preview:	/*!. * GSAP 3.1.1. * https://greensock.com. * . * @license Copyright 2020, GreenSock. All rights reserved.. * Subject to the terms at https://greensock.com/standard-license or for Club GreenSock members, the agreement issued with that membership.. * @author: Jack Doyle, jack@greensock.com. */..!function(t,e){"object"==typeof exp orts&&"undefined"!=typeof module?e(exports):"function"==typeof define&&define.amd?define(["exports"],e):e((t=t||self).window=t.window||{})}(this,function(e){"use strict"; function _inheritsLoose(t,e){t.prototype=Object.create(e.prototype),(t.prototype.constructor=t).__proto__=e}function _assertThisInitialized(t){if(void 0===t)throw new Ref erenceError("this hasn't been initialised - super() hasn't been called");return t}function n(t){return"string"==typeof t}function o(t){return"function"==typeof t}function p(t){retu rn"number"==typeof t}function q(t){return void 0===t}function r(t){return"object"==typeof t}function s(t){return!1!==t}function t(){return"undefined"!

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\helvetica[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	29917
Entropy (8bit):	5.035402319919693
Encrypted:	false
SSDEEP:	192:ZVlDpZKJ56E/Zn5v5D2Z9Ye+RUVMn0DpUZM9MBkzmNNfNefNtL/+8/U7748NWDYD:i1diD8FGS/PaL5ENOOz9oy
MD5:	39099ECA9738473EAA97CA6D87F4A5BF
SHA1:	6BA90D5D62954E52271BB44A2F5EE008CA576FAE
SHA-256:	2A238BAB6155365B6F5257D64D17277B0E70E5A217B90D53F2A3FC96F6707A9E
SHA-512:	641C0EACB9829FC34D4CC678E33BA96B156E54EE67F5D90C0238B9B241E8AFC24F7C1A0817CFFB27F8E805F33BBD9BD15E2B5243925A6B803B2612840D22E63F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/v7/helvetica.css
Preview:	/* fonts helvetica */../*@import url("//fast.fonts.com/t/1.css?apiType=css&projectid=33bd0973-5b82-45be-bb77-837225874dfe");*/..html{. background-image:url("//fast.fonts.com/t/1.css?apiType=css&projectid=33bd0973-5b82-45be-bb77-837225874dfe");.}.../* Original old fonts */..@font-face {. font-family: "Helvetica Neue";. src: url("//static.parastorage.com/services/third-party/fonts/Helvetica/Fonts/b7693a83-b861-4aa6-85e0-9ecf676bc4d6.eot?#iefix") format("embedded-opentype"),. url("//static.parastorage.com/services/third-party/fonts/Helvetica/Fonts/bcf54343-d033-41ee-bbd7-2b77df3fe7ba.woff") format("woff"),. url("//static.parastorage.com/services/third-party/fonts/Helvetica/Fonts/b0ffdcf0-26da-47fd-8485-20e4a40d4b7d.ttf") format("truetype"),. url("//static.parastorage.com/services/third-party/fonts/Helvetica/Fonts/da09f1f1-062a-45af-86e1-2bbdb3dd94f9.svg#da09f1f1-062a-45af-86e1-2bbdb3dd94f9") format("svg");.}..@font-face {. font-family: "Helvetica Neue Thin";. font-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\identity[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	11633
Entropy (8bit):	5.7883624283841515
Encrypted:	false
SSDEEP:	192:sCQHyB0Qt5BeeOvnJdTQn8dMf2IUiVIgqgxdbYpH380QtKgSbq8kjMc9Ix0vvOuG:sCJBTMMf2IUiGUU8QgSbqRFy0vvpi
MD5:	A4B4E2FB56CBAC0AA769F30236149A3B
SHA1:	2B80252D14157774F2F06A65EE9B55B66CF4D8DB
SHA-256:	3BEA34F20C813024F046166FB0AD98A8EB93D5AB93052CEB993EEE238ECE5B66
SHA-512:	46D1C72B70B054EAC2B6C511F7C09ECC176566037322AC0FAEA7FFC10071503CD71903EB514D6C482A21185BB53571400359EC2B2080BB1DCA9AD6146566E79
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://connect.facebook.net/signals/plugins/identity.js?v=2.9.33
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\intersection-observer-polyfill.5f183a8d.chunk.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	8906
Entropy (8bit):	5.142345649054618

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\intersection-observer-polyfill.5f183a8d.chunk.min[1].js	
Encrypted:	false
SSDEEP:	192:Vg/PYNqqzDODGgXdDDo4SpQmNhhWa3ghHUtigFmgJWBC425NVGpJYh3gkC6YFZm+:VgH8t3ihXdDjsQmNhh3gpUJDJWBCjcaa
MD5:	E49C2097D1FA87F363C38775C6C4C0DD
SHA1:	0D637B238E866D1C866B4587DE0EA05EF4F5C2BC
SHA-256:	13590CA936462AB3DCE0C4BA5C2AC714F0F5BA0B5D3FB14FBFC5B8BD94F4394D
SHA-512:	D38C357EE66C3E14B3418F22E228188B68CFC97FEEA68FB9C731A6472C0F214E61C5170A53028A9F03A90B8A5636D25EDFA335C06D9F179FDE78910E2D21BC1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-thunderbolt/dist/intersection-observer-polyfill.5f183a8d.chunk.min.js
Preview:	(window.webpackJsonp__wix_thunderbolt_app=window.webpackJsonp__wix_thunderbolt_app||[]).push([[62],{781:function(t,e){!function(){"use strict";if("object"==typeof window)if("IntersectionObserver"in window&&"IntersectionObserverEntry"in window&&"intersectionRatio"in window.IntersectionObserverEntry.prototype)"isIntersecting"in window.IntersectionObserverEntry.prototype||Object.defineProperty(window.IntersectionObserverEntry.prototype,"isIntersecting",{get:function(){return this.intersectionRatio>0}});else{var t=window.document,e=[],n=null,o=null;r.prototype.THROTTLE_TIMEOUT=100,r.prototype.POLL_INTERVAL=null,r.prototype.USE_MUTATION_OBSERVER=!0,r._setupCrossOriginUpdater=function(){return n||(n=function(t,n){o=t&&n?a(t,n):{top:0,bottom:0,left:0,right:0,width:0,height:0},e.forEach((function(t){t._checkForIntersections()}))},n},r._resetCrossOriginUpdater=function(){n=null,o=null},r.prototype.observe=function(t){if(!this._observationTargets.some((function(e){return e.element==t}))){if(!t|

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\layout.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	145097
Entropy (8bit):	5.27080890708655
Encrypted:	false
SSDEEP:	1536:smMr3o1C+p78HehPcX4d4jMicDeEWuC5RARwWeLFXU1MRPw25:ZWo1CdHehPcIKMifEWuC5+VcDPw25
MD5:	0C18CD68DC0C70A886D910F73B16A78A
SHA1:	5254DF79E9B58E5203357A31F65D7D9653591AC4
SHA-256:	2663165F94D02964715CD215616749F2DF17BB640326EEDC85C6C02876D1349B
SHA-512:	73011B1A6DADA79963309CE9A600B293ADD7FEFECECD90D7C20E919A487E20D41A7E1537A86CC3340E5EBD37A7C3D1B6269C90EEA7670451E06313C885E0A37
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7107.0/node_modules/wix-santa/dist/packages-bin/layout/layout.min.js
Preview:	define("layout",["lodash","zepto","experiment","warmupUtils","warmupUtilsLib","image-client-api","santa-components-layout"],(function(e,t,i,n,r,o,a){return function(e){var t={};function i(n){if(t[n])return t[n].exports;var r=t[n]={i:n,l:!1,exports:{}};return e[n].call(r.exports,r,r.exports,i),r.l=!0,r.exports}return i.m=e,i.c=t,i.d=function(e,t,n){i.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:n})},i.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},i.t=function(e,t){if(1&t&&(e=i(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var n=Object.create(null);if(i.r(n),Object.defineProperty(n,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var r in e)i.d(n,r,function(t){return e[t]}.bind(null,r));return n},i.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};return i.d(t,"a",t),t},i.o=function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\main.v2.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	89496
Entropy (8bit):	5.360020370550665
Encrypted:	false
SSDEEP:	1536:wbhQM1RxVnSFfdfFMbAq1jwOU9dlYTAfZpSMTndG9xZfFNJNO7uEW2:I8XqpwOESMTndO9NzO7k2
MD5:	999A976CF2D3A69A8B8FDA9F07F33699
SHA1:	F91E5D08D071C1281D37A89605CADB80735DF3D5
SHA-256:	08EC4DCE6974BFC4AAA527179BDD8D66D137748CD47D159849CEC2125A6CC89D
SHA-512:	AA62EFC16DCACBA74E7F2D1DA1FB3FA14EEAE5CDA9E209935D760D82E6A11D3652C9FD083E82BC29C9B4558CB33F5AF9A85D5A00A30C02ECDE817288CED87993
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/chrome/static/js/main.v2.min.js
Preview:	(function(){var f,aa="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){a!=Array.prototype&&a!=Object.prototype&&(a[b]=c.value)},k="undefined"!=typeof window&&window===this?this:"undefined"!=typeof global&&null!=global?global:this;function ba(){ba=function(){};k.Symbol||(k.Symbol=ca)}var ca=function(){var a=0;return function(b){return"jscomp_symbol_"+(b||"")+a++}}();.function l(){ba();var a=k.Symbol.iterator;a||(a=k.Symbol.iterator=k.Symbol("iterator"));"function"!=typeof Array.prototype[a]&&aa(Array.prototype,a,{configurable:!0,writable:!0,value:function(){return da(this)}});l=function(){}}function da(a){var b=0;return ea(function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}})}function ea(a){l();a={next:a};a[k.Symbol.iterator]=function(){return this};return a}function m(a){l();var b=a[Symbol.iterator];return b?b.call(a):da(a)}.var fa="function"==typeof Object.create?Object.create:function(a){function b(){}b.prototype=a;return new b},ha;if("functio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\main.v3.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\main.v3.min[1].css	
Size (bytes):	203048
Entropy (8bit):	5.066880694984304
Encrypted:	false
SSDEEP:	1536:4pD7iyiUL+5eSLMd6Ll0sRslr6YY1llN2hDts52j9sJwW7jWlelqnVDXhUqjqQQg:UrkQeiB
MD5:	91344A7129A5AE2742F61BEC35FB482D
SHA1:	4C8EEBCD76434ACA23B55CE81816E45D10B3937C
SHA-256:	CE71AFE1D89A0C658F0EEB7F15A5232C6EF30C7D287E2683498656A0B84B50B7
SHA-512:	F408D40A08E986586935B2B760363A52684C2C818829CD6FEAFD07276046EF8E8A90001DFC1F915684CDC61653996E56DD11C81D9833DA0D3DC009D57270933C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/chrome/static/css/main.v3.min.css
Preview:	.chr-accordion__image img,.chr-card-and-image__image,.chr-fifty-fifty__half-1 img,.chr-fifty-fifty__half-2 img,.chr-google-translate__device-image,.chr-scrollable__image{ height:auto;width:100%}.chr-modal-dialog.eula ul,.chr-footer-social__list,.chr-footer-links__list,.chr-footer-glinks__list,.chr-footer-help-language,.chr-header-v3__drawer-nav-list,.chr-header-v3__drawer-subnav-list{list-style:none;padding:0}.chr-modal-dialog__buttons .throbber,.chr-modal-dialog.eula .eula-content,.chr-modal-dialog.eula . other-platform,.chr-modal-dialog.eula .os,.chr-modal-dialog.eula .platform,.chr-modal-dialog.eula .chrome-os,.chr-modal-dialog.eula .other-platform.mac .other-mac,.chr-mo dal-dialog.eula .other-platform.win .other-win,.chr-modal-dialog.eula .other-platform.win64 .other-win64,.chr-modal-dialog.eula .other-platform.linux .other-linux,.chr-modal-dialog.eula .other-platform.betachannel.win49 .chr-modal-dialog__button,.chr-modal-dialog.eula .other-platform.betachannel.mac49 .chr-modal-dialog

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\mobileLayoutUtils.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	291205
Entropy (8bit):	5.502659448401162
Encrypted:	false
SSDEEP:	3072:ClSyhMUsKZFcQDvbX6r5xmMadzxNv12M3owkvSa5boPGiZIU2yCS87:khzssvbgr5M3owkvR5boPGAN2yCSK
MD5:	F2ABF3FFAED32767721FE0D1A7057402
SHA1:	CBE465E33E10F40B724E6A777D2B12BC2C7FD654
SHA-256:	3A17C94CEECF26457342B187D9DD86D1EC7F1A54786E22D7B4C206FFEE871003
SHA-512:	B0F0823915F5ED60E8606C5044AF60539028A9C17E671B1422E291A0A8844B976BA54ED13A3FBB3FBF2300F6E2B61FE76D60B45F0A034F423D8EB8922CFB3707
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/unpkg/@wix/santa-mobile-core@1.1227.0/dist/mobileLayoutUtils.min.js
Preview:	define(["lodash"],(function(e){return function(e){var t={};function n(r){if(t[r])return t[r].exports;var i=t[r]={i:r,l:!1,exports:{}};return e[r].call(i.exports,i,i.exports,n),i.l=!0,i.expor ts}return n.m=e,n.c=t,n.d=function(e,t,r){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:r})},n.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStrin gTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},n.t=function(e,t){if(1&t&&(e=n(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var r=Object.create(null);if(n.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:e}),2&t&&"string"!=ty peof e)for(var i in e)n.d(r,i,function(t){return e[t]}.bind(null,i));return r},n.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};return n.d(t, "a",t),t},n.o=function(e,t){return Object.prototype.hasOwnProperty.call(e,t)},n.p="",n(n.s=128)}([function(t,n){t.exports=e},function(e,t,n)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\modernizr[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	18121
Entropy (8bit):	5.487052413899393
Encrypted:	false
SSDEEP:	384:sEVrsUrsbn8b9EID9HW590TpJGd+xesmAnxpakrwHVXHh1pz:RV/Q8b9wD5jebALak0HVXHI
MD5:	22B1D136ACE6916B80EE05FD4889066E
SHA1:	03903EC6E52233623AFE851E351E160B72ED2828
SHA-256:	8C2D2E5D88589A1283EC0CDF49BEDC2DD3A8F40FE77C39C3E00ED8CEF1968FF3
SHA-512:	9BBBCBA7803D76C8F8CBD9974733211D8ED703E640B2FC673715DCC091413A2FE3E385CE1886DFCD7C5153EBDC154B1A5D83D0F004369C355EBCEDD841E2E F7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/external_hosted/modernizr/modernizr.js
Preview:	/**. * @license. * MIT License. * Copyright (c) 2009.2011. * Permission is hereby granted, free of charge, to any person obtaining a copy. * of this software and associated documentation files (the "Software"), to deal. * in the Software without restriction, including without limitation the rights. * to use, copy, modify, merge, publish, distribute, sublicense, and/or sell. * copies of the Software, and to permit persons to whom the Software is. * furnished to do so, subject to the following conditions:. * The above copyright notice and this permission notice shall be included in. * all copies or substantial portions of the Software.. * THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR. * IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,. * FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE. * AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER. * LIABILITY, WHETHER IN AN ACTION OF CONTRACT, T

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\pfavico[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 16x16, 32 bits/pixel

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\pfavico[1].ico	
Category:	downloaded
Size (bytes):	1150
Entropy (8bit):	1.2100731437092027
Encrypted:	false
SSDEEP:	3:3NhDllvlNl/khXhCC1111111111111111111111111111111111111111111111111H:7Jq55555555555555R
MD5:	B53CE85A6CCE2AE00037A6CA13C90866
SHA1:	292D9AEB457AB7FEDBAD452854332AEFF267A78E
SHA-256:	33C1436F8C40CA2582D091C449FCCC34ED9BF73F02526C5FDEF44F4F06C6321B
SHA-512:	9271B4BD6B07C15662E9265359AD80CBEDF971C127F8C17EF289AE7A552C3BDA93A8416881493196E956FDC5B2A4DF03CBDA838F4203C7F7B12DCDBFE27B31B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/client/pfavico.ico
Preview:	..... .h.....(..... ....@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\polyfill.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	downloaded
Size (bytes):	22629
Entropy (8bit):	5.262393792354482
Encrypted:	false
SSDEEP:	384:x/2ggnPTclMcL65uNlPvgtDj6WnW+Y6/cTxJtlwMHnWazh5vd2uZvOC1:x/hL60NlPkW+F/cTxfXHWazhDXZvOC1
MD5:	42E531D2C282ACC7A2EC77E00CEC1D10
SHA1:	87B8F7A381B07C2771F3CF4B651F304470B5F4D8
SHA-256:	38F84B4BF4D91C67D64FFBEE5CC4B6A39BAA9653E5369532D902F9F06F650A57
SHA-512:	BAC8A94B872E3E196CA45906E2780ED1E546B42DDC2318A9FF4F1B4D14EF7FC49783160C3295AD39B54C1B051DE61F7BCBF2935C5FD368E24B2E5E39FDA00F6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://polyfill.io/v3/polyfill.min.js?features=fetch
Preview:	/* Disable minification (remove `.min` from URL path) for more info */..(function(self, undefined) {function Call(t,l){var n=arguments.length>2?arguments[2]:[];if(!1===IsCallable(t))throw new TypeError(Object.prototype.toString.call(t)+"is not a function.");return t.apply(l,n)}function CreateMethodProperty(e,r,t){var a={value:t,writable:!0,enumerable:!1,configurable:!0};Object.defineProperty(e,r,a)}function Get(n,t){return n[t]}function HasOwnProperty(r,t){return Object.prototype.hasOwnProperty.call(r,t)}function IsCallable(n){return"function"==typeof n}function SameValueNonNumber(e,n){return e===n}function ToObject(e){if(null===e||e===undefined)throw TypeError();return Object(e)}function GetV(t,e){return ToObject(t)[e]}function GetMethod(e,n){var r=GetV(e,n);if(null===r||r===undefined)return undefined;if(!1===IsCallable(r))throw new TypeError("Method not callable: "+n);return r}function Type(e){switch(typeof e){case"undefined":return"undefined";case"boolean":return"boolean";case"numbe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\skin-utils[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	284572
Entropy (8bit):	5.517855793283513
Encrypted:	false
SSDEEP:	3072:Mdc7/01xDZFcQ41NRr5M8GMpdzxNv5u2po8kvSA8FPrPZvU2yCSrc://+xW1LC8c2po8kv18FPrhs2yCSo
MD5:	C4F04FB651FD898F85DE8643B1ABDEAC
SHA1:	35C0115DF95291AD67E1DEE57A2A92739523EF4F
SHA-256:	A3876C20B36B29CAE94FF0BE2354008917235E1D97D498156434E6B6F6F48812
SHA-512:	3DFE2D888BBDA47F9F88C051BC9943014EB678947E47CFDCBB36634BCA980CF215C733E9E6708C60B60A87C6285AE5F24C74820E6B4910F2F97D6850B0D05A8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/unpkg/@wix/santa-skin-utils@1.1685.0/dist/skin-utils.js
Preview:	!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t(require("lodash"),require("color")):"function"==typeof define&&define.amd?define(["lodash","color"],t):"object"==typeof exports?exports["skin-utils"]=t(require("lodash"),require("color")):e["skin-utils"]=t(e.lodash,e.color)}(this,(function(e,t){return function(e){var t={};function n(r){if(t[r])return t[r].exports;var i=t[r]={i:r,l:!1,exports:{}};return e[r].call(i.exports,i,i.exports,n),i.l=!0,i.exports}return n.m=e,n.c=t,n.d=function(e,t,r){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:r})},n.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},n.t=function(e,t){if(1&t&&(e=n(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var r=Object.create(null);if(n.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var i in e)n.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\skins.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\skins.min[1].js	
Category:	downloaded
Size (bytes):	393702
Entropy (8bit):	5.370441249701614
Encrypted:	false
SSDEEP:	12288:j4WQCBH8AAULsDm10EtpJe5jTK9EDNHWKOzVpSbKu1wqryUJ+0CyBe9zI6Y5b+AA:j4+yBe9zIMA3Q
MD5:	40587291FA2E7431517216BC208600B4
SHA1:	131A4AEB87B630D0E96D7A5E17C27E12274B8F98
SHA-256:	76FD2F7C71D5CF7E208603BE997E23A6573820A9353A0833350DF13648FDED4F
SHA-512:	8636BBC2FAD01E39BAF47E4A2FD7E95BA7F82EA6C16F4F13D49D40598D20FABFA461C8986F5EE115A98182C96F4B1A328929B2FAD8C6D72854AA49B3DF2350E3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7107.0/node_modules/wix-santa/dist/packages-bin/skins/skins.min.js
Preview:	define("skins",["lodash","santa-components","santa-core-utils","skinUtils"],(function(t,e,o,r){return function(t){var e={};function o(r){if(e[r])return e[r].exports;var a=e[r]={i:r,l:!1,exports:{}};return t[r].call(a.exports,a,a.exports,o),a.l=!0,a.exports}return o.m=t,o.c=e,o.d=function(t,e,r){o.o(t,e)||Object.defineProperty(t,e,{enumerable:!0,get:r})},o.r=function(t){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(t,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(t,"__esModule",{value:!0})},o.t=function(t,e){if(1&e&&(t=o(t)),8&e)return t;if(4&e&&"object"==typeof t&&t&&t.__esModule)return t;var r=Object.create(null);if(o.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:t}),2&e&&"string"!=typeof t)for(var a in t)o.d(r,a,function(e){return t[e]}.bind(null,a));return r},o.n=function(t){var e=t&&t.__esModule?function(){return t.default}:function(){return t};return o.d(e,"a",e),e},o.o=function(t,e){return Object.prototype.hasOwnProperty.call(t,e)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\src=2542116;type=2542116;cat=chrom0;ord=8924832293155;gtm=2wg3o0;~oref=https___www.google[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	42
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEy:1QEoy
MD5:	D89746888DA2D9510B64A9F031EAECD5
SHA1:	D5FCEB6532643D0D84FFE09C40C481ECDF59E15A
SHA-256:	EF1955AE757C8B966C83248350331BD3A30F658CED11F387F8EBF05AB3368629
SHA-512:	D5DA26B5D496EDB0221DF1A4057A8B0285D15592A8F8DC7016A294DF37ED335F3FDE6A2252962E0DF38B62847F8B771463A0124EF3F84299F262ED9D9D3CEE4
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\tc_imp[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	3.142069457963608
Encrypted:	false
SSDEEP:	3:CU1urkltxlHh/:gg/
MD5:	DB04C7B378CB2DB912C3BA8A5A774EE3
SHA1:	DEE34BD86C3484D31002182AA2B7CAA4699126B8
SHA-256:	98B3D9D20E032F90ACA49E9B116225D539FF6FBDB7E42C3C363F63896AC03D2A
SHA-512:	826225FC21717D8861A05B9D2F959539AAD2D2B131B2AFED75D88FBCA535E1B0D5A0DA8AC69713A0876A0D467848A37A0A7F926AEAFAD8CF28201382D16466AB
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\thirdPartyAnalytics.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	C source, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	9873
Entropy (8bit):	5.205156652219834
Encrypted:	false
SSDEEP:	192:jcvj1yLBPBT2nQc94VE9Mz9hrbZ4iDwwpzH1AKyfCpsJ+W4:g1ymnXWV6OdPDllH1ECmJ+W4
MD5:	907C5062AE2E2C1732B12348708E30A0
SHA1:	832E34675A984610BF11BE4810D0ECEEF30FE240

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\thirdPartyAnalytics.min[1].js	
SHA-256:	32567FEC7314C675F45B50A968C9B6AB076AB459C00362CFE7EC8CFD08A18D1A
SHA-512:	68A85A9558E42AAF2BF2475FC2D8A435B98EA5AB50A6B465A2BE895180EA0AF52FB740D68EE452B2AE39B53C48018EB38A2EEF654F7AD2D062A4ED14BA05792F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7107.0/node_modules/wix-santa/dist/packages-bin/thirdPartyAnalytics/thirdPartyAnalytics.min.js
Preview:	define("thirdPartyAnalytics",["lodash","warmupUtils","santa-core-utils"],(function(n,e,t){return function(n){var e={};function t(i){if(e[i])return e[i].exports;var r=e[i]={i:i,l:!1,exports:{}};return n[i].call(r.exports,r,r.exports,t),r.l=!0,r.exports}return t.m=n,t.c=e,t.d=function(n,e,i){t.o(n,e)||Object.defineProperty(n,e,{enumerable:!0,get:i})},t.r=function(n){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(n,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(n,"__esModule",{value:!0})},t.t=function(n,e){if(1&e&&(n=t(n)),8&e)return n;if(4&e&&"object"==typeof n&&n&&n.__esModule)return n;var i=Object.create(null);if(t.r(i),Object.defineProperty(i,"default",{enumerable:!0,value:n}),2&e&&"string"!=typeof n)for(var r in n)t.d(i,r,function(e){return n[e]}.bind(null,r));return i},t.n=function(n){var e=n&&n.__esModule?function(){return n.default}:function(){return n};return t.d(e,"a",e),e},t.o=function(n,e){return Object.prototype.hasOwnProperty.call(n,e)},t.p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\tpaComponents.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	91651
Entropy (8bit):	5.348329174205209
Encrypted:	false
SSDEEP:	1536:FM1ivfr+qBZTzPlJ2FipSA2FGsi81BEMzIJU:Lr+qBZTzNJ2Fip3ai81BEMzIJU
MD5:	911DB28187DDD73B3F184BF58D58489B
SHA1:	4E64B1645E34AD48125C611CEF8E895AD6765A54
SHA-256:	11F64D3DD79AA58863B8FA0506F5D001003763B342A6595CB58ECD53F9CA26D3
SHA-512:	22EA82ADBE08E816A701C90F48FCF2C2585494DFF7559032D4AD96B0B83953C6E5D28BD66B25F8646155766779837F73005925E4FD9E34AFC1572230EC9C5BD3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7107.0/node_modules/wix-santa/dist/packages-bin/tpaComponents/tpaComponents.min.js
Preview:	define("tpaComponents",["lodash","coreUtils","santa-components","componentsCore","prop-types","skins","reactDOM","zepto","experiment","warmupUtils","santa-core-utils","create-react-class","react","layout"],(function(e,t,i,n,s,r,o,a,p,c,d,l,u,h){return function(e){var t={};function i(n){if(t[n])return t[n].exports;var s=t[n]={i:n,l:!1,exports:{}};return e[n].call(s.exports,s,s.exports,i),s.l=!0,s.exports}return i.m=e,i.c=t,i.d=function(e,t,n){i.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:n})},i.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},i.t=function(e,t){if(1&t&&(e=i(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var n=Object.create(null);if(i.r(n),Object.defineProperty(n,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var s in e)i.d(n,s,function(t){return e[t]}.bind(null,s));return n},i.n=function(e){var t=e&&e.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ugc-viewer[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	129
Entropy (8bit):	3.0950611313667666
Encrypted:	false
SSDEEP:	3:CUMllRPQEsJ9psOjBMllRPQEsJ9psOjBMllRPQEsJ9pse:Gl3QEsJLsMal3QEsJLsMal3QEsJLse
MD5:	D2566C366F730CCD475BD1BF9C09CB6C
SHA1:	EA3CBBAD88A086493CD4FD035513BEC67B27BF52
SHA-256:	A7C2383A000E585F7FFF39FD181F1F236DDAD954BC1722753BB1ACFAA0AC8B51
SHA-512:	1A436C0F5D7A23051DD74B887BCA53E87C08A69E371B4530D184E8CD5BCB6FB0070DF988380B9826A32A17DEFCAF81CA80CBE2CAA841FB5382EB1DD4AE3519D
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....L..;GIF89a.....!.....,.....L..;GIF89a.....!.....,.....L..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\wix-code-sdk-providers.3a33b93f.chunk.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	21967
Entropy (8bit):	5.195471144417698
Encrypted:	false
SSDEEP:	384:bRn9hWQn0pfB9UYAP0LmGK8XObt0sxhc8Ln7N3bC3GN/E7Oqc0H4:bV9hnsgPC3Q/0H4
MD5:	B392F208AE22E5B8A9ADE9A83954D51A
SHA1:	F54B32ABC34DD3F4F6839DE389D74E09CE1AA9BE
SHA-256:	D4D99A7C3214ADF1C2440ED27034D66AD748FB1FCF7B65E7B606EB7B8F8B7906
SHA-512:	E2DE00A789C486747935B8B7D41D2FBF2D5711A7160C1E58C22C891575CBD9428E5A348650AC745AB668F4F92F49D68D9EB6853020DB3C51AA59878917BC4142
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\wix-code-sdk-providers.3a33b93f.chunk.min[1].js	
IE Cache URL:	http://https://static.parastorage.com/services/wix-thunderbolt/dist/wix-code-sdk-providers.3a33b93f.chunk.min.js
Preview:	(window.webpackJsonp__wix_thunderbolt_app=window.webpackJsonp__wix_thunderbolt_app||[]).push([[3],{281:function(t,e,n){"use strict";n.r(e),n.d(e,"site",(function(){return i}));var r=n(117),o=n(247);n.d(e,"name",(function(){return o.a})),n.d(e,"namespace",(function(){return o.b}));var i=function(t){t(r.q).to(n(572).dashboardWixCodeSdkHandlers)}},309:function(t,e,n){"use strict";n.r(e),n.d(e,"site",(function(){return d})),n.d(e,"name",(function(){return a.a})),n.d(e,"namespace",(function(){return a.b}));var r=n(117),o=n(27),i=n(366),u=n(367),a=n(218),c=Object(o.h)([i.a,Object(o.f)(u.e,a.a),r.p],(function(t,e,n){var r=e.pageIdToTitle,o=n.mode;return{platformEnvData:{site:{experiments:t,isResponsive:n.site.isResponsive,pageIdToTitle:r,mode:o}}}})),s=Object(o.h)([Object(o.g)(u.a)],(function(t){return{getSdkHandlers:function(){return{getSitemapFetchParams:function(e){return t?t.getSitemapFetchParams(e):null}}}}})),d=function(t){t(r.g).to(c),t(r.q).to(s)}},310:function(t,e,n){"use strict";n.r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\wix-dom-sanitizer[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	19220
Entropy (8bit):	5.284078809599163
Encrypted:	false
SSDEEP:	384:3YyrTijbyGi/LA7A0MpCdzxv8ZlMiIV/iMewjtYC23MiVjfhuYrY9:vTxLsd9v8bMiS/iDGtYC23ZbuYr2
MD5:	BF53692C2D49A9E59E611AF682416BB4
SHA1:	87ED7DA4FD43B66A124D4180CE69596C88672F6D
SHA-256:	76F4A71B7ED39504017336D133F172CECEF1B2505E2557746E44F4647097BE5E
SHA-512:	B7BCA4D406D02950A849709DA913B2B4A0DD4A2F3E9B0CD5A4A9E93301F59F8F5F5C168D3EA80FC4A3BE9541848F806F415157FF07CB604A28D315A3E12A1DD5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/unpkg/@wix/wix-dom-sanitizer@1.783.0/dist/wix-dom-sanitizer.js
Preview:	!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==typeof define&&define.amd?define([],t):"object"==typeof exports?exports["wix-dom-sanitizer"]=t():e["wix-dom-sanitizer"]=t()}(this,(function(){return function(e){var t={};function r(n){if(t[n])return t[n].exports;var o=t[n]={i:n,l:!1,exports:{}};return e[n].call(o.exports,o,o.exports,r),o.l=!0,o.exports}return r.m=e,r.c=t,r.d=function(e,t,n){r.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:n})},r.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},r.t=function(e,t){if(1&t&&(e=r(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var n=Object.create(null);if(r.r(n),Object.defineProperty(n,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var o in e)r.d(n,o,function(t){return e[t]}.bind(null,o));return n},r.n=function(e){var t=e&&e.__esMod

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\wixFreemiumBanner.min[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):	91411
Entropy (8bit):	5.445500119924285
Encrypted:	false
SSDEEP:	768:M8vtZ/lLqS9E399jKhHp9l0QF80X1P9W8wlX1k4X17Tq/X1sJ:M8vtZ/lLqSE3bjKhHXITF8aWnPA++
MD5:	EDFA821708DFE708B6CE87916D065BF7
SHA1:	081DB9DCC04A981F57FB17CC7F63AECFB7F25F82
SHA-256:	7CF1B47A2B5EF91B4CA85B59488641630662 0F2A19DD0EE217DFCB0A874015BB
SHA-512:	E38B3FBAD963666B991BCB1FBF37F0EC18A481DA57526CF14A869A4F3DA7D51B627FC456F9EDB54841281B0042A0921A8B45CED98848A705B2845DA23270A6CD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7107.0/node_modules/wix-santa/dist/packages-bin/wixFreemiumBanner/wixFreemiumBanner.min.js
Preview:	define("wixFreemiumBanner",["lodash","coreUtils","santa-components","componentsCore","prop-types","react"],(function(e,t,o,r,a,n){return function(e){var t={};function o(r){if(t[r])return t[r].exports;var a=t[r]={i:r,l:!1,exports:{}};return e[r].call(a.exports,a,a.exports,o),a.l=!0,a.exports}return o.m=e,o.c=t,o.d=function(e,t,r){o.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:r})},o.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},o.t=function(e,t){if(1&t&&(e=o(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var r=Object.create(null);if(o.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var a in e)o.d(r,a,function(t){return e[t]}.bind(null,a));return r},o.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};return o.d(t,"a",t),t},o.o=function(e,t){return Object

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\wixMadefor[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	4339
Entropy (8bit):	4.828748558866936
Encrypted:	false
SSDEEP:	96:/QPOPLLQPbPU9QPfPgdQH4rDWQ1SpQZ+ADWQ4xlQKvjDWQTcTQoh/DWQpOO:/D7DQDADZ
MD5:	D76884A66F7EE1E86BE1841EE2B954F4
SHA1:	7BA60D9EAECD1E5CC809368B5912BBA8F370D3E2
SHA-256:	DB704B465A4ED21E3950FE3FFD95DBAA22F130D73AE7064D7E1EB643BF68A4C1
SHA-512:	89221219FA4868B78DB5480587FFA7C5065E179AD2D143F68F36EA08024B9638BBB86397D3F8E4AE0F5634684E423AEA516A41CE474FD30B770D7E5D71CC94E8
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\wixMadefor[1].css	
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/v11/wixMadefor.css
Preview:	/* new wixMadefor font*/.../* Madefor Display */.@font-face{. font-family:"Madefor-Display";. src: url("//static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/WixMadefor/v2/WixMadeforDisplay_W_Rg.woff2") format("woff2"),. url("//static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/WixMadefor/v2/WixMadeforDisplay_W_Rg.woff") format("woff");.}..@font-face{. font-family:"Madefor-Display-Bold";. src: url("//static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/WixMadefor/v2/WixMadeforDisplay_W_Bd.woff2") format("woff2"),. url("//static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/WixMadefor/v2/WixMadeforDisplay_W_Bd.woff") format("woff");.}..@font-face{. font-family:"Madefor-Display-ExtraBold";. src: url("//static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/WixMadefor/v2/WixMadeforDisplay_W_XBd.wo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\xss.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):	27954
Entropy (8bit):	5.2180021601732784
Encrypted:	false
SSDEEP:	384:DDJ6NokIwHWvsSHzxc5R61A0+3PJ8K73imq2fw/94HFzKvkGuIcDYP8ALJiy+03V:DEfIwZ9ztyyw/etKvvqI7lmpo
MD5:	03A1F336E798CB76FD006A89BB5C86CD
SHA1:	22DD332C6E792D26784CA427F4E95BB45AB5EDA1
SHA-256:	7021FC60565C79ECBE0D8113A83DBF68E9E719EFEAC07B360D9CDA18863E5A55
SHA-512:	9CC7CDB71F2426EA9878703AD9D1FD992C4605B0F96D7360575965995A73C09875FC755220DEA60C74B6FB61B55666B7D90A0DFD861F0A9DA4849C1F53893478
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/unpkg/xss@0.2.18/dist/xss.min.js
Preview:	(function e(t,n,r){function s(o,u){if(!n[o]){if(!t[o]){var a=typeof require=="function"&&require;if(!u&&a)return a(o,!0);if(i)return i(o,!0);var f=new Error("Cannot find module '"+o+"'");throw f.code="MODULE_NOT_FOUND",f}var l=n[o]={exports:{}};t[o][0].call(l.exports,function(e){var n=t[o][1][e];return s(n?n:e)},l,l.exports,e,t,n,r)}return n[o].exports}var i=typeof require=="function"&&require;for(var o=0;o<r.length;o++)s(r[o]);return s})({1:[function(require,module,exports){var FilterCSS=require("cssfilter").FilterCSS;var getDefaultCSSWhiteList=require("cssfilter").getDefaultWhiteList;var _=require("./util");function getDefaultWhiteList(){return{a:["target","href","title"],abbr:["title"],address:[],area:["shape","coords","href","alt"],article:[],aside:[],audio:["autoplay","controls","loop","preload","src"],b:[],bdi:["dir"],bdo:["dir"],big:[],blockquote:["cite"],br:[],caption:[],center:[],cite:[],code:[],col:["align","valign","span","width"],colgroup:["align","valign","span","width"],d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\zepto.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	26386
Entropy (8bit):	5.176792166274628
Encrypted:	false
SSDEEP:	384:He+VbNwN6J4wfYRWzmEABSF0ztlbtj4jXh2FYx:HbNwvRWh2xlBjCx2e
MD5:	50A4556B0089CFA1CB61E88EA23BBCCE
SHA1:	6865443A258954FA19B8AA682E1F4C77D42493D1
SHA-256:	BEB9F5E32ED61FBCE010497242A9B6B8219242B5FFC636038E7891510C773725
SHA-512:	06BBD560D84A87AC924F6E04E4363F2E8A4B3B977EF0A626217CABA41209D8F2BE0B2C89C3F70B486FC17C9A2658B0B521B94DAE688958696B1AE78A2DDFC49 3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/unpkg/zepto@1.2.0/dist/zepto.min.js
Preview:	/* Zepto v1.2.0 - zepto event ajax form ie - zeptojs.com/license */.!function(t,e){"function"==typeof define&&define.amd?define(function(){return e(t)}):e(t)}(this,function(t){var e=function(){function $(t){return null==t?String(t):S[C.call(t)]||"object"}function F(t){return"function"==$(t)}function k(t){return null!=t&&t==t.window}function M(t){return null!=t&&t.nodeType==t.DOCUMENT_NODE}function R(t){return"object"==$(t)}function Z(t){return R(t)&&!k(t)&&Object.getPrototypeOf(t)==Object.prototype}function z(t){var e=!!t&&"length"in t&&t.length,n=r.type(t);return"function"!=n&&!k(t)&&("array"==n||0===e||"number"==typeof e&&e>0&&e-1 in t)}function q(t){return a.call(t,function(t){return null!=t})}function H(t){return t.length>0?r.fn.concat.apply([],t):t}function I(t){return t.replace(/::/g,"/").replace(/([A-Z]+)([A-Z][a-z])/g,"$1_$2").replace(/([a-z\d])([A-Z])/g,"$1_$2").replace(/_/g,"-").toLowerCase()}function V(t){return t in l?l[t]:l[t]=new RegExp("(^|\\s)"+t+"(\\s|$)")}function _(t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\050b1948-f226-4d20-a65a-15d8ed031222[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22912, version 1.0
Category:	downloaded
Size (bytes):	22912
Entropy (8bit):	7.981203288200719
Encrypted:	false
SSDEEP:	384:9llcXrCfMOBb/3v42KcHscKd5Hz5TUEbtYXQjVa7ZZx+YdkaUpSV/QRBsbQJ:9llc7AbfVHSFUXuyZZElaUpG/q
MD5:	6AA6E18FE4F8FCAF8147E6196A2ED4F2
SHA1:	94850CC02FDD10CE3626B4717A20BA2A84E36720
SHA-256:	4A636E6C5A476278C861C00829AFB12B122F074B1E34693C8C6788D857D66D2F
SHA-512:	BF9211CB4EB1D8EE2C5DA099044D2911A647958D5DC4215B651C84D721919B5B94277677046511453455F5231FE5D918F9FEA1DD955CBCE9F53024FCD3B9D535

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\050b1948-f226-4d20-a65a-15d8ed031222[1].woff	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/Helvetica/v2/050b1948-f226-4d20-a65a-15d8ed031222.woff
Preview:	wOFF.....Y.....S.....GPOS...l.....^.O..OS/2.....T...`e...VDMX...p...\....p.x|cmap.....g.....cvt ...4...X.....:..fpgm.....,...gasp.....glyf... ..:C..]. .@head..Hd...6...6..}.hhea..H.... ...$...,hmtx..H.....mloca..J....\.....*.`maxp..M.... ... ...Tname..M0.....post..S..... ...2prep..S.....x..S.k.A..f.d7?l..".. ".....6..%V[.bL. [D..*(9.GQP...{... .B..4....k....H...o.4l.*...f..{ow.o.....a....5.8.....J.....6_*.X.~...J..9@k..pV.lE...N4.H<Z{R...#b...]...r.:.....C(")>?.7...ot.U..>.....X...P..<D.~.....f..m4.../..0.*WU ...rzG..z....fu.....&.m..Z...o...i..r....k.....2q.v=F..d.Lf=H.(a.7Av...]....%..e..<.@..@.X$....[D....V...<..w...N=<| .>..#7..~.>.....|.....^.A...u....RS..Ym.v.vp.*.....X.k.....0.0..;l....*.s.. ...+..BF.W...n...5N.....IrhTH..2.5....:!.>.S...r.Me...'...O.O.&..*..D.r...*.B...}..S...}s.cnc.....#.}.-.6$/..p....~..]_?..{O.+}T'~rl..."...v+j....Ej.(.1./.4.D....3-...\"...t...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\1001175813[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	42
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEy:1QEoy
MD5:	D89746888DA2D9510B64A9F031EAECD5
SHA1:	D5FCEB6532643D0D84FFE09C40C481ECDF59E15A
SHA-256:	EF1955AE757C8B966C83248350331BD3A30F658CED11F387F8EBF05AB3368629
SHA-512:	D5DA26B5D496EDB0221DF1A4057A8B0285D15592A8F8DC7016A294DF37ED335F3FDE6A2252962E0DF38B62847F8B771463A0124EF3F84299F262ED9D9D3CEE4
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\1006927621[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	42
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEy:1QEoy
MD5:	D89746888DA2D9510B64A9F031EAECD5
SHA1:	D5FCEB6532643D0D84FFE09C40C481ECDF59E15A
SHA-256:	EF1955AE757C8B966C83248350331BD3A30F658CED11F387F8EBF05AB3368629
SHA-512:	D5DA26B5D496EDB0221DF1A4057A8B0285D15592A8F8DC7016A294DF37ED335F3FDE6A2252962E0DF38B62847F8B771463A0124EF3F84299F262ED9D9D3CEE4
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\3d84bae5ad4d4d8a96de15e9f4b79a08[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1385
Entropy (8bit):	4.129066840649089
Encrypted:	false
SSDEEP:	24:tCzcRj04WwUzoJpfM6Ve6KmZYRVILgQqTmXMIIXuK7KLAWF3Ds5YuFQaAE:wijf/M0pf9V5fYOgQqTmXotOLBghFQab
MD5:	4D0FFCA03B31AE92FB3459ACF490DB9A
SHA1:	4D94E2F3BEF0A284997C1D18EAF83514C40F1F72
SHA-256:	C2DC7E0BECDBAB5E9A5C79E527BB95FEC10667645CC6F2F8177F5E0F4F585EA1
SHA-512:	D69CFBFF8A535504DB28F6850A7CD6978364896647BA16821606042BD839AC94D783AC693A14258EED993EC63C314EFDE399BBF1DA11E2C51E001FB311DCE34
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.wixstatic.com/shapes/3d84bae5ad4d4d8a96de15e9f4b79a08.svg
Preview:	<svg data-bbox="0 0 50 50" data-type="shape" xmlns="http://www.w3.org/2000/svg" width="50" height="50" viewBox="0 0 50 50">. <g>. <path d="M25 48.077c-5.924 0-11.31-2.252-15.396-5.921 2.254-5.362 7.492-8.267 15.373-8.267 7.889 0 13.139 3.044 15.408 8.418-4.084 3.659-9.471 5.77-15.385 5.77m.278-35.3c4.927 0 8.611 3.812 8.611 8.778 0 5.21-3.875 9.456-8.611 9.456s-8.611-4.246-8.611-9.456c0-5.066 3.684-8.878 8.611-8.878M25 0C11.193 0 0 11.193 0 25c0 .915.056 1.816.1522.705.032.295.091.581.133.873.085.589.173 1.176.298 1.751.073.338.169.665.256.997.135.515.273 1.027.439 1.529.114.342.243.675.37 1.01.18.476.369.945.5771.406.149.331.308.657.472.98.225.446.463.883.714 1.313.182.312.365.619.56.922.272.423.56.832.856 1.237.207.284.41.568.629.841.325.408.671.796 1.02 1 .182.22.244.432.494.662.728.405.415.833.801 1.265 1.186.173.154.329.325.507.475l.004-.011A24.886 24.886 0 0 0 25 50a24.881 24.881 0 0 0 16.069-5.861.126.126 0 0 1 .003.01c.172-.144.324-.309.49-.458.442-.392.88-.787 1.293

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\4UabrENHsxJlGDuGo1OIlLU94bt3[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 82716, version 1.1
Category:	downloaded
Size (bytes):	82716
Entropy (8bit):	**7.993713530548**
Encrypted:	**true**
SSDEEP:	1536:hijC7nihKxAiyoVOuS+VhAhFO22tkZWEleJ/oItoGIN9:gIgKThK+XPkZ7It9k
MD5:	6108B8DFDDDD5F9D46A75347D4D803BE
SHA1:	E6A27CF8C983E886B7FBFE3BC8D51E7C797D2F89
SHA-256:	F811A1FE35E8D890E072467515DF338DB4CE562E1CEFDCAC5CB8F76E505AE89B
SHA-512:	52D04EFDC8F3A9F52F7227CEA3E5E5808C3B8E1C12D9D98EB5BABFE2E7953162FA2E13639CD850D595B15214357FB42340B4494E300EC9E4D25C00A2F577BDE7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/googlesans/v27/4UabrENHsxJlGDuGo1OIlLU94bt3.woff
Preview:	wOFF.....C.....GDEF.....XkvkWGPOS...X..;.....GSUB..=....<..#X....OS/2..P8...U...`k.\.cmap..P.....@Y..Dcvt ..V.....fpgm..W8.....uo..gasp.._.....glyf.._.....u.ua.8head.....6...6..'.hhea...T... ...$....hmtx...t.....H.Nq(loca..$.....&..8.maxp..-.... ... ....name..-,...m.....H.post../.....*N....prep..Ad.....^....x.EO%T@.....{...i..4.4\...t.z...7..mgi....`RR.H.....9...C.I.....)..._.h.^C.g...|@,.r.....8d.q.....lp.x....p\Lc.sX`...}.p...T...H.DW..N...Q.x.....B..H..zI....A..&%P+.R8Vf..UVE]mu.k`O..).9.57h....1tx..Y.t.G...kv%.....1.....0..%v....h..!l.7....1..N.....f.~US]..F... ..\5...>.X.=.wC....!g..>.O.p0.#...a..(m0w(BY.9Q.rT...qh'T.}.a..`34A..)gEAN.....p.....|.C.....k>....R....i@T.b.QM.ZYu..7..r...;...:~.a....N<!.4B..I....8...P.....3.w-.tw{.....r3...>.I.....<..q ....p".....2a..-c...v...P;..5..i.....Y...8G..8....K....+..k...(..:XG.d...{..gm.M.I...h....?.R..!..YH.q..K

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\642100862[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	84
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEqjdfXPQE/xlEy:1QEoqh3QEoy
MD5:	6A3F2D147842187CD48B1546EDDD5BA0
SHA1:	AB278C31189DF2939428CF81A3850A2C6DBF5E2E
SHA-256:	D4990F907BCA02F02B3D41216EEA5461609D4BCBA07A3CBEE0D7CF28A6D0D864
SHA-512:	998F55BF5C3D4A71CB3C23782B788F71E7625DF83A37FE8A18F915AAA3BDE5420183A3C709816664E262069EE2FE245CA44799E3476B6DE507B5D68FC86F8960
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D.;GIF89a.....!.....,.....D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\819384062[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	84
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEqjdfXPQE/xlEy:1QEoqh3QEoy
MD5:	6A3F2D147842187CD48B1546EDDD5BA0
SHA1:	AB278C31189DF2939428CF81A3850A2C6DBF5E2E
SHA-256:	D4990F907BCA02F02B3D41216EEA5461609D4BCBA07A3CBEE0D7CF28A6D0D864
SHA-512:	998F55BF5C3D4A71CB3C23782B788F71E7625DF83A37FE8A18F915AAA3BDE5420183A3C709816664E262069EE2FE245CA44799E3476B6DE507B5D68FC86F8960
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D.;GIF89a.....!.....,.....D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ScrollToPlugin.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):	2852
Entropy (8bit):	5.217000388303245
Encrypted:	false
SSDEEP:	48:QXSHhNKsC6TmTAJpI5ZQ5wamo7VJm6fAjyud3qZtzqOyAFqVCG7EPEQEWs9XCYYQ:C8KsCEmTAJpI5ZQ5wamSRfAutWOfF0Tx
MD5:	D29232AA62F9740CB6F1A8CEDC26D8DC
SHA1:	E6742CEE6B36AE8EB1BF26D4529BC7BA2AEB8D3E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ScrollToPlugin.min[1].js	
SHA-256:	7090E6A71A15E2D47E830528798A657BECC16D41B78EADE27EC8624EA6A38812
SHA-512:	917465EA8903E6700A0B4A50C3236AF1A3F327560A6C3FCC6D55A9A693CFAA3B093675936B8EDD2D8243439D2658CF737E9077DCDE9EE3366CAAE8AD4A65DDA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/unpkg/@wix/santa-external-modules@1.644.0/tweenmax-plugins/3.1.1-transition-phase/ScrollToPlugin.min.js
Preview:	!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports):"function"==typeof define&&define.amd?define(["exports"],e):e((t=t||self).window= t.window||{})}(this,function(t){"use strict";var e,i,o,s,n,r,l,u=function(){return"undefined"!=typeof window},f=function(){return e||u()&&(e=window.gsap)&&e.registerPlugi n&&e},p=function(t){return"string"==typeof t},a=function(t,e){var i="x"===e?"Width":"Height",r="scroll"+i,l="client"+i;return t===o||t===s||t===n?Math.max(s[r],n[r])-(o[" inner"+i]||s[l]||n[l]):t[r]-t["offset"+i]},c=function(t,e){var i="scroll"+("x"===e?"Left":"Top");return t===o&&(null!=t.pageXOffset?i="page"+e.toUpperCase()+"Offset":t=null!=s[i]? s:n),function(){return t[i]}},h=function(t,e){var i=r(t)[0].getBoundingClientRect(),l=!e||e===o||e===n,u=!?{top:s.clientTop-(o.pageYOffset||s.scrollTop||n.scrollTop||0),le ft:s.clientLeft-(o.pageXOffset||s.scrollLeft||n.scrollLeft||0)}:e.getBoundingClientRect(),f={x:i.left-u.left,y:i.top-u.top};return!l&&e&&(f.x+=c(e,"x"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\WixMadeforDisplay_W_Bd[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 27080, version 1.13107
Category:	downloaded
Size (bytes):	27080
Entropy (8bit):	7.984576267611114
Encrypted:	false
SSDEEP:	384:YGJNjRUmxJdaYP4ekBDEggz90TzZWzjlru54l0AkjRrk31JNbGpN6MDfcWG:9rUmxJYYP43FY7qWv1JZEzFG
MD5:	19D333269CAABD296357B1A7E72FBB5D
SHA1:	FBE6AB746415B8713FFFE51DFFFDC3C9D59BC40C
SHA-256:	8A6A9A30D97D0C3591326A34B222515BA5A5B7D16E68F4FF49DDBE0FA13EB541
SHA-512:	00861456CC778E5150AB1F1498F3BCBF1A3770580DE621927560D3DC4D448D7CC01BE21C426C7F06A5BEFE9335456A03798C8EA65E10DC66FCFD394CCDDA23A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/WixMadefor/v2/WixMadeforDisplay_W_Bd.woff
Preview:	wOFF.....i.....33.....GDEF..W0.....".."!GPOS..W.....E.&.{EGSUB..e.....fOS/2.....X...`....cmap.....X..:.cvt ...h.....$^.%fpgm.....0.6gasp..W$..... ..glyf.....CO..s.v>..head.....6...6.mI.hhea..... ...$...ehmtx...P...Z...h.3bloca...$...t.....maxp..... ... .D..name..U....%....@BlVpost..W..... ...>prep...h....._$i.....33v.w+_. <.....+/.....x.c`d``.....X..EP..-.....P...X...../.a.....x.%...B1../..4H...i.....2H6`.T..'w..%. Iv.....zYE....b.T.....f.@. ....4....Zx....tG....[.6>/>...m.m#.m..j.. ..t&o...;.8w..4J....j...l.|..s.0[X(\.....b^.=.....-...P.'.~..`o)..q.xWK.U.7n.Y.j...E.55,...K.p..ak...Y.q.!\.>.p..NW.p.{gcOW.....L..k.b.f.....*xB3P.HX.....`..Kj.v...6Jl.....7.....R.}.q.#.2. ....q..s..Q.a9...^..a.+|.5.h<.....hNt.....B....I..37k....P.r.ST.+..E.cT...%,.E.A.?.az..i@|.;,..'k..-v=..O.>.n%.....We..>.)..p.om.5.#NP.....i.}.!...j\

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\WixMadeforText_W_Bd[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26940, version 1.13107
Category:	downloaded
Size (bytes):	26940
Entropy (8bit):	7.983196044654624
Encrypted:	false
SSDEEP:	768:ei+5ISPc4Mq85akb8yCh/uX2Qfvj566p4ruUR2FG:waSPcNq85dzChGGYJKruURb
MD5:	1B77CABA6C9D4D264DD5E101A8326D9D
SHA1:	0AEF11FFF06D2A166705A50E44E545B3D7FE5DF3
SHA-256:	640522494DAF6FB6A791DC1D67AE7A3884D25F87E439A83EC59BAF71D5E39D63
SHA-512:	BA83A6976FB8329D04EBD8897F863289AF694EFC34291D248BE9F9D576E43B61B4B261F2453B89A68BFA8BDC2CB16600B565CED54AFAB47611076A42A6B6EB51
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/WixMadefor/v2/WixMadeforText_W_Bd.woff
Preview:	wOFF.....i<.....33.....GDEF..WP.....".."!GPOS..W....O..C....qGSUB..e,.....fOS/2.....Y...`....cmap.....X..:.cvt ...d.....$..Afpgm.....0.6gasp..WD..... ...glyf.....Co..s.x..head.....6...6..I.hhea..... ...$...Fhmtx...T...\...h.3<aloca...$...v.....}c.maxp..... ... .9..name..V....!....=tidpost..W0..... ...@prep...l.....Q.T.....33..._.<.... .....+/.....&.....x.c`d``....e.....X..EP..-.....M...X...../.a.....x.%....0../..Q(\....[..{.. .d....wx....d.$.....LC.f...w....@.`<..H.|iy.h..t..I.@....!..[...x.....Y..OU?.m.k.m.. .q..m..._en..'\M...(.c_k...Z...&.....7:..h...-.r..Z..w.Q.~EW..#\'.....p..??H#.'..c...WW?[C}-..5.W.x.C#X..s.....O..P.....U.;F.mw.ND.Q....'..!.....4'..nS;r..k.t....7L.....+.N....`7..... ..i.o..~..S...nb.^.f.k. .*.ubL-6W.K.^m.....-.].x..`S..TG.....e?i..q\.Av.:..v....;..z.....F..\m.....m`..;..z.....h.N....w.w.....+Z.....5.....m..>.~.../=;..i...>~(.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\WixMadeforText_W_MdIt[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 29748, version 1.13107
Category:	downloaded
Size (bytes):	29748
Entropy (8bit):	7.985185178927653
Encrypted:	false
SSDEEP:	768:HnkhSzpM44Q3IOYkOyF9afGJ2zeEwILUppcQKRWAUXFSEgFG:Hkh0xwuhbafGJ2dLMUWA2Sy
MD5:	32F3E3707D0AB7F9D86367FB30425ABF
SHA1:	BE74B2636AE55828943F0145479557A1F44FBD8A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\WixMadeforText_W_MdIt[1].woff	
SHA-256:	0570726D9B35862B303637EFFD8718EE7E2BE3088EFFD566BEE07D443AEEE6EB
SHA-512:	106398645129198 15EC77AFC5EBB457495BCC0B2F8E118AA63236B2354B2D069DF26E295B00ED68C30B0CE43B3A8FF72319CDFC26972112C70B72007F4DE2C5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/WixMadefor/v2/WixMadeforText_W_MdIt.woff
Preview:	wOFF.....t4.....d..33.....GDEF..._.....".."!GPOS..``.....J.D..vGSUB..p$.....fOS/2.....\...`.=..cmap...X.....X..:.cvt .....&...fpgm...h.....0.6gasp..._..... ...glyf...,..JJ..yta...head.....6...6.@..hhea.....#...$....hmtx...X.....h..<tloca.....y....t.U.maxp..... ... .D..name..^x...5...PP.}.post..._..... ...@prep.....B.es.....33.ld._.<.. .....x.c`d``.....,..._0\f@.....P...U...../.a.....x.%..AQ....2.Jw;k.-T..Z...b..H.{9...:....So..Y.ld.u..M.zj..@8.]..|;..Yn...>$..@.....cx....%A.D.j.m.m.m. m.m....;....Z..._>!....G.!....7....o.sq0[&c.....{.....~.....u.1...?...g...8.....4.BkKd.RH..H3.).'.P\.....\|g~G:..2..9.-C...h2.uyn..@..l<WP: ..A9.s.\...R/$.e...~.H&.7.{"C./..P.....ss.W ...^U..^S..S...m..D.6p....h4.8...Y...^d.IH..PI. .vFY.(..+.....Hw.uc.O.j...{..Y.a!Z...b....%Hp9....CI;g!...W$.4..).....'..y.+ ..7... 71S.1f3..i&.l.K.z..1%3}1.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\WixMadeforText_W_Md[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 27876, version 1.13107
Category:	downloaded
Size (bytes):	27876
Entropy (8bit):	7.981912701503317
Encrypted:	false
SSDEEP:	768:4ykhSNOuWMXnoEpsfdZnfNPlNtH5E4dVQFG:zkhsOuPK1zP7tZEGB
MD5:	7EFC62924AA0D697C0FE9592A2DA44A5
SHA1:	27D1436BD7E9C36ECCBD295622584E1332E8DDE5
SHA-256:	158A4B3011AB5707FA5A4AE4FD3858A187A13022E1AA9C98EE5ACDF04AC4C6BF
SHA-512:	5F659A9D77DD36DE3AAD302FE1003E2A14A35E02C861E35F8B0C72D2BE8AB809FBBB0FEE64958BDC5F2399DC2A5C4DEA48AE6805DB36B30B7260151FAA6E6 1F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/WixMadefor/v2/WixMadeforText_W_Md.woff
Preview:	wOFF.....I.....33.....GDEF..Zp.....".."!GPOS..Z.....C.I..GSUB..h.....fOS/2.....[...`.=..cmap.....X..:.cvt ...L.....&...fpgm.....0.6gasp..Zd.....glyf.... ..E...v"A7..head.....6...6.sI.hhea..... ...$...Rhmtx...T...i...h..I.loca.....v.....k.maxp..... ... .D..name..Y....3....C.u$post..ZP..... ...@prep...|.....B.es.....332..._.<.....+/ .....1.....x.c`d``....e....WXZ."(.....N...X...../.a.....x.%....P...+^Q.....3L...;.....-....x.....#..l.....,.K.P.*(5.....Pz.cR.....x....;..W.....m[.m.m...c.m{.6m .U<s./...z.N....Y.....z..=m.m..t.....U..c.xk..N...O.<...k...J.....,.@..D.d....r...\.....G.z...ID..h.B.z...Qd.7..u....n.....i....;v.0...C.....d(..a...H..%!$....j..^J...3....y.4[.kj. A..V..HV.Y._$ ..r^[q.....%..U...N.sP..fo.P`.`.r...r.W.T."....N.....H.w9...z...8.N..<....4T....q.T.:.L.w.:.I.KH.a.U..N...../Z;..O..W"A..B..do;.....2..d.x.gI..h...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\activityi;src=2542116;type=2542116;cat=chrom0;ord=8924832293155;gtm=2wg3o0;~oref=https___www.google[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	369
Entropy (8bit):	5.430143478811698
Encrypted:	false
SSDEEP:	6:hn8FQiowadCc4svmzw9xUpCX96v6OqPbRmEH7fuUo1xwQpzj0Mo:hnMQbwuOaxyCkv4AEH7GXfwQpP0N
MD5:	E2796BB82FE61808CE81EDFDD05743BD
SHA1:	B50CF42D377D2A8EC5D717DD31411BAF7EAA4DEE
SHA-256:	AFB46093D85306368B784956B29EE95C6AE40B4A9AD173B7B524C0D21D772D77
SHA-512:	CFC665A07CB2FCAF7976CF2E3F45CB6B249E9D9B4F6FC9F5F2D8EAAEFD71F5B582C498A184E83BABBE9021168E9DF7E8FF4ABD894C2AEEAFE7C8FA407CE5 E8D0
Malicious:	false
Reputation:	low
IE Cache URL:	http:// https://2542116.fls.doubleclick.net/activityi;src=2542116;type=2542116;cat=chrom0;ord=8924832293155;gtm=2wg3o0;~oref=https%3A%2F%2Fwww.google.com%2Fintl %2Fen%2Fchrome%2F?
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"><html><head><title></title></head><body style="b ackground-color: transparent"></body></html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\activityi;src=4382365;type=count;cat=websi0;ord=1;num=1196866999169;gtm=2wg3o0;auiddc=666480753.1617249090;u1=fffb8729-a9da-45fc-9840-773923f9b2e7;~oref=https___www.wix[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	560
Entropy (8bit):	5.494485096690619
Encrypted:	false
SSDEEP:	12:hnMQbwuOaxyCkv4A1ZHwV7ewyA3yxs3AEIAgKWwka2W2KD:hMiRO9w03WqAgKKyl
MD5:	BE830AC14B901D9913160214D029A0EF
SHA1:	32CE7309B583B240F02C8DBCC6631DFAD8E181D9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\activityi;src=4382365;type=count;cat=websi0;ord=1;num=11968669 99169;gtm=2wg3o0;auiddc=666480753.1617249090;u1=fffb8729-a9da-45fc-9840-773923f9b2e7;~oref=https___www.wix[1].htm	
SHA-256:	0D4B9DCA93D4ACF11DBCDD8C8D92A014A7DB5AA54E98127AC37F39685B5ACC03
SHA-512:	0AEDE120995DC785E31E0574312FC3F5382B1842121E01A79FFEB5A876B4E84DB61AC742D5D96591F5B34071E4338D1DDAA87F0273E6DB866A98A8129E333B49
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"><html><head><title></title></head><body style="background-color: transparent"><iframe src="https://adservice.google.com/ddm/fls/i/src=4382365;type=count;cat=websi0;ord=1;num=1196866999169;gtm=2wg3o0;auiddc=666480753.1617249090;u1=fffb8729-a9da-45fc-9840-773923f9b2e7;~oref=https%3A%2F%2Fwww.wix.com%2Foutdated-browser%2Finternet-explorer%3FforceBolt%3D%26ssrIndicator%3Dfalse" width="1" height="1" frameborder="0" style="display:none"></iframe></body></html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bolt-components[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	32233
Entropy (8bit):	5.339293024216153
Encrypted:	false
SSDEEP:	768:kspK1cgUt7ZfRBjvxjo476T/d3A2FWG59S68W1:1fRBjvxjo0w/d3A2FPj
MD5:	C8C93DF05D76F873FC3E591CBE0E4ADE
SHA1:	6AA17E2C785EE5310F768A63D16AC6FE3E20C30F
SHA-256:	ECD3F04926C5DD040448BEE00DDC20F512635E2724C77D2F4F4E06B8E26022FE
SHA-512:	CDAE42BA49A31933052A8EF06B9855A2E98FBC8CA2377FEBC29AB5873DA114DE2055C96DEBBA58E4F680888FB8FA9258EFC26EC246B4B6B98CD9A3467651AB A1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7107.0/node_modules/bolt-components/dist/bolt-components.js
Preview:	!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t(require("react"),require("prop-types"),require("santa-components"),require("lodash"),require("santa-core-utils")):"function"==typeof define&&define.amd?define(["react","prop-types","santa-components","lodash","santa-core-utils"],t):"object"==typeof exports?exports["bolt-components"]=t(require("react"),require("prop-types"),require("santa-components"),require("lodash"),require("santa-core-utils")):e["bolt-components"]=t(e.react,e["prop-types"],e["santa-components"],e.lodash,e["santa-core-utils"])}(this,function(e,t,r,o,n){return function(e){var t={};function r(o){if(t[o])return t[o].exports;var n=t[o]={i:o,l:!1,exports:{}};return e[o].call(n.exports,n,n.exports,r),n.l=!0,n.exports}return r.m=e,r.c=t,r.d=function(e,t,o){r.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:o})},r.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Objec

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bolt-main-r.animations[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	15274
Entropy (8bit):	5.080529892478533
Encrypted:	false
SSDEEP:	192:rckTmdKq52wUOFZZUj20KAH5KFe6fpC9zBLPuN4LKvDRUhrn2TADIpIaNFtNpIGV:YYmd1dgH8epuNPXpFU3zjsMKp5U+P
MD5:	C32870DC55DFA4744D99E83759A1EB74
SHA1:	F79CCE00E4F8CC918DC02C34E670C52D4E360052
SHA-256:	5295872441FD446B4D7F8705B044D62FF4C491CD5D41903EC73B817296ED4B33
SHA-512:	2788C3F4CC4ACE7EE209D717E9D09A115C24D5CB7FF8EDBF0A98F871D5A5D06970D3891AB30A1FD8DF04755C7B4D82FC2EEA9E238C4FAE787823C0D45A251 7F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.7107.0/bolt-main/app/bolt-main-r.animations.js
Preview:	(this.webpackJsonp=this.webpackJsonp||[]).push([[1],{147:function(e,t,n){"use strict";var i=n(861),a=n(865).init,r=n(867).AnimationManager,o=null;e.exports={runWarmupAnimations:function(e,t,n,s,c){var l,u=e["santa-animations"],f=e.gsap3,d=e.ScrollToPlugin3;return l=function(){var e=i.create(f.gsap,[d.ScrollToPlugin]),l=new r({santaAnimations:u,tweenEngineAndFactory:e},t),p=window.warmupData&&!n&&window.warmupData.animationData||{},m=window.rootNavigationInfo?window.rootNavigationInfo.pageId:"",v=!!Object.keys(p).length;o=a({manager:l,model:p,pageId:m}),v&&(o.start(),c(!0)),s(l)},void("loading"===document.readyState?window.document.addEventListener("DOMContentLoaded",l):Promise.resolve().then(l))},stopWarmupAnimations:function(){return o&&o.stop()}}},861:function(e,t,n){"use strict";var i=n(862),a=n(863);e.exports={create:function(e,t){var n=a.create(e,t);return{factory:i.create(),engine:n}}}},862:function(e,t,n){"use strict";var i={error:function(){var e;return(e=console).error.apply(e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bootstrap-features.53cf58f0.chunk.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	130735
Entropy (8bit):	5.222976997836822
Encrypted:	false
SSDEEP:	1536:hiMBqgJxJ7NlnQE4Gr+8vw03YbXvGaqc5iEKM6fBUpoA0S6rtbxd1mK+:xJxtNFQwcqVE4yF
MD5:	F46478B1D58B4F802AD3A817B0B3A778
SHA1:	93AF85D7594C2EAF374805CDE7C94745DE0E0357

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bootstrap-features.53cf58f0.chunk.min[1].js	
SHA-256:	6D3B8499E126497EA7ADCC38E9E645A03B2F3AA316B1915412CD2D5E044BCE71
SHA-512:	C23C2392D5A262960CAE276A5B29B6EE4363DBFFDAE2EC4F484C0030B2453B86BB00466E9620AB69932F64A7DE0690C94D840F6EB4992C84148E47DEDFF53E4A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-thunderbolt/dist/bootstrap-features.53cf58f0.chunk.min.js
Preview:	(window.webpackJsonp__wix_thunderbolt_app=window.webpackJsonp__wix_thunderbolt_app||[]).push([[0],[,,,,function(t,e,n){"use strict";n.d(e,"e",(function(){return r})),n.d(e,"g",(function(){return o})),n.d(e,"c",(function(){return i})),n.d(e,"a",(function(){return u})),n.d(e,"b",(function(){return a})),n.d(e,"f",(function(){return c})),n.d(e,"d",(function(){return s})),n.d(e,"h",(function(){return l})),n.d(e,"i",(function(){return d})),n.d(e,"j",(function(){return f}));var r=Symbol("Router"),o={Dynamic:Symbol("DynamicRoutingMiddleware"),Protected:Symbol("ProtectedRoutingMiddleware"),BlockingDialogs:Symbol("BlockingDialogsRoutingMiddleware")},i=Symbol("PageJsonFileNameMiddleware"),u=Symbol("CustomNotFoundPageMiddleware"),a=Symbol("CustomUrlMiddleware"),c=Symbol("RoutingLinkUtilsAPI"),s=Symbol("PopHistoryStateHandler"),l=Symbol("UrlChangeHandlerForPage"),d=Symbol("UrlHistoryManager"),f="router"},,,,function(t,e,n){"use strict";n.d(e,"c",(function(){return r})),n.d(e,"a",(function(){return {return

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bt[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	86
Entropy (8bit):	3.0950611313667666
Encrypted:	false
SSDEEP:	3:CUMllRPQEsJ9psOjBMllRPQEsJ9pse:Gl3QEsJLsMal3QEsJLse
MD5:	BE36F8869549C7991811C657D7D3775F
SHA1:	8A0CDEAE965A2FA569B2E8677F21D5D71FBAF8BC
SHA-256:	555F405B368AAE998B4C727B5994E0BC9F1D73FCBDBA5DD108DF004A04649A39
SHA-512:	01EE71EE2213737732BF78590F01F56FC19C38D8A48274D11AC4716547A2E13AF32C03C1A37B6FC8961DEB7968814B3C71A926AE91E3688F0E78D59761B24F4D
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....L..;GIF89a.....!.....,.....L..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ca003289-5ee3-45c2-94ad-36c743c35fc1[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 31147, version 1.0
Category:	downloaded
Size (bytes):	31147
Entropy (8bit):	7.987396350283174
Encrypted:	false
SSDEEP:	768:C9IfZeyachSjRMkny9BzuEUnCQJbPaZ3kI1irZQo:C9MqjRj8Qn1pak0iio
MD5:	F3471862C553872A8A36648B3D1F55D4
SHA1:	FD60A4A0674CFCB218C2CC425222501D78815087
SHA-256:	8177D7B57C7E74E786593452C92DCCE54B2610766530F30E856848E56A603E46
SHA-512:	3A5073177947A16028012E6571EEE0CCA99E7B908FDD9EFDEF06F2C1555A5BED784EF610E2C645BD463FD712F59BB9C7B0E46D0A67F78ED03701F385047FBB0A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/fonts/Helvetica/v2/ca003289-5ee3-45c2-94ad-36c743c35fc1.woff
Preview:	wOFF.....y.....t.....GPOS.....GSUB...(.....OS/2.....S...`eDz.VDMX...P...Z....r.y.cmap.....'cvt ...|...K.....fpgm.....,...gasp...T.....glyf...\..P.....head..fH...6...6.z}.hhea..f....!...$.>.Lhmtx..f.....(.G3sloca..i`.....,j.maxp..m`... ... .Y.Mname..m.....!l..$post..sL..... ...2prep..s`.....y..x..TMOSQ.=.J.mi-Vl..Q..hLP.".4iSQ.jD..qc.QKX...\.A..4Q.....[....a.....y...E}'w.w./.B..0.W.....C.b8.>....B&.C|....R.#.....W.R.V.*....s...qP.Q..jO.M.M.....:U...C..J;...F+u....pM.....!.B.6i.9.+.Tp..V.@.....W[&99..+.Zm.....k...c....|.....P.T|.<.....I..oo....*.y....."...1....o|.5j/..(.....2..n..w.l.3.9..._...\...,...S].r...o..6,...A?.%..!8.NF...E..q..ad1.[.'&p.....f..O../0.y,.%....x..A$...X...@.a.n.Yz.z....OX..K....a.E.,..;.?.s.0K6.|s.'..|..Z".....rF.....8.D.....Du.U....Q.Q.Ji.."Zp..3D..k.....KD+F.z\&.0J.U..\!..J.p...:.]5...coS.....~".O....%| .2>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\chrome-logo-new[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 121 x 40, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	2064
Entropy (8bit):	7.804367689715755
Encrypted:	false
SSDEEP:	48:38DhfQf3qtjhOc0TkbYJDSeNu57dXCoIf3NUHwOjdyc81RmXj:381YiCkb0SeNudby9vAz
MD5:	4B9A71E5C15A4DA1E20F200E9D250780
SHA1:	BD6B89544D35B20E50B439F3A3970F75B39A431D
SHA-256:	A2062146BA85EEAEDD0B68706FF94C3DF4022F6B08D7E2B5ADF18F24DFB91DEC
SHA-512:	A11EA249CD58AA8E94E5B883D9C76F6479B8597AB84F645F1AC4D32CBF90D00D16FF9F2B15F21177161224EDC221546EAF549091487099F7B002457A4A3D2CA5
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\chrome-logo-new[1].png	
IE Cache URL:	http://https://www.google.com/chrome/static/images/chrome-logo-new.png
Preview:	.PNG.....IHDR...y...(.....)....PLTE..._bh^ah``h_bg_ch`ah`en^bh_ch_bh_cg^cg_bg`hh^bh`ci`bf_cg.e[..Y..[^ch.qj..[.>`gh.8_ch..@.^S`dh..^.cX..E.._.WL..b.RE..B..@..?..Z.b V..>.]Q..?..^..@..Z.\P.L?..]..@.N@.K?_bh+.k.UK..C^ah^.[..Y.SG..@..H.>.<.j^.l`..b.e]..F.@..@8.s.L.pe..@_bi_bh_ch..D..B..A.OC.MAJ...._.....`..^K..M....c.QE..b..\".e.SG.K?.R FL..H....]..[.UI.J=.THL....`.....@..C.N@..?.....Z..X.RF.QD..@.L>.....I.PC..B.H:.....L.WK..A.h<_.....e..U..S..P..O..D.j<..;.9.D7.C6.....`..M.....{r..n+.g,.`@.X.\Q_wPk .O^.M..K.M@.J=..<.m;.k;.I;.:.:.m:.L:.H9.8.7.A4b.....k.....y.yE.wp.w3.q.vm.md.yb.mb.xa'.VQ}R..QsqQ.O..N2.N2.M..L..L..L.XL..K.Y@.f=.A4R..d...QtRNS..` .@....o.P ._0.@@ . .@! ..pP .....po`P@0 .....o``PPO@@00...=.O....IDATX...s.A....+.%.....m..^.(..mBJ.h....._...\..o.e..i.7....{ow..!....2.%.r....:G...,...J.)U...&8.D= z.hg.....U-..z.....SjO..R.j.?.]..5}.'.. &f..A=.....Tq...)S.7A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\chrome[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	223832
Entropy (8bit):	5.448281377195453
Encrypted:	false
SSDEEP:	3072:YVTWj4Hn9YapEEwJ67iTdp4j1A/fSr5573hxieWU:69AEWo79
MD5:	F77A13E0857020F088336E1A3B2C2719
SHA1:	124E12E80C6984777BDBA682878AADA1D7CBF3D0
SHA-256:	5272FB57E5FCC9001CEF4A2AE23727FBD4F7013DED08097F7CCF8405129BE604
SHA-512:	50FBC351F0F04066C61147212745588EB6E52CF4D785FFEF42009D114398F1720AA401B44C1877C8408FB4C1B4FB029981842893E58834C742ED43E01E9EB037
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>. [if IE 9]> <html class="no-js ie ie9" lang="en" dir="ltr"> <![endif]-->. [if IE 8]> <html class="no-js ie ie8" lang="en" dir="ltr"> <![endif]-->. [if IE 7]> <html class="no-js ie ie7" lang="en" dir="ltr"> <![endif]-->. [if IE 6]> <html class="no-js ie ie6" lang="en" dir="ltr"> <![endif]-->. [if (gte IE 10)|!(IE)]> > <html ite mscope itemtype="https://schema.org/WebPage" class="no-js no-ie" lang="en" dir="ltr"> <![endif]-->.<head>. <meta charset="utf-8">. <meta http-equiv="content-language" content="en-us">.. <link rel="preconnect" href="https://fonts.gstatic.com" crossorigin>. <link rel="preconnect" href="https://tools.google.com" >. <link rel="preconnect" href="https://www.youtube.com" >. <link rel="preconnect" href="https://s.ytimg.com" >. <link rel="preconnect" href="https:/ /www.googletagmanager.com" >. <link rel="preconnect" href="https://adservice.google.c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\chrome_throbber_fast[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 24 x 24
Category:	downloaded
Size (bytes):	4469
Entropy (8bit):	6.7695629044778185
Encrypted:	false
SSDEEP:	48:HwGZ9KnRJzLTMYtb62yy6J/7aQ5xhU8gACGyL7orC:HzHgHMcauQ5x5eLH
MD5:	81247683E65B6F536D25AF4B2917E823
SHA1:	331043F7F52D006377003B2AFAE4EC8EB877CEE5
SHA-256:	3E846532CACBDA65EB384367C713A798D6D6D619D97ED30D136C6ECB911AB9BB
SHA-512:	075EF7168959423DC01D3057384B1D6ADDCF7848162C44405ADCD8A8FE9412C8FF30B80259302D96D25BF262AB382E362626482AF3D5036E19817D1A5D6B9A39
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/chrome/static/images/chrome_throbber_fast.gif
Preview:	GIF89a.....4f...t.....L~.....\.....<r.....\....T~....Dr...4j...|...\.....d.....T.....Dv.....!..NETSCAPE2.0.....!..... .,..... ...b@.p.....q..B.....8...aeb"..@l.....P.A..v..x.CJ. p.A..Z...C.cc..C.a..C.Z..B...~.....A.!.....,.....4f...d.....Lz.....Dv.t.....\..<n.....4j...l.....T..|....\.....U.'..tp.P. ...R.t..8.....}...R.M..D..]v5.Quu|.....+..`4j!!N.....~.....d!.!.....,.....4f...t..Lz....\.....Lv....\.....<n...T.....d..4j...t..T~....\.....S.&..0B.Q.q..xL. .x.X1.=9...P.D....V. ..Sr.8... ...$...xA3..#.m...|N.....~.....|!.!.....,.....4f.....t..T~.....Dr.....\.....<n.....Lv.....4j.....|..\.....Dv.....d.....U.'..(....0.i@.L6A.....`.W..z.G.6..&....9L...EA ...O..c$ ..Bxj@m..|N.....~....."!.!.....,.....4f...d.....Lz.....Dr...t..T.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\close-icon[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	380
Entropy (8bit):	6.947082124793556
Encrypted:	false
SSDEEP:	6:6v/lhPkMFKQ6sXRBOgM1Vi/rlsZ/DuujMnD673pN6BOQwVMBQbKRU6z8l0Q+jp:6v/7sDQpSc/yZ/DFjf75N6BOQ1mbx6zX
MD5:	C4EC8F447FC5E74D5344720083582D0E
SHA1:	BA55F17FF89D96F909B79B396EC88098240C8B67
SHA-256:	129A06E9E3C9F1F7AA75B0EE630F000184F08A36E9BFB14CBA1DF578C5013FE6
SHA-512:	21FF30024F47E06C143B555669A8F2971E30FFEEA61A7603F67B57A428EC9CECDCAA793D301249508F5163A5E7549A018D27FA2F2952C5DCC8FDBAE4F23AB9D E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/chrome/static/images/close-icon.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\close-icon[1].png	
Preview:	.PNG.....IHDR... ... .D.....BPLTE.....:;? !%.....TVYTUYq.w\....tRNS.... ..._0.`.....IDAT8.....0.C.-.(`(...u...J+`.)....B.....>D'5};....]...7.hz..c...5.....d..x.`....o...~"38.P....$(Q;.au.....:.....:_.....z.]8.du.:..B/.Q..O.~..P..v:..0.H.....y:.%.ewu..g..6...i...@..dY'}.+...../|..Sl....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\collect[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	35
Entropy (8bit):	2.9889227488523016
Encrypted:	false
SSDEEP:	3:CUdrllHh/:HJ/
MD5:	28D6814F309EA289F847C69CF91194C6
SHA1:	0F4E929DD5BB2564F7AB9C76338E04E292A42ACE
SHA-256:	8337212354871836E6763A41E615916C89BAC5B3F1F0ADF60BA43C7C806E1015
SHA-512:	1D68B92E8D822FE82DC7563EDD7B37F3418A02A89F1A9F0454CCA664C2FC2565235E0D85540FF9BE0B20175BE3F5B7B4EAE1175067465D5CCA13486AAB4C582C
Malicious:	false
Reputation:	low
Preview:	GIF89a.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\f[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	36195
Entropy (8bit):	5.4956916474428485
Encrypted:	false
SSDEEP:	384:KU+DSK2hCxjo7BcGfF2O2tqLGadLKqWiYgMkHRKDNCnRDAzFotwBc3T9yFVuIr6t:kDDfOSaoPgMkxKHPTr6IBxmf
MD5:	7F0BD087C305D9450CAC19B6F729B3E0
SHA1:	A171271C1602A36D65EE606629FC5F3865E9AF11
SHA-256:	B3BCD37CBDD3273EC26B2FE7FE823C9A07E14809480BA6FD08280E409C0AB0D6
SHA-512:	9B52D0793840BEE3A894A2219BFC8B89CA55A57D1304DFF5AD53A644480093EC5E85C2DED340493E4228F2FB9A5FE87B860D716F77DFD748B040E20D61861D2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.googleadservices.com/pagead/conversion_async.js
Preview:	(function(){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .function aa(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}var ba="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a}; .function ca(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}var da=ca(this),ea="function"===typeof Symbol&&"symbol"===typeof Symbol("x"),l={},fa={};function p(a,b){var c=fa[b];if(null==c)return a[b];c=a[c];return void 0!==c?c:a[b]} .function u(a,b,c){if(b)a:{var d=a.split(".");a=1===d.length;var e=d[0],f;!a&&e in l?f=l:f=da;for(e=0;e<d.length-1;e++){var g=d[e];if(!(g in f))break a;f=f[g]}d=d[d.length-1];c=ea&&"es6"===c?f[d]:null;b=b(c)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\f[2].txt	
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):	2038
Entropy (8bit):	5.850628628251471
Encrypted:	false
SSDEEP:	48:0VUUIqzPrqTnJcgVhkG+lkSEW5gHdyWOi/K7FiAQEjpX:+UURWTCgVhktlkSEWORyMXGX
MD5:	B05B6D4B8BBDFCC885E8F6EFCB0FDFD7
SHA1:	63EC5B90E50F71A4F00D92FA32C8BFC97129E12D
SHA-256:	77A103A88BAD0D7FA1F2EAD801C0BAC84BA01789600E0F21278AF2D79060151B
SHA-512:	F67C69E40DCF8E05BD762EFCE6C892662F67F11DF17E6D2167CF4C8F73DEEF43686B4570CAE431D183C6256CD8747CFE388921C9D543C1020124A7F543A1DE2
Malicious:	false
Reputation:	low
Preview:	(function(){var s = {};(function(){/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0 */ var c={},f=this||self;var l=/#|$/;function n(d){var g=d.search(l),a;a:{for(a=0;0<=(a=d.indexOf("fmt",a))&&a<g;){var b=d.charCodeAt(a-1);if(38==b||63==b)if(b=d.charCodeAt(a+3),!b||61==b||38==b||35==b)break a;a+=4}a=-1}if(0>a)return null;b=d.indexOf("&",a);if(0>b||b>g)b=g;a+=4;return decodeURIComponent(d.substr(a,b-a).replace(/\+/g," "))};function r(d,g,a){function b(){--p;if(0>=p){var e;(e=d.GooglebQhCsO)||(e={});var q=e[g];q&&(delete e[g],(e=q[0])&&e.call&&e())}}for(var p=a.length+1,m=0;m<a.length;m++){var h=n(a[m]),k=null;1!=h&&2!=h||!(h=d.document.getElementById("goog_conv_iframe"))||h.src||(k=h);k||(k=new Image);k.onload=b;k.src=a[m]}b()}var t=["ss_"],u=s||f;t[0]in u||"undefined"==typeof u.execScript||u.execScript("var "+t[0]); for(var v;t.length&&(v=t.shift());)t.length||void 0===r?u[v]&&u[v]!==Object.prototype[v]?u=u[v]:u=u[v]={}:u[v]=r;}).call(this);;s.ss_(window,'

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\focus-within-polyfill[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\focus-within-polyfill[1].js	
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1171
Entropy (8bit):	5.1458024367829545
Encrypted:	false
SSDEEP:	24:YXw4ZXLL8jdOAT3r8j/uZp93ceY90l78BQLoOiQL4mT6xQMnmb3q/FcEmzNchNhx:6IMI38/8Xr+0l78B2vN4W6CRb31XzNcv
MD5:	C187011C9A45C15A6FCBF5D62A5D755F
SHA1:	E3FD6FAED2154EE94559F362EA0390B46ABF75BB
SHA-256:	452A163BE231D77006015E7D6F2A5B8AB5987D915C1F1E6907DDFBBA3AEC6EEC
SHA-512:	E5025DB65F3A66552C838B24374071130040D2E0CF13A4E4F75DA3A8C8DB00228EEAB8F45695F709CB834FF43D4B2DB757D8AA9046AB6A8E1990A4227AC0B4A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/unpkg/focus-within-polyfill@5.0.9/dist/focus-within-polyfill.js
Preview:	'use strict';(function(){(function(){function e(a){for(var b=[];a=a.parentNode||a.host||a.defaultView;)b.push(a);return b}function f(a){return function(b){var c="undefine d"!==typeof b.getAttribute?b.getAttribute("class")||"":void 0;"undefined"!==typeof c&&-1===c.indexOf(a)&&b.setAttribute("class",c.concat(" ",a).trim())}}function g(a){return function(b){var c="undefined"!==typeof b.getAttribute?b.getAttribute("class")||"":void 0;if(c){var d=c.indexOf(a);0<=d&&(0===d||0<=h.indexOf(c.charAt(d-1)))&&(c=c.re place(a,"").trim(),""===c?b.removeAttribute("class"):b.setAttribute("class",c))}}}function k(){var a=function(b){function a(){d=!1;"blur"===b.type&&Array.prototype.slice. call(e(b.target)).forEach(g("focus-within"));"focus"===b.type&&Array.prototype.slice.call(e(b.target)).forEach(f("focus-within"))}if(!d){window.requestAnimationFrame(a);var d=!0}};document.addEventListener("focus",a,!0);document.addEventListener("blur",a,!0);f("js-focus-within")(document.body);return!0}var h=["\n","\t"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ga-audiences[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	84
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEqjdfXPQE/xlEy:1QEoqh3QEoy
MD5:	6A3F2D147842187CD48B1546EDDD5BA0
SHA1:	AB278C31189DF2939428CF81A3850A2C6DBF5E2E
SHA-256:	D4990F907BCA02F02B3D41216EEA5461609D4BCBA07A3CBEE0D7CF28A6D0D864
SHA-512:	998F55BF5C3D4A71CB3C23782B788F71E7625DF83A37FE8A18F915AAA3BDE5420183A3C709816664E262069EE2FE245CA44799E3476B6DE507B5D68FC86F8960
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D.;GIF89a.....!.....,.....D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\google-chrome-logo[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, 160x24, frames 3
Category:	downloaded
Size (bytes):	2745
Entropy (8bit):	7.741604826071945
Encrypted:	false
SSDEEP:	48:4ewFmUlcfuDKaAooAhjZQKNFaSze+coezpM6yDdEC5axXO8lldq:ZwRlmu+aIAbbNNbeVMBDdECzYII
MD5:	DABB508820425E63D8138A1F7E94FDE0
SHA1:	E16615B860F2C203488E000CA7C489D49B2B5521
SHA-256:	84D5A4525BE1835AE8F3DEA212A449572B0200C0AA1CBD5D0CFB68783B6034F9
SHA-512:	6723552796917C2841DAD928F7912DE2E6F1B9967DF099BC6D49C724B84275AF807E44B503F30B50ADE8F12645394B709EB72B33C51262D8BE795FF5DBD4A49C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/chrome/static/images/fallback/google-chrome-logo.jpg
Preview:	.....JFIF.....C.....C.....x.N..Z.o 9[..{.`{...MM..Xs..5A".....3.B...?D..2.\.....W.C...O./..Ve-.....T/..l"6ftkq..TV.^o.,-.Z...L...*.7 %FTZ..sj.@.....$.....!12".....G.v.m..[.W...!.7....[.~..h.E..f.^... T#..y\|...Y".....#..3.*.U..b...F.X....<s...o...J.t.l"4U{5W(g}.>....v*...e)m.]k.....O.9.,M.7...Ek...;..YJe.....R..:.....K.n..;..*QF.0...N.G7./._..O>=#.V#...UF....O^.$~.z#|.^...5.?.....)...1g.N....2.Qc.....A....XL.R.)$....N. ~(X..^sch...u....|.G*.1..2..a.d.Tf._.'.?.._..+...:f...+.#....LM-... ..|.lo..Lt|.J.4._....VzH.....g.....J.NH.....8!o.!.....*.&.C.~c+.p....5...GsA.5.%n.:} E...=...g1...}.....:.P.....f.b..r.X..;.P..].2.".t3D..h.8.:.....)3.IW...l(l.|..7,fD..5xL...6...h..d.q

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\hero-anim-bottom-left[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 400 x 400, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	10370
Entropy (8bit):	7.893992617262281
Encrypted:	false
SSDEEP:	192:sSFk37+mY6YnIYbLW+UKaSSVMm+L2VhAu9O2ENR7YkM3oZ413iSgqDP3TGQ:ri37+gYbLVULWrS9O2IA3W6SrqDiQ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\hero-anim-bottom-left[1].png	
MD5:	63082350A0AD4DF2A5E62FF571BB239D
SHA1:	47F5367BE0A58EEC1D754CD6B74978C73E015DC2
SHA-256:	8FFC1F0C1364321C2A9612AB498316EE83D24EF84E78EF737C1255279B864878
SHA-512:	DABEB2706093A1CDBDA6DA2C919FAC8D95C418020619DA884F19FAC827FD08E0F95ADF4FC384C2CB15BA217EB1457357FCD1B1729866CBC8FD26272395B9B 31
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/chrome/static/images/homepage/hero-anim-bottom-left.png
Preview:	.PNG.....IHDR.....6.....pHYs.....sRGB.....gAMA.....a...(.IDATx....wT.....%..1"=.3....=.AR.{.}..I?.!.w..~....M..c.....".T2.9=N.*!...a#....{..k....T.....*..M.Ws..6...., Ve2.;.KZ../.7e.2i.=...r....eiO.....7.....N.....u.>..S..N.u.F..`H4...I6#...`0.=....6.%.G...j..W.....)..&...Y.y..j..?.cSm...UK.d.x3Y.....,_.d.....6.Bg1....._....L5.X..*.. @P(O....E2.. ....C3R...4.y...A.`C....n..%...<lB.m...F.T.....z../R..h...LkEa...>.s..PE..1Ucd.[Y..!+..! .j3`.-[.g.5.z...g6....u2O.`.....".....W../jP..J.7....s!LB..L.].h"3/O\.PA?. .f`..b..~.=..3.}.] !,...g.Q..4....]t..h.+.h.@A.. .].c.W..s.Iyu.k...a}-....6.?.U...@...@..c...b%.\.....k.T.C`....=.....C..V.$.3;5.(@.....u.ac9.Z%.....E.Q|..".....I1a~...g..[.....]ihTBh.(9/.j`.r.z.a.m f..ma.q9.....\.v....$.m^.`/.....7C....nfY.....9.+...ar.0.N..lZX.y{*...in.#4...a.Z.r.6.Z. .....4..'.&..mZ.e.....$...2...cw).....8q.]..Gh`'.}':3..^....Z\.(..,l<. cF..mQ.|..o..).

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\imageClientApi[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	35995
Entropy (8bit):	5.575170334715127
Encrypted:	false
SSDEEP:	768:LlTm0T2sEA93iTuoaL1/QsUjpv0scpd1dpbxvFNdlcdmdsEs/dbgL0ziK:Vd3iTuoaL1/VXMPGL0eK
MD5:	BF11A31D6BD9EAD3F8EF9C871D38EAB7
SHA1:	EF16C90A04FF70B304F222A6FFC97336D817FED9
SHA-256:	7A1E77C13481F363D05F6612817E84C7C27F2E294AB84609C5442542F63C80AF
SHA-512:	6480175F9F08D142F4D71B31DB9AF6AF6E9E79EA804E50F7E576761E2FDFF8C2A271C388BA47C022735214A14D5A6CC47FF6CFF6FAE87625973B46DB58D18CC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/unpkg/image-client-api@1.4060.0/dist/imageClientApi.js
Preview:	!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==typeof define&&define.amd?define([],t):"object"==typeof exports? exports.imageClientApi=t():e.imageClientApi=t()}(this,(function(){return function(e){var t={};function i(r){if(t[r])return t[r].exports;var a=t[r]={i:r,l:!1,exports:{}};return e[r] .call(a.exports,a,a.exports,i),a.l=!0,a.exports}return i.m=e,i.c=t,i.d=function(e,t,r){i.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:r})},i.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},i.t=function(e,t){if(1&t&& (e=i(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var r=Object.create(null);if(i.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:e}),2& t&&"string"!=typeof e)for(var a in e)i.d(r,a,function(t){return e[t]}.bind(null,a));return r},i.n=function(e){var t=e&&e.__esModule?function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\insight.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	4322
Entropy (8bit):	5.34276622153142
Encrypted:	false
SSDEEP:	96:LvleavwqOcvwM6kpL5CN6Cysim8jvuoHFmtXgM4nldI2XDzxp:Zvwkvw/8Ao7vjmtQ5lW2hp
MD5:	D3B7F1A92DD6719F87830997E69F3675
SHA1:	A8BC777FD7187E3A56D5214A3BBDDD95EC575DED
SHA-256:	5F3B103A1268F862A5E432D607F8E5220DEA9D301D13565B0ECDED3AD9C25AB2
SHA-512:	FDBBB5FB56922C71CBF877CA1CD901AFD243342106303C85F3074868EEF27AC1E0E6C0AB0A46961457C8441A2A2A1C75136977FF908EDC68C59A3386117E765
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://snap.licdn.com/li.lms-analytics/insight.min.js
Preview:	!function(){"use strict";function n(){return(new Date).getTime()}function l(n,e){var i=n.cookie.match(new RegExp("(?:^|;)"+encodeURIComponent(e).replace(/([\.$?*|{}\(\)\ [\]\\\/\+^])/g,"\\$1")+"=([^;]*)"));return i?decodeURIComponent(i[1]):""}function _(n,e,i,t){var r=t.days_until_expiration,o=void 0===r?1:r,a=t.path,d=void 0===a?"/":a,c= t.domain,l=void 0===c?null:c,_=function(n){var e=(new Date).getTime()+n,i=new Date;return i.setTime(e),i.toUTCString()}(864e5*o),s=encodeURIComponent(e)+"="+enc odeURIComponent(i);s=s+";expires="+_,l&&(s=s+";domain="+l),s=s+";path="+d,n.cookie=s}function t(n){return n.webkit&&n.webkit.messageHandlers&&n.webkit .messageHandlers.LIPixli||!1}function e(n,e){var i="https://px.ads.linkedin.com/collect?"+e;t(n)?n.webkit.messageHandlers.LIPixli.postMessage(i):(new n.Image).src=i}funct ion i(n,e){var i="https://px.ads.linkedin.com/insight_tag_errors.gif?"+e;t(n)?n.webkit.messageHandlers.LIPixli.postMessage(i):(new n.Image).src=i}function s(n){return n.m ap(functio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\installer.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	55423
Entropy (8bit):	5.4774704387403395
Encrypted:	false
SSDEEP:	768:eag7mwt+1GF5Dc5I5OI1+c8/KxBOfs8Iu6DF45r9h3EX+G/pIjb9bZowiS3J:Smwt+1K5WI1Qiafs8iwFE+G/pIjBFuSZ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\installer.min[1].js	
MD5:	CCCC73EBC4889A3E8CB921A1F09684D7
SHA1:	E8FC1BD1AB5BE395EE6FB96C361EC3FA0C078212
SHA-256:	0A61524429200ACDD270D7761B4AF9DAA8DA5604BAD5ABFCF441D0B499B4CDB5
SHA-512:	71C060468FD12BEEE18C6C354B0DCA44478E10182375236704D1F670E32EBFFB5F6B98F48C4DCE8196DDF158A4758C9876DA9DC5909DBB2D283AA2A5706FFB1F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/chrome/static/js/installer.min.js
Preview:	(function(){var h,aa="function"==typeof Object.create?Object.create:function(a){function b(){}b.prototype=a;return new b},ba;if("function"==typeof Object.setPrototypeOf)ba=Object.setPrototypeOf;else{var ca;a:{var da={Mb:!0},ea={};try{ea.__proto__=da;ca=ea.Mb;break a}catch(a){}ca=!1}ba=ca?function(a,b){a.__proto__=b;if(a.__proto__!==b)throw new TypeError(a+" is not extensible");return a}:null}var fa=ba,k=this;function l(a){return"string"==typeof a}function ha(){}.function n(a){var b=typeof a;if("object"==b)if(a){if(a instanceof Array)return"array";if(a instanceof Object)return b;var c=Object.prototype.toString.call(a);if("[object Window]"==c)return"object";if("[object Array]"==c||"number"==typeof a.length&&"undefined"!=typeof a.splice&&"undefined"!=typeof a.propertyIsEnumerable&&!a.propertyIsEnumerable("splice"))return"array";if("[object Function]"==c||"undefined"!=typeof a.call&&"undefined"!=typeof a.propertyIsEnumerable&&!a.propertyIsEnumerable("call"))return"function"}else return"nul

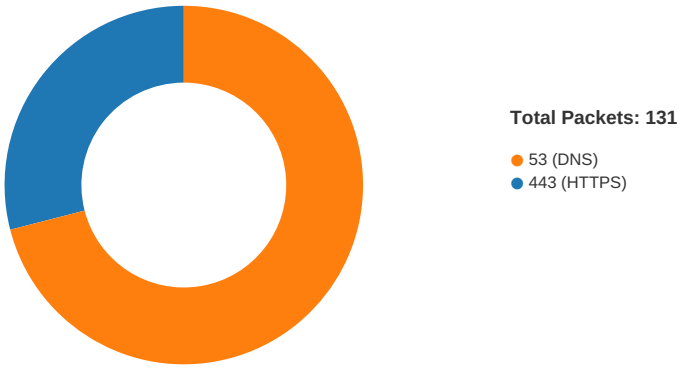
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\js[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	94232
Entropy (8bit):	5.529102234619335
Encrypted:	false
SSDEEP:	1536:JupMsRGbOlh0E+HGDv+/HRE6cszcpE5KZQXL8Q6uS+01W9nKP9dQflAods+:JupMFuh0u+5ss7XL8Qa++f+
MD5:	7D17BE47A811055E233A12606B0C28F2
SHA1:	4000EEE365E44CEAA7B2DA17E5D705444DA6C2AD
SHA-256:	D86C6B76F3F5FF3BD63CF44F2C6048BC55DD50E1C2A22EDA32B94C12601E4228
SHA-512:	CA0D3B32338ACE54DB9433BB133CFC1E65F8BADD56352E7A45778D6698122965C4337745999483F9B5FB576FEF7C246034A854982092AED0599F42B46C3DF04D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.googletagmanager.com/gtag/js?id=AW-1006927621
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}}},ca=function(a){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return b?b.call(a):{next:ba(a)}},da="function"==typeof Object.create?Object.create:function(a){var b=function(){};b.prototype=a;return new b},ea;.if("function"==typeof Object.setPrototypeOf)ea=Object.setPrototypeOf;else{var ha;a:{var ia={a:!0},ma={};

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 31, 2021 20:51:17.028155088 CEST	49713	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.028997898 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.088849068 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.088974953 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.091392040 CEST	443	49713	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.091519117 CEST	49713	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.096075058 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.097394943 CEST	49713	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.155714989 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.159394026 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.159419060 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.159430981 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.159446955 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.159457922 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.159593105 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.159631968 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.159959078 CEST	443	49713	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.163860083 CEST	443	49713	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.163882971 CEST	443	49713	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.163899899 CEST	443	49713	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.163917065 CEST	443	49713	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.163932085 CEST	443	49713	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.163964987 CEST	49713	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.164014101 CEST	49713	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.210325956 CEST	49713	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.214524984 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.218280077 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.218530893 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.218905926 CEST	49713	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.271806002 CEST	443	49713	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.272026062 CEST	49713	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.272119045 CEST	443	49713	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.272192001 CEST	49713	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.272708893 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.272854090 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.272892952 CEST	49713	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.273123980 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.273197889 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.273526907 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.276797056 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.276814938 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.277493000 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.280186892 CEST	443	49713	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.280369043 CEST	49713	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.374672890 CEST	443	49713	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.375423908 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.531604052 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.531625986 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.531693935 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.531729937 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.539225101 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.539252996 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.539268970 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.539283037 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.539302111 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.539321899 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.539340019 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.539355993 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.539375067 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.539443970 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.590392113 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.590424061 CEST	443	49714	35.246.6.109	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 31, 2021 20:51:17.590440989 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.590457916 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.590542078 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.590593100 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.597955942 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.597990036 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.598006964 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.598023891 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.598076105 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.598094940 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.598112106 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.598114967 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.598129988 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.598148108 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.598160982 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.598166943 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.598186016 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.598197937 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.598201036 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.598218918 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.598226070 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.598237038 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.598253012 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.598256111 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.598268986 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.598297119 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.598336935 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.648680925 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.648708105 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.648720026 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.648737907 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.648753881 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.648771048 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.648787022 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.648802042 CEST	443	49714	35.246.6.109	192.168.2.3
Mar 31, 2021 20:51:17.648857117 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.648904085 CEST	49714	443	192.168.2.3	35.246.6.109
Mar 31, 2021 20:51:17.656238079 CEST	443	49714	35.246.6.109	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 31, 2021 20:51:08.657546043 CEST	50620	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:08.714842081 CEST	53	50620	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:08.844675064 CEST	64938	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:08.893254995 CEST	53	64938	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:09.975414038 CEST	60152	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:10.021522045 CEST	53	60152	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:10.728665113 CEST	57544	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:10.774629116 CEST	53	57544	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:11.515619993 CEST	55984	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:11.564688921 CEST	53	55984	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:12.521249056 CEST	64185	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:12.568609953 CEST	53	64185	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:13.337366104 CEST	65110	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:13.385243893 CEST	53	65110	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:14.838440895 CEST	58361	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:14.887031078 CEST	53	58361	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:15.731678963 CEST	63492	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:15.789653063 CEST	53	63492	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:15.997243881 CEST	60831	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:16.061563015 CEST	53	60831	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:16.943938017 CEST	60100	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:17.018285990 CEST	53	60100	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 31, 2021 20:51:17.201951981 CEST	53195	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:17.259357929 CEST	53	53195	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:17.614217043 CEST	50141	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:17.632236958 CEST	53023	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:17.671493053 CEST	53	50141	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:17.680982113 CEST	53	53023	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:18.425321102 CEST	49563	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:18.471260071 CEST	53	49563	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:20.861649990 CEST	51352	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:20.933553934 CEST	53	51352	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:21.256818056 CEST	59349	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:21.320404053 CEST	53	59349	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:21.610842943 CEST	57084	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:21.662157059 CEST	53	57084	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:22.401583910 CEST	58823	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:22.444768906 CEST	57568	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:22.462054968 CEST	53	58823	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:22.493501902 CEST	53	57568	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:22.784935951 CEST	50540	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:22.831439972 CEST	53	50540	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:23.019530058 CEST	54366	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:23.090606928 CEST	53	54366	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:26.953408003 CEST	53034	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:27.000489950 CEST	53	53034	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:27.027640104 CEST	57762	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:27.083897114 CEST	53	57762	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:28.652971983 CEST	55435	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:28.708580971 CEST	53	55435	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:28.919217110 CEST	50713	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:28.965559959 CEST	53	50713	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:30.351587057 CEST	56132	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:30.364800930 CEST	58987	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:30.377557039 CEST	56579	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:30.388154030 CEST	60633	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:30.406838894 CEST	53	56132	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:30.423383951 CEST	53	56579	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:30.427361965 CEST	53	58987	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:30.452819109 CEST	53	60633	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:30.469827890 CEST	61292	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:30.492784977 CEST	63619	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:30.523822069 CEST	64938	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:30.530145884 CEST	53	61292	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:30.540040970 CEST	53	63619	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:30.584112883 CEST	53	64938	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:31.133421898 CEST	61946	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:31.185112953 CEST	64910	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:31.193300009 CEST	53	61946	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:31.245342970 CEST	53	64910	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:33.068571091 CEST	52123	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:33.125242949 CEST	53	52123	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:33.135236025 CEST	56130	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:33.202090979 CEST	53	56130	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:33.417886972 CEST	56338	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:33.428091049 CEST	59420	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:33.464857101 CEST	53	56338	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:33.496385098 CEST	53	59420	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:33.838910103 CEST	58784	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:33.845408916 CEST	63978	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:33.849868059 CEST	62938	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:33.900602102 CEST	53	58784	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:33.904436111 CEST	53	62938	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:33.904814005 CEST	53	63978	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:33.962333918 CEST	55708	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:33.983583927 CEST	56803	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 31, 2021 20:51:34.016674995 CEST	53	55708	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:34.046838045 CEST	53	56803	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:34.089498997 CEST	57145	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:34.135597944 CEST	53	57145	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:34.404982090 CEST	55359	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:34.484647989 CEST	53	55359	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:34.655558109 CEST	58306	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:34.712714911 CEST	53	58306	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:34.835005045 CEST	64124	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:34.885004997 CEST	53	64124	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:34.908627033 CEST	49361	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:34.968578100 CEST	53	49361	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:35.162910938 CEST	63150	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:35.213906050 CEST	53279	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:35.221936941 CEST	53	63150	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:35.270142078 CEST	53	53279	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:35.600112915 CEST	56881	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:35.648838043 CEST	53	56881	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:36.441538095 CEST	53642	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:36.487483978 CEST	53	53642	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:37.702764034 CEST	55667	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:37.752866030 CEST	53	55667	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:43.596988916 CEST	54833	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:43.644684076 CEST	53	54833	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:45.769751072 CEST	62476	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:45.816149950 CEST	53	62476	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:46.385698080 CEST	49705	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:46.448173046 CEST	53	49705	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:46.901540041 CEST	62476	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:46.963745117 CEST	53	62476	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:47.181586027 CEST	61477	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:47.253992081 CEST	53	61477	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:47.397869110 CEST	49705	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:47.452394009 CEST	53	49705	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:47.899952888 CEST	62476	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:47.950927019 CEST	53	62476	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:48.413372040 CEST	49705	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:48.460226059 CEST	53	49705	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:49.898367882 CEST	62476	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:49.944962025 CEST	53	62476	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:50.413913012 CEST	49705	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:50.470839977 CEST	53	49705	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:53.910523891 CEST	62476	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:53.956559896 CEST	53	62476	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:54.426182985 CEST	49705	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:54.481187105 CEST	53	49705	8.8.8.8	192.168.2.3
Mar 31, 2021 20:51:59.382438898 CEST	61633	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:51:59.439214945 CEST	53	61633	8.8.8.8	192.168.2.3
Mar 31, 2021 20:52:02.732532024 CEST	55949	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:52:02.800316095 CEST	53	55949	8.8.8.8	192.168.2.3
Mar 31, 2021 20:52:03.087088108 CEST	57601	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:52:03.123452902 CEST	49342	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:52:03.129937887 CEST	56253	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:52:03.147192001 CEST	49667	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:52:03.149554968 CEST	53	57601	8.8.8.8	192.168.2.3
Mar 31, 2021 20:52:03.175296068 CEST	55439	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:52:03.180140972 CEST	53	56253	8.8.8.8	192.168.2.3
Mar 31, 2021 20:52:03.192837954 CEST	53	49342	8.8.8.8	192.168.2.3
Mar 31, 2021 20:52:03.203757048 CEST	53	49667	8.8.8.8	192.168.2.3
Mar 31, 2021 20:52:03.222490072 CEST	53	55439	8.8.8.8	192.168.2.3
Mar 31, 2021 20:52:03.432455063 CEST	57069	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:52:03.493473053 CEST	53	57069	8.8.8.8	192.168.2.3
Mar 31, 2021 20:52:04.076479912 CEST	57659	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:52:04.126140118 CEST	53	57659	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 31, 2021 20:52:04.442135096 CEST	54717	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:52:04.506119013 CEST	53	54717	8.8.8.8	192.168.2.3
Mar 31, 2021 20:52:04.550143003 CEST	63975	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:52:04.615253925 CEST	53	63975	8.8.8.8	192.168.2.3
Mar 31, 2021 20:52:04.893630028 CEST	56639	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:52:04.940596104 CEST	53	56639	8.8.8.8	192.168.2.3
Mar 31, 2021 20:52:05.622042894 CEST	63975	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:52:05.683562040 CEST	53	63975	8.8.8.8	192.168.2.3
Mar 31, 2021 20:52:06.693169117 CEST	63975	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:52:06.747278929 CEST	53	63975	8.8.8.8	192.168.2.3
Mar 31, 2021 20:52:08.708560944 CEST	63975	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:52:08.754580021 CEST	53	63975	8.8.8.8	192.168.2.3
Mar 31, 2021 20:52:12.724536896 CEST	63975	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:52:12.788995981 CEST	53	63975	8.8.8.8	192.168.2.3
Mar 31, 2021 20:52:16.352564096 CEST	51856	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:52:16.403296947 CEST	56546	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:52:16.417663097 CEST	53	51856	8.8.8.8	192.168.2.3
Mar 31, 2021 20:52:16.467612982 CEST	53	56546	8.8.8.8	192.168.2.3
Mar 31, 2021 20:52:18.114768028 CEST	62152	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:52:18.176908016 CEST	53	62152	8.8.8.8	192.168.2.3
Mar 31, 2021 20:52:24.928836107 CEST	53470	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:52:24.974698067 CEST	53	53470	8.8.8.8	192.168.2.3
Mar 31, 2021 20:52:27.866569042 CEST	56446	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:52:27.924967051 CEST	53	56446	8.8.8.8	192.168.2.3
Mar 31, 2021 20:52:55.302460909 CEST	59631	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:52:55.378180981 CEST	53	59631	8.8.8.8	192.168.2.3
Mar 31, 2021 20:52:55.506390095 CEST	55515	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:52:55.568317890 CEST	53	55515	8.8.8.8	192.168.2.3
Mar 31, 2021 20:52:55.745435953 CEST	64547	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:52:55.809951067 CEST	53	64547	8.8.8.8	192.168.2.3
Mar 31, 2021 20:52:58.558541059 CEST	51759	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:52:58.614609003 CEST	53	51759	8.8.8.8	192.168.2.3
Mar 31, 2021 20:53:00.919732094 CEST	59207	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:53:00.977323055 CEST	53	59207	8.8.8.8	192.168.2.3
Mar 31, 2021 20:53:03.188898087 CEST	54269	53	192.168.2.3	8.8.8.8
Mar 31, 2021 20:53:03.259339094 CEST	53	54269	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 31, 2021 20:51:16.943938017 CEST	192.168.2.3	8.8.8.8	0xeb39	Standard query (0)	www.foothillsvaccineclinic.com	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:17.614217043 CEST	192.168.2.3	8.8.8.8	0xca0f	Standard query (0)	static.parastorage.com	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:17.632236958 CEST	192.168.2.3	8.8.8.8	0x2a67	Standard query (0)	polyfill.io	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:18.425321102 CEST	192.168.2.3	8.8.8.8	0x8f20	Standard query (0)	frog.wix.com	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:20.861649990 CEST	192.168.2.3	8.8.8.8	0x29e3	Standard query (0)	en.wix.com	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:21.256818056 CEST	192.168.2.3	8.8.8.8	0x3ed7	Standard query (0)	www.wix.com	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:22.401583910 CEST	192.168.2.3	8.8.8.8	0x40d1	Standard query (0)	fast.fonts.com	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:22.444768906 CEST	192.168.2.3	8.8.8.8	0x9485	Standard query (0)	browser.sentry-cdn.com	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:23.019530058 CEST	192.168.2.3	8.8.8.8	0xd3ea	Standard query (0)	siteassets.parastorage.com	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:27.027640104 CEST	192.168.2.3	8.8.8.8	0x5c01	Standard query (0)	static.wixstatic.com	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:30.364800930 CEST	192.168.2.3	8.8.8.8	0xd66c	Standard query (0)	4382365.fls.doubleclick.net	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:30.469827890 CEST	192.168.2.3	8.8.8.8	0xce50	Standard query (0)	s.pinimg.com	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:30.492784977 CEST	192.168.2.3	8.8.8.8	0xb973	Standard query (0)	cdn.taboola.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 31, 2021 20:51:30.523822069 CEST	192.168.2.3	8.8.8.8	0x14c5	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:31.133421898 CEST	192.168.2.3	8.8.8.8	0x4293	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:31.185112953 CEST	192.168.2.3	8.8.8.8	0xf303	Standard query (0)	ob.cheqzone.com	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:33.068571091 CEST	192.168.2.3	8.8.8.8	0x77cd	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:33.135236025 CEST	192.168.2.3	8.8.8.8	0x9217	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:33.417886972 CEST	192.168.2.3	8.8.8.8	0x6051	Standard query (0)	trc.taboola.com	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:33.428091049 CEST	192.168.2.3	8.8.8.8	0x2a85	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:33.838910103 CEST	192.168.2.3	8.8.8.8	0x5f90	Standard query (0)	obs.cheqzone.com	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:33.849868059 CEST	192.168.2.3	8.8.8.8	0xcaf7	Standard query (0)	www.google.ch	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:33.983583927 CEST	192.168.2.3	8.8.8.8	0xa2c0	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:34.089498997 CEST	192.168.2.3	8.8.8.8	0xec4a	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:34.404982090 CEST	192.168.2.3	8.8.8.8	0xb044	Standard query (0)	adservice.google.ch	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:34.655558109 CEST	192.168.2.3	8.8.8.8	0xa01	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:34.908627033 CEST	192.168.2.3	8.8.8.8	0x7793	Standard query (0)	trc-events.taboola.com	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:35.162910938 CEST	192.168.2.3	8.8.8.8	0xecca	Standard query (0)	static.parastorage.com	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:35.213906050 CEST	192.168.2.3	8.8.8.8	0x9b23	Standard query (0)	cx.atdmt.com	A (IP address)	IN (0x0001)
Mar 31, 2021 20:52:04.442135096 CEST	192.168.2.3	8.8.8.8	0x8f0f	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Mar 31, 2021 20:52:04.893630028 CEST	192.168.2.3	8.8.8.8	0x2e7b	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)
Mar 31, 2021 20:52:16.403296947 CEST	192.168.2.3	8.8.8.8	0x482	Standard query (0)	2542116.fls.doubleclick.net	A (IP address)	IN (0x0001)
Mar 31, 2021 20:52:55.302460909 CEST	192.168.2.3	8.8.8.8	0xc6fe	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Mar 31, 2021 20:52:55.745435953 CEST	192.168.2.3	8.8.8.8	0x91d1	Standard query (0)	www.google.ch	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 31, 2021 20:51:17.018285990 CEST	8.8.8.8	192.168.2.3	0xeb39	No error (0)	www.foothillsvaccineclinic.com	www218.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:17.018285990 CEST	8.8.8.8	192.168.2.3	0xeb39	No error (0)	www218.wixdns.net	balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:17.018285990 CEST	8.8.8.8	192.168.2.3	0xeb39	No error (0)	balancer.wixdns.net	5f36b111-balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:17.018285990 CEST	8.8.8.8	192.168.2.3	0xeb39	No error (0)	5f36b111-balancer.wixdns.net	td-balancer-euw2-6-109.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:17.018285990 CEST	8.8.8.8	192.168.2.3	0xeb39	No error (0)	td-balancer-euw2-6-109.wixdns.net		35.246.6.109	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:17.671493053 CEST	8.8.8.8	192.168.2.3	0xca0f	No error (0)	static.parastorage.com	n2.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:17.680982113 CEST	8.8.8.8	192.168.2.3	0x2a67	No error (0)	polyfill.io		151.101.130.109	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:17.680982113 CEST	8.8.8.8	192.168.2.3	0x2a67	No error (0)	polyfill.io		151.101.2.109	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:17.680982113 CEST	8.8.8.8	192.168.2.3	0x2a67	No error (0)	polyfill.io		151.101.194.109	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:17.680982113 CEST	8.8.8.8	192.168.2.3	0x2a67	No error (0)	polyfill.io		151.101.66.109	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 31, 2021 20:51:18.471260071 CEST	8.8.8.8	192.168.2.3	0x8f20	No error (0)	frog.wix.com	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:18.471260071 CEST	8.8.8.8	192.168.2.3	0x8f20	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		34.202.131.150	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:18.471260071 CEST	8.8.8.8	192.168.2.3	0x8f20	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		34.199.153.199	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:18.471260071 CEST	8.8.8.8	192.168.2.3	0x8f20	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		34.235.49.255	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:18.471260071 CEST	8.8.8.8	192.168.2.3	0x8f20	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		54.84.69.181	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:18.471260071 CEST	8.8.8.8	192.168.2.3	0x8f20	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		34.227.36.18	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:18.471260071 CEST	8.8.8.8	192.168.2.3	0x8f20	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		3.212.73.210	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:18.471260071 CEST	8.8.8.8	192.168.2.3	0x8f20	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		3.94.177.97	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:18.471260071 CEST	8.8.8.8	192.168.2.3	0x8f20	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		54.236.107.104	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:20.933553934 CEST	8.8.8.8	192.168.2.3	0x29e3	No error (0)	en.wix.com	username.wix.com		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:20.933553934 CEST	8.8.8.8	192.168.2.3	0x29e3	No error (0)	username.wix.com	5f36b111-username.wix.com		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:20.933553934 CEST	8.8.8.8	192.168.2.3	0x29e3	No error (0)	5f36b111-username.wix.com	td-username-euw2-6-109.wix.com		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:20.933553934 CEST	8.8.8.8	192.168.2.3	0x29e3	No error (0)	td-username-euw2-6-109.wix.com		35.246.6.109	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:21.320404053 CEST	8.8.8.8	192.168.2.3	0x3ed7	No error (0)	www.wix.com	wwworigin.wix.com		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:21.320404053 CEST	8.8.8.8	192.168.2.3	0x3ed7	No error (0)	wwworigin.wix.com	179.www.sv5.wix.com		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:21.320404053 CEST	8.8.8.8	192.168.2.3	0x3ed7	No error (0)	179.www.sv5.wix.com		185.230.61.179	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:22.462054968 CEST	8.8.8.8	192.168.2.3	0x40d1	No error (0)	fast.fonts.com		104.17.70.188	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:22.462054968 CEST	8.8.8.8	192.168.2.3	0x40d1	No error (0)	fast.fonts.com		104.17.71.188	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:22.493501902 CEST	8.8.8.8	192.168.2.3	0x9485	No error (0)	browser.sentry-cdn.com		151.101.194.217	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 31, 2021 20:51:22.493501902 CEST	8.8.8.8	192.168.2.3	0x9485	No error (0)	browser.sentry-cdn.com		151.101.66.217	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:22.493501902 CEST	8.8.8.8	192.168.2.3	0x9485	No error (0)	browser.sentry-cdn.com		151.101.2.217	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:22.493501902 CEST	8.8.8.8	192.168.2.3	0x9485	No error (0)	browser.sentry-cdn.com		151.101.130.217	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:23.090606928 CEST	8.8.8.8	192.168.2.3	0xd3ea	No error (0)	siteassets.parastorage.com	static.parastorage.com		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:23.090606928 CEST	8.8.8.8	192.168.2.3	0xd3ea	No error (0)	static.parastorage.com	n2.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:27.083897114 CEST	8.8.8.8	192.168.2.3	0x5c01	No error (0)	static.wixstatic.com	gcp.media-router.wixstatic.com		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:27.083897114 CEST	8.8.8.8	192.168.2.3	0x5c01	No error (0)	gcp.media-router.wixstatic.com		34.102.176.152	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:30.427361965 CEST	8.8.8.8	192.168.2.3	0xd66c	No error (0)	4382365.fls.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:30.427361965 CEST	8.8.8.8	192.168.2.3	0xd66c	No error (0)	dart.l.doubleclick.net		216.58.215.230	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:30.530145884 CEST	8.8.8.8	192.168.2.3	0xce50	No error (0)	s.pinimg.com	s-pinimg-com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:30.530145884 CEST	8.8.8.8	192.168.2.3	0xce50	No error (0)	s-pinimg-com.gslb.pinterest.com	2-01-37d2-0006.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:30.540040970 CEST	8.8.8.8	192.168.2.3	0xb973	No error (0)	cdn.taboola.com	tls13.taboola.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:30.540040970 CEST	8.8.8.8	192.168.2.3	0xb973	No error (0)	tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:30.540040970 CEST	8.8.8.8	192.168.2.3	0xb973	No error (0)	tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:30.540040970 CEST	8.8.8.8	192.168.2.3	0xb973	No error (0)	tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:30.540040970 CEST	8.8.8.8	192.168.2.3	0xb973	No error (0)	tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:30.584112883 CEST	8.8.8.8	192.168.2.3	0x14c5	No error (0)	snap.licdn.com	wildcard.licdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:31.193300009 CEST	8.8.8.8	192.168.2.3	0x4293	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:31.193300009 CEST	8.8.8.8	192.168.2.3	0x4293	No error (0)	scontent.xx.fbcdn.net		185.60.216.19	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:31.245342970 CEST	8.8.8.8	192.168.2.3	0xf303	No error (0)	ob.cheqzone.com	cheqzone2.b-cdn.net		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:31.245342970 CEST	8.8.8.8	192.168.2.3	0xf303	No error (0)	cheqzone2.b-cdn.net		89.187.165.193	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:33.125242949 CEST	8.8.8.8	192.168.2.3	0x77cd	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:33.125242949 CEST	8.8.8.8	192.168.2.3	0x77cd	No error (0)	stats.l.doubleclick.net		108.177.15.155	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:33.125242949 CEST	8.8.8.8	192.168.2.3	0x77cd	No error (0)	stats.l.doubleclick.net		108.177.15.156	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:33.125242949 CEST	8.8.8.8	192.168.2.3	0x77cd	No error (0)	stats.l.doubleclick.net		108.177.15.154	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:33.125242949 CEST	8.8.8.8	192.168.2.3	0x77cd	No error (0)	stats.l.doubleclick.net		108.177.15.157	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 31, 2021 20:51:33.202090979 CEST	8.8.8.8	192.168.2.3	0x9217	No error (0)	googleads.g.doubleclick.net		172.217.168.66	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:33.464857101 CEST	8.8.8.8	192.168.2.3	0x6051	No error (0)	trc.taboola.com	tls13.taboola.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:33.464857101 CEST	8.8.8.8	192.168.2.3	0x6051	No error (0)	tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:33.464857101 CEST	8.8.8.8	192.168.2.3	0x6051	No error (0)	tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:33.464857101 CEST	8.8.8.8	192.168.2.3	0x6051	No error (0)	tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:33.464857101 CEST	8.8.8.8	192.168.2.3	0x6051	No error (0)	tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:33.496385098 CEST	8.8.8.8	192.168.2.3	0x2a85	No error (0)	px.ads.linkedin.com	mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:33.496385098 CEST	8.8.8.8	192.168.2.3	0x2a85	No error (0)	mix.linkedin.com	glb-na.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:33.496385098 CEST	8.8.8.8	192.168.2.3	0x2a85	No error (0)	glb-na.mix.linkedin.com	pop-eda6.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:33.496385098 CEST	8.8.8.8	192.168.2.3	0x2a85	No error (0)	pop-eda6.mix.linkedin.com		108.174.11.69	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:33.900602102 CEST	8.8.8.8	192.168.2.3	0x5f90	No error (0)	obs.cheqzone.com		54.83.110.109	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:33.900602102 CEST	8.8.8.8	192.168.2.3	0x5f90	No error (0)	obs.cheqzone.com		34.199.234.25	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:33.900602102 CEST	8.8.8.8	192.168.2.3	0x5f90	No error (0)	obs.cheqzone.com		35.172.245.152	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:33.900602102 CEST	8.8.8.8	192.168.2.3	0x5f90	No error (0)	obs.cheqzone.com		52.45.196.192	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:33.900602102 CEST	8.8.8.8	192.168.2.3	0x5f90	No error (0)	obs.cheqzone.com		50.16.211.97	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:33.900602102 CEST	8.8.8.8	192.168.2.3	0x5f90	No error (0)	obs.cheqzone.com		3.227.190.204	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:33.904436111 CEST	8.8.8.8	192.168.2.3	0xcaf7	No error (0)	www.google.ch		172.217.168.67	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:34.046838045 CEST	8.8.8.8	192.168.2.3	0xa2c0	No error (0)	www.google.co.uk		216.58.215.227	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:34.135597944 CEST	8.8.8.8	192.168.2.3	0xec4a	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:34.484647989 CEST	8.8.8.8	192.168.2.3	0xb044	No error (0)	adservice.google.ch	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:34.484647989 CEST	8.8.8.8	192.168.2.3	0xb044	No error (0)	pagead46.l.doubleclick.net		172.217.168.34	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:34.712714911 CEST	8.8.8.8	192.168.2.3	0xa01	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:34.712714911 CEST	8.8.8.8	192.168.2.3	0xa01	No error (0)	star-mini.c10r.facebook.com		185.60.216.35	A (IP address)	IN (0x0001)
Mar 31, 2021 20:51:34.968578100 CEST	8.8.8.8	192.168.2.3	0x7793	No error (0)	trc-events.taboola.com	am-trc-events.taboola.com		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:34.968578100 CEST	8.8.8.8	192.168.2.3	0x7793	No error (0)	am-trc-events.taboola.com	am-vip001.taboola.com		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:34.968578100 CEST	8.8.8.8	192.168.2.3	0x7793	No error (0)	am-vip001.taboola.com		141.226.228.48	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 31, 2021 20:51:35.221936941 CEST	8.8.8.8	192.168.2.3	0xecca	No error (0)	static.parastorage.com	n2.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:35.270142078 CEST	8.8.8.8	192.168.2.3	0x9b23	No error (0)	cx.atdmt.com	atlas.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:51:35.270142078 CEST	8.8.8.8	192.168.2.3	0x9b23	No error (0)	atlas.c10r.facebook.com		185.60.216.6	A (IP address)	IN (0x0001)
Mar 31, 2021 20:52:04.506119013 CEST	8.8.8.8	192.168.2.3	0x8f0f	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:52:04.506119013 CEST	8.8.8.8	192.168.2.3	0x8f0f	No error (0)	stats.l.doubleclick.net		108.177.15.154	A (IP address)	IN (0x0001)
Mar 31, 2021 20:52:04.506119013 CEST	8.8.8.8	192.168.2.3	0x8f0f	No error (0)	stats.l.doubleclick.net		108.177.15.157	A (IP address)	IN (0x0001)
Mar 31, 2021 20:52:04.506119013 CEST	8.8.8.8	192.168.2.3	0x8f0f	No error (0)	stats.l.doubleclick.net		108.177.15.155	A (IP address)	IN (0x0001)
Mar 31, 2021 20:52:04.506119013 CEST	8.8.8.8	192.168.2.3	0x8f0f	No error (0)	stats.l.doubleclick.net		108.177.15.156	A (IP address)	IN (0x0001)
Mar 31, 2021 20:52:04.940596104 CEST	8.8.8.8	192.168.2.3	0x2e7b	No error (0)	www.google.co.uk		216.58.215.227	A (IP address)	IN (0x0001)
Mar 31, 2021 20:52:16.467612982 CEST	8.8.8.8	192.168.2.3	0x482	No error (0)	2542116.fls.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 20:52:16.467612982 CEST	8.8.8.8	192.168.2.3	0x482	No error (0)	dart.l.doubleclick.net		216.58.215.230	A (IP address)	IN (0x0001)
Mar 31, 2021 20:52:55.378180981 CEST	8.8.8.8	192.168.2.3	0xc6fe	No error (0)	googleads.g.doubleclick.net		172.217.168.66	A (IP address)	IN (0x0001)
Mar 31, 2021 20:52:55.809951067 CEST	8.8.8.8	192.168.2.3	0x91d1	No error (0)	www.google.ch		172.217.168.67	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
Mar 31, 2021 20:51:17.159457922 CEST	35.246.6.109	443	192.168.2.3	49714	CN=foothillsvaccineclinic.com CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Sat Mar 13 01:00:00 CET 2021 Thu Jan 01 01:00:00 CET 2004 Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Sat Jun 12 01:59:59 CEST 2021 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 31, 2021 20:51:17.163932085 CEST	35.246.6.109	443	192.168.2.3	49713	CN=foothillsvaccineclinic.com CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Sat Mar 13 01:00:00 CET 2021 Thu Jan 01 01:00:00 CET 2004 Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Sat Jun 12 01:59:59 CEST 2021 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
Mar 31, 2021 20:51:17.773564100 CEST	151.101.130.109	443	192.168.2.3	49719	CN=f3.shared.global.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 Mar 25 16:40:23 CET 2021 Wed Aug 19 02:00:00 CEST 2015	Sat Mar 26 14:08:54 CET 2022 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		
Mar 31, 2021 20:51:17.823719978 CEST	151.101.130.109	443	192.168.2.3	49718	CN=f3.shared.global.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 Mar 25 16:40:23 CET 2021 Wed Aug 19 02:00:00 CEST 2015	Sat Mar 26 14:08:54 CET 2022 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 31, 2021 20:51:18.849613905 CEST	34.202.131.150	443	192.168.2.3	49724	CN=*.wix.com CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Thu Dec 17 01:00:00 CET 2020 Thu Jan 01 01:00:00 CET 2004 Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Wed Jun 16 01:59:59 CEST 2021 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
Mar 31, 2021 20:51:18.851020098 CEST	34.202.131.150	443	192.168.2.3	49725	CN=*.wix.com CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Thu Dec 17 01:00:00 CET 2020 Thu Jan 01 01:00:00 CET 2004 Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Wed Jun 16 01:59:59 CEST 2021 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 31, 2021 20:51:21.087480068 CEST	35.246.6.109	443	192.168.2.3	49727	CN=*.wix.com CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Thu Dec 17 01:00:00 CET 2020 Thu Jan 01 01:00:00 CET 2004 Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Wed Jun 16 01:59:59 CEST 2021 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
Mar 31, 2021 20:51:21.090179920 CEST	35.246.6.109	443	192.168.2.3	49726	CN=*.wix.com CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Thu Dec 17 01:00:00 CET 2020 Thu Jan 01 01:00:00 CET 2004 Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Wed Jun 16 01:59:59 CEST 2021 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 31, 2021 20:51:21.747324944 CEST	185.230.61.179	443	192.168.2.3	49728	CN=*.wix.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Dec 17 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Wed Jun 16 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Mar 31, 2021 20:51:21.749438047 CEST	185.230.61.179	443	192.168.2.3	49729	CN=*.wix.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Dec 17 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Wed Jun 16 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Mar 31, 2021 20:51:22.551320076 CEST	104.17.70.188	443	192.168.2.3	49731	CN=*.fonts.com, O=Monotype Imaging Inc., L=Woburn, ST=Massachusetts, 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	Mon Nov 02 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Wed Nov 17 00:59:59 CET 2021 Wed Mar 08 13:00:00 CET 2023	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 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		
Mar 31, 2021 20:51:22.555685043 CEST	104.17.70.188	443	192.168.2.3	49732	CN=*.fonts.com, O=Monotype Imaging Inc., L=Woburn, ST=Massachusetts, 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	Mon Nov 02 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Wed Nov 17 00:59:59 CET 2021 Wed Mar 08 13:00:00 CET 2023	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		
Mar 31, 2021 20:51:22.593099117 CEST	151.101.194.217	443	192.168.2.3	49734	CN=*.sentry-cdn.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Mon Feb 22 20:39:57 CET 2021 Tue Jul 28 02:00:00 CEST 2020	Sat Mar 26 20:39:57 CET 2022 Sun Mar 18 01:00:00 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Mar 31, 2021 20:51:22.626142025 CEST	151.101.194.217	443	192.168.2.3	49733	CN=*.sentry-cdn.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Mon Feb 22 20:39:57 CET 2021 Tue Jul 28 02:00:00 CEST 2020	Sat Mar 26 20:39:57 CET 2022 Sun Mar 18 01:00:00 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Mar 31, 2021 20:51:27.164535046 CEST	34.102.176.152	443	192.168.2.3	49739	CN=*.wixstatic.com CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Feb 05 01:00:00 CET 2021 Thu Jan 01 01:00:00 CET 2004 Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Thu Aug 05 01:59:59 CEST 2021 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
Mar 31, 2021 20:51:27.168436050 CEST	34.102.176.152	443	192.168.2.3	49740	CN=*.wixstatic.com CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Feb 05 01:00:00 CET 2021 Thu Jan 01 01:00:00 CET 2004 Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Thu Aug 05 01:59:59 CEST 2021 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
Mar 31, 2021 20:51:30.549418926 CEST	216.58.215.230	443	192.168.2.3	49748	CN=*.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 Mar 16 20:28:03 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jun 08 21:28:02 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		
Mar 31, 2021 20:51:30.576155901 CEST	216.58.215.230	443	192.168.2.3	49749	CN=*.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 Mar 16 20:28:03 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jun 08 21:28:02 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		
Mar 31, 2021 20:51:31.120842934 CEST	151.101.1.44	443	192.168.2.3	49752	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020	Mon Dec 27 00:59:59 CET 2021 Tue Sep 24 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

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 TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Mar 31, 2021 20:51:31.125278950 CEST	151.101.1.44	443	192.168.2.3	49753	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020	Mon Dec 27 00:59:59 CET 2021 Tue Sep 24 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 TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Mar 31, 2021 20:51:31.377464056 CEST	185.60.216.19	443	192.168.2.3	49758	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	Wed Feb 10 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Tue May 11 01:59:59 CEST 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		
Mar 31, 2021 20:51:31.381381035 CEST	185.60.216.19	443	192.168.2.3	49759	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	Wed Feb 10 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Tue May 11 01:59:59 CEST 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		
Mar 31, 2021 20:51:31.407850027 CEST	89.187.165.193	443	192.168.2.3	49760	CN=ob.cheqzone.com CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co. CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Mar 10 09:08:35 CET 2021 Wed Oct 07 21:21:40 CEST 2020 Sat Sep 30 23:12:19 CEST 2000	Tue Jun 08 10:08:35 CEST 2021 Wed Sep 29 21:21:40 CEST 2021 Thu Sep 30 16:01:15 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		
					CN=DST Root CA X3, O=Digital Signature Trust Co.	CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Sep 30 23:12:19 CEST 2000	Thu Sep 30 16:01:15 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 31, 2021 20:51:31.408140898 CEST	89.187.165.193	443	192.168.2.3	49761	CN=ob.cheqzone.com CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co. CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Mar 10 09:08:35 CET 2021 Wed Oct 07 21:21:40 CEST 2020 Sat Sep 30 23:12:19 CEST 2000	Tue Jun 08 10:08:35 CEST 2021 Wed Sep 29 21:21:40 CEST 2021 Thu Sep 30 16:01:15 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		
					CN=DST Root CA X3, O=Digital Signature Trust Co.	CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Sep 30 23:12:19 CEST 2000	Thu Sep 30 16:01:15 CEST 2021		
Mar 31, 2021 20:51:33.230917931 CEST	108.177.15.155	443	192.168.2.3	49763	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	Thu Mar 11 15:54:02 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Thu Jun 03 16:54:01 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		
Mar 31, 2021 20:51:33.231602907 CEST	108.177.15.155	443	192.168.2.3	49762	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	Thu Mar 11 15:54:02 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Thu Jun 03 16:54:01 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		
Mar 31, 2021 20:51:33.330404043 CEST	172.217.168.66	443	192.168.2.3	49764	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	Thu Mar 11 15:54:02 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Thu Jun 03 16:54:01 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		
Mar 31, 2021 20:51:33.331016064 CEST	172.217.168.66	443	192.168.2.3	49765	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	Thu Mar 11 15:54:02 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Thu Jun 03 16:54:01 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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		
Mar 31, 2021 20:51:33.582957029 CEST	151.101.1.44	443	192.168.2.3	49767	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020	Mon Dec 27 00:59:59 CET 2021 Tue Sep 24 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 TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Mar 31, 2021 20:51:33.583758116 CEST	151.101.1.44	443	192.168.2.3	49766	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020	Mon Dec 27 00:59:59 CET 2021 Tue Sep 24 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 TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Mar 31, 2021 20:51:33.866369009 CEST	108.174.11.69	443	192.168.2.3	49769	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		
Mar 31, 2021 20:51:33.868235111 CEST	108.174.11.69	443	192.168.2.3	49768	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		
Mar 31, 2021 20:51:34.021615028 CEST	172.217.168.67	443	192.168.2.3	49772	CN=*.google.ch, 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	Thu Mar 11 16:02:00 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Thu Jun 03 17:01:59 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 31, 2021 20:51:34.021677017 CEST	172.217.168.67	443	192.168.2.3	49773	CN=*.google.ch, 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	Thu Mar 11 16:02:00 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Thu Jun 03 17:01:59 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		
Mar 31, 2021 20:51:34.157655001 CEST	54.83.110.109	443	192.168.2.3	49770	CN=obs.cheqzone.com 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.	Sun Feb 14 10:28:10 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Sat May 15 11:28:10 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		
Mar 31, 2021 20:51:34.157974005 CEST	54.83.110.109	443	192.168.2.3	49771	CN=obs.cheqzone.com 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.	Sun Feb 14 10:28:10 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Sat May 15 11:28:10 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		
Mar 31, 2021 20:51:34.794065952 CEST	185.60.216.35	443	192.168.2.3	49787	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	Wed Feb 10 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Tue May 11 01:59:59 CEST 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		
Mar 31, 2021 20:51:34.794107914 CEST	185.60.216.35	443	192.168.2.3	49786	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	Wed Feb 10 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Tue May 11 01:59:59 CEST 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 31, 2021 20:51:35.071870089 CEST	141.226.228.48	443	192.168.2.3	49789	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020	Mon Dec 27 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
Mar 31, 2021 20:51:35.072899103 CEST	141.226.228.48	443	192.168.2.3	49790	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020	Mon Dec 27 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
Mar 31, 2021 20:51:35.355220079 CEST	185.60.216.6	443	192.168.2.3	49792	CN=*.atlassolutions.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	Fri Jan 29 01:00:00 CET 2021	Thu Apr 29 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=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		
Mar 31, 2021 20:51:35.356122971 CEST	185.60.216.6	443	192.168.2.3	49793	CN=*.atlassolutions.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	Fri Jan 29 01:00:00 CET 2021	Thu Apr 29 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=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		
Mar 31, 2021 20:52:04.624672890 CEST	108.177.15.154	443	192.168.2.3	49822	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	Thu Mar 11 15:54:02 CET 2021	Thu Jun 03 16:54:01 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=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
Mar 31, 2021 20:52:04.626200914 CEST	108.177.15.154	443	192.168.2.3	49821	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	Thu Mar 11 15:54:02 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Thu Jun 03 16:54:01 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		
Mar 31, 2021 20:52:16.619580030 CEST	216.58.215.230	443	192.168.2.3	49828	CN=*.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 Mar 16 20:28:03 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jun 08 21:28:02 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		
Mar 31, 2021 20:52:16.662074089 CEST	216.58.215.230	443	192.168.2.3	49827	CN=*.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 Mar 16 20:28:03 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jun 08 21:28:02 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		
Mar 31, 2021 20:52:55.510157108 CEST	172.217.168.66	443	192.168.2.3	49838	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	Thu Mar 11 15:54:02 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Thu Jun 03 16:54:01 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		
Mar 31, 2021 20:52:55.511009932 CEST	172.217.168.66	443	192.168.2.3	49839	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	Thu Mar 11 15:54:02 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Thu Jun 03 16:54:01 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
Mar 31, 2021 20:52:55.929136038 CEST	172.217.168.67	443	192.168.2.3	49842	CN=*.google.ch, 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	Thu Mar 11 16:02:00 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Thu Jun 03 17:01:59 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		
Mar 31, 2021 20:52:55.936229944 CEST	172.217.168.67	443	192.168.2.3	49843	CN=*.google.ch, 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	Thu Mar 11 16:02:00 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Thu Jun 03 17:01:59 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		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5620 Parent PID: 792

General

Start time:	20:51:14
Start date:	31/03/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff672360000
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: 5556 Parent PID: 5620

General

Start time:	20:51:15
Start date:	31/03/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5620 CREDAT:17410 /prefetch:2
Imagebase:	0x3d0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 6664 Parent PID: 5620

General

Start time:	20:52:00
Start date:	31/03/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5620 CREDAT:82966 /prefetch:2
Imagebase:	0x3d0000
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

Disassembly