

JOeSandbox Cloud BASIC



ID: 332393

Cookbook: browseurl.jbs

Time: 20:48:43

Date: 18/12/2020

Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents	2
Analysis Report https://www.305covidtest.com/	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Yara Overview	4
Sigma Overview	4
Signature Overview	4
Mitre Att&ck Matrix	5
Behavior Graph	5
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	7
URLs	7
Domains and IPs	8
Contacted Domains	8
Contacted URLs	8
URLs from Memory and Binaries	9
Contacted IPs	11
Public	11
General Information	12
Simulations	13
Behavior and APIs	13
Joe Sandbox View / Context	13
IPs	13
Domains	13
ASN	13
JA3 Fingerprints	14
Dropped Files	14
Created / dropped Files	14
Static File Info	46
No static file info	46
Network Behavior	46
Network Port Distribution	46
TCP Packets	47
UDP Packets	48
DNS Queries	50
DNS Answers	51
HTTPS Packets	53
Code Manipulations	65
Statistics	65
Behavior	65
System Behavior	65
Analysis Process: iexplore.exe PID: 5228 Parent PID: 792	65
General	65
File Activities	66
Registry Activities	66

Analysis Process: iexplore.exe PID: 5532 Parent PID: 5228	66
General	66
File Activities	66
Registry Activities	66
Disassembly	66

Analysis Report <https://www.305covidtest.com/>

Overview

General Information

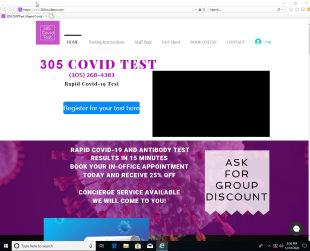
Sample URL:

<http://https://www.305covidtest.com/>

Analysis ID:

332393

Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Score:

1

Range:

0 - 100

Whitelisted:

false

Confidence:

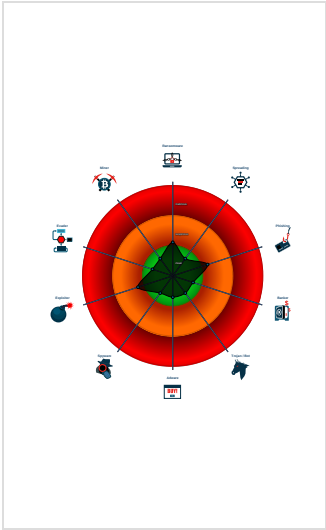
80%

Signatures

Allocates a big amount of memory (p...

Found iframes

Classification



Startup

- System is w10x64
-  iexplore.exe (PID: 5228 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
 -  iexplore.exe (PID: 5532 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5228 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- Phishing
- Software Vulnerabilities
- Networking
- System Summary



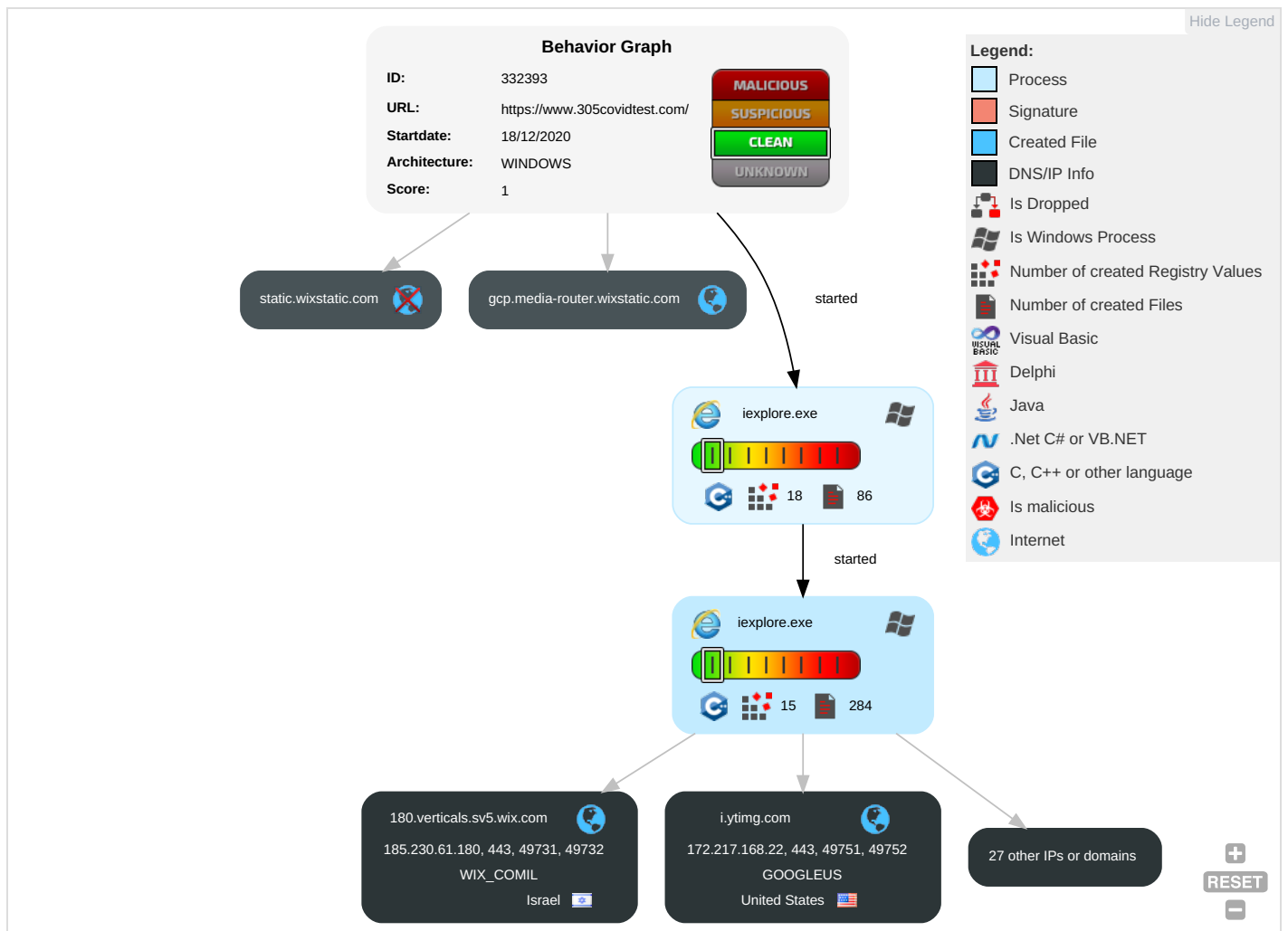
Click to jump to signature section

There are no malicious signatures, [click here to show all signatures](#).

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Drive-by Compromise 1	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Extra Window Memory Injection 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups

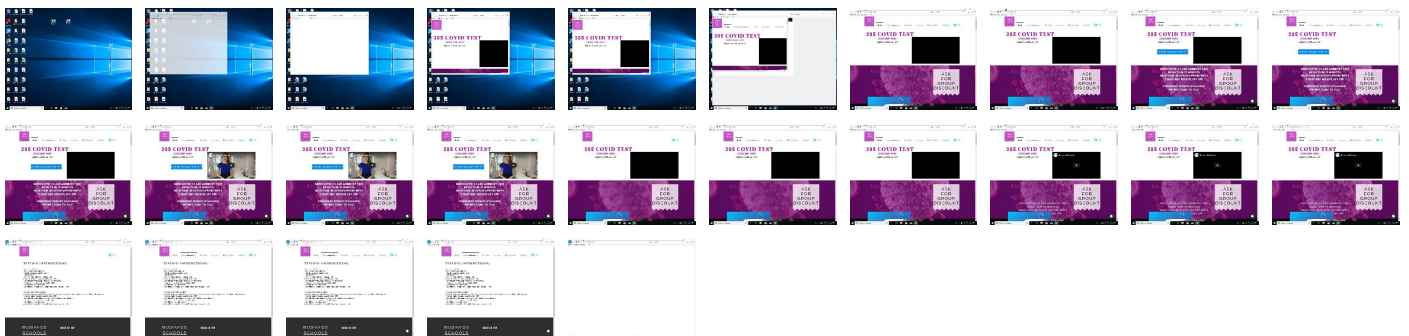
Behavior Graph

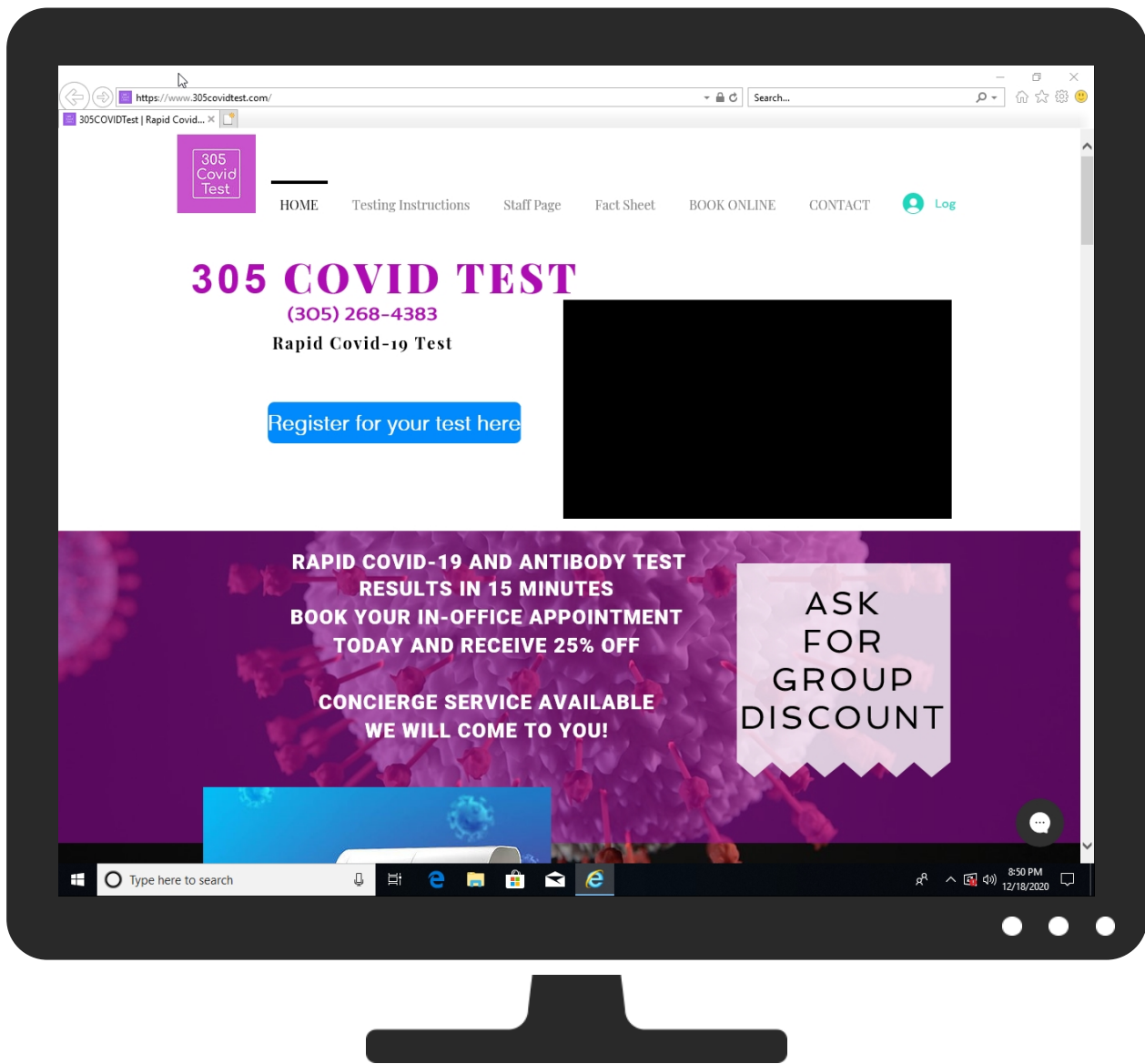


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://www.305covidtest.com/	0%	Virustotal		Browse
http://https://www.305covidtest.com/	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
td-balancer-euw2-6-109.wixdns.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://my-url/video.webm	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://www.305covidtest.com/registration-form	0%	Avira URL Cloud	safe	
http://polymer.github.io/AUTHORS.txt	0%	Avira URL Cloud	safe	
http://https://www.305covidtest.com/2ting-instructionsiteRevision%22%3A%22610%22%2C%22consentPolicy%22%3A%7	0%	Avira URL Cloud	safe	
http://https://www.305covidtest.com/testing-instructionsNTesting	0%	Avira URL Cloud	safe	
http://polymer.github.io/PATENTS.txt	0%	Avira URL Cloud	safe	
http://https://d8ec26b2-28d6-41f2-b06e-8c76091f9420.static.pub.wix-code.com/static/v2/69b79778-3e4a-49a0-b4	0%	Avira URL Cloud	safe	
http://https://drafts.fxtf.org/geometry/#dictdef-domrectinit	0%	Avira URL Cloud	safe	
http://polymer.github.io/LICENSE.txt	0%	Avira URL Cloud	safe	
http://https://www.305covidtest.com/Root	0%	Avira URL Cloud	safe	
http://https://w3c.github.io/pointerevents/#widl-PointerEvent-isPrimary	0%	Avira URL Cloud	safe	
http://https://drafts.fxtf.org/geometry/#domrectreadonly	0%	Avira URL Cloud	safe	
http://https://recaptcha.net/recaptcha/api.js	0%	Avira URL Cloud	safe	
http://https://browser.sentry-cdn.com/4.6.2/bundle.min.js	0%	Avira URL Cloud	safe	
http://https://browser.sentry-cdn.com/5.7.1/bundle.min.js	0%	Avira URL Cloud	safe	
http://https://www.305covidtest.com/book-online	0%	Avira URL Cloud	safe	
http://my-url/video.mp4	0%	Avira URL Cloud	safe	
http://www.linotype.comhttp://www.linotype.com/fontdesignersNOTIFICATION	0%	Avira URL Cloud	safe	
http://polymer.github.io/CONTRIBUTORS.txt	0%	Avira URL Cloud	safe	
http://jedwatson.github.io/classnames	0%	Avira URL Cloud	safe	
http://https://facebook.github.io/react/docs/top-level-api.html#react.createclass	0%	Avira URL Cloud	safe	
http://https://my-url/video.mp4	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pagead46.l.doubleclick.net	172.217.168.66	true	false		high
td-static-34-96-106-200.parastorage.com	34.96.106.200	true	false		high
browser.sentry-cdn.com	151.101.2.217	true	false	0%, Virustotal, Browse	unknown
td-balancer-euw2-6-109.wixdns.net	35.246.6.109	true	false	0%, Virustotal, Browse	unknown
sentry-nlb-e70282e8a06dcc98.elb.us-east-1.amazonaws.com	52.2.188.208	true	false		high
i.ytimg.com	172.217.168.22	true	false		high
gcp.media-router.wixstatic.com	34.102.176.152	true	false		high
photos-ugc.l.googleusercontent.com	216.58.215.225	true	false		high
wix-engage-visitors-prod-20.firebaseio.com	35.201.97.85	true	false		high
d2rddclowni6h8.cloudfront.net	65.9.68.81	true	false		high
bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com	54.87.207.230	true	false		high
180.verticals.sv5.wix.com	185.230.61.180	true	false		high
yt3.ggpht.com	unknown	unknown	false		high
www.305covidtest.com	unknown	unknown	false		unknown
siteassets.parastorage.com	unknown	unknown	false		high
static.wixstatic.com	unknown	unknown	false		high
d8ec26b2-28d6-41f2-b06e-8c76091f9420.static.pub.wix-code.com	unknown	unknown	false		unknown
engage.wixapps.net	unknown	unknown	false		high
static.doubleclick.net	unknown	unknown	false		high
googleads.g.doubleclick.net	unknown	unknown	false		high
frog.wix.com	unknown	unknown	false		high
sentry.wixpress.com	unknown	unknown	false		high
www.youtube.com	unknown	unknown	false		high
static.parastorage.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.305covidtest.com/testing-instructions	false		unknown
http://https://www.305covidtest.com/	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://player.vimeo.com/api/player.js	wixui.VideoPlayer.chunk[1].js.2.dr	false		high
http://https://my-url/video.webm	wixui.VideoPlayer.chunk[1].js.2.dr	false	Avira URL Cloud: safe	low
http://https://www.305covidtest.com/registration-form	IVS0AW9K.htm.2.dr	false	Avira URL Cloud: safe	unknown
http://https://developer.mozilla.org/en-US/docs/Web/API/CSSRule	wixui.VideoPlayer.chunk[1].js.2.dr	false		high
http://https://github.com/zloirock/core-js	minified[1].js.2.dr	false		high
http://bo.wix.com/bi-catalog-webapp/#/sources/19/events/3	wixui.VideoPlayer.chunk[1].js.2.dr	false		high
https://static.wixstatic.com/media/48ccc5_8e21a7c68c974c6e919f0ecd2533092~mv2.jpg/v1/crop/x_703	IVS0AW9K.htm.2.dr	false		high
https://static.wixstatic.com/media/11062b_8f4c5838a8454b13afa035cdae64621f~mv2_d_5360_3574_s_4_2.jpg	IVS0AW9K.htm.2.dr	false		high
http://youtube.com/streaming/otf/durations/112015	base[1].js.2.dr	false		high
http://https://static.parastorage.com/services/wix-ui-santa/1.1467.0/	viewerComponentService.bundle[1].js.2.dr, dataRefs.bundle.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://static.parastorage.com/services/wix-bolt/1.6850.0	IVS0AW9K.htm.2.dr	false		high
http://https://www.youtube.com	iframe_api[1].js.2.dr, www-widgetapi[1].js.2.dr	false		high
http://https://www.youtube.com/iframe_api	wixui.VideoPlayer.chunk[1].js.2.dr	false		high
http://https://static.parastorage.com/services/tag-manager-client/1.240.0/siteTags.bundle.min.js	IVS0AW9K.htm.2.dr	false		high
http://https://admin.youtube.com	base[1].js.2.dr	false		high
http://static.wixstatic.com/media/139571a1212e4d3d8074041626ba3ed6.jpg	bolt-main-prod-old[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://www.whatwg.org/specs/web-apps/current-work/multipage/comms.html#crossDocumentMessages	wixui.VideoPlayer.chunk[1].js.2.dr	false		high
https://static.wixstatic.com/media/48ccc5_559838b644e94acf903cd64ed867b15b%7Emv2.png/v1/fill/w_32%2C	IVS0AW9K.htm.2.dr	false		high
http://www.redd.it.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://www.305covidtest.com/2ting-instructionsiteRevision%22%3A%22610%22%2C%22consentPolicy%22%3A%7	~DFC8E9EC2B4AB47E72.TMP.1.dr	false	Avira URL Cloud: safe	unknown
http://www.linotype.com/fontdesigners	b7693a83-b861-4aa6-85e0-9ecf676bc4d6[1].eot.2.dr	false		high
http://https://www.305covidtest.com/2	2[1].htm.2.dr	false		unknown
http://https://www.youtube.com/generate_204?cpn=	base[1].js.2.dr	false		high
http://https://www.305covidtest.com/testing-instructionsNTesting	{94B8BF3D-41B5-11EB-90E4-ECF4B862DED}.dat.1.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://https://github.com/marcj/css-element-queries/blob/1.0.2/src/ElementQueries.js#L340-L393	wixui.VideoPlayer.chunk[1].js.2.dr	false		high
http://https://d8ec26b2-28d6-41f2-b06e-8c76091f9420.static.pub.wix-code.com/static/v2/69b79778-3e4a-49a0-b4	xfeqr[1].js.2.dr, h5mgj[1].js.2.dr	false	Avira URL Cloud: safe	unknown
http://https://static.parastorage.com/unpkg/requirejs-bolt	IVS0AW9K.htm.2.dr	false		high
https://static.parastorage.com/services/skins/2.1229.80/images/wysiwyg/core/themes/base/cursor_zoom_	2[1].htm.2.dr	false		high
http://https://drafts.fxtf.org/geometry/#dictdef-domrectinit	wixui.VideoPlayer.chunk[1].js.2.dr	false	Avira URL Cloud: safe	unknown
http://https://github.com/marcj/css-element-queries/blob/1.0.2/src/ElementQueries.js#L384-L390	wixui.VideoPlayer.chunk[1].js.2.dr	false		high
http://https://engage.wixapps.net/chat-widget-server/renderChatWidget/index?cacheKiller=1608320009145&commo	{94B8BF3D-41B5-11EB-90E4-ECF4B862DED}.dat.1.dr	false		high
http://polymer.github.io/LICENSE.txt	bolt-custom-elements.min[1].js.2.dr	false	Avira URL Cloud: safe	unknown
http://https://discuss.dev.twitch.tv/t/twitch-embedded-player-updates-in-2020/23956	wixui.VideoPlayer.chunk[1].js.2.dr	false		high
http://https://static.parastorage.com/services/admin-pages-platform-app/1.350.0/	admin-pages-viewer-app.bundle[1].js.2.dr	false		high
http://https://developer.mozilla.org/en/DOM/window.postMessage	wixui.VideoPlayer.chunk[1].js.2.dr	false		high
http://youtube.com/yt/2012/10/10	base[1].js.2.dr	false		high
http://https://www.305covidtest.com/Root	{94B8BF3D-41B5-11EB-90E4-ECF4B862DED}.dat.1.dr	false	Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.wix.com/dashboard/	admin-pages-viewer-app.bundle[1].js.2.dr	false		high
http://https://static.wixstatic.com/media/cfc5f6_f76ceb0c1837454aafd95222db446948~mv2.jpg	enriched[1].json.2.dr	false		high
http://https://greensock.com/standard-license	gsap.min[1].js.2.dr	false		high
http://https://www.305covidtest.com/	{94B8BF3D-41B5-11EB-90E4-ECF4B8B62DED}.dat.1.dr	false		unknown
http://https://engage.wixapps.net/chat-widget-server/renderChatWidget/index?cacheKiller=1608320868719&commo	{94B8BF3D-41B5-11EB-90E4-ECF4B8B62DED}.dat.1.dr	false		high
http://https://static.parastorage.com/unpkg/core-js-bundle	IVS0AW9K.htm.2.dr	false		high
http://rock.mit-license.org	minified[1].js.2.dr	false		high
http://www.youtube.com/	msapplication.xml7.1.dr	false		high
http://www.youtube.com/videoplayback	base[1].js.2.dr	false		high
http://https://api.dmdcn.net/all.js	wixui.VideoPlayer.chunk[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://www.wix.com/contact/	messages_en[1].json0.2.dr	false		high
http://https://w3c.github.io/pointerevents/#widl-PointerEvent-isPrimary	wixui.VideoPlayer.chunk[1].js.2.dr	false	Avira URL Cloud: safe	unknown
http://https://player.twitch.tv/js/embed/v1.js	wixui.VideoPlayer.chunk[1].js.2.dr	false		high
http://https://static.parastorage.com/services/wix-perf-measure/1.258.0/wix-perf-measure.bundle.min.js	IVS0AW9K.htm.2.dr	false		high
http://https://static.wixstatic.com/media/11062b_8deb790af4fc4a8684a730e0d287669d~mv2.jpg/v1/fill/w_480	IVS0AW9K.htm.2.dr	false		high
http://https://github.com/faisalman/ua-parser-js	wixcode-worker[1].js.2.dr	false		high
http://https://static.wixstatic.com/media/cfc5f6_7020fbc4328945a9a8cc038617e65534~mv2.jpg/v1/fill/w_171	IVS0AW9K.htm.2.dr	false		high
http://https://static.parastorage.com/services/santa/1.11783.0	IVS0AW9K.htm.2.dr	false		high
http://https://drafts.fxtf.org/geometry/#domrectreadonly	wixui.VideoPlayer.chunk[1].js.2.dr	false	Avira URL Cloud: safe	unknown
http://https://npm.io/search?q=ponyfill	lodash.min[1].js.2.dr	false		high
http://https://gist.github.com/aFarkas/a7e0d85450f323d5e164	wixui.VideoPlayer.chunk[1].js.2.dr	false		high
http://https://recaptcha.net/recaptcha/api.js	wixui.Captcha.chunk[1].js.2.dr	false	Avira URL Cloud: safe	unknown
http://https://browser.sentry-cdn.com/4.6.2/bundle.min.js	IVS0AW9K.htm.2.dr	false	Avira URL Cloud: safe	unknown
http://static.wixstatic.com/media/d967ba93f0314c78924edc8a8c8cfa15.jpg	bolt-main-prod-old[1].js.2.dr	false		high
http://static.wixstatic.com/media/bc001baa4397444f809fa5f147c28a9e.jpg	bolt-main-prod-old[1].js.2.dr	false		high
http://static.wixstatic.com/media/bc001baa4397444f809fa5f147c28a9e.jpg	bolt-main-prod-old[1].js.2.dr	false		high
http://https://browser.sentry-cdn.com/5.7.1/bundle.min.js	sentry-lazy-load[1].js.2.dr	false	Avira URL Cloud: safe	unknown
http://https://tools.ietf.org/html/rfc7230#section-3.2	fetch.umd[1].js.2.dr	false		high
http://https://www.305covidtest.com/book-online	IVS0AW9K.htm.2.dr	false	Avira URL Cloud: safe	unknown
http://https://frog.wix.com/bt?src=29&evid=3	IVS0AW9K.htm.2.dr	false		high
http://www.amazon.com/	msapplication.xml.1.dr	false		high
http://www.linotype.com/licenseHelveticaNeueLT	b7693a83-b861-4aa6-85e0-9ecf676bc4d6[1].eot.2.dr	false		high
http://https://static.parastorage.com/unpkg/whatwg-fetch	IVS0AW9K.htm.2.dr	false		high
http://www.twitter.com/	msapplication.xml5.1.dr	false		high
http://my-url/video.mp4	wixui.VideoPlayer.chunk[1].js.2.dr	false	Avira URL Cloud: safe	low
http://youtube.com/streaming/metadata/segment/102015	base[1].js.2.dr	false		high
http://https://engage.wixapps.net/chat-widget-server/renderChatWidget/index?cacheKiller=1608320868719&c	testing-instructions[1].htm.2.dr	false		high
http://https://static.wixstatic.com/media/48ccc5_559838b644e94acf903cd64ed867b15b~mv2.png/v1/fill/w_32%2Ch_	imagestore.dat.2.dr	false		high
http://https://youtu.be/	base[1].js.2.dr	false		high
http://www.linotype.com	b7693a83-b861-4aa6-85e0-9ecf676bc4d6[1].eot.2.dr	false		high
http://www.linotype.comhttp://www.linotype.com/fontdesignersNOTIFICATION	b7693a83-b861-4aa6-85e0-9ecf676bc4d6[1].eot.2.dr	false	Avira URL Cloud: safe	unknown
http://img.youtube.com/vi/CakiQCH5ZY0/mqdefault.jpg	bolt-main-prod-old[1].js.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.linotype.com/license	b7693a83-b861-4aa6-85e0-9ecf676bc4d6[1].eot.2.dr	false		high
http://https://github.com/madrobby/zepto/blob/master/MIT-LICENSE	imageClientApi[1].js.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[2].js.2.dr	false		high
http://polymer.github.io/CONTRIBUTORS.txt	bolt-custom-elements.min[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://jedwatson.github.io/classnames	wixui.VideoPlayer.chunk[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://facebook.github.io/react/docs/top-level-api.html#react.createclass	wixui.Captcha.chunk[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://siteassets.parastorage.com/pages/singlePage/viewerViewerModeJson	IVS0AW9K.htm.2.dr	false		high
http://www.apache.org/licenses/LICENSE-2.0	wixui.VideoPlayer.chunk[1].js.2.dr	false		high
http://www.nytimes.com/	msapplication.xml3.1.dr	false		high
http://https://greensock.com	gsap.min[1].js.2.dr	false		high
http://https://my-url/video.mp4	wixui.VideoPlayer.chunk[1].js.2.dr	false	• Avira URL Cloud: safe	low
http://https://youtube.com/api/drm/fps?ek=uninitialized	base[1].js.2.dr	false		high
http://webfonts.fonts.com	IVS0AW9K.htm.2.dr, fontFace[1].css.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.96.106.200	unknown	United States		15169	GOOGLEUS	false
216.58.215.225	unknown	United States		15169	GOOGLEUS	false
185.230.61.180	unknown	Israel		58182	WIX_COMIL	false
151.101.2.217	unknown	United States		54113	FASTLYUS	false
52.2.188.208	unknown	United States		14618	AMAZON-AESUS	false
35.246.6.109	unknown	United States		15169	GOOGLEUS	false
35.201.97.85	unknown	United States		15169	GOOGLEUS	false
65.9.68.81	unknown	United States		16509	AMAZON-02US	false
172.217.168.66	unknown	United States		15169	GOOGLEUS	false
172.217.168.22	unknown	United States		15169	GOOGLEUS	false
34.102.176.152	unknown	United States		15169	GOOGLEUS	false
54.87.207.230	unknown	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	332393
Start date:	18.12.2020
Start time:	20:48:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://www.305covidtest.com/
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:	16
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:	clean1.win@3/243@16/12
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://www.305covidtest.com/ • Browsing link: https://www.305covidtest.com/testing-instructions • Browsing link: https://www.305covidtest.com/2

Warnings:	Show All - Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, dllhost.exe, ielowutil.exe, SgrmBroker.exe, conhost.exe, svchost.exe, Usoclient.exe - TCP Packets have been reduced to 100 - Created / dropped Files have been reduced to 100 - Excluded IPs from analysis (whitelisted): 104.42.151.234, 13.64.90.137, 23.60.220.29, 216.58.215.227, 52.255.188.83, 172.217.168.46, 172.217.168.78, 216.58.215.238, 216.58.215.234, 172.217.168.10, 172.217.168.74, 172.217.168.38, 152.199.19.161, 23.54.113.104, 172.217.168.4, 23.0.174.200, 23.0.174.185, 204.79.197.200 - Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, au.download.windowsupdate.com.edgesuite.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, audownload.windowsupdate.nsatc.net, www.google.com, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, ieonline.microsoft.com, au-bg-shim.trafficmanager.net, skypedataprdcolwus17.cloudapp.net, fonts.googleapis.com, fs.microsoft.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, www.googleapis.com, static-doubleclick-net.l.google.com, skypedataprdcoleus17.cloudapp.net, youtube-ui.l.google.com, any.edge.bing.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net - Report size exceeded maximum capacity and may have missing behavior information. - Report size exceeded maximum capacity and may have missing network information. - Report size getting too big, too many NtCreateFile calls found. - Report size getting too big, too many NtDeviceIoControlFile calls found. - Report size getting too big, too many NtQueryAttributesFile calls found. - Report size getting too big, too many NtReadFile 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\31M6V5CL\www.youtube[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\explore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2675
Entropy (8bit):	5.090209514367853
Encrypted:	false
SSDEEP:	48:XnUfUiNAriNA46uriNA46uhriNA46uriNA46kE:XwLy+y46u+y46uh+y46u+y46u+y4kE
MD5:	296693BF205BA41B309E90755E102E85
SHA1:	ACDE0445722F3E25979CFDBB2D4C99E5FF3E960A
SHA-256:	7446707AFA37626FFBA1140A28289D682FBCB35CF56CCAC0574CDDEBA7F0EC43
SHA-512:	873C5A33DA22DD4B4E897204BEB8B9547F4EAB96C318D62B227295F57D2A53116AF95649C297252F11A5C76F095DF44BC8AEFC8EDC399B97EA179CDB17EC26B
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root></root><root></root><root></root><item name="__sak" value="1" ltime="1772449968" htime="30856642" /></root><root></root><root><item name="__sak" value="1" ltime="1826809968" htime="30856642" /></root><root></root><root><item name="yt-remote-device-id" value="{"data&q uot:"fb2d0ce8-c5a7-4113-a5e0-520d28d33369", "expiration"::1639889408166, "creation"::1608353408182}" ltime="1827969968" hti me="30856642" /></root><root><item name="yt-remote-device-id" value="{"data":"fb2d0ce8-c5a7-4113-a5e0-520d28d33369", "expirati on"::1639889408166, "creation"::1608353408182}" ltime="1827969968" htime="30856642" /><item name="yt-remote-connected-devices" value="{&qu ot;data":"[]", "expiration"::1608439808330, "creation"::1608353408330}" ltime="1828929968" htime="30856642" /></root><root><item name="yt-remote-device-id" value="{"data":"fb2d0ce8-c5a7-4113-a5e

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\FCL1523P\www.305covidtest[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):	9168
Entropy (8bit):	5.275314570724019
Encrypted:	false
SSDEEP:	96:0DUaUDUDHUDUDHz+bnUDHzbbKuUeuHzbbKuUeuHzbbKu5UeuHzbbKuUeuZzbb:/a
MD5:	96DEF2DB4C7A92962C81A3C8942A082F
SHA1:	8504836ED3890C05EBE20F244FDAD0BE1780E49B
SHA-256:	C15D6EDAD3C004F4CE7E661348F2EA237078959A7AFC4D60A622BAEDD683B75B
SHA-512:	F825B5A50B748E37ADC812D122FA7BB9F381652A18B5027F9C78791457F24368F2274C041202A47824F9B9B6DB5424383D1AA1B1E9C1A35AECFC62AD6035D79
Malicious:	false
Reputation:	low
Preview:	<pre><root></root><root><item name="fedops.logger.sessionId" value="a171b19c-87be-4466-8847-5311d0d08a06" ltime="1482199968" htime="30856642" /></root><root> <item name="fedops.logger.sessionId" value="a171b19c-87be-4466-8847-5311d0d08a06" ltime="1482199968" htime="30856642" /><item name="" value="" ltime ="1483949968" htime="30856642" /></root><root><item name="fedops.logger.sessionId" value="a171b19c-87be-4466-8847-5311d0d08a06" ltime="1482199968" hti me="30856642" /></root><root><item name="fedops.logger.sessionId" value="a171b19c-87be-4466-8847-5311d0d08a06" ltime="1482199968" htime="30856642" /> <item name="wixSessionTS" value="1608353376672" ltime="1512459968" htime="30856642" /></root><root><item name="fedops.logger.sessionId" value="a171b19c- 87be-4466-8847-5311d0d08a06" ltime="1482199968" htime="30856642" /><item name="wixSessionTS" value="1608353376672" ltime="1512459968" htime="30856642" /></root><root><item name="fedops.logger.sessionId" value="a171b19c-87be-4466-8847-5311d0d08a06" l</pre>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\UNTORQMW\engage.wixapps[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):	5449
Entropy (8bit):	5.0820856244028185
Encrypted:	false
SSDEEP:	96:E7kCkCW2kCkC/kCkCkC2kCkCkCkCkCkCkCkCzvkCzv3kCv3kCv3ksuv3kfv3kg:HbnnIAAAsnU
MD5:	247345190215B220119114B3D1A07A11
SHA1:	FAD94FDA6C3A26752AB4BFDB57A8C1F6372D627D

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\DOMStore\UNTORQMW\engage.wixapps[1].xml	
SHA-256:	93BDE96F6F05733B111DCF3E70BF44E3D443C3CA7960A27AB62D0066CE9E3DE8
SHA-512:	EAB2C2079D6626FFE1A7CD8F5135122D9FDDC8265745002F66B9DF8D2B1F9B3FBB87BF7A3C7A03A96BD60D9D5F4685E3678F280DAC779F0E2DA00ACFCD81C0D
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="fedops.logger.sessionId" value="af4a9983-533a-459e-abca-ea8e249d5697" ltime="1601649968" htime="30856642" /></root><root><item name="fedops.logger.sessionId" value="af4a9983-533a-459e-abca-ea8e249d5697" ltime="1637119968" htime="30856642" /></root><root><item name="fedops.logger.sessionId" value="af4a9983-533a-459e-abca-ea8e249d5697" ltime="1637119968" htime="30856642" /></root><root><item name="firebase.sentinel" value="cache" ltime="1695939968" htime="30856642" /></root><root><item name="fedops.logger.sessionId" value="af4a9983-533a-459e-abca-ea8e249d5697" ltime="1637119968" htime="30856642" /></root><root><item name="fedops.logger.sessionId" value="af4a9983-533a-459e-abca-ea8e249d5697" ltime="1637119968" htime="30856642" /></root><root><item name="__sak" value="1" ltime="1708409968" htime="30856642" /></root><root><item name="fedops.logger.sessionId" value="af4a9983-533a-459e-abca-ea8e249d5697" ltime="1637119968" htime="30856642" /></root><root><item name="fedops.logger.session

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{94B8BF3B-41B5-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	39000
Entropy (8bit):	1.9310441033354127
Encrypted:	false
SSDEEP:	192:rDZAZL2G9WktHf9RM5lS5pf5g8r53hf5z7r5rg:rFQCGUw/Y5lS5Z5V5B575s
MD5:	9AB05521CB735D8E53B3D6F074C64E0A
SHA1:	916D7D0A6E0EA10EDCE4E0EB8E5ED0D445EB1A4A
SHA-256:	409362CA7F92C372B310B24671E77D9850BBC8B3322F95D144E7D0C9E8B9170B
SHA-512:	96BBAE0340C17FF4C4F9ADDAD64207943E33A74BE97B62691B87D881EDD8311C3812CEB824E8CDC8CB50CFB3FC45A8D3E3A17EB14096D931FAE4BF265BDD126
Malicious:	false
Reputation:	low
Preview:	R.o.o.t. .E.n.t.r. y.....

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{94B8BF3D-41B5-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	129556
Entropy (8bit):	2.962224725697434
Encrypted:	false
SSDEEP:	3072:DkBPkBykBjkBPkBykBLkBWkBvkBoJjkBH8kBHVkBHQ+d:E
MD5:	0A224ED80975A8F88C9EDE7A1BF0BFBF
SHA1:	6EF1BDF3F998DD0A1F0359A70FEFE31C787562A
SHA-256:	FD4F6F168150443FD9AFE3100BF292CC797C67441803FD3728D018B756CB15AF
SHA-512:	ADB0032DF3617334C269EF441A4F6028FDE75DA106BB8F1CCD3F25C2C77D4AAB630B01722509398BC85E923AA15611FE948059F1926D16994BE672041F6FF1D3
Malicious:	false
Reputation:	low
Preview:	R.o.o.t. .E.n.t.r. y.....

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9B3B1B4D-41B5-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5862721865355096
Encrypted:	false
SSDEEP:	48:lwI0GcprlGwpatG4pQKGrpbSurGQpKTG7HpRSsTGlpX2/GApm:rl0ZvQP68BSuFAiTs4Fug
MD5:	B32BF81D9F18876BF22932F4B8F9F3D8
SHA1:	D796CBA19BD5A26CF043127126B1C9A4B37BBC1A
SHA-256:	E5D5F5689886ED70C3077B2A91B6E56CB722B169A1B6DCFD77E14B184C14FF2C
SHA-512:	675763FA45010251F833230B30E64CB513E0C2EB6F6CB3C9E256D7647F26D20D5BA97B201A77B365059DCB8A57213323B82AA94488D5543918E2BEFDA29E1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9B3B1B4D-41B5-11EB-90E4-ECF4BB862DED}.dat

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):	5.070809854238551
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEAbVb94nWiml002EtM3MHdNMNxOEAbVb94nWiml00ObVbkEtMb:2d6NxOhl94SZHKd6NxOhl94SZ76b
MD5:	A08CAC2587C151A6CDFC38C065A5E5D5
SHA1:	BDF526862D1B525149ADBED4CF72341844E1A5A7
SHA-256:	29D81906E10B3722A706F2F554F9423E8CC1D6B32E5C3AFF012D3F9629DDD877
SHA-512:	7832D5551C4DA3DD4D9EA603F7612D6024AB5BF001D98EE626CB3DD96782AC8AF07D456B6FCF4EA72120663313714F5580512BDDA6BC4BF8F0798E6614EC266
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x6c17adcb,0x01d6d5c2</date><accdate>0x6c17adcb,0x01d6d5c2</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>0x6c17adcb,0x01d6d5c2</date><accdate>0x6c17adcb,0x01d6d5c2</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):	5.112710629476415
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2k7tgbbotgbb94nWiml002EtM3MHdNMNxe2k7tgbbotgbb94nWiml0/:2d6Nxrsfglfg94SZHKd6Nxrsfglfg94o
MD5:	1F171364FB06DAF7F499222FC8B1D237
SHA1:	BCE819FB5681AE863AB718D5D47F1A894DF25F66
SHA-256:	A7AE47FE77755196C390C9602387FA1D637858C450E56A32C546FCAD1DE527C2
SHA-512:	1EE342615B7CBFC77F3AE4D26DBD305147F31DC227613A252F1DA2A668CBCFEF5E8861FB65A117799A8D29229D5F9C1850359DF4B72EB0A4D56FF9BA3C1FD74
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x6c0fbe78,0x01d6d5c2</date><accdate>0x6c0fbe78,0x01d6d5c2</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>0x6c0fbe78,0x01d6d5c2</date><accdate>0x6c0fbe78,0x01d6d5c2</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):	5.116452690038717
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLcBtb94nWiml002EtM3MHdNMNxvLcBtb94nWiml00ObmZEtMb:2d6Nxvwn94SZHKd6Nxvwn94SZ7mb
MD5:	0C355BE42CDBB7D205104D49F945EE29
SHA1:	4715E0D06AEA7E1BB344C30698CDF493EDAEE028
SHA-256:	253C43690B0DE030F22F9F8DA68A7FAFC99856E77E10C73CB9126BE023589664
SHA-512:	53BC2DFAFD6E166F777B2A72B533F1758790FE5D98E5D6397D5C075335E0F1EF64205BA631CCFD6853723A07C51340C04FF2802F3F25997B329DD992A465195
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x6c184a08,0x01d6d5c2</date><accdate>0x6c184a08,0x01d6d5c2</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>0x6c184a08,0x01d6d5c2</date><accdate>0x6c184a08,0x01d6d5c2</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):	5.10908705718581
Encrypted:	false
SSDEEP:	12:TMHdNMNxidbYb94nWiml002EtM3MHdNMNxidb3b94nWiml00Obd5EtMb:2d6NxMe94SZHKd6NxML94SZ7Jjb
MD5:	946FD5E4EE6D344829F3FF331CD1FE6F
SHA1:	F244826E17BEF552D06B37E7928C97905B8DB066
SHA-256:	C2F62C564D3349A54F73490F13F1450A65769FCB2A566E9F60E82EF79F698A42
SHA-512:	7F3808D3E73F50BD928D0B88A98D84F243FA88F880C272139D0625E4439E42DC054DEDE96718FB743D9B24C39E32D3B1037A3DE05DEC61470D621EE12F3562C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x6c13680c,0x01d6d5c2</date><accdate>0x6c13680c,0x01d6d5c2</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>0x6c13680c,0x01d6d5c2</date><accdate>0x6c14044e,0x01d6d5c2</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):	5.14222391743032
Encrypted:	false
SSDEEP:	12:TMHdNMNhxGwnbKb94nWiml002EtM3MHdNMNhxGwnb2b94nWiml00ObK075EtMb:2d6NxQEE94SZHKd6NxQEw94SZ7YKajb
MD5:	31259F34916664CB1E3846FD0E344B93
SHA1:	1518FC5E08AD859887182D72C152B02F08FC844F
SHA-256:	74C2AA1A818E5D7488D7A566B0027FEABCCCE544D91CC4E2433BC100D0CF95C21
SHA-512:	C88AD000B7E003D0F5143AA51B7F0888031A5DE40411C1CFC2B0B6708B79DB429DC7488DAE1C813E47EF1282174044B4BBFDD96453CCF0CDF00A923B8C4DE48
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x6c18e641,0x01d6d5c2</date><accdate>0x6c18e641,0x01d6d5c2</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>0x6c18e641,0x01d6d5c2</date><accdate>0x6c19828c,0x01d6d5c2</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):	5.106660987502675
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nuMbVMb94nWiml002EtM3MHdNMNx0nuMbVMb94nWiml00ObxEtMb:2d6Nx0uSVS94SZHKd6Nx0uSVS94SZ7nb
MD5:	15DBF1930BC8629F83BE32093AC272E4
SHA1:	3B982C5D2ED15650FC7DD94187598B0BC17F37E4
SHA-256:	A06A0DD2B52122829B2A3A72713AD76611E5B80E67DBC2262007D320502BB179
SHA-512:	667DA3568D3EA6D2C3FFA80FBF92F182C0E7E99DFE5176EDA0CA87546FF6BD50AE96E5C9ECF6C36D0EDBADDFECD5D57B65A88E54E0DD411182654FD7653FD3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x6c171189,0x01d6d5c2</date><accdate>0x6c171189,0x01d6d5c2</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>0x6c171189,0x01d6d5c2</date><accdate>0x6c171189,0x01d6d5c2</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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Entropy (8bit):	5.12765973243921
Encrypted:	false
SSDEEP:	12:TMHdNMNxxpbYb94nWiml002EtM3MHdNMNxxpbYb94nWiml00Ob6Kq5EtMb:2d6NxPe94SZHKd6NxPe94SZ7ob
MD5:	EF489DE2FAC49817A6AEF0BD18B72054
SHA1:	FCA17248EC45C3FB2E5A4EB55947BF0656D743A5
SHA-256:	2EAD4D72685C2296F9336739850A68B2D24DF289C08C0D75063D378BB5F44A4C
SHA-512:	DD5536178B9BB0B6C893EAD85634530B19E98381BAC9505C9AB1A47309169E316C82401B146490CE894A95B308231E59C7FFEDE932BFAC46E0C69C81EB486404
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x6c16753e,0x01d6d5c2</date><accdate>0x6c16753e,0x01d6d5c2</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>0x6c16753e,0x01d6d5c2</date><accdate>0x6c16753e,0x01d6d5c2</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):	5.0901182280640676
Encrypted:	false
SSDEEP:	12:TMHdNMNxcQxb9xb94nWiml002EtM3MHdNMNxcQxbuw94nWiml00ObVtMb:2d6NxX794SZHKd6NxXf94SZ7Db
MD5:	723330F62CA0302CAA14470E1D9EDDA2
SHA1:	48F50CF3E633CDD74FC6A859907DF14FE845926A
SHA-256:	2339011948B782D70F78C8ABEFB61BB512DFAE58B8898F07E3BEFC48E96D0DBB
SHA-512:	F26D203EFD608ADE2D5BECAF73886C61ED13BD9070AB987410489259855BE501BE8718B99F731943F78A6556F5E67D39BBFECD6A4E5D7F08643C12BCE38D968
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x6c122fa0,0x01d6d5c2</date><accdate>0x6c122fa0,0x01d6d5c2</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>0x6c122fa0,0x01d6d5c2</date><accdate>0x6c12cbca,0x01d6d5c2</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):	5.073642257917846
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnpwb94nWiml002EtM3MHdNMNxfnpwbYb94nWiml00Obe5EtMb:2d6Nxc94SZHKd6Nxc94SZ7jib
MD5:	4FCC630E06544256CAB2FE85EF4C6EAB
SHA1:	E276B04E1B384C549BE05C0462567B296F530404
SHA-256:	1C8788DC0C4A6A43D8B8F492BA164CFE743F7983FAE5859AA28C71089BE2F9F8
SHA-512:	4346BBE497288ECB07ADAF8522102EB86A8733085E1431852E3353B5A6A5E8809D4D9A46877C4F93AEE3A83A5C3633D56A4415EC1669CE87155D0D4E0958A01C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x6c12cbca,0x01d6d5c2</date><accdate>0x6c12cbca,0x01d6d5c2</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>0x6c12cbca,0x01d6d5c2</date><accdate>0x6c13680c,0x01d6d5c2</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):	1826
Entropy (8bit):	7.346392632173963
Encrypted:	false
SSDEEP:	48:hyUSU16Yr3y99X1t7CfXV91uGrcBDXbKgg2:A34w9X1gTbQBD2gP
MD5:	80742E0C84669F0408C7D6BC4230FE13
SHA1:	0E8CD150306723FEE78DA2283CED0D825C1A3695
SHA-256:	B2C4B39C4828FE6BB186AFCFC8F56CD4F9682971F334F12CC929AE7152A1BA7

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynf0jx\imagestore.dat	
SHA-512:	8D5C3CC3FFF6707DEC1650AC1F63C297F2BFB34F8B889E84627EE1C79975C0EE9157D98A4BB66F74D8858FF61D5FB060BF01B566DA8AC120E974B55BD428786C
Malicious:	false
Reputation:	low
Preview:	..h.t.t.p.s://.s.t.a.t.i.c...w.i.x.s.t.a.t.i.c...c.o.m/.m.e.d.i.a./4.8.c.c.c.5_5.5.9.8.3.8.b.6.4.4.e.9.4.a.c.f.9.0.3.c.d.6.4.e.d.8.6.7.b.1.5.b~.m.v.2...p.n.g./v.1./f.i.l.l./w._3.2.%2.C.h._3.2.%2.C.l.g._1.%2.C.u.s.m._0...6.6_1...0.0_0...0.1./4.8.c.c.c.5_5.5.9.8.3.8.b.6.4.4.e.9.4.a.c.f.9.0.3.c.d.6.4.e.d.8.6.7.b.1.5.b~.m.v.2...p.n.g.....PNG....IHDR.....szz.....pHYs.....~.....JIDATX..WYo.W...T..}.Z.5t;..l.K.mY*U.B%P.B[.H..l...Cv.\$.....H..(4)...x..x..Mx.z.u.R..l..pt..... ;wft[...i3^...e:~9.....k..@t.9UF.R.%..`k=...6/}%r.....v...U..o.....DFkXR%..L.bJ....0.....Ne.8...d..#.\8_Eg...s....g.8J.w.szd..9.T.t.x.k.a.t.! w..H..c..6.%..cGa..l7....7s.....S.f.8..mT...K....(J.Q.l... Wkt..F.....)JB...@.....^..)M..5.N....0....".%..=...b)B.5..."..x.j]...h.o.D.4.h.Q..Y?F.....e.....y'E...% h.....p.;...H...q..C..Q...h.Y..#...O...l..%.c.q..C.....L...j.q.=...k.to.....f..Y.vd.(..eB.J.H)..._...j(,...m

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\03805817-4611-4dbc-8c65-0f73031c3973[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\explore.exe
File Type:	Web Open Font Format, TrueType, length 22084, version 1.0
Category:	downloaded
Size (bytes):	22084
Entropy (8bit):	7.978115387503532
Encrypted:	false
SSDEEP:	384:jFyJ/0LAzwcgu660ZMMu+L6BPWlkms5VoLnBNE0csDFd5CFLpvaah1A++jsJ0fjBmDi6BPDkms5rbBNjRDFd5CFtl
MD5:	2D1A6CCE2E11A0D7659EB3E09181750B
SHA1:	B01F6B398BF9D414B16705513B6EA17E1B1FF221
SHA-256:	9B7C81D3E669C7BFF62527A61525AD1B80F776021655FD3A63DC927B0F0D624B
SHA-512:	BFBE801F65B71C951A6D85A116F5AB1F3327A3DDF1D76B3D3CCDEBC72E1DFD30D912521BE63B628FED2961475C3E5F70EF367C87FBBB319823B00DDC531A625
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/third-party/fonts/user-site-fonts/fonts/03805817-4611-4dbc-8c65-0f73031c3973.woff
Preview:	wOFF.....VD.....OS/2...X...U...`e...cmap.....cvt ...@...M.....o.(fpgm.....+...P...gasp.....glyf.....;#..w...ohead..B....6...6...1hhea..C.....\$....hmtx..C@.....t.*.kern..E.....".loc..l(.....maxp..J.....m..name..K...P...p.>.post..TT.....2prep..Th.....H..8Gx.c`fR`.....@....A.(...>~.@.WQ....A...-...9&6....@.....x.c``d`.b.....@Z.A...`e.c.....X.X.8.....).9.%5...+5.J...u.u.`.bL.....V.P.QP.....O.....?..... ....[.l].....w..B....1.x.c.....a.....0.1...o..'_...a...(.#...../O..M...4..fP<.....x..VOo.G..j`\$\$.].8.....R6.v...Y.lq..v...a...8#UJO.M>D?.[NNO.8=...zFzBT U.....'j...7....o;.....o.....7..jy...W>...'W.. ... t.....x.g....S.....c.C9 c.Z.j..u`.../!....._~.T.6.MY..+..L..~.:L..s...YGE.!W6^.....Ce .b+..).x...v]...Y@.>~.....Sd..Oow.....U...A.6#w...;b..l~...JX...l..f.....H..X....

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\48ccc5_559838b644e94acf903cd64ed867b15b~mv2[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\explore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1432
Entropy (8bit):	7.825112878339571
Encrypted:	false
SSDEEP:	24:2glvuZP6i8uBwcELic86vASTGyCbbXYM9ZP/uGrkl1cBDITQmj+leTggZ:26Yr3y99X1t7CfXV91uGrcBDXbKggZ
MD5:	58FE63A5105F2EECD1BB550E23FFC851
SHA1:	F4A6EEC57380CFC1E0F2E527CF68D2DF8C4B7852
SHA-256:	CAA477D8C8D21F2D29C8EBF2D9CFEC7B294A63DE657F01B13F470C0D0EDDE3D2
SHA-512:	24A3E0A0EA92FC318675FF323BC8B4B2BC58D470BCAC85EB41AD447C233CC96CA27B3FA08CEA6349E8C71F23E5F94614B64867BC6C0262C0114AF24C9B93F3D
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....szz.....pHYs.....~.....JIDATX..WYo.W...T..}.Z.5t;..l.K.mY*U.B%P.B[.H..l...Cv.\$.....H..(4)...x..x..Mx.z.u.R..l..pt..... ;wft[...i3^...e:~9.....k..@t.9UF.R.%..`k=...6/}%r.....v...U..o.....DFkXR%..L.bJ....0.....Ne.8...d..#.\8_Eg...s....g.8J.w.szd..9.T.t.x.k.a.t.! w..H..c..6.%..cGa..l7....7s.....S.f.8..mT...K....(J.Q.l... Wkt..F.....)JB...@.....^..)M..5.N....0....".%..=...b)B.5..."..x.j]...h.o.D.4.h.Q..Y?F.....e.....y'E...% h.....p.;...H...q..C..Q...h.Y..#...O...l..%.c.q..C.....L...j.q.=...k.to.....r..Y.vd.(..eB.J.H)..._...j(,...m..O6)^..\$E.....0..P.P.9....>.3.X.s.....(o...=nX.FD...N..c#..a?.... A.>.. p.e%.#.[V...p.2.v.....d.(c)0H..@....\=..sF.wB.x{..E22g.p...f.g..l..*7;...> 0{aYA....4.\$..DL.`.....[.m.a..M..#..QR9..w..[.....[.l...a...P.._...f?2.....1/F(\$H.E.....N..3.....&'A>f.....E.'b.6...l8..`[.lzk.)...b.y.Dd#...@...v...b..+1.0%F

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\5ff158be45cb4298b1d6827c8a075c99[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\explore.exe
File Type:	[TIFF image data, little-endian, direntries=6, orientation=upper-left, xresolution=86, yresolution=94, resolutionunit=2], progressive, precision 8, 245x164, frames 3
Category:	dropped
Size (bytes):	7645
Entropy (8bit):	7.855983188303572
Encrypted:	false
SSDEEP:	192:Px/BOeMc8Kle1LlXGDx/ig67NVg/0X9O2364c:Px/BOen39LGF/iz7DNNO2K/
MD5:	EFDDC2B9F0FDE5C6B4B541018000CDBF
SHA1:	BDEE8FDAE4ED79E277D96058BCA1FE5777D8B2FA
SHA-256:	6F6C5D45F05A61A1B64E014BF81FBFB4E1E6A9F908939354A8854F6BDE741B02
SHA-512:	E0FDD0A7A34F600C5AF801928999660E285ED0A72F9344919371B9DE582BB2ACAA7A52629C493C2A04E0E2B2A4F3F1D84CFA36BE29FB9507F3DF13DE98F3E20
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUI\5ff158be45cb4298b1d6827c8a075c99[1].jpg	
Reputation:	low
Preview:	JFIF.....Exif..II*.....V.....^.....i.....f.....8c.....8c.....0210.....0100.....C..... %...#... , #&)*)...-0-%()(...C.....((.....((.....c..S\z..u .&.*..V.U.R...Fu.x.UB@..... \$!.....Z<..6.Z.!t'...Y.R..#06..Q 7.z..VeG.*.....Y6Qmt..)Q.....5.4p..))+[l.T"...z....].b....6.*lj...#k@....WTDR.Yh....,o..9fJ.n=*3.Yi..%K...J.!D-....^..d.c9..).Y...1...].-..V7.H...IV.. ..Sj"...T..Xe6K.n...A...._p....g....^u..z.,r.H{S...7.Kc.`%.....H.kB.9.-~{..i.i.j.qN....8n]...._g..L./>....YI.*../.L.li.t%eKE....XY.vkW....;xo:0.*.Y.X...].a.D+..\Q.6.Y.-..iO*.Pf.Z..). ...W'.h...A.X. u.p.' .l.e.L^.....&..u...#Bgd.t.[.[..V+."g.9.....lj..4z.P...s\..2..o..U..b....x..j.j..

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUI\61bd362e-7162-46bd-b67e-28f366c4afbe[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22303, version 1.0
Category:	downloaded
Size (bytes):	22303
Entropy (8bit):	7.979944644774919
Encrypted:	false
SSDEEP:	384:gO4Hui2AWjz+3dOtQT8dQInDeD5bLJbhJBqQ0Xd3ah2Fcm3z45wPwK:gO4ui2F+3dOt3K1bNP/h2FcrUdoK
MD5:	9DE46E344E47C7432887C85C9583AAFE
SHA1:	6E7117358ADF1A06CFDD60404093CF4C9FABC3D5
SHA-256:	E7B057ACF773D27E5D5D8CEE13584EE00BC86934CEB8DED58058DDC50852D76
SHA-512:	A16C21089A54A753D7B17D10E482ACFC6C74D1E820AD0DE2BA5B62E6C8D7ACD6B1EA72DD16E44FE63D6724A7E9DCAD7EAD21EF0D357C42C452ACD10F8F8FB780
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/third-party/fonts/user-site-fonts/fonts/61bd362e-7162-46bd-b67e-28f366c4afbe.woff
Preview:	wOFF.....W.....Q.....GPOS...l...u.....OS/2.....T...fM...VDMX...8... ..n.u.cmap.....c....L...cvtO....W...fpgm...L.....,gasp.....glyph.....89..\ ...head..F...6...6...hhea..FT... ..\$...hmtx..Ft.....;hloca..Hl...\ G4.{..+..l].HL4.QbB...{Vw...n]}...=...R...~;s....."j..l.n]..jU2"...[.7...c...i=fD.y\./. [m..&.ltAi..7.9...].h.....2...q3.W.r..7...h.gKy../2...Kr.T..O....L).U.....b....f.*..Y5s-...s..... ...ga....E.....T..5..m%.=...XE...d+X}....M.....]u..E.....UK~.....3~z..jV].Q.....4.!kDc..&5+...U].u.=v.O...vA.{az!.J..P.W....P.'/.0C]....#B.1..i}l..8..6E4....-A.J<..N D...R..5..eomE....d9.vZN.:.....6.S.`....8.....l.)..4...*.....n.B...>...V.^].U[....k..].....7....Ch.#..c%....3..9t^..5..FoQ~..9>@>B;....V3..D.....t....x.c`

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUI\84770f_8506293a29b44887a8a0cb383c0c2078[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=6, orientation=upper-left, xresolution=86, yresolution=94, resolutionunit=2], progressive, precision 8, 980x839, frames 3
Category:	dropped
Size (bytes):	219993
Entropy (8bit):	7.979904012968387
Encrypted:	false
SSDEEP:	6144:NEWd82nRxSghAuEcVBE/f5M+jlqtXP9iLasWR:NZOgHEliYViLwR
MD5:	471D24C03919D9309FF703A5048ABE61
SHA1:	2FD3F22E672334C518A96FE282F784006CD80CCD
SHA-256:	C96678DCBC10B7ECBB128DA7BD59B4B06502374C3FCECCEF9161BB92319CFA61
SHA-512:	B2713DE8021AEC4B5499728380354CB6A69D086883A472356632767506C0D3652B91C7E944C999BCA8AE8E115A7BCE174C644A65EFF95AAC74E385B887813153
Malicious:	false
Reputation:	low
Preview:	JFIF.....Exif..II*.....V.....^.....i.....f.....8c.....8c.....0210.....0100.....G.....C.....!....."\$%. \$.....C.....G.....L.R...*.GJ.+W7r+..lR... Fw+w5s.Wsw!3A...c....2...bU.....X..)`r...-*WeX...b..i.S%..U\..D.1....b.v..S...),*..`..L...).%..l%X.e..C..cD...*.v.....r.w!3JT4u2.....(..)Ew14....A.c5.,N..T...K.T.sV..f..X0... ..R.Wr....e..E.3.@..j).K..4....n.T.).3<.....3J%{...oX...J..JC.J..].Y..D..&.....D....dJ".i..%(SE..P.` V.aQ.U..leZU...(L..&s.*....Ph.....s3R..U)T.."iKV^...AK*....%..d.B.2....)..T.V.)@&Wd.H..KW ...*...][...Z:i*.j*....K*...hR...LgT.....1(.d....*i..&h.e!S(*)..V....9.c."o]si3N...J.f.@.C.KV.Z...lKw9.n.ZJ...cG

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUI\8vIU7ww63mVu7gtR-kwKxNvkNOjw-tbnfY3lCw[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 16372, version 1.1
Category:	downloaded
Size (bytes):	16372
Entropy (8bit):	7.968846044212757
Encrypted:	false
SSDEEP:	384:fG5pL2MJq6wvtv8XHfldnHjAyDH8CzPg+CJDhVp:O5pL2wqNvaeFICyrP
MD5:	2A518C71CCFD06B5BF5C387436778A50
SHA1:	999AA2B5C2F45734A6433F5FA3D5734B96FFA315
SHA-256:	26E17BE4C483220EB6BA8006A42EB4ED9C61CD2604B635453A83CE094DC9CBF4
SHA-512:	4E5E362AEC79CE287553C42612ACD5CED87316AA3A17B3FD136921D2DDE8475E713CAFA2681875B8337B189EC19E93F943612701580B71291FD77327BCDCCFF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/cinzel/v10/8vIU7ww63mVu7gtR-kwKxNvkNOjw-tbnfY3lCw.woff

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\8vIU7ww63mVu7gtR-kwKxNvkNOJw-tbnfY3lCw[1].woff

Preview:	wOFF.....?.....}.....GDEF.....l...k.....1.<GPOS..... j7.N.GSUB.....\...r...OS/2...L...O...`...USTAT.....+...y.l.cmap.....L.6=_gasp...X.....glyf...`./a..PR 8...head.....6...6...!.[hhea.....\$F.Ahmtx.....~...+..loca.<.....maxp.>..... ..Dname.>.....+..L.post..?..... ..2prep..?.....h...x.....E.....\$D) .%AB....}.C..... ...H.P.+L.../..V.k.....GN~V.(.n.w...o...W.....V.Sz...n.x.l.C.\$l...*...m..elkm..em\6.k..yk.7...x.....n.....\$.<u.b.n_s.N.....l.m..*p'.R.T.mu..{8>Yyh...q.5.5qv1.....t.U.>=..... C.0.....q..Q_{8#A..>4....J.0.o tHx.....B..6..#.D.Gl...fF}HJ.....u.@.Z.ta0..Ma-.....c.q:...K...v.1vr.....o...c/.9..8?.K.w<..k.m..h...a.73.../g...S..=MK5...Qx...z...j.Fj..j..j .6j.....).....y...Z.EZ.Z.uZ...L)...g%.o~.3.....<...f~...yC...u.]89.x.<J..._..._1.....3..._+.`7.< ..c...wx.T[q...Y...XqH...lM9K...O...[z...x....
----------	--

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\KFOjCnqEu92Fr1Mu51TzBic6Csl[1].woff

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 21588, version 1.1
Category:	downloaded
Size (bytes):	21588
Entropy (8bit):	7.973550860004932
Encrypted:	false
SSDEEP:	384:9do1erd5msN48bPbceGykR88v9yGLRkcl46tW6amtMQSJCo:9+1erd5vCfRzluCSJV
MD5:	81F57861ED4AC74741F5671E1DFF2FD9
SHA1:	AC3993E9EDC4C30C97FE670AA1E8A7088AA69E31
SHA-256:	EEC142608EB8417E2ACB6E5301A750047A04E2C5A6563223CAAE499E19EA08EE
SHA-512:	F23A7D58BE44E474CB65C368B048EB68AA1B6FEFA4A12797A4A19C8D9E2F1BB7AB6FCEAE2AD17C59283616503107C332EA6245BF9F721BC49A676E8C92F46EC4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v20/KFOjCnqEu92Fr1Mu51TzBic6Csl.woff
Preview:	wOFF.....TT.....GDEF.....G...d...GPOS.....~...GSUB.....'.....r.OS/2.....O...`u...cmap...X.....W.cvt ...P...J...J...ofpgm.....3...c...gasp..... ...glyf.....@W..n.S...hdmx..M4...n.....head..M...6...6...`hhea..M..."...\$...hmtx..N.....=-..loca..P.....maxp..Rh... .. (.name..R.....-=post..Sh.....a.dprep..S.. ...9...Bx...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h~R....R...A.J.x....dK...{....?..F?. ~.m...ms.{Z.;.....U.]7s.....\=D.=7...>...x...D..O].U:... o..3.x.j.r"B...../.)x \$""j.....1LGmaGxQxG....~..".A..hd.z..k.KO.....^}H #z...O.....R..A...9..A..!(/..."...lq1.r.s..r.7r.7s..q.wf....nz..]...2..d4c..c....d...T.1...d.....\.....c9k.g..Yv.#O."%..... ..t"uM..%.....j .#^.....}c.q.i...<jy.D...C.01.2.r.....V...z.W.7b..L.S.41].kUs.X/6..b.....(.([...K...{.^.'.....`#./..B.....N+p.m`...].IQ....Drg.M..Kx.^S.*.....h ..\$k.'Hy.l.ze..4z.-T.....

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\KFOkCnqEu92Fr1Mu51xlIzQ[1].woff

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 21952, version 1.1
Category:	downloaded
Size (bytes):	21952
Entropy (8bit):	7.970421989516302
Encrypted:	false
SSDEEP:	384:LANJRPuW1egrV1qAeQjd3PHH7fS3SIHwip3fzp7lYMa8/h3ELZ2owoRE1F:LAN/Pl1egR7QjRp+3SIHwcLpMYC/h+9U
MD5:	FE65B8335EE19DD944289F9ED3178C78
SHA1:	E9E842D5ED5321DDD719599057E9F8643B2AD539
SHA-256:	80815EFE3BD9317C666DF0F2E6D701335E178954F64EB1E99103FEA81C2AA137
SHA-512:	6E7995EDEBAEF0218C921F5485CDA2B1FDCCFCDC9ED5CF988AA005096BB64BC844CAFA93CE081CFB5A8C896492BD5D70CA2B4D7B71EE9A9EE801A721F9F451087
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v20/KFOkCnqEu92Fr1Mu51xlIzQ.woff
Preview:	wOFF.....U.....GDEF.....G...d...GPOS.....GSUB.....'.....r.OS/2.....O...`t.Rcmap...\$.....W.cvtR...R...-fpgm...p...4....s...gasp.....glyf.. ...A...q^...Phdmx..N...m.....head..O...6...6...ehhea..O8..."...\$...hmtx...O\...v.....}?..loca..Q.....E.'maxp..S..... (.name..S.....:post..T.....a.dprep..T.....D..]x...1.. .P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h~R....R...A.J.x.l.h.a.....l.m.6.1+X...i...y....&.....63.5...2>...x D...ct.Kx..H@b.3.l.l.#u...L.*.....^*4.....rP..{*.....Q... JT::Xu>..T./>...oq.....~.@.....lq./... ..#..".&8.H\$.r...J)..jj...&.f.=9..N9.....'F..8.4...m...m...m.m.n.&X...}.S.n.....PHaE...J*...4..MjJ*..nW)..rn3'/.....ks5zY 5c...Mgg.5...p..rR{c...p..t\8.c=-p...X.(.....7...=-.....!...H(0...{q.JT?.b..z].T...m..vNi...t...:P.R..H...t.....&?.:j.51+S."j.SK'l.^...)S.i.

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\KFOmCnqEu92Fr1Mu4mxM[1].woff

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20268, version 1.1
Category:	downloaded
Size (bytes):	20268
Entropy (8bit):	7.970212610239314
Encrypted:	false
SSDEEP:	384:LyfRPUY1e32pJd75q1DzPjsnouCrZsZtetWFNFfiP0clWvdzNcrm:uJPb1em3dSPjKrZyTwnTk0wvdzh
MD5:	60FA3C0614B8FB2F394FA29944C21540
SHA1:	42C8AE79841C592A26633F10EE9A26C75BCF9273
SHA-256:	C1DC87F99C7FF228806117D58F085C6C573057FA237228081802B7D8D3CF7684
SHA-512:	C921362A52F3187224849EB566E297E48842D121E88C33449A5C6C1193FD4842BBD3EF181D770ADE9707011EB6F4078947B8165FAD51C72C17F43B592439FFF4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v20/KFOmCnqEu92Fr1Mu4mxM.woff

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\KF0mCnqEu92Fr1Mu4mxM[1].woff	
Preview:	wOFF.....O.....P.....GDEF.....G...d...GPOS.....GSUB.....'.....r.OS/2.....P...`t...cmap...\$.....W.cvt.....T...T+...fpgm...p...5...w.`gasp..... ...glyf.....;Q..ID...&0hdmx..H...n.....head..Hx...6...6.j.zhhea..H.....\$...hmtx..H...t.....Xdloca..KD.....BC%.maxp..M0... ..(.name..MP.....t.U9.post..N......mdprep.. N4.....l.f..x...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s..x.h~R...R...A.J.x.l.h.a.....l.m.6.1+.X...i...y...&..._.63.5....2>...x D...ct.Kx..H@b.3..l.#u....L.*.....^*.4....rP..{*Q...JT.:Xu>..T./>...oq.....~..@.....lq./......#..".&8.H\$.f...J)..jj...&.f.=9..N9.....'F..8.4....m...m..m..n..&.X..}...S. ...n.....PHaE...J*...4..MjJ.*..nW)..m3/.....ks5zY 5c...Mgg.5..p..rR{c..p..tl.8.c=..p..X.(.....7...=.....!...H.....(0...{q.JT?.b..z}.'T...m..vNi.....t....:P.R..H...t.....&?..j.51+.S.."j.SK'l.^....)S.i.

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\YouTube%2520Profile%2520Image_edited[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=6, orientation=upper-left, xresolution=86, yresolution=94, resolutionunit=2], progressive, precision 8, 97x97, frames 3
Category:	dropped
Size (bytes):	3417
Entropy (8bit):	7.539112413327532
Encrypted:	false
SSDEEP:	96:0+OEaia3/zmRypvnohFSQ+4ra+wW9sZiD42jr:vxA/zhvnySQ+4GWOYD4Or
MD5:	C020FEFCF4A828B63F9CB66980CEB311
SHA1:	98673FDABD2989E2E3732A9563E6F0AA20C6E186
SHA-256:	7B30EC3923D056F49C356FA8DC4CD89A4A2DCECF25191CB05EEDE20E162394F01
SHA-512:	7CF17B055B92A39CAE0ECC8396FCAC059381D2F97B14F6B53C3B1E886F5B2EF9787A23BEED5C31B22DE67D43034CAF4858BC9C1FDE70DA9A788227B30659FE61
Malicious:	false
Reputation:	low
Preview:	JFIF.....Exif..II*.....V.....^..(.....i.....f.....H.....H.....0210.....0100.....a.....a.....C.....%...#... , #&*)*)--0-(0%)(.....C.....(.....((.....a.a.....q....zGz..Q..)?.^N5 Q^..Q...Q.Wl.=98.g..."[...cx..2.t..-%...U..~.w.LOWD..k~..DaU.3..k....UDKv..DKw~x.I0.Mi.....TD.`.dg.....M@.....\$. 34..!"2@P.....).Pf ...hi%!.M]C5...QG+fD...p..?..=!...M...y.=%6.....E.....('H...W.z.%)D/.....qm...H.E.. 7...kF..G!...\.%...W...0.....!1... "ABQRq...2..3@Pa.....?..%.*)..R ...qVT.....J.....E...y#.T.=..w....._K.....;l.NmB./t.#}...XA....D.^q;..5gm.)v..0..."..k...MZ.:F..i0Q..j...@.....

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\ad_status[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	29
Entropy (8bit):	4.142295219190901
Encrypted:	false
SSDEEP:	3:lZOWFQvn:lQw6n
MD5:	1FA71744DB23D0F8DF9CCE6719DEFCB7
SHA1:	E4BE9B7136697942A036F97CF26EBAF703AD2067
SHA-256:	EED0DC1FDB5D97ED188AE16FD5E1024A5BB744AF47340346BE2146300A6C54B9
SHA-512:	17FA262901B608368EB4B70910DA67E1F11B9CFB2C9DC81844F55BEE1DB3EC11F704D81AB20FDDA973378F9C0DF56EAAD8111F34B92E4161A4D194BA902F82F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.doubleclick.net/instream/ad_status.js
Preview:	window.google_ad_status = 1;.

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\backgroundCommon.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	59902
Entropy (8bit):	5.275476692670295
Encrypted:	false
SSDEEP:	768:0swFxn3u/d+H6zABiBO8XY5CqCYqAgNlPzYxgZFbz7Smz9P4hPGKL46R:0NW0H6sBn8XEqAgNI7B7b4hPh4a
MD5:	35C06A0063B4DBFCFE925C054BABC7CE1
SHA1:	247D78D777E30017AD9CC37753E470313AEE3D7C
SHA-256:	032FC6339688D4684B5383715DDD75AF243498DF2B7903FED1ED9564A379858C
SHA-512:	AAFF14E5140ED94D5F278C0F24728E41B2EB587E2E5BA75EAC959C2D0960A80E6FBF01122B55161650AA490810307C1D35820FB9D9C67C0171764F48F3E8D60C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.6850.0/node_modules/wix-santa/dist/packages-bin/backgroundCommon/backgroundCommon.min.js
Preview:	define("backgroundCommon",["lodash","coreUtils","santa-components","componentsCore","prop-types","skins","warmupUtils","image-client-api","color","pmrpc"],(function(e,t,i,o,a,n,r,s,p,d){return function(e){var t={};function i(o){if(t[o])return t[o].exports;var a=t[o]={o:!,1,exports:{}};return e[o].call(a.exports,a,a.exports,i),a.!=!0,a.exports}return i.m=e,i.c=t,i.d=function(e,t,o){i.o(e,t) Object.defineProperty(e,t,{enumerable:!0,get:o})},i.r=function(e){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.__esModule)return e;var o=Object.create(null);if(i.r(o),Object.defineProperty(o,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var a in e)i.d(o,a,function(t){return e[t]}.bind(null,a));return o},i.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\base[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1556733
Entropy (8bit):	5.576014107543884
Encrypted:	false
SSDEEP:	12288:GuLFoHEMevDNX7LSBGnoZ8f3srbkadrIMi8lw8Yxb3M:bFokMevD17LSwoZ8f3sUKrYP8j
MD5:	4292A9819ADA7B8FCDEDA9C651BDBAEC
SHA1:	45CB20010FCC602B2A1D830C1A31EFEFACE672A1
SHA-256:	9389E2AF2966AA42314AE946A5EE068D9CEBAD0FEFA68CF1825F01EA39AC8239
SHA-512:	B04E0DED4C47CA001AA9F8813F38561DD112EE6C4990ECEABFC9CA805DCDF6B66F9B22180A4EAB02C618458B885BDADCB68359DE473C3BC889865835B65D2FD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube.com/s/player/2e6e57d8/player_ias.vflset/en_US/base.js
Preview:	<pre>var _yt_player={};(function(g){var window=this;/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var ba,da,aaa,ha,ia,ka,pa,qa,ra,sa,ta,u a,baa,caa,va,wa,daa,xa,ya,za,Aa,Ca,Da,Ea,Ia,Ga,La,Ma,gaa,haa,Wa,Xa,Ya,iaa,jaa,\$a,kaa,bb,cb,laa,maa,eb,lb,naa,sb,tb,oa,yb,vb,paa,wb,qaa,raa,saa,Gb,Jb, Kb,Ob,Qb,Rb,Zb,bc,ec,fc,ic,jc,vaa,kc,mc,oc,wc,yc,Bc,Gc,Mc,Nc,Sc,Pc,zaa,Caa,Daa,Eaa,Wc,Xc,Zc,Yc,ad,dd,Faa,Gaa,cd,Haa,ld,md,nd,qd,sd,td,Jaa,ud,vd,zd,Ad, Bd,Cd,Dd,Ed,Fd,Gd,Ld,Nd,Od,Qd,Sd,Td,Laa,Ud,Vd,Wd,Xd,Yd,Zd,fe,he,ke,oe,pe,ve,we,ze,xe,Be,Ee,De,Ce,Qaa,me,Qe,Oe,Pe,Ue,Te,Ie,Ve,We,Saa,\$e,bf,Ze,df,ef,ff, gf,hf,jf,Kf,lf,Taa,uf,qf,Hf,Uaa,Lf,Nf,Pf,Vaa,Qf,Sf,Tf,Uf,Vf,Xf,Yf,Zf,ag,\$f,bg,cg,Yaa,\$aa,aba,cba,hg,ig,kg,mg,ng,dba,og,eba,pg,fba,qg,tg,zg,Ag,Dg,gba,Gg,Fg,Hg,hba,Qg,Rg,S g,iba,Tg,Ug,Vg,Wg,Xg,Yg,Zg,jba,\$g,ah,bh,kba,lba,ch,eh,dh,gh,hh,kh,ih,nba,jh,lh,mh,oh,nh,oba,ph,qba,pba,rba,sh,sba,uh,vh,wh,th,xh,tba,yh,uba,vba,Bh,xb,Dh,Eh,Fh, yba,Hh,Jh,Mh,Ph,Sh,Oh,Nh,Th,zba,Uh,Vh,Wb,Xb,Bba,bi</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\bolt-components[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	29642
Entropy (8bit):	5.309386095525225
Encrypted:	false
SSDEEP:	768:ksXW1cgUt7e8RojAviT/d3A2F0GbM2GOQb:H8RojAvI/d3A2Fzu
MD5:	4AAA5B353FC13CC4D663255ED0CEE7C7
SHA1:	B377411DCD8DAE53A57636620CED628EC716263F
SHA-256:	61665413ECBD4B293E42FFB74DF9D777FEE7B88ED79F56E7738786B131E1E254
SHA-512:	EEC062E9FC74CC2AAED9A8FC9F38F763E6325567F63DB43F7FF663932A2F6492DFCDA9F6D414F93F2AF3FA5DE90F6388E5D6BECC6A443374C440BC4FB3A5CFE6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.6850.0/node_modules/bolt-components/dist/bolt-components.js
Preview:	<pre>!function(e,t){"object"!==typeof exports&&"object"!==typeof module?module.exports=t(require("react"),require("prop-types"),require("santa-components"),require("lo dash"),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</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\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):	334423
Entropy (8bit):	5.444331445326094
Encrypted:	false
SSDEEP:	3072:S6MB+bZrFa4uaKS6UGskNvLJm2jGD89VpTyxsGxohTHZHB8KoRB0PNLW4dspYx6v:JMokQG5oGTdMFM+5
MD5:	28F6BFEE0E92BC77D9E44C862DBAF2227
SHA1:	E6ADD47A203267249338B015214CE197DF79D835
SHA-256:	F8CC79C9C00726285236E3FD345896DDA1D9CCDBACB286779BC30B481949ED1B
SHA-512:	8DE580BE0E77286884F7D18B9952B5EB80E70DFA273102D8F0E523A51C628C017BFD3BF486174E4F3EA08C3A6120304D8C93DA8E307342E5753D810E642B8E04
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.6850.0/bolt-main/app/bolt-main-r.init.js
Preview:	<pre>(this.webpackJsonp=this.webpackJsonp []).push([[4],[214:function(e,n,r){"use strict";e.exports={prefersReducedMotion:function(e){return!(e=e ("undefined"!==typeof wind ow?window:void 0)) [e.matchMedia]&&e.matchMedia("(prefers-reduced-motion: reduce)")].matches}}},215:function(e,n,r){"use strict";function t(e,n){return function(e){if(Arr ay.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()}finally{if(o)throw a}}return r}(e,n)} function(){throw new TypeError("Invalid attempt to destructure non-iterable instance")}{})var o=(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]}}},259:function(e,n,r</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\bolt-main-r.vendors~init[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):	55563
Entropy (8bit):	5.4191008007415284
Encrypted:	false
SSDEEP:	768:QRqKuyYT+yDVLn044tuNzID1tDvj7Z8e1E40NuTOF7g0AP6Xa5VR:QklbL0bwlDfvxuNuTOFBk
MD5:	710D2935DD20DFE14C4365959E5D7EE2
SHA1:	90ADED93A850B2107E687CDA8CB5F14B027E0CAA
SHA-256:	C705DCEAB53921910A621ABA479506047471297349D712918D9234A7E6F77985
SHA-512:	8AA576A0DBB221B844F8E7E9C03E096A4FFA2648050CBFF63DD49EC93175FBF55BFD1FA56CE15D5F74118916B21D0978C5158BFB17912B2F8CAFFD38CE8A585C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.6850.0/bolt-main/app/bolt-main-r.vendors~init.js
Preview:	(this.webpackJsonp=this.webpackJsonp []).push([[8],[183:function(e,l,a){"use strict";Object.defineProperty(l,"__esModule",{value:!0}),l.isRotated=l.getContainerHeight=l.fitToContentHeight=l.height=l.bottom=l.left=l.top=void 0;var o=a(54);l.top=function(e){return e.top},l.left=function(e){return e.left},l.bottom=function(e){return e.top+e.height},l.height=function(e){return e.height},l.fitToContentHeight=function(e){return Boolean(e.fitToContentHeight)},l.getContainerHeight=function(e){return o.max([e.height],o.minHeight[0])},l.isRotated=function(e){return o.isNumber(e.rotationInDegrees)&&0!==(e.rotationInDegrees)},260:function(e,l,a){"use strict";Object.defineProperty(l,"__esModule",{value:!0});var o=a(434);l.isPolicyAllowsBsi=function(e){return l[e].policy e.policy[o.ConsentPolicyCategories.Analytics]&&e.policy[o.ConsentPolicyCategories.Functional]},261:function(e,l,a){"use strict";Object.defineProperty(l,"__esModule",{value:!0}),l.validateExternalApi=function(e){for(var l=[],a=

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\c4392d634a0148fda8b7b2b0ad98293b[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	981
Entropy (8bit):	7.735575389183118
Encrypted:	false
SSDEEP:	24:OghSDouG4NG1H5kUdiNuZyFK8+30PIEmn:3ZH5nQN6f0Pemn
MD5:	A0E4DBD6AA2B04F72AD4D5F66D9D82BB
SHA1:	1057D0E735254A37475FA2E11C1F9E99B579912D
SHA-256:	52DE1FF0683A95E5113B6E179DBAE6A7440862514CBF5E780AAA1CFFD534BA22
SHA-512:	7B50670E4D6BE4A978A62A1BCC6A26F66A9CF9B5B18E0C399B8CD1171DCB10CAEEF5E674B96351D153310D03728F9B837390E000EDDEFDCC3B50435BFEE1D8F11
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....0.....pHYs.....~.....IDATH..W.Mq..o<l,+.i,d#?.D).....i....2~.,Y<....#.l... ..5..Y....{>g.9~.y.....9.s.~...J.F.....sd6.)5..w0....K'.....t=A.p\$Lz.x.....n..P.J.T...xMF.....'.RrGj.. ..D.....9.csN..x.....#.w.BP...i.l.i.#.....B#...*(.'f.l ...(.~R.D...Nbk.r&.)L=..e9...`C.M1...3'E.6;...F..j.*.9...\$Q..1.Ct...n.....\$.)~.N.1S6..].""p.....]FCm...&2.lea=p.k.[.o.D;W.\fS.X(...V::5j /.....*....nq0.i....!\$#.n.... ..u.R.J..@...:"J..l.o.w. S)(K.....)7R.....Dp...w...RDU%.9R&>.z...6.h.1..._y....e d....xN..6.1. ...G...(G.P.y3..U=+N.E.-zb.....8f.".....W..6...8...=.)w5.F>.....O...((.....W.O.y%/"me.?.... ...E::J..X..n.;!Peww.x.....bT...~.O...'.Of.o(~7...x!...1.8..S..n.2.Q....I7..2.w.\v....<.....6.F.....?m.w.\$ju<p...4.v.Z.2.....8.\Y.O.N3.&-...T)f.....^..#R.....V.5....Ys..S.X.E.Z.W&.._@.q....8B6.....t.r.\....].HWr...0o..F.....P9.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\chat-interactivity.chunk.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	97985
Entropy (8bit):	5.7230211830589
Encrypted:	false
SSDEEP:	1536:ZVH8LW3JN4PN8kQTdGUvXqtbXNt1K70SV86d0+kXArqLdLKU+c+hKiZaJBzpCASGO:kQgXH1K70YwSG5lztuciQ
MD5:	8DC4F35492DAFD7EA4FC5296D3B89685
SHA1:	72E55546583EDAA2263D20E969801F03CE8A3DB7
SHA-256:	E41F4E092DBBB6C073BA3E43FB93EBE759A4F42C7CCD81B66584AF00E815B53F
SHA-512:	13201A19D284522390F24DA4EADDF2BBD4BC8082187B8AFE8F0F2FE2FA5C46F0DB759FF571FFBD1BB256B73293FC073138F574B05676E6C36F1223760AA60DD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/chat-widget/1.1761.0/chat-interactivity.chunk.min.css
Preview:	@-webkit-keyframes d5U8T{0%{transform:rotate(0deg)}to{transform:rotate(1turn)}}@keyframes d5U8T{0%{transform:rotate(0deg)}to{transform:rotate(1turn)}}@-webkit-keyframes pulSN{0%{transform:rotate(0deg)}to{transform:rotate(-1turn)}}@keyframes pulSN{0%{transform:rotate(0deg)}to{transform:rotate(-1turn)}}.MKfU-{position:absolute;width:1px;height:1px;overflow:hidden;clip:rect(0,0,0,0)}[dir] .MKfU-{padding:0;margin:-1px;border:0}.fmOgX{display:flex;flex-direction:column;flex:1 1 0px;font-family:HelveticaNeueW01-45Ligh,HelveticaNeueW02-45Ligh,HelveticaNeueW10-45Ligh,Helvetica Neue,Helvetica, Arial,...\, meiryo,..... pro w3,hiragino kaku gothic pro,"sans-serif";position:relative}.chat-madefor .fmOgX,.fmOgX.chat-madefor{font-family:Madefor;font-weight:400}.fmOgX.KdL7Z{flex:1 1 0px;font-family:Avenir-LT-W01_35-Light14 75496,sans-serif}[dir] .fmOgX.KdL7Z{background-color:#fff}.fmOgX._2P3Pr{display:none}._3o5yw{display:flex;justify-content:center;align-items:center;position:abs

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\chat-interactivity.chunk.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\chat-interactivity.chunk.min[1].js	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	1135782
Entropy (8bit):	5.582671882804419
Encrypted:	false
SSDEEP:	12288:F24yBISTSGhp7cOlyx3cme0ToAXj35GL1n8TWN:F/yr1hplolj35GLyWN
MD5:	B3203E579B17659F94E299EAF3E5A886
SHA1:	B819A6FB28A4CAACEB7DA726FF64795BC030D28C
SHA-256:	E5D3F02FD0C578FEC1775E67075432530A662030D6BD89B3CF3D887F3890546E
SHA-512:	3F1DDBD7D15D178EE8EC6D7417416FAACB76D23B94B9FC06B72148AF40EEAC58377C57D57A265494F5CAC02B55E0EDFD59F77B9F7DD42E825384756154B77C0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/chat-widget/1.1761.0/chat-interactivity.chunk.min.js
Preview:	(window.webpackJsonp__wix_chat_widget=window.webpackJsonp__wix_chat_widget []).push([([1],[,function(e,t,n){"use strict";var r=n(1),o=n(18),i=376,a=70,s=100,c=90,u=376,l=310,d=320,p=310,f=376,h=647,m=376,g=549;t.a={navigateToSection:function(e,t,n){return window.Wix.Utills.navigateToSection(e,t,n)},getLocale:function(){return window.Wix.Utills.getLocale()},getCompld:function(){return window.Wix.Utills.getCompld()},getDeviceType:function(){return window.Wix.Utills.getDeviceType()},isMobileDevice:function(){return"mobile"===this.getDeviceType()},colorationDecision:function(e){var t=e.userChoice,n=e.addPanelColor,r=e.defaultColor,i=e.color1;if(t)return t;var a=n r;return a?o.a.isWhite(a)?i:a:""},getColorByParam:function(e){return window.Wix.Styles.getStyleColorByKey(e)},getStyleParams:function(){return new Promise(function(e){window.Wix.Styles.getStyleParams(e)})}),isResponsive:function(){return Object(r.__awaiter)(this,void 0,void 0,function(){var e;return Object(r.__generator)(this,(fun

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\chat-web_translations_6.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):	2782
Entropy (8bit):	4.83911218854014
Encrypted:	false
SSDEEP:	48:IDWXOjGpuDEn/0O2nT0XfqpEtwDp1Dvs4wbLaSj5ZGjjQ6I+4u+LuLoLyLq9BG7n:tCuYncTnT0POEwsn1ZGgqwmMccy
MD5:	7E0F593263ED812D4064DFB321F5F225
SHA1:	AEFFC5C9B28D1C16289B9B85725CCED8B83E0485
SHA-256:	C48A5BD7D207C79DA7BC66FDBDCCD55708DB0953A241303AB79FA414D6C0EE8A
SHA-512:	FE270727134BADDD71F6CCAF10CC5B3173312CFB6B1CC1E4DD95950450279D6BDB0A5037A1C1F1B2764DAF6BE0983871818130B79EC6B7504796086CE2AF8B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/chat-widget/1.1761.0/chat-web_translations_6.chunk.min.js
Preview:	(window.webpackJsonp__wix_chat_widget=window.webpackJsonp__wix_chat_widget []).push([([29],[810:function(e){e.exports=JSON.parse('{"input.placeholder":"Type your message\u0026","input.send":"Send","error.oops":"Oops!","error.unsupported.file.format":"This file type isn\t supported.","error.choose.another.file":"Choose another file","error.file.too.large":"File size is too large. (max size 15MB)","header.availability.available":"Online","header.availability.away":"Offline","pro.tip.sends.on.enter":"When visitors are online, press Enter to send a message.","messages.title.aria-label":"Chat Messages","message.failed.to.send":"Failed to send","message.resend":"Resend","header.cancelButton":"Cancel","header.collapseButtonAriaLabel":"Minimize Chat","header.backButtonAriaLabel":"Back","messages.file-bubble.download-button.aria-label":"Download {{fileName}}","input.buttons.tooltip.emoji":"Emojis","input.buttons.tooltip.attach":"Files","input.buttons.tooltip.close":"Close","input.attachment.bu

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\color.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	18954
Entropy (8bit):	5.462041906644879
Encrypted:	false
SSDEEP:	384:DmUI8qSy0vgJON6aAPXVhuR7DOegpSnoVTX6W9FDW6+I65nFuM9:DTFHN6vPX+7DOegpSnoVT7FDW6bM9
MD5:	7F8F0363808B72AE76DE192F51689D33
SHA1:	212EEE29A63222FD2B558CC5F432347EE31407D8
SHA-256:	CE88CFE2A86DD05C6ED0B3A876C0FD93C3B5CCCAE146D2FB9CF0BA2E2EC729F6
SHA-512:	4846DB41108A0BE652B183C0081746FC0180AC7233B9977254270B3C0073EB09200ABC62A6F8BCD5ADAF3D1F5B56FA746FE495E63316113D486DF22E60E9C697
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/unpkg/santa-external-modules@1.642.0/color-convert/0.2.0/color.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);throw new Error("Cannot find module '"+o+"'")}var f=n[o]={exports:{}};t[o][0].call(f.exports,function(e){var n=t[o][1][e];return s(n?n:e)}),f.f,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){Color=require("./color")},"./color":2}],2:[function(require,module,exports){var convert=require("color-convert"),string=require("color-string");module.exports=function(cssString){return new Color(cssString)};var Color=function(cssString){this.values={rgb:[0,0,0],hsl:[0,0,0],hsv:[0,0,0],cmyk:[0,0,0,0],alpha:1};if(typeof cssString=="string"){var vals=string.getRgba(cssString);if(vals){this.setValues("rgb",vals)}else if(vals=string.getHsla(cssString)){this.setValues("hsl",vals)}}else if(typeof cssString=="object"){var vals=cssString;if(vals["r"]!=un

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\comboBoxInput.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):	28601
Entropy (8bit):	5.409770418089791
Encrypted:	false
SSDEEP:	768:1alrfX1017qTvNX3017qTeXPQk17qTi/kye:AlfX1017qTvNX3017qTeXPQk17qTi/k1
MD5:	395B12E39F05CFC1BC1103B6A4B6FFD9
SHA1:	2F25819F81A2ADFAA7D4CB46ED0351E9DBC80BCB
SHA-256:	716DD9ECD6E34AE60F43FDA9BE789CAE5E63E75BC228F43209AE0ACE600EF2CA
SHA-512:	67DBC90C0519447828FCC99E728F897CFF9BA07EE5FADE1990AC1CC1E481747BFD92C2807BAA5A9A55E7C57C17434994BA624F43558B6171A34C4BA6B486A66
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.6850.0/node_modules/wix-santa/dist/packages-bin/comboBoxInput/comboBoxInput.min.js
Preview:	<pre>define(["comboBoxInput",["!odash","santa-components","componentsCore","prop-types","skins","textCommon"],(function(e,t,o,r,i,l){return function(e){var t={};function o(r){if(t[r])return t[r].exports;var i=t[r]={r,i:!1,exports:{}};return e[r].call(i.exports,i,i.exports,o),i.l=!0,i.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.__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 i in e)o.d(r,i,function(t){return e[t]}.bind(null,i));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.pr</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\componentsCore.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	34991
Entropy (8bit):	5.17646837365467
Encrypted:	false
SSDEEP:	384:k6wh8l/vgtweWdueyEjmRelaHZLVwmZJFDnG23KbVsyzQ3CTKE/fjLwyq4JO:E8zPWC3elaHZLtr/+
MD5:	4FAD83D806007F88A7BC371B7017B383
SHA1:	11ECC2DE685FECE50EB38FC2DF12EAA5FD4D7D6D
SHA-256:	D0EFA80EC69317FB7F6A6FD61C0323F84B7A4C61906AAEA5ADC5B430FE60BCC
SHA-512:	6374290FEDE49B5BB91044D9B340D39BE548F993399BFA16FB47A794655E8163A899B44D139CAFC5C4C3073CBCFE5721E758D4B575B12BFA1A489B576335E84F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.6850.0/node_modules/wix-santa/dist/packages-bin/componentsCore/componentsCore.min.js
Preview:	<pre>define(["componentsCore",["!odash","coreUtils","santa-components","prop-types","skins","reactDOM","zepto","santa-core-utils","warmupUtilsLib","create-react-class","react"],(function(e,t,n,i,r,o,s,a,c,l,u){return function(e){var t={};function n(i){if(t[i])return t[i].exports;var r=t[i]={i:i,l:!1,exports:{}};return e[i].call(r.exports,r,r.exports,n),r.l=!0,r.exports}return n.m=e,n.c=t,n.d=function(e,t,i){n.o(e,t) Object.defineProperty(e,t,{enumerable:!0,get:i})},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.__esModule)return e;var i=Object.create(null);if(n.r(i),Object.defineProperty(i,"default",{enumerable:!0,value:e})),2&t&&"string"!=typeof e)for(var r in e)n.d(i,r,function(t){return e[t]}.bind(null,r));return i},n.n=function(e){var t=e&&e.__esModule?function(){return e.default}:f</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\conductAllInScope[1].json	
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):	324
Entropy (8bit):	4.721870897720395
Encrypted:	false
SSDEEP:	6:YWZcNsiDASI1RjRKsHi5aWRpcNsiDASI1RjRKsHi5aWR7:YWZcHcSDVRKjwWRpcHcSDVRKjwWR7
MD5:	A1687DA587FEE4E2028C48B1422B1E7E
SHA1:	3C9F57E300ED8CFDB5A158AB2918F4D66E3A04F4
SHA-256:	CF707377B5910A3E4F595659EFE00AE483ECCFB02D99220C8747050B5F4976EA
SHA-512:	6097D657A6599D46FCDF9D6103734690571B47348A28BE30AD2396B6D9E91D850639ECE1870870CD86DF521B928126FD7B1511C1BEB0D4C989E5BAE9A8D14EC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.305covidtest.com/_api/wix-laboratory-server/laboratory/conductAllInScope?scope=bookings-viewer-script
Preview:	<pre>{ "specs.bookings.TimetableCleanLoading": "false", "specs.bookings.ViewerScript.DisplayBookButtonOnTT": "true", "specs.bookings.ExpandAllTimeTableElementsOnCsr": "true" }</pre>

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

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\controller.min[1].js	
Size (bytes):	2893
Entropy (8bit):	5.3561144497909865
Encrypted:	false
SSDEEP:	48:N4iuMY62+cSM07ky8ZFZacXKPWFbzh4gbRNL0W41JBALnJJy1wzAdm:NLnpzQr0BWF19NLXYOnJJuwEA
MD5:	46CF0F868FEE119EF3A27AFF2E75B11F
SHA1:	9C823100FBCB657BC3A5A59B5EADD00BEC72BB3B
SHA-256:	DEB2F01E5ABA4EAD0D0DBC9E09F84096F84675E132EB5F327CF063114A89CCCC0
SHA-512:	0858D4CA39320A71DB73BA41CB051CF657047ABCE9AE5C0A5F8BE1A08B81C2C183F3727DBFA015BCA5161DB5371E5E5813E43FDF3DE5B652EE04C6D4612276F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.6850.0/node_modules/wix-santa/dist/packages-bin/controller/controller.min.js
Preview:	<pre>define("controller",["!odash","componentsCore","skins"],(function(e,t,n){return function(e){var t={};function n(i){if(!t[i])return t[i].exports;var o=t[i]={};return e[i].call(o.exports,o,o.exports,n),o.l=!0,o.exports}return n.m=e,n.c=t,n.d=function(e,t){n.o(e,t) Object.defineProperty(e,t,{enumerable:!0,get:i}),n.r=function(e){!function e(i){if(!t[i])return e;if(4&t&&(e=n(e)),8&t)return e;if(4&t&&"object"!==typeof e&&e&&e.__esModule)return e;var i=Object.create(null);if(n.r(i),Object.defineProperty(i,"default",{enumerable:!0,value:e}),2&t&&"string"!==typeof e)for(var o in e)n.d(i,o,function(t){return e[t]}.bind(null,o));return i},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=544)}}(</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\embed[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	30302
Entropy (8bit):	5.551312747838574
Encrypted:	false
SSDEEP:	384:QQRnBfgfFLYRgyq+e8kPVY4dqesOryZ8o51RsKg8rceC9YqorzB/eCPfb7Ye/e2t:QJt+1k9Y4geK551e/EzCzN2RWbUx9II
MD5:	4C813AD38522FEB8B5C6F1091C88BC06
SHA1:	A7B1BB19A147B4263368CA2F841519F53E06739E
SHA-256:	1AA9583F1C65B4B9A6DFABFC88BFF657A762BF23A80A7F28DE9565058672A56D
SHA-512:	B2857F68F81EC2EE1C245D905869C00233BEB587A84018C8CF384EB889A2F84CB894AB7CEC8F3C53888B75E4879ECD3CBC1FAEC7CF422178E2905C8896F443FB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube.com/s/player/2e6e57d8/player_ias.vflset/en_US/embed.js
Preview:	<pre>(function(g){var window=this;var x4=function(a,b){g.mf(a,u,8*b+2);var c=a.u.end();a.C.push(c);a.B+=c.length;c.push(a.B);return c},y4=function(a,b){var c=b.pop();for(c=a.B+a.u.length()-c;127<c;){b.push(c&127 128),c>>>=7,a.B++;b.push(c);a.B++;}Ofa=function(a,b,c){null!=c&&(g.mf(a,u,8*b+1),a=a.u,b=c>>>0,c=Math.floor((c-b)/4294967296)>>>0,g.zf=b,g.Af=c,g.pf(a,g.zf),g.pf(a,g.Af)),z4=function(a,b,c){null!=c&&(g.mf(a,u,8*b),a.u.u.push(c?1:0)),A4=function(a,b,c){if(null!=c){b=x4(a,b);for(var d=a.u,e=0;e<c.length;e++){var f=c.charCodeAt(e);if(128>f)d.u.push(f);else if(2048>f)d.u.push(f>6 192),d.u.push(f&63 128);else if(65536>f)if(55296<=f&&56319>=f&&e+1<c.length){var h=c.charCodeAt(e+1);56320<=h&&57343>=h&&(f=1024*(f-55296)+h-56320+65536,d.u.push(f>18 240),d.u.push(f>12&63 128),d.u.push(f>6&63 128),d.u.push(f&63 128),e++)}else d.u.push(f>12 224),d.u.push(f>6&63 128),d.u.push(f&63 128)}y4(a,b))},B4=function(a,b,c,d){null!=c&&(b=x4(a,b),d(c,a),y4(a,b)),C4=function(a,b,c,d){if(null!=c)f</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\fetch-polyfill[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Pascal source, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	8543
Entropy (8bit):	5.238064281324506
Encrypted:	false
SSDEEP:	192:oQHdiEslZc0rsNYNU5mSJHqI03aej6tZoaMLQO/x5/P80+HcW:ocHslLsP5muHqI0J6tZUO/x5+V
MD5:	04E3CC8A9641B3F9F9C9370F4E9B5BDD
SHA1:	9602A891F583094BB04FD407B253ABCAFFB8C8D0
SHA-256:	DE6C4FFA2BD9FD283610E28D0DB2EC48607AAB39D213A51AEF248673A0A7E980
SHA-512:	58942BCC0F39D620A475B65C1AEB4F18872F68F22C89DEC076906A0DB8BC2B7CCA9357710A7824A0FA7404FF73F41013AECA34609CAACD2187414F7BD0D490F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube.com/yts/jsbin/fetch-polyfill-vfl6MZH8P/fetch-polyfill.js
Preview:	<pre>/*.. Copyright (c) 2014-2016 GitHub, Inc... Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including, without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:.. The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software... THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\focus-visible.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\focus-visible.min[1].js	
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2568
Entropy (8bit):	4.926125141171361
Encrypted:	false
SSDEEP:	48:YFS6+PRAPnJA/xerfQnF6LziHCYJQz2zHUyQgzK0kD6tKDrDhdm:2nA++zK0k4KXj6
MD5:	71959C3FBA69003122E325B1D61CE944
SHA1:	D13BC42139C0A00CB5EAACBF56BD910A81395BDB
SHA-256:	4E128EC13619825F39E42C248E64816A5D1141AD61EC74C700E46C528859F489
SHA-512:	2CE232DE191C731A0E68F47BFEA3E77F6B35B5F17DDE056CC25E88C23D35B13A5B86191BAC842608275299347D834BAA2FAE8CE8C4CEA6420CC043792D927C D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/unpkg/focus-visible@4.1.1/dist/focus-visible.min.js
Preview:	<pre>!function(e,t){"object"==typeof exports&&"undefined"!=typeof module?module?module.exports=t():"function"==typeof define&&define.amd?define(t):t():(0,function(){["use strict";!function(e){var t;function n(o){t (t=!0,e())}"complete"===document.readyState?e():(t=!1,document.addEventListener("DOMContentLoaded",n,!1),window.addEventListener("load",n,!1))}(function(){var e=!0,t=!1,n=null,o={text:!0,search:!0,url:!0,tel:!0,email:!0,password:!0,number:!0,date:!0,month:!0,week:!0,time:!0,datetime:!0,"datetime-local":!0};function d(t){e=!1}function i(){document.addEventListener("mousemove",u),document.addEventListener("mousedown",u),document.addEventListener("mouseup",u),document.addEventLstener("pointermove",u),document.addEventListener("pointerdown",u),document.addEventListener("pointerup",u),document.addEventListener("touchmove",u),document.addEventListener("touchstart",u),document.addEventListener("touchend",u)}function u(t){"html"!==t.target.nodeName.toLowerCase()&&(e=!1,document.removeEventListener("mousemove",</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\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+IAg68JD2kD63:3yQQFVQmwckf9mJQPes852T3
MD5:	D829108208F1EB9B9BC884C5E6C43A54
SHA1:	05A79B7F0738CFD2F2FE3C6CEBDBD0A7702EB44C
SHA-256:	22EE05C11B27143CF6474926408154A2723EC321249FAF6684BACA657F64B723
SHA-512:	51646E8E2B5557949EB5A77B10092ABA6E8575C17E696477CDEF012687E857E9D01B5BD33E511892EFCB8292DB3781323C1CD7440CB9E41C82F8B298A849A1E
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:	<pre>!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,n) 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 Object.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</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\i18next.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	35339
Entropy (8bit):	5.207797263564734
Encrypted:	false
SSDEEP:	768:kWyv90tK1vlfLKA1x0A48z7Xsi79o0438gK4Go:CStK9sAUA48zdzq1
MD5:	3152A9E48E25A997A7B261BE5209854D
SHA1:	D51D8D3C17842240125067135F224191A76227E1
SHA-256:	72223C5F23A10723F6AE2EDF55B04CC2440AE2957E35119BC0A21B96DDB09715
SHA-512:	608FC8A7B7E95D0635F481EE8A3D284D8FB5CB0FD3D1E0C7EB2F44066F62880527BAC12C899F25D4DAE01614003A671A693D69076DEA65A1BD8FFDEDC33FC C3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/unpkg/i18next@10.6.0/dist/umd/i18next.min.js
Preview:	<pre>!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?module.exports=e():"function"==typeof define&&define.amd?define(e):i18next=e()}(this,function(){["use strict";function t(t){return null==t?"":(""+t).forEach(function(t){e[t]&&(n[t]=e[t])})}function n(t,e,n){function o(t){return t&&t.indexOf("#")>-1?t.replace(/##/g,".")}:t}function r(o){return t[t]?"string"==typeof t?for(var i="string"!=typeof e?[],concat(e):e.split("."),i.length>1;(if(r))return;var s=o(i.shift()):t[s]&&n&&(t[s]=new n),t=t[s])return r(o)?{}:{obj:t,k:o(i.shift())}function o(t,e,o){var r=n(t,e,Object),i=r.obj,s=r.k;[s]=o}function r(t,e,o,r){var i=n(t,e,Object),s=i.obj,a=i.k;s[a]=s[a] [],r&&(s[a]=s[a].concat(o)),r[s[a],push(o)]function i(t,e){var o=n(t,e),r=o.obj,i=o.k;if(r)return r[i]}function s(t,e,n){for(var o in e)in e?o in t?"string"==typeof t[o] t[o].instanceof String "string"==typeof e[o] e[o].instanceof String?n&&(t[o]=e[o]):s(t[o],e[o],n):t[o]=e[o];return t}function a(t){retu</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\icon.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	3853
Entropy (8bit):	5.208030590767258
Encrypted:	false
SSDEEP:	96:W42sv+sSOs6h09EKf0zjkWFJagjhGSoEJEFAI:W4tGZb64EKWjkeJJjhGU+W
MD5:	D3DB3ECB054750107A04A354BD99EC00
SHA1:	F3FFFF30683F03E302E4A1542563A03102A0A952
SHA-256:	FBBDE913D2C197C8AB54AB4AC60E555C9108C6CED670D4A2DBFA326DE2EDFE8D
SHA-512:	684523471672541110B0E308F21BB1B8F25963364CD88F9E0AA7833940D4E6441FB3F214E7F70E3ACDE32081A4945C0D2D4FD8F442BACAAEFF1E5A01E8FD7C95
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.6850.0/node_modules/wix-santa/dist/packages-bin/icon/icon.min.js
Preview:	<pre>define("icon",["lodash","santa-components","componentsCore","prop-types","skins","image-client-api","svgShape"],(function(e,t,i,n,s,o,r){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){if("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=f unction(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};return i.d(t,"a",t),t,i.o=function(e,t){return</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\imageZoom.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	38750
Entropy (8bit):	5.269536434389615
Encrypted:	false
SSDEEP:	768:ow2dO+YfHaRdEtM//FBzCqGICmdqUEPO8e8dWJxhAcSv:owSRdEK//FBzCqGICmdqUEPO8Xwb+
MD5:	F42FB164AFC6F7AD5EC3A1CC7981BAC6
SHA1:	1700D79F85DAEB008CCBB8E6F63CA6CCA439F161
SHA-256:	1769FE29326B8DFOD1ECCF798E055ACD7AE4F07C4B926589D0DE913F2617DD55
SHA-512:	CD782EA22049767485F6707E0A8FC083F64E6B5964B279A066D35106CF6D0F7523F54C8FA8E54FC7FACFF966F2D45BF6BF6C382B6A3C5568B4376DBFFE506464
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.6850.0/node_modules/wix-santa/dist/packages-bin/imageZoom/imageZoom.min.js
Preview:	<pre>define("imageZoom",["lodash","coreUtils","santa-components","componentsCore","prop-types","skins","reactDOM","zepto","image-client-api"],(function(t,e,i,n,o,s,a,r,p){return function(t){var e={};function i(n){if(e[n])return e[n].exports;var o=e[n]={i:n,l:!1,exports:{}};return t[n].call(o.exports,o,o.exports,i).o.l=!0,o.exports}return i.m=t,i.c=e,i.d=function(t,e,n){i.o(t,e) Object.defineProperty(t,e,{enumerable:!0,get:n})},i.r=function(t){if("undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(t,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(t,"__esModule",{value:!0})),i.t=function(t,e){if(1&e&&(t=i(t)),8&e)return t;if(4&e&&"object"==typeof t&&t&&t.__esModule)return t;var n=Object.create(null);if(i.r(n),Object.defineProperty(n,"default",{enumerable:!0,value:t}),2&e&&"string"!=typeof t)for(var o in t)i.d(n,o,function(e){return t[e]}.bind(null,o));return n},i.n=function(t){var e=t&&t.__esModule?function(){return t.default}:function(){return t};return i.d(e,"a",e</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\index[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	17345
Entropy (8bit):	5.483964980087909
Encrypted:	false
SSDEEP:	384:toBlrTQKXuXfCNgKAGA58//IOGVW8ZUpryoogLLnhlwzGYzedt5HdCVjsamH/pCaU:tcTQKXuXf9R9osMfc
MD5:	DB7971B6EF2368EDD4A476B3023ADDB4
SHA1:	F8DBCBD8EF841AD0AC7DF44A8308A5EE195E2805
SHA-256:	66FD37B6F7EF5BF62C7975ABF3CA5F9EEF2B3719F9A8AEE3F91583C71281A7EB
SHA-512:	11B481160095EA737232B5872F99D4A1A6EF43765460D003F90058378C9CF573D0916D4601396878ED287A33BD90DB0F24E35E6F65E39FA21FE2487351DED1C3
Malicious:	false
Reputation:	low
Preview:	<pre><!DOCTYPE html>.<html dir="ltr">.<head>.<meta charset="utf-8">.<title>Chat</title>.<meta name="viewport" content="width=device-width, height=device-height, initial-scale=1, user-scalable=0">.<link type="image/png" href="//www.wix.com/favicon.ico" rel="shortcut icon">.<script>.<startLoadTime.<window.startLoadTime = Date.now();.</script>.<script src="//static.parastorage.com/polyfill/v3/polyfill.min.js?features=default,es2015,es2016,es2017,es2018,es2019,fetch&flags=gated&unknown=polyfill" crossorigin></script>.<script src="//static.parastorage.com/services/chat-widget/1.1761.0/assets/sentry-lazy-load.js" crossorigin></script>.<script src="//static.parastorage.com/unpkg-semver/fedops-logger@5/fedops-logger.bundle.min.js" crossorigin></script>.<script>.<window.fedopsLogger &&window.fedopsLogger.reportAppLoadStarted("chat-widget");.</script>.<link rel="stylesheet" href="//static.parastorage.com/services/third-party/fonts/Helv</pre>

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

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\languages[1].css	
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	147852
Entropy (8bit):	5.388217935026759
Encrypted:	false
SSDEEP:	768:TgWunx7fP7BKtMMWGW7fa+8eVnT2xM2TE9gr5hQetnKSQBcDjubWym9rmu3wQDOv:8WuntPwwWa+VnT1y4+lemuRqrda
MD5:	77D01F82174315CD56F3866094D6FC16
SHA1:	6EDF46993DD4E68E1C18CF4DB8E57C62ED2D64A7
SHA-256:	D953AC17FBD2BCAB6B88C651CCBBA98B668577ACD838CAD472BBEF1684234216
SHA-512:	142999267CBC41B231965816A04776CBCB45580C5A56303AA147339F79D8430EC19F9E84C42192393BC5105BDBED95D1BBA3E69D1103665A2571CB52EF55F509
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/santa-resources/resources/viewer/user-site-fonts/v10/languages.css
Preview:	/* This CSS resource incorporates links to font software which is the valuable copyrighted property of Monotype Imaging and/or its suppliers. You may not attempt to copy, install, redistribute, convert, modify or reverse engineer this font software. Please contact Monotype Imaging with any questions regarding Web fonts: http://webfonts.fonts.com. */ @font-face { font-family: "Helvetica-W01-Roman"; src: url("/static.parastorage.com/services/third-party/fonts/user-site-fonts/fonts/ea95b44a-eab7-4bd1-861c-e73535e7f652.eot?#iefix") 2.eot?#iefix" format("eot"), url("/static.parastorage.com/services/third-party/fonts/user-site-fonts/fonts/4021a3b9-f782-438b-aeb4-c008109a8b64.woff") format("woff"), url("/static.parastorage.com/services/third-party/fonts/user-site-fonts/fonts/669f79ed-002c-4ff6-965c-9da453968504.ttf") format("truetype"), url("/static

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\linkBar.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	6869
Entropy (8bit):	5.216632414121463
Encrypted:	false
SSDEEP:	96:sdV/XMHhVjbOdVBWFJ1JzvWIDDpq/tML2YUaOrFLWZAilphsXO:sdV0BVjbOdVBeJ1JalDpqKL2R6A8IO
MD5:	6BD6B74867500E418E1133B9FE4BECF6
SHA1:	F0356FF4E7B01745557BA80331C4F052D56C2991
SHA-256:	98532B43C8F1CC372BC2571A0491C0884A8997905F9DF0D2F6FDA228389557C2
SHA-512:	FC4DB371F21692ECD72D86BAFA9CF5B5C42BBD7EBAD891EEE6F7AA3BB6D5E78EDAEB806792071A4893CB5E0E86C1767152653BBD77BA9E6D12221F6EBBAF0C1F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.6850.0/node_modules/wix-santa/dist/packages-bin/linkBar/linkBar.min.js
Preview:	<pre>define(["linkBar", "lodash", "coreUtils", "santa-components", "componentsCore", "prop-types", "skins"], (function (i, e, t, n, s, o) { return function (i) { var e = {}; function t(n) { if (e[n]) return e[n].exports; var s = e[n] = {i: n, l: 1, exports: {}}; return i[n].call(s.exports, s, s.exports, t); } s.l = 0; s.exports = t; m = i, t.c = e, t.d = function (i, e, n) { t.o(i, e) Object.defineProperty(i, e, {enumerable: !0, get: n}); }; t.r = function (i) { if ("undefined" != typeof Symbol && Symbol.toStringTag && Object.defineProperty(i, Symbol.toStringTag, {value: "Module"}), Object.defineProperty(i, "__esModule", {value: !0})), t.t = function (i, e) { if (1 && (i !== t(i), 8 & e)) return i; if (4 && "object" === typeof i && !i.__esModule) return i; var n = Object.create(null); if (t(n), Object.defineProperty(n, "default", {enumerable: !0, value: i}), 2 && "string" != typeof i) for (var s in i) t.d(n, s, function (e) { return i[e].bind(null, s); }); return n; }, t.n = function (i) { var e = i && !i.__esModule ? function () { return i.default; } : function () { return i; }; return t.d(e, "a", e), t.o = function (i, e) { return Object.prototype </pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\loginSocialBar.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	23495
Entropy (8bit):	5.304552647334787
Encrypted:	false
SSDEEP:	384:PNPJU0O47kCjTicm2U2JmzJbdyeJNvYPZEsGmLprB6DmHV1h:PNwCjFuvFbOTHpV6aR
MD5:	8BFC3EAC99B0273BF0536D0235C4FFC7
SHA1:	04FDB4877783CC503951B9BCA4973E83B473766A
SHA-256:	04C486558F39EDC950C519895522CB64D6B0440AE46A812A4465A562F9A98618
SHA-512:	D7AE4A6C0A1D53D4C1B6464D86DC6A211B5BD0D36349AFFB02D82DAA734FBC79E58468FA9291DBEA970D3F7B5F9890A9881F9BA096D162823BAC1EA1DDB0BE8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.6850.0/node_modules/wix-santa/dist/packages-bin/loginSocialBar/loginSocialBar.min.js
Preview:	<pre>define(["loginSocialBar", "lodash", "coreUtils", "santa-components", "componentsCore", "prop-types", "skins", "ReactDOM", "zepto", "textCommon", "icon"], (function (t, e, n, i, o, a, r, s, p, l) { return function (t) { var e = {}; function n(i) { if (e[i]) return e[i].exports; var o = e[i] = {i: i, l: 1, exports: {}}; return t[i].call(o.exports, o, o.exports, n); } o.l = 0; o.exports = t; n.m = t, n.c = e, n.d = function (t, e, i) { n.o(t, e) Object.defineProperty(t, e, {enumerable: !0, get: i}); }; n.r = function (t) { if ("undefined" != typeof Symbol && Symbol.toStringTag && Object.defineProperty(t, Symbol.toStringTag, {value: "Module"}), Object.defineProperty(t, "__esModule", {value: !0})), n.t = function (t, e) { if (1 && (t !== n(t), 8 & e)) return t; if (4 && "object" === typeof t && !t.__esModule) return t; var i = Object.create(null); if (n(i), Object.defineProperty(i, "default", {enumerable: !0, value: t}), 2 && "string" != typeof t) for (var o in t) n.d(i, o, function (e) { return t[e].bind(null, o); }); return i; }, n.n = function (t) { var e = t && !t.__esModule ? function () { return t.default; } : function () { return t; }; return n.d(e, "a", e), n.o = function (i, e) { </pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\main-r.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):	187768
Entropy (8bit):	5.273513878490774
Encrypted:	false
SSDEEP:	1536:a59bq/cmzVXq+7dojCXRaQ0PPVCchD4BuBLHGHEhghURTCx3N8a2KH1NjOF287qc:tBzZojCht8gveGH1cDnb4Y
MD5:	C65F2967BD01DADD4FFCD9E349AB0191
SHA1:	C18C7294EE5D5F457ACE195B399594BA2B540486
SHA-256:	BDDC24B4F45DF2C663A7342A61787ECA4AA3ACFE45CB28AC9AECEEE2646D2918
SHA-512:	440C7844D9C9641E6B8FF0B234345909FA2F65C39ED0B478E24A4D83C8942F76C86BC72F6DEAD1F55ECFB2CEC978FE966D0A8421E3326420FE84BB477C946BA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.6850.0/bolt-main/app/main-r.min.js
Preview:	!function(e){function t(t){for(var n,o,i=t[0],a=t[1],s=0,c=[];s<i.length;s++)o=i[s],Object.prototype.hasOwnProperty.call(r,o)&&r[o]&&c.push(r[o][0]),r[o]=0;for(n in a)Object.prototype.hasOwnProperty.call(a,n)&&(e[n]=a[n]);for(u&&u(t);c.length;)c.shift(){}var n={},r=[5:0];function o(t){if(n[t])return n[t].exports;var r=n[t]={t,t:!1,exports:{}};return e[t].call(r.exports,r,r.exports,o),r.l=!0,r.exports}o.e=function(e){var t=[],n=r[e];if(!n)if(n)t.push(n[2]);else{var i=new Promise(function(t,o){n=r[e]=[t,o]};t.push(n[2]=i);var a,s=document.createElement("script");s.charset="utf-8",s.timeout=1800,o.nc&&s.setAttribute("nonce",o.nc),s.src=function(e){return o.p+"bolt-main-r."+(1:"animations",2:"bolt-ds-viewer-manager",3:"custom-elements",4:"init",6:"vendors-bolt-ds-viewer-manager",7:"vendors-custom-elements",8:"vendors-init",9:"vendors-pro-layouts")][e]]e)+"}.js"}(e),o!==s.src.indexOf(window.location.origin+"/")&&(s.crossOrigin="anonymous");var u=new Error;a=function(t){s.onerror=s.on

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\moment.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):	51679
Entropy (8bit):	5.447871951833024
Encrypted:	false
SSDEEP:	768:TZUhhcH6fhB0KWkh32WUsW3wQ3hglmJbP38l/tOC:NUckhBbWA2fsWthJbPsT
MD5:	8999B8B5D07E9C6077AC5AC6BC942968
SHA1:	5E8A4CF3C77C1BB13E966E702422E9D25B98BA14
SHA-256:	0AEB4ECF1091B9C52C9FA0BA4DC118B1ABAFBD88A51278935E574F6BAFF0BB49
SHA-512:	3B663C843F373D0B517FCBDCAF437ECB1C11B44AC855A1C9E0D3A9A23CEADB2BD49A18896D0213F4E018BB6EEDFA6564F35E2DFA89E00551B1F981B294809591
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/unpkg/moment@2.22.2/min/moment.min.js
Preview:	!function(e,t){"object"===typeof exports&&"undefined"!==typeof module?module.exports=t(:"function"===typeof define&&define.amd?define(t):e.moment=t()){this,function(){use strict";var e,i;function c(){return e.apply(null,arguments)}function o(e){return e instanceof Array "object Array"===Object.prototype.toString.call(e)}function u(e){return null!=e&&"object Object"===Object.prototype.toString.call(e)}function l(e){return void 0===e}function d(e){return"number"===typeof e "object Number"===Object.prototype.toString.call(e)}function h(e){return e instanceof Date "object Date"===Object.prototype.toString.call(e)}function f(e,t){var n,s=[];for(n=0;n<e.length;++n)s.push(t(e[n],n));return s}function m(e,t){return Object.prototype.hasOwnProperty.call(e,t)}function _(e,t){for(var n in t)m(t,n)&&(e[n]=t[n]);return m(t,"toString")&&(e.toString=t.toString),m(t,"valueOf")&&(e.valueOf=t.valueOf),e}function y(e,t,n,s){return Ot(e,t,n,s,0).utc()}function g(e){return null==e._pf&&(e._pf={emp

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\nuFvD-vYSZviVYUbj_r3ij__anPXJzDwcbmjWBN2PKeiunDXbtU[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 33480, version 1.1
Category:	downloaded
Size (bytes):	33480
Entropy (8bit):	7.9856119299250405
Encrypted:	false
SSDEEP:	768:+rn9WMDGnbbzfE7sZ4l1ESbfjld0sDrkN16kl1E0OYG1cNq:M9RKbb2sZ4ICSDjldHDrw6S1E0OYOcA
MD5:	CF6BD31685B729A7FD0B5E9764C675A1
SHA1:	D54CAEC10CD0894EF14E78366DA7DC1F40A27D93
SHA-256:	CFAF5FEA94455E72D8A8CE2BE5CE9C0C72F6C15E4194755D3288712C842C909C
SHA-512:	1F90504C13398BC68F66686EC5D6E669E035107359A1BB35B845D9A440F0E66FB7181B3BE803E939718588C4FE85B61A431D74911956FE3CBBA680A6D86F0BE1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/playfairdisplay/v21/nuFvD-vYSZviVYUbj_r3ij__anPXJzDwcbmjWBN2PKeiunDXbtU.woff
Preview:	wOFF.....GDEF.....>...X.h...GPOS.....]/.w6GSUB...4...*.x...QOS/2...`...O...`]#.?STAT.....=...R.F.cmap.....tk.Fqcv...P...(.fpgm.....6.gasp.."......glyf..".X...r.#.head..{H...6...6...hhea..{.....\$.Ehmtx..{.....^!.loca..~(.Y...Z)...maxp.....name.....U...S.nPost.....prep.....Zx....P...i...l3..j.4D.....5..l.k...Js.xJ.%.....W.x.L...@.....s...m.m.m.6...7.....(.r...ap...))".X.....Y.....4o.....Y.....N.x..6Lj)n9l...@.lr.r.f[...>...o;.....]m..d\$.m.*.K.c.FuO..K...k.A...WQ).E...r..nO..._j.N_L.....6...%...dmp%.O/%.R]...W^.ZT..NT..G...].V...T.g..Y.....E..FO.z...g..aq..!.IGs.`.40....>o[.7..].5.hN7....C9....6.%c.&1.....X.XM.b..c.6b..Y..d9..<V..Y..d->U?.l3].n..f..X.f.....{..#K...l.m..6.f.....~.m...lg.m.W.s.{V/.N...Y...H.DK....Q]-.J.d.3....\BQ.Q...4e(K9.S..T..?T.

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\platform-viewer[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.0950611313667666
Encrypted:	false
SSDEEP:	3:CUMIRPQEsJ9pse:Gl3QEsJLse
MD5:	AD4B0F606E0F8465BC4C4C170B37E1A3
SHA1:	50B30FD5F87C85FE5CBA2635CB83316CA71250D7
SHA-256:	CF4724B2F736ED1A0AE6BC28F1EAD963D9CD2C1FD87B6EF32E7799FC1C5C8BDA
SHA-512:	EBFE0C0DF4BCC167D5CB6EBDD379F9083DF62BEF63A23818E1C6ADF0F64B65467EA58B7CD4D03CF0A1B1A2B07FB7B969BF35F25F1F8538CC65CF3EEBDF8A910
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://frog.wix.com/platform-viewer?_msid=4594be45-f3c2-4e13-aa22-94a76fbc6c3c&rid=1608321044.06512581992101218&vsi=7530f800-331a-45fe-8bb8-ace90ad7a83b&_av=bolt-1.6850.0&_siteOwnerId=48ccc542-6eb6-4698-bfaa-668208aa2b85&_viewMode=site&_apld=675bbcef-18d8-41f5-800e-131ec9e08762&_instanceId=d8ec26b2-28d6-41f2-b06e-8c76091f9420&src=79&_brandId=wix&_ms=-1&evid=133&worker_id=xfeqr&_visitorId=3884edc5-fe34-4c8c-b42d-83c326a81294&_siteMemberId=undefined&bsi=5a2cde2a-5fd4-4dc6-b63c-07a8a10c35cd%7C1&_lv=2.0.875&_id=16083534672330
Preview:	GIF89a.....!.....L.;

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\popupContainer.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	6177
Entropy (8bit):	5.167940769159615
Encrypted:	false
SSDEEP:	192:HWCCp/yj6CpyBKAcM+sLHEmcS3V/pQireJv:JrCrCEBGKz4v
MD5:	E7B5D380A01AF8CB4A151E73122C1457
SHA1:	A5521D720F82D1C66241FBFB3CD48CCECA6950ED
SHA-256:	D6E586C7557F7338C8A925A092C872AF7AD48010D86E8198E24297AABAC6693E
SHA-512:	5C22A4AFBB38A17D7FC948E575F5C5EC3FF1125151503DA9BF12970255737D309BDC3133E834C638E52CEEF4B5AEEBBB80F08B14EF53B87F5463B946C131173
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.6850.0/node_modules/wix-santa/dist/packages-bin/popupContainer/popupContainer.min.js
Preview:	<pre>define("popupContainer",["!odash","santa-components","componentsCore","reactDOM","components"],(function(e,n,t,i,r){return function(e){var n={};function t(i){if(n[i])return n[i].exports;var r=n[i]=[{i,i,!1,exports:[]}];return e[i].call(r,exports,r,exports,t),r.l=!0,r,exports;return t.m=e,t.c=n,t.d=function(e,n,i){t.o(e,n) Object.defineProperty(e,n,{enumerable:!0,get:i});},t.r=function(e){("undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})),t.t=function(e,n){if(1&n&&(e=t(e)),8&n)return e;if(4&n&&"object"==typeof e&&e.__esModule)return e;var i=Object.create(null);if(t.r(i),Object.defineProperty(i,"default",{enumerable:!0,value:e})),2&n&&"string"!=typeof e)for(var r in e)t.d(i,r,function(n){return e[n]}).bind(null,r);return i},t.n=function(e){var n=e&&e.__esModule?function(){return e.default}:function(){return e};return t.d(n,"a",n),n},t.o=function(e,n){return Object.prototype.has</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\runtime-configuration[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	18
Entropy (8bit):	3.683542362433231
Encrypted:	false
SSDEEP:	3:YNEXM9wq:YQMj
MD5:	672AB3C59846686D319B74E1AA8C1321
SHA1:	0D0003A5ACB476774A5E8AA9BF2DAA1669ACE009
SHA-256:	F4C08C763C671201ADA6CE004013B1393011AB32021BADAF9AB6C9B98B495BA8
SHA-512:	6B27810F687D55872398793406A7F6E77EC02901EC0F448D85303115CD1E7FA3FF415FF3475D12AA67A5EFC3755365E6816DD6AC6271DF02C970E1CED2A54DE3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.305covidtest.com/_api/wix-code-telemetry-registry-public/v1/sites/4594be45-f3c2-4e13-aa22-94a76fbc6c3c/telemetry/runtime-configuration
Preview:	{"hasSinks":false}

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\sentry-lazy-load[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1860
Entropy (8bit):	5.447318412294747

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\sentry-lazy-load[1].js	
Encrypted:	false
SSDEEP:	48:R6wWcKtffGvcwAjZhHzh9zeg4FzaCGMeI6tAClsqBLCC8/dyZ:DMtffGkZzhF9zsmZIH3S8kZ
MD5:	CF3EE43C2A9A4A84B14C14876D3EE790
SHA1:	EEB5B175059C1D4A5E166D85B0E4CA42F2B49B97
SHA-256:	85E5479C4A58725CB283FBFE701C4A9144B00D144655FD0BB31F20C582686F47
SHA-512:	F1194F085D10CDF958ECA38B68F8D0A9C0FC68911A735BD48091ECD26A4191C3500F1EB57A30452919E3B12363E711365D5DE10ACB72F424E17E69752B8590A7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/chat-widget/1.1761.0/assets/sentry-lazy-load.js
Preview:	<pre>(function(c,u,v,n,p,e,z,A,w){function k(a){if(!x){x=!0;var l=u.getElementsByTagName(v)[0],d=u.createElement(v);d.src=A;d.crossorigin="anonymous";d.addEventListener("load",function(){try{c[n]=r;c[p]=t;var b=c[e],d=b.init;b.init=function(a){for(var b in a)Object.prototype.hasOwnProperty.call(a,b)&&(w[b]=a[b]);d(w)};B(a,b)}catch(g){console.error(g)}}).parentNode.insertBefore(d,l)}}function B(a,l){try{for(var d=m.data,b=0;b<a.length;b++)if("function"===typeof a[b])a[b]();var e=!1,g=c.__SENTRY__,u=undefined;!===.typeof g&&g.hub&&g.hub.getClient()&&(e=!0);g=1;for(b=0;b<d.length;b++)if(d[b].f){g=!0;var f=d[b];!1===e&&"init"!==f.f&&l.init();e=!0;lf.f.apply(l,f.a)}!1===e&&!1===g&&l.init();var h=c[n],k=c[p];for(b=0;b<d.length;b++)d[b].e&&h?h.apply(c,d[b].e):d[b].p&&k&&k.apply(c,d[b].p)}catch(C){console.error(C)}}for(var f=!0,y=1,q=0;q<document.scripts.length;q++)if(-1<document.scripts[q].src.indexOf(z)){f="no"!==document.scripts[q].getAttribute("data-lazy");break}var x=!1,h=[],m=function(a</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\site-widget.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):	401631
Entropy (8bit):	5.481225197889377
Encrypted:	false
SSDEEP:	6144:rYTRxhqB2Xzn742zQyuuROuyV5/7t27hm21la81yx3cme0D:sqB2D7RLyx3cme0D
MD5:	8FACDB92D1A0486CDE8C7F84246D47EB
SHA1:	5DABEDF153B0F2FBF79CE4037D636D39BE1D6AB5
SHA-256:	CD04FFF81101B1519F98866892FD16814795914F6ADD45F571D6DD6C500AEF4F
SHA-512:	A083B07F8A56CA0601C04FE66104FA29912A5F9839F44A5486B4119F5D451528B9A19DEE8B7222D0824ECF3D790DFD6B7BD0E412B66338ED2D88C30B72BB7695
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/chat-widget/1.1761.0/site-widget.bundle.min.js
Preview:	<pre>!function(e){function t(t){for(var n,r,i=t[0],a=t[1],s=0,u=[],j:s<i.length;s++)r=i[s],Object.prototype.hasOwnProperty.call(o,r)&&o[r]&&u.push(o[r][0]),o[r]=0;for(n in a)Object.prototype.hasOwnProperty.call(a,n)&&(e[n]=a[n]);for(c&&c(t);u.length;)u.shift(){}var n={},r={37:0},o={37:0};function i(t){if(!n[t])return n[t].exports;var r=n[t]={i:t,l:!1,exports:{}};return e[t].call(r.exports,r,r.exports,i),r.l=!0,r.exports}i.e=function(e){var t=[];r[e]?t.push(r[e]):0!==r[e]&&{1:1}[e]&&t.push(r[e]=new Promise(((function(t,n){for(var o={1:"chat-interactivity",2:"chat-web_translations_0",3:"chat-web_translations_1",4:"chat-web_translations_10",5:"chat-web_translations_11",6:"chat-web_translations_12",7:"chat-web_translations_13",8:"chat-web_translations_14",9:"chat-web_translations_15",10:"chat-web_translations_16",11:"chat-web_translations_17",12:"chat-web_translations_18",13:"chat-web_translations_19",14:"chat-web_translations_2",15:"chat-web_translations_20",16:"chat-web_translations_21",17:"cha</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\siteRegionContainer.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1616
Entropy (8bit):	5.09951754547316
Encrypted:	false
SSDEEP:	24:P6oyWYbVOEBmGaFza9ywMasBLMCizflpkxfqgUALh4iUMH7IPPcUWSGjPjJie+sy:2douBa9yVB4hokM0Lh4MH7AUUWFJxDm
MD5:	046F1DCE78A38E778EC6D09DCBAFE51F
SHA1:	B245636E56F97C87F656C3907E2C5D29A4C38087
SHA-256:	57B006EB597A387160060A8C773067D8E3523E31AA722AE0909A602AA74AA032
SHA-512:	0905696C2810FAEBD901AA918E6BB9A70D3DB27A0CE73AF1A10C0269A08F52431D08BDDC98D7A074F6DA621D7DDDA2619AAFD132ABB09E7542ED9B5FB0D4CCE7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.6850.0/node_modules/wix-santa/dist/packages-bin/siteRegionContainer/siteRegionContainer.min.js
Preview:	<pre>define("siteRegionContainer",["lodash","santa-components","componentsCore"],(function(e,n,t){return function(e){var n={};function t(r){if(!n[r])return n[r].exports;var i=n[r]={i:r,l:!1,exports:{}};return e[r].call(i.exports,i,i.exports,t),i.l=!0,i.exports}return t.m=e,t.c=n,t.d=function(e,n,r){t.o(e,n) Object.defineProperty(e,n,{enumerable:!0,get:r})},t.r=function(e){"undefined"!==typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},t.t=function(e,n){if(1&n&&(e=t(e)),8&n)return e;if(4&n&&"object"===typeof e&&e.__esModule)return e;var r=Object.create(null);if(t.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:e}),2&n&&"string"===typeof e)for(var i in e)t.d(r,i,function(n){return e[n]}.bind(null,i));return r},t.n=function(e){var n=e&&e.__esModule?fuction(){return e.default}:function(){return e};return t.d(n,"a",n),t.o=function(e,n){return Object.prototype.hasOwnProperty.call(e,n)},</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\siteTags.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):	10023
Entropy (8bit):	5.40195664160435

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\E\0W10PBUV\siteTags.bundle.min[1].js	
Encrypted:	false
SSDEEP:	192:LhPo3b3jpHMjTPoCkKZqWMqDuE6zuG+PFFrjuutdbTPV6rGgLBS:9Po3zFHMBWQaGWFF+42a
MD5:	7393002F4FC8EF5F38345DCFB8CC8CE3
SHA1:	E664B02F56BDD85DE327CAAD4691CDF91E5F9C3E
SHA-256:	A99795E2EA888569C3089C0E7074DC969CB6A60D565F491C86D6ED7B980396A4
SHA-512:	BB353997BC0C9A5591B4808B7975ACC123A86983299425C8C83D1F8FD2514C9B53A23D445B063EA2402581DA8DC689BE50F97183A2964B80A03A5D93718D8148
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/tag-manager-client/1.240.0/siteTags.bundle.min.js
Preview:	<pre>!function(t){var e={};function n(o){if(e[o])return e[o].exports;var r=e[o]={:o,!1,exports:{}};return t[o].call(r.exports,r,r.exports,n),r.l=!0,r.exports}n.m=t,n.c=e,n.d=function(t,e,o){n.o(t,e) Object.defineProperty(t,e,{enumerable:!0,get:o})},n.r=function(t){"undefined"!==typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(t,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(t,"__esModule",{value:!0})},n.t=function(t,e){if(1&e&&(t=n(t)),8&e)return t;if(4&e&&"object"===typeof t&&t.__esModule)return t;var o=Object.create(null);if(n.r(o),Object.defineProperty(o,"default",{enumerable:!0,value:t}),2&e&&"string"!==typeof t)for(var r in t)n.d(o,r,function(e){return t[e]}.bind(null,r));return o},n.n=function(t){var e=t.__esModule?function(){return t.default}:function(){return t};return n.d(e,"a",e),n.o=function(t,e){return Object.prototype.hasOwnProperty.call(t,e)},n.p="https://static.parastorage.com/services/tag-manager-client/1.240.0/",n.s=7)}(function(t,e,n){"use</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\E\0W10PBUV\svgShape.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	13927
Entropy (8bit):	5.23032371042699
Encrypted:	false
SSDEEP:	384:gOf19xvP64xBFgU32KY2SKFgJFg8igHAURsjfi:fJ3mkVFgF1imAusO
MD5:	640ED0A10AC9425DD849732EAFDB4E10
SHA1:	9AC4124CD7BD69DA68AE9F2A34DD0773E409E72E
SHA-256:	2DEE769F4A07C891E2975748F08A9C0874070FE48E07A461F034B4988BCA23BC
SHA-512:	CBD96C1A9FF8E0075E7B72330C5EB7565047DCDD39560A0D7FCD481D03476489E29390A13BF16275D1BDDA212205EA354AC20C1B6B85E7970EA0325873F58C1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.6850.0/node_modules/wix-santa/dist/packages-bin/svgShape/svgShape.min.js
Preview:	<pre>define("svgShape",["lodash","coreUtils","santa-components","componentsCore","prop-types","skins"],(function(e,t,i,o,s,n){return function(e){var t={};function i(o){if(t[o])return t[o].exports;var s=t[o]={i:o,!1,exports:{}};return e[o].call(s.exports,s,s.exports,i),s.l=!0,s.exports}return i.m=e,i.c=t,i.d=function(e,t,o){i.o(e,t) Object.definePropeerty(e,t,{enumerable:!0,get:o})},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.__esModule)return e;var o=Object.create(null);if(i.r(o),Object.defineProperty(o,"default",{enumerable:!0,value:e}),2&t&&"string"!==typeof e)for(var s in e)i.d(o,s,function(t){return e[t]}.bind(null,s));return o},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(e,t){return Object.prototype</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\E\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):	5.203479999750975
Encrypted:	false
SSDEEP:	192:jczj1yqBPBT2nQc94VEqMz9hrbZ4IDDwzgH1AdyfCpncv4:01yznXWVNodPDkyH1fC1cv4
MD5:	AF5B3F24573746CD1C4BBC45DB91343B
SHA1:	A7CDDA921BC1620A5F8E99C0A9A23A6AAB5BB87B
SHA-256:	708FEF38A7C33DB9EB397A8B8422002D1947974886F3D16EE7BF6B3A312D1DCA
SHA-512:	6E0CBC3C13C6AAA88969A1F207DC335FA6C97ACDC86001FB71C8C2DD4CC278D6345DBA6C10578D7EE8B7D66D2BBF34685EBEDE3C81D78FD9A98A4C24BAE1178
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.6850.0/node_modules/wix-santa/dist/packages-bin/thirdPartyAnalytics/thirdPartyAnalytics.min.js
Preview:	<pre>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,!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.__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),t.o=function(n,e){return Object.prototype.hasOwnProperty.call(n,e)},t.p</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\E\0W10PBUV\verticalMenu.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	47602
Entropy (8bit):	5.397672265225456

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\verticalMenu.min[1].js	
Encrypted:	false
SSDEEP:	768:EjISEmDDVt+VLktJbCKjVgM3+/KSiriD9GPMi6L1iD3tiwfltTtiEttV:EjP+ZkJCM3+8iD9lmrM
MD5:	2F0C28835B813FF1C4D4E06A5BE49592
SHA1:	8CFB28547E083D292A3959B75BEE812FA66A87E6
SHA-256:	0FCD9DC97E2C03BC1F70CA0E7A4523CC74A853ADC827AA684088F0A8954D3A36
SHA-512:	1A9BAC33845322FF92D08942BDE0C95BE131E97EBAB752F80B6A23ED9CD47D1EE7665F7FF2578896474DD47BCF2040A949EF612A7394CAF6AB1605ABBE439C/3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.6850.0/node_modules/wix-santa/dist/packages-bin/verticalMenu/verticalMenu.min.js
Preview:	<pre>define(["verticalMenu",["lodash","coreUtils","santa-components","componentsCore","skins","reactDOM","zepto","create-react-class","react","comboBoxInput"],(function(e,t,n,i,a,r,o,s,l,u){return function(e){var t={};function n(i){if(t[i])return t[i].exports;var a=t[i]=[i,i,!1,exports:{}]};return e[i].call(a.exports,a,a.exports,n),a.l=!0,a.exports)return n.m=e,n.c=t,n.d=function(e,t){n.o(e,t) Object.defineProperty(e,t,{enumerable:!0,get:i})},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.__esModule)return e;var i=Object.create(null);if(n.r(i),Object.defineProperty(i,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var a in e)n.d(i,a,function(){return e[t]}.bind(null,a));return i},n.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\w8gYH2oyX-I0_rvR6HmX23YM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 13628, version 1.1
Category:	downloaded
Size (bytes):	13628
Entropy (8bit):	7.9490664619580045
Encrypted:	false
SSDEEP:	192:vfsiidjHrkxKUVajUiB67PqyY6+jQxj8Js0/B2+TOoCoKFQDcFWuf9BSo07LbP:UTyajf6pq/n/B2+TOoCoxcF19UPP
MD5:	A6EB5E20688668FD618395D28F68A4B7
SHA1:	8C1B2B68E62E1CE08E81360880A4C83EB28D30F1
SHA-256:	6B113506CB8B2708BEF061A89B204195C162FE25F5572A6EEBC36CD075E01C0D
SHA-512:	2AD6633C56976B760EC9E8D6AD5F53C5CADF91D4B6F960C4AB9A7793075696B586AFA1E0009DF9E8AC7E057690F267B36DE11A78F512D1D866967BC584348D9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/spinnaker/v12/w8gYH2oyX-I0_rvR6HmX23YM.woff
Preview:	<pre>wOFF.....5<.....P.....GDEF.....l.....GPOS.....OS/2.....W....`jv..cmap.....q....j.m]cvt ...`...&...&O.lfpgm.....a.A..gasp...x.....glyf.....*...B...v.head...d...4...6... hhea.....\$.{\hmtx.....%...l...].loca..0.....maxp...2....Lname...2.....(D.post..3.....0...-prep..54.....h.....x.c f..8.....u..1...<f...d.400.... 8.Y...AAa{?l.....@aF.....x.c`...bf ...H.0..Ex...3.2.3.c..tGADAJANAI.Ja...@U....APYa.....%H.....O.....o.l{.....}.....T.%.....*.....x..j..f.@...Mzm.....M.@...C.rG.w(...2.....6l.....f."S!..Q./...1....Q.h.....EIT.8+..f.T...U...=..I.8..)D.o....9..=0.Z\$.&.1.G....t.v...R.oj...9..\$R...cp..-6..Q?.e..fkq....\`.....].2h^....":...EW.M.IN.&M...Ej...N....'k\.....x.{@S...o.d%\$.6..De..L.q....Xq.p."(uT...U...:k...Z*...%....j.#..s.9...=...N..L...</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\warmupUtils[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):	127409
Entropy (8bit):	5.517468044228542
Encrypted:	false
SSDEEP:	1536:OPfgCbzdzxNvzTBy9WFJ+JgzNyqRToMnkQrP76:KNzdxzNvZyuJ+4NyqRToMkQrPO
MD5:	F5A2A7713F1331A46E2464BA77E729D4
SHA1:	EA39D479C6D761A16861337D35D7882FAFDB2A2B
SHA-256:	480B4064A778A695E9BF840CDED3E0F60DE010B25E614B4BCA8CEC896D95EC8E
SHA-512:	106492D84740C638E08722EF223214E18A4006E4F8624AE93B18EF7AEAD1407EE01882D20E75FBCE66E8AA7DC01C16AC58F74389F2E4B3964D7D0766D492960F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/unpkg/santa-core-utils@1.2685.0/dist/warmupUtils.js
Preview:	<pre>!function(e,a){"object"==typeof exports&&"object"==typeof module?module.exports=a(require("lodash"),require("zepto"),require("image-client-api")):"function"==typeof define&&define.amd?define(["lodash","zepto","image-client-api"],a):"object"==typeof exports?exports.warmupUtils=a(require("lodash"),require("zepto"),require("image-client-api")):e.warmupUtils=a(e.lodash,e.zepto,e["image-client-api"])}(this,(function(e,a,t){return function(e){var a={};function t(i){if(a[i])return a[i].exports;var r=a[i]=[i,i,!1,exports:{}]};return e[i].call(r.exports,r,r.exports,t),r.l=!0,r.exports)return t.m=e,t.c=a,t.d=function(e,a,i){t.o(e,a) Object.defineProperty(e,a,{enumerable:!0,get:i})},t.r=function(e)("undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},t.t=function(e,a){if(1&a&&(e=t(e)),8&a)return e;if(4&a&&"object"==typeof e&&e.__esModule)return e;var i=Object.create(null);if(t.r(i),Objec</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\wixcode-worker[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with LF, NEL line terminators
Category:	downloaded
Size (bytes):	766264
Entropy (8bit):	5.338859820606061

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\wixcode-worker[1].js	
Encrypted:	false
SSDEEP:	6144:h/YUwrCmFz6BZZI2a3Jb2hZxcL405TsRRKRRSuf4elxLD:Hw9exYJbo4Lj5oRRKRRZF4A
MD5:	797A0E4CDA8DBC29B125E1FDAB456CAF
SHA1:	54F68A708F0A7AB8A883E492E318A616130DC382
SHA-256:	D5086F1C355134BA0070AD1A0A1F8A7C19F104BF37C995BDB6344DE0C7A8879A
SHA-512:	2341430D3CF3E6CB310FEBF292D248BDA2BC75C6990C2D390377C62FFDED690076A7D680E268942BC2AC9434CE6E81944DE14F76F8EEA7B851722A4334BE922
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.305covidtest.com/_partials/wix-bolt/1.6850.0/node_modules/viewer-platform-worker/dist/wixcode-worker.js
Preview:	!function(e){var t={};function __webpack_require__(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,__webpack_require__),r.l=!0,r.exports}__webpack_require__.m=e,__webpack_require__.c=t,__webpack_require__.d=function(e,t,n){__webpack_require__.o(e,t){Object.defineProperty(e,t,{enumerable:!0,get:n})}},__webpack_require__.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},__webpack_require__.t=function(e,t){if(1&t&&(e=__webpack_require__(e)),8&t)return e;if(4&t&&"object"==typeof e&&e.__esModule)return e;var n=Object.create(null);if(__webpack_require__.r(n),Object.defineProperty(n,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var r in e)__webpack_require__.d(n,r,function(t){return e[t]}.bind(null,r));return n},__webpack_require__.n=function(e){var t=e&&.__esModule?function(){return e.d

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\www-embed-player[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	158179
Entropy (8bit):	5.572597210173082
Encrypted:	false
SSDEEP:	1536:8YO2jaPL8+0umrda+4WR3w/nMUI7UMHl1mnfYKSL10pQl2nGaXyegz2iCArJCzye:SgGWgX6QD/aXyeKQn3Fkzer2F+2RO/
MD5:	4C8A1C5F426B866BA2D65C46DEE55FB8
SHA1:	97748E566D4287DC656A7238DF885B1D6B2D80D0
SHA-256:	98D5FD76B756305B41A77DBAF34D99D2A0FBE26D4CC000CA1EB16D5BB3A8B39A
SHA-512:	6335D042CF1FEA390DE968D20955308D11C48BAE0F2158B306424846899B020CC8FDCE015AC421C41F3145F5BAA9D1A23FDBBFFE5AC22208E4A17AA02FD49D0F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube.com/s/player/2e6e57d8/www-embed-player.vflset/www-embed-player.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/var n,function aa(a){var b=0;return function(){return b<a.length?(done:!1,value:a[b++]).{done:!0}}.var ba="function"==typeof Object.defineProperty?Object.defineProperty:function(a,b,c){if(a==Array.prototype a==Object.prototype)return a;a[b]=c.value;return a};function da(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}.var ea=da(this);function t(a,b){if(b)a:{for(var c=ea,d=a.split("."),e=0;e<d.length-1;e++){var f=d[e];if(!f in c)break a;c=c[f]}d=d[d.length-1];e=c[d];f=b(e);fl=e&&null!=f&&ba(c,d,{configurable:!0,writable:!0,value:f})}}.t("Symbol",function(a){function b(e){if(this instanceof b)throw new TypeError("Symbol is not a constructor");return new c("jscomp_symbol_"+(e "")+ "_"+d++

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\www-player[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	342215
Entropy (8bit):	5.235976614317677
Encrypted:	false
SSDEEP:	1536:X6u/Cd+RN6DQI03rpHrpY/fn8MZv8M5q4ayPOP5fRrDjciMfByr5G0TwecZecoXM:X6u/nLOXdzPv2QAG
MD5:	DA54234E5F30E70692D14628B8FDDDD39
SHA1:	4265F8B536EE60714F9C381FC382CA18195BC569
SHA-256:	1ADEA903BB714598209EAC077B6AADCA23D978364B6F7494C05184A96F31E043
SHA-512:	670694AEF5AD9C4E0E3D13E601AC8A16E0E59CC72F9B3898BA5ED6577B280BB3F66B78CA816B84973BAF21AE779E4FFBC27EFD021EC70431D7C776E511A5AFED
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube.com/s/player/2e6e57d8/www-player.css
Preview:	.html5-video-player{position:relative;width:100%;height:100%;overflow:hidden;z-index:0;outline:0;font-family:"YouTube Noto",Roboto,Arial,Helvetica,sans-serif;color:#eee;text-align:left;direction:ltr;font-size:11px;line-height:1.3;-webkit-font-smoothing:antialiased;-webkit-tap-highlight-color:rgba(0,0,0,0);touch-action:manipulation;-ms-high-contrast-adjust:none}.html5-video-player:not(.ytp-transparent),.html5-video-player.unstarted-mode,.html5-video-player.ad-showing,.html5-video-player.ended-mode,.html5-video-player.ytp-fullscreen{background-color:#000;ytp-big-mode{font-size:17px}.ytp-autohide{cursor:none}.html5-video-player a{color:inherit;text-decoration:none;-moz-transition:color .1s cubic-bezier(0,0,0,0.2,1);-webkit-transition:color .1s cubic-bezier(0,0,0,0.2,1);transition:color .1s cubic-bezier(0,0,0,0.2,1);outline:0}.html5-video-player a:hover{color:#fff;-moz-transition:color .1s cubic-bezier(0,4,0,0,1,1);-webkit-transition:color .1s cubic-bezier(0,4,0,0,1,1);transition:co

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\1ef5834e68214aa6a18823ce92a9e76c[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=6, orientation=upper-left, xresolution=86, yresolution=94, resolutionunit=2], progressive, precision 8, 1263x906, frames 3
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\1ef5834e68214aa6a18823ce92a9e76c[1].jpg	
Size (bytes):	163151
Entropy (8bit):	7.976996444636384
Encrypted:	false
SSDEEP:	3072:EEKgbP/y4tRh9YRkEO4G5IEfkGgG6Gp0nr7c3horJPVz3mT:EVgzDh9YCFTpBpp0nfcCVz3mT
MD5:	86097EA410B8A0927C6726F91A9C17A8
SHA1:	88FF5FD818FFF164EC3D16F9EC533E5039AEEC07
SHA-256:	3B25B3B59DF1A24E3117AAD1C43A328E7A0D47D61FE3988BE0459C907EB6ABFF
SHA-512:	C4F1F53520685DC5D4BC59CE01E440E6B8666953239DFD65C3798EBAC9A177E888D569F7FA098C1580560A86D36E88B78538AD7044CDF6F4A7D8F85EEAC7211
Malicious:	false
Reputation:	low
Preview:	JFIF.....Exif..II*.....V.....^.....(.....i.....f.....8c.....8c.....0210.....0100.....ICC_PROFILE..... ..lcms.....mntrRGB XYZacspMSFT.....sawscrtl.....-hand...=@...=@t..."......desc....._cpvt.....wpt.....rXYZ.....gXYZ...@...bXYZ...T.. ..rTRC...h...`gTRC...h...`bTRC...h...`desc.....uRGB.....text...CC0.XYZT.....XYZo...8...XYZb.....XYZ\$......curv.....*...u....N....b.....j.. C\$.j..~3.9.?.FWM6Tv..d..l..uV~...,6.....e.w.....C.....l....."\$".\$.C.....i.c..l..\$.N8..\$.B... ..8.8.8.RN\$.I\$.I9f..I\$...\$.N\$.N8... ..8...VN8... ..8..

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\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 8.878 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 1.816.152 2.705.032.295.091.581.133.873.085.589.173 1.176.298 1.751.073.338.169.665.256.997.135.515.273 1.027.439 1.529.114.342.243.675.37 1.01.18.476.369.945.577 1.406.149.331.308.657.472.98.225.446.463.883.714 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 1.182.22.444.342.494.662.728.405.415.833.801 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\NetCache\IE\MEEXW4H4\17177d158c36d432b93f51e54f80e2f3c[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 22 x 22, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	634
Entropy (8bit):	7.545667213369081
Encrypted:	false
SSDEEP:	12:6v/7+0mH/oeexdxIoPwBQz6INTvgn4YWEcs/0qPgLxnOnc:v0mflDPloPIQuMsNPExb
MD5:	73BE2697BF39B0CC1CAC65DB744ADAD6
SHA1:	290A074B6E1B04C9FF0B5370E34BFCA088696501
SHA-256:	44B599805F020322BBA77BD2D08816AEF1152C9E10559D25573D0A258A0EBD9B
SHA-512:	0823C6EF002927934357BF3768F12C235A40A2F715F2BD2AB12623E5C6EE2C2A60343D59BE96ADDB062CFFC27E1886C830EA487AADBA80C33B2837E452C8017
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....[.....pHYs.....~.....IDAT8..U.N.A.=A...!D...>)R#.....l.....IDG...[...*%[d.XrC,h.RPD.RR...wys.;c.*Y.inwv.....~?h.A...k.M4....^/...A.EA..\."9...f.;Bj\$(k.Z.k.Z..D...\$.2.p.H^x'.....k._'X...[Q.^B.q..r]...R.*.X.E--0.d'.%.. ...o....#...[.....Ez.....HR)...[w..U.T.;<.....H.N[.8.....E h`.5..l.W..2V..l...bK-....D...^DFb..~.....<.....VY.j;V.o.&.SO[:.q.[.....U.ye..j.?6o...Sr.. W"L[...s...hb..S...j5.....[...l...W.....0...m.[...F.U.. .....N..gH..u.7....nw.-.?...L..?...&..m.T*.v.....i.....?9.....E.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\180c34ad2-27c2-4d99-90fa-985fd64ab81a[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 30020, version 1.0
Category:	downloaded
Size (bytes):	30020
Entropy (8bit):	7.979293085282587
Encrypted:	false
SSDEEP:	768:AtJY2qy2d921nq8roOpK9hc50ofFZmke+AC6:AzjWwdp+WHmkQC6

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\80c34ad2-27c2-4d99-90fa-985fd64ab81a[1].woff	
MD5:	1BE02808B155074BFC2142997613C9F6
SHA1:	BD36CFF3F0995CF8F927B76164D70FE6EEEEBC8D2
SHA-256:	0F09BBCE04E459AF7E81A503AA70615E7A1BC25AD9CA68FC841A34ADADFDC4F5
SHA-512:	0212E75DBAEBE491B1F030E07443189D8EBC8920E12FBD976836A57C571BC63C10FEDEC9D20C1F10186DB1AE757F85EF1F950F7E412ED71AAB526C0821FAAE8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/third-party/fonts/user-site-fonts/fonts/80c34ad2-27c2-4d99-90fa-985fd64ab81a.woff
Preview:	wOFF.....uD.....\$......OS/2...X...`...H.cmap.....2.....C.cvt.....M.....o.(fpgm...4...+...P...gasp...`.....glyf...h..N.....~Jhead..W`...6...6.R.4hhea..W....`...\$... ...hmtx..W.....H.kern..ZL...V...Rpat.loca.f.....maxp.i....._name.i.....N..post..sT.....2prep..sh.....H..8Gx.c`f.g.....@....a).....x...).LL..=c8.[... ...d.....d..c&..x...O+Q...s.;&4.4.d.4.s5..M.4FS\$....4..._.E>..Av.6d.>....Vz..b.....<W...D....@..B.*""bBT....._w.]zw^....4*.b....^S..e).....jSl..q...3..9.an.(.8..Nr....Z.F..L.EQL:- '.5.....N.lh...K.../i.m.>.[{e3..vX; m...yp....).AS0.&gz..7<..\.....zFO.Q..1.y..}.]M.uZ.UZ.R.....H.xm..x.c.....a.....0.1....o.'..._a....(.#...../0..M...4..fP<..... ..x..VOo.G..j]\$\$.].8.....R6.v...Y!q...v....a...8#UJO.M>D?.[NNO.8=...zFzBT U.....'j...7....o.....7..}y....W>...'W]...[t.....x..g....S.....c.C9)c

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\BookingServicePageController.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):	223615
Entropy (8bit):	5.389118193460554
Encrypted:	false
SSDEEP:	3072:AW7SBvJ/cv92ipIRhIqj6T4RDeJEXKkQt4cnNX:AwS7/pipIHIGF9eC6ucnNX
MD5:	F99301D54F4C504CC5154C8FE14A4EB3
SHA1:	B71EF9B1603F7F4F79FBB6D4281D7F939B6D5320
SHA-256:	E4634603FCE8462071653C022A26AB906099E39E6CCC2FB753D4E0E5A485B3DA
SHA-512:	ABD556609356F820AC03B71A7EA27071118B52FE9DD5C609A31EAE2DB14CA5727C401AC6E7937D68DDFA025B2E30F32D918342CA116915FDD58BF528862513B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/bookings-service-details-widget/1.578.0/BookingServicePageController.bundle.min.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.BookingServicePageController=t():e.BookingServicePageController=t()))(self,function(){return function(e){var t=[];function n(i){if(t[i])return t[i].exports;var o=t[i]=[i, l:1,exports:{}]};return e[i].call(o,exports,o,o,exports,n),o.l=!0,o.exports}return n.m=e,n.c=t,n.d=function(e,t,i){n.o(e,t) Object.defineProperty(e,t,{enumerable:!0,get:i})},n.r=f unction(e){if("undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{va lue:!0})),n.t=function(e,t){if(1&t&&(e=n(e)),8&t)return e;if(4&t&&"object"===typeof e&&e.__esModule)return e;var i=Object.create(null);if(n.r(i),Object.defineProperty(i ,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var o in e)n.d(i,o,function(t){return e[t]}.bind(null,o));return i},n.n=function(e){va

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\IVS0AW9K.htm	
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):	622698
Entropy (8bit):	5.608991588710549
Encrypted:	false
SSDEEP:	6144:8T8tfrDQW8PwERy4+IemuRmdsISFWVpVyei+wgD8PwERy4+IemuRmdLQWVpVn
MD5:	4B9EA844BD6EFC47DF90F06699FA1874
SHA1:	6FED4C8B6C282E9B24D0305FABD39A2C1F2E56FA
SHA-256:	08C7FDD4512C08FF0555489C49791057DF686BAF8915C9E4B6A1F8FA9FD43C99
SHA-512:	80B71F307E73DE128B8A8BA18A97938A99871A8782FAC6DE6306E1326B654E05F64DA2F6778173EEF2243D9564BAAD30EB418A5379EB4D8D3202FF3043ECCBF/
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.305covidtest.com/
Preview:	<!DOCTYPE html>.<html lang="en">.<head>.<meta http-equiv="X-UA-Compatible" content="IE=Edge"/>.<meta charset="utf-8"/>.<meta name="generator" c ontent="Wix.com Website Builder"/>.<link rel="shortcut icon" href="https://static.wixstatic.com/media/48ccc5_559838b644e94acf903cd64ed867b15b%7Emv2.png/v1/f ill/w_32%2Ch_32%2Clg_1%2Cusm_0.66_1.00_0.01/48ccc5_559838b644e94acf903cd64ed867b15b%7Emv2.png" type="image/png"/>.<link rel="apple-touch-icon" hre f="https://static.wixstatic.com/media/48ccc5_559838b644e94acf903cd64ed867b15b%7Emv2.png/v1/fill/w_32%2Ch_32%2Clg_1%2Cusm_0.66_1.00_0.01/48cc c5_559838b644e94acf903cd64ed867b15b%7Emv2.png" type="image/png"/>.<meta http-equiv="X-Wix-Meta-Site-Id" content="4594be45-f3c2-4e13-aa22- 94a76fbc6c3c"/>.<meta http-equiv="X-Wix-Application-Instance-Id" content="c3f57661-0fd2-4cdf-b78d-7e0167881a75"/>.<meta http-equiv="X-Wix- Published-Version" content="610"/>.<meta name

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\J_JJD_e5-5g[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	45209
Entropy (8bit):	5.9296177623393875
Encrypted:	false
SSDEEP:	768:uCD/BR6oVfOKUvkNW6m8PliqEaoUi9wwY9TQ9JMRlBAWlyM:PUvoWRLJEHUCy9IlbYM

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\KFOMCnqEu92Fr1Mu4mxM[1].woff	
SSDEEP:	384:ozNCb8EbW9Wg166uwroOp/taiap3K6MC4fsPPuzt+7NCXzS65XZELt:K4zbWcDVwt230hfs+x+Bb65X2
MD5:	BAFB105BAEB22D965C70FE52BA6B49D9
SHA1:	934014CC9BBE5883542BE756B3146C05844B254F
SHA-256:	1570F866BF6EAE82041E407280894A86AD2B8B275E01908AE156914DC693A4ED
SHA-512:	85A91773B0283E3B2400C773527542228478CC1B9E8AD8EA62435D705E98702A40BEDF26CB5B0900DD8FECC79F802B8C1839184E787D9416886DBC73DFF22A64
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOMCnqEu92Fr1Mu4mxM.woff
Preview:	wOFF.....Mp.....P.....GDEF.....G...d....GPOS.....hGSUB.....7b..OS/2.....R...`tq#.cmap.....L....cvt.....T...T+...fpgm.....5....w.`gasp...@..... ...glyf...L...+...j....hdmx..Fx...g.....head..F...6...6.j.zhhea..G.....\$....hmtx..G8...].....Vloca..l.....?..#maxp..Kt... ..name..K.....tU9.post..Ld......m.dprep..Lx.....l .f.x...1..P.....PB..U..-l..@..B)..w.....Y.e.u.m.C.s...x.h..~R....R.....2.x....[#N..m.m.m.mfm....SP..NuM..9].=-.U..l..[.....w...].....^p...H.....).....;.EoDo....E.E.D.. ..0.GG.aA.H.V.MxXA...../.d3.Eb..J...R.^v.....\^ob.}.z.k.x).v\$\$.O)+.2..*....y)6`C6b.6cs...l.....!.....<..o....l%4.L.Sl.&C.6..f'...{...c..l.J.(.2.C....V.A..?.M<nG.v..m.;.R.C..aj.H...=-.{>:.....}j_.....o.&k..KY.2..6k....l}.{.p}.//.....VO3.oj.fj....R-TZ...;..RN..&V...C...3.?.....&..z.s&D....r,l...t.R..a\$K..Mm..Y.U...+b.%kQ..

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\UC3ZEjagJi85gF9qFaBgIMITpqSvb0EhPNqvdm-qG4s[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 39200, version 1.1
Category:	downloaded
Size (bytes):	39200
Entropy (8bit):	7.988476528497157
Encrypted:	false
SSDEEP:	768:q/qT2SfXajfRAQqdqUipouEYPSKekld90b93WkL53Xhq:n:iAfUlqdqh5ZP30ub9m653Rqn
MD5:	EF6258EE945F6CAE26A89326C61B1530
SHA1:	08E36BB0B86A58F0BB5619FB581DFBB1FE191C91
SHA-256:	BBA4D2A847FEB1C4988D78B5AAF66AC1FA20A41D661677DFE13F0837CEFC6264
SHA-512:	B701B529E525453DD1344E33B5C82ED049C1245142A193821B29437E86BE5E9FA53CA7F2CB3881D582DF4262D47F4EEEE41E542C36A69620999C9D31EA86C8B36
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/playfairdisplay/v13/UC3ZEjagJi85gF9qFaBgIMITpqSvb0EhPNqvdm-qG4s.woff
Preview:	wOFF.....GDEF.....@...F.V.GGPOS.....0~b...GSUB...T.....l.kOS/2...T...O...`]...cmap.....Y.Jcvt.....E....."fpgm.....F...m>...gasp..". ...glyf..."gE.....>.head...h...6...6....hhea.....\$.f..hmtx.....loca.....D.qmaxp.....^..name.....'?..X.post.....}T"Rprep... .....`x.%...0...h#.....b/n"... ~+.3]ab`E6.jp.;?...K..l.....x.V..dW.....m.....m.v...m...V.y...U.....Q...3...K.t.p.K...sX...;.....>.;.3...x..c.8..."*.d.-:.[[[:Z.[Z.V....g=l.h...iw.7...w....O...-.'.R..R\$.R ".R&...-.....5.W..@\$.l*.J.;.n.G...yP..7.. K.Q...D.....34).h>J.2H.K...J]!.....l....W.d.".....)y@...&..[.d.<?.dE.'Ef..\$Y..+IV...d.!+DV...Ya.#...#H....Ky.Z..~m\$[-.+V.L.....i2.d..j#+. ..f..Opi..UO.]H.jPh..1.J..@..V.....J.s..\$Z...M.2...Y.9..s.=^.....d...i..G+.51...v.?...OR.D.Z.J."-f]e<..g.-7....H^#9..k....re0Q..X;w...5....K..L.\$

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\YaMN4Oy8AhH-iW3da0J-Nuczn6meMMc-yumwdmwUIQ[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):	21984
Entropy (8bit):	5.5594185274243
Encrypted:	false
SSDEEP:	384:T7PhU5RRSU8QcV74RNeiDhSnK2XYylSohrNsHKTqM0s+LbYHiw52hK0Ud:HKrTcV0ZQNUqShK4QTd
MD5:	C3B7FD6FD68E34D3619107F3C29921D8
SHA1:	91E1FB9AF705728CF2B995E7058B5B8D362F27E2
SHA-256:	61A30DE0ECBC0211FE896DD6B427E36E7339FA99E30C73ECAE9B0766C085084
SHA-512:	1821103406952E044454C250419656318B5BEB89D70522A154E8016BBBD759676337377AA2EA0A043E47449EBB204CC13D81E59EC24196F8A82F7C3525BC77D1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/js/bg/YaMN4Oy8AhH-iW3da0J-Nuczn6meMMc-yumwdmwUIQ.js
Preview:	(function(){var J=function(Q,I){if(!(I=(Q=null,v).trustedTypes,I)) I.createPolicy)return Q;try{Q=I.createPolicy("bg",{createHTML:r,createScript:r,createScriptURL:r})}catch(h){v.console.log&&v.console.error(h.message)}return Q},r=function(Q){return Q},v=this self;(0,eval)(function(Q){return(Q=J())&&1===eval(Q.createScript("1"))?function(I){return Q.createScript(I)}:function(I){return""+I})()}(Array(7824*Math.random()) 0).join(""+n")+ (function(){var QX,m=function(Q,I){return(I=typeof Q,"object")===I&&null!=Q} "function"===I},R=this self,l=ofunction(Q,I){return I<Q?-1:I>Q?1:0},vB=function(Q,I){function v(){((Q.prototype=(Q.U5=(v.prototype=l.prototype,l).prototype,new v),Q).prototype.const ructor=Q,Q).D\$=function(h,H,r){for(var J=Array(arguments.length-2),U=2;U<arguments.length;U++)J[U-2]=arguments[U];return l.prototype[H].apply(h,J)}};rg=function(Q){for(Q=0;64>Q;++Q)Z[Q]="ABCDEFGHIJKLMNPOQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789-_" .charAt(Q),B["ABCDEFGHIJKLMNPOQRSTUVWXYZabcdefghijklmnopqr

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\la896d9_d443be72e31c4eea992d3f969d0f3841[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 69 x 69, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	433
Entropy (8bit):	7.138785974210364
Encrypted:	false
SSDEEP:	12:6v/7j Ox31AbQOFBVyJdNevl7hqWDMnNqBf27:ke31MFBVzI7YWiNcf0

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\app.bundle.min[1].js	
SHA-512:	5E2019D434F777554AC914399606CEFFA361E45E7CBAB370A81541D263303BBFCD9364F309D8A6F5E966AFCAFA543C6201B56D4CE9C77296CEFFAC591EBDB
Malicious:	false
Reputation:	low
IE Cache URL:	http://static.parastorage.com/services/santa-members-viewer-app/1.639.0/app.bundle.min.js
Preview:	<pre>!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():("function"==typeof define&&define.amd?define("santa-members-viewer-script",[],t):("object"==typeof exports?exports["santa-members-viewer-script"]=t():e["santa-members-viewer-script"]=t())("undefined"!=typeof self?self:this,(function(){return funct ion(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=functio n(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,Sym bol.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,fun</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\app[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):	74992
Entropy (8bit):	5.354305690847076
Encrypted:	false
SSDEEP:	1536:IV7t5vQePXd2i6L2zc/ZBxhbD+NxpeBi0:z7t5vbXd2VL2zaZ5D+Nxx
MD5:	F4F925A874B278C63D7168D2E2C10714
SHA1:	934B9BB0F26097D82FC3935D4C889228CE227AF6
SHA-256:	9FCD949430740F683400178CDDF67509C82FC8D1A10D2846C26B8FD4C216C9EF
SHA-512:	B3EDC43CB3E0B809B54A5D00A49F172648E2F22EC1EFC7D14AF6A2C9366965009D0CC45F05D0EED66E1C599B54A58FF39B4C2A6AD652EF70754BC14FA03B2EB9
Malicious:	false
Reputation:	low
IE Cache URL:	http://static.parastorage.com/services/wix-code-viewer-app/1.702.0/app.js
Preview:	<pre>!function(e,r){"object"==typeof exports&&"object"==typeof module?module.exports=r(require("_")):"function"==typeof define&&define.amd?define(["_"],r):("object"==typeof exports?exports["wix-code-viewer-app"]=r(require("_")):e["wix-code-viewer-app"]=r(e._))("undefined"!=typeof self?self:this,function(e){return function(t,n) {if(r[r])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}return t.m=e,t.c=r,t.d=function(e,r,n){t.o(e,r) Object. defineProperty(e,r,{enumerable:!0,get:n})},t.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Mo dule"}),Object.defineProperty(e,"__esModule",{value:!0})},t.t=function(e,r){if(1&r&&(e=t(e)),8&r)return e;if(4&r&&"object"==typeof e&&e&&e.__esModule)return e;var n=Object.create(null);if(t.r(n),Object.defineProperty(n,"default",{enumerable:!0,value:e}),2&r&&"string"!=typeof e)for(var o in e)t.d(n,o,function(r){return</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\app[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):	315354
Entropy (8bit):	5.288526690574326
Encrypted:	false
SSDEEP:	3072:aYnaYUv6FdKMMTcwIxtcZQKf65OgSgUcX9axZ8rqkcm45YQZ+2:aYnaYUCFdS44qPf65dSgPX9axnQ457+2
MD5:	B53039D29A5712E94959BFAB428DB6E0
SHA1:	5FA0FC8F9CDE36DEB5BA3B2EBCB86BFB970528ED
SHA-256:	115534237607D731E88E96DC2A7074A831D1AF712678E5F886795E57994F65C1
SHA-512:	6D6DE9C820E4A7B4B8043BEF4C9656EBF00F58247D61DFE02682746C7B6D13191D91E757E526B689E98D4BA0CBA63BEDCFAED3D1FD5BCA8184887E7D069BD08
Malicious:	false
Reputation:	low
IE Cache URL:	http://static.parastorage.com/services/dbsm-viewer-app/1.1306.0/app.js
Preview:	<pre>!function(e,t){if("object"==typeof exports&&"object"==typeof module)module.exports=t(require("_"));else if("function"==typeof define&&define.amd)define(["_"],t);else{var r="object"==typeof exports?t(require("_")):t(e._);for(var n in r)("object"==typeof exports?exports:e)[n]=r[n]]("undefined"!=typeof self?self:this,function(e){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)</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\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):	143190
Entropy (8bit):	5.396828825207751
Encrypted:	false
SSDEEP:	1536:Qq8fTtKiTuoaL1/9tk1DQSV5MuPihSkTumn5UG6UHSrxaetuftvXwgqc/Rd4XtY7:84tLSrxapiyhKSrxam3hsc
MD5:	4448232F66DAC2C850E38B05E8B9C1F5

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\bolt-custom-elements.min[1].js	
SHA1:	744573E707C5B1F5B2EF732BCE0FBFBF1EB55D80
SHA-256:	93BC99440527F916BD92CFF556A9CD4DA5BCDA118530A1E44BBD09E4B8A417B5
SHA-512:	A32287665DC7372B1DB10D32BDC10533CA216B005240ABAB267ABF9FA0AC222ACCE15B73785AC55BC42CDE62BB1C5E1A5D2A08B6AD636ACEF8969332CB1E468C
Malicious:	false
Reputation:	low
IE Cache URL:	http://static.parastorage.com/services/wix-bolt/1.6850.0/bolt-main/app/bolt-custom-elements.min.js
Preview:	<pre>var customElementsPackage=function(e){function t(t){for(var i,n,o=t[0],a=t[1],s=0,u=[];s<o.length;s++)n=o[s],Object.prototype.hasOwnProperty.call(r,n)&&r[n]&&u.push(r[n][0]),r[n]=0;for(i in a)Object.prototype.hasOwnProperty.call(a,i)&&(e[i]=a[i]);for(c&&(t).u.length;u.shift()&&)var i={},r={0:0};function n(t){if(!t)return i[t].exports;var r=i[t]=[];!1},exports:[];return e[t].call(r,exports,r,exports,n),r.l=!0,r,exports}n.e=function(e){var t=[],i=r[e];if(0!==i)if(!t.push(i[2]));else{var o=new Promise(function(t,n){i=[e]=[t,n]});t.push(i[2]=o);var a,s=document.createElement("script");s.charset="utf-8",s.timeout=120,n.nc&&s.setAttribute("nonce",n.nc),s.src=function(e){return n.p+""+e+"".bolt-custom-elements.min.js}(e);var c=new Error;a=function(t){s.onerror=s.onload=null,clearTimeout(u);var i=r[e];if(0!==i)if(!i){var n=t&&("load"===t.type?"missing":t.type),o=t&&t.target&&t.target.src;c.message="Loading chunk "+e+" failed.\n("+n+": "+o+")",c.name="ChunkLoadError",c.type=n,c.reqe</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\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):	1965744
Entropy (8bit):	5.615636367568405
Encrypted:	false
SSDEEP:	49152:wLiKrfeponi/RmgbI9iSv5gat6eo2cxronmIFv2lv7n845O9+BH:ycmAiSvuccxronmIFv2lv7n845O9+BH
MD5:	5839CACA6479B882D31336CBA8AEF4B6
SHA1:	D80D887A9227DF79F9827218C84D61AB313668A1
SHA-256:	5841EF1A786E3B3C3A16947769BCB7F8AA86649485975154B9F752907E30052B
SHA-512:	AA561C356997C555408E7F1CEDBFFE61E530F77588ED2FC409C473EB39AF32B2DEA0E5BD946B50439B02FA42222667ECB4F8F26A8419971D4C54E56EAF0218
Malicious:	false
Reputation:	low
IE Cache URL:	http://static.parastorage.com/services/wix-bolt/1.6850.0/bolt-main/app/bolt-main-prod-old.js
Preview:	<pre>define(["lodash","coreUtilsLib","react","prop-types","warmUpUtils","zepto","react-dom","santa-components","coreUtils","tpaComponents","color","thirdPartyAnalytics","creat-e-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(!r)return t[r].exports;var a=t[r]={};!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)</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\bookingsViewerScript.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):	361825
Entropy (8bit):	5.461475695235454
Encrypted:	false
SSDEEP:	3072:CUFb5NnVr8p8oNGRz65DBmLBA4xac+GIWEjklD0jpjt7:CTkd65DcjjklD05
MD5:	DA1AF11BDA1DBFD3CC0D17D5AD75E4DA
SHA1:	436944EA44B2282782AC49596F9A824A58FC73A8
SHA-256:	0927FB7EA0E8A46CC2E65F316FD98C731C642BDD207B72049AE5950C4D6F5FA7
SHA-512:	807688D9C22ED8E4E7D35361EC53B072922B4722A83DD8F4B4D04F2A6901533D01573F5A3A2E3BCA14C2BB735FB4B619615BFF1A0B666113DF382C7DC3394A1
Malicious:	false
Reputation:	low
IE Cache URL:	http://static.parastorage.com/services/bookings-viewer-script/1.1067.0/bookingsViewerScript.bundle.min.js
Preview:	<pre>!function(e,t){"object"===typeof exports&&"object"===typeof module?module.exports=t(require("lodash")):"function"===typeof define&&define.amd?define(["lodash"],t):"object"===typeof exports?exports.bookingsViewerScript=t(require("lodash")):e.bookingsViewerScript=t(e._)}("undefined"!==typeof self?self:this,(function(e){return function(e){var t={};function n(i){if(!i)return t[i].exports;var r=t[i]={};!1,exports:[];return e[i].call(r,exports,r,exports,n),r.l=!0,r,exports}return n.m=e,n.c=t,n.d=function(e,t,i){n.o(e,t) Object.defineProperty(e,t,{enumerable:!0,get:i})},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 i=Object.create(null);if(n.r(i),Object.defineProperty(i,"default",{enumerable:!0,value:e}),2&t&&"string"===typeof e)for(var r in e)n.d(i,r,function</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\cdn_detect[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	11
Entropy (8bit):	3.459431618637298
Encrypted:	false
SSDEEP:	3:OWY:OWY
MD5:	7C12772809C1C0C3DEDA6103B10FDFAO

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\cdn_detect[1]	
SHA1:	12039D6DD9A7E27622301E935B6EEFC78846802E
SHA-256:	4795A1C2517089E4DF569AFD77C04E949139CF299C87F012B894FCCF91DF4594
SHA-512:	3775186C9EDAD1CBDD412A66873511F2C34A65C93862C6B7AA4E1A39EBE354BE0B7E0353B3A24DAC6C09855D32F7630B496466F028E1420B38D2E35E2ECC026C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/cdn_detect
Preview:	1234567890.

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\cfc5f6_7020fbc4328945a9a8cc038617e65534~mv2[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=6, orientation=upper-left, xresolution=86, yresolution=94, resolutionunit=2], progressive, precision 8, 171x114, frames 3
Category:	dropped
Size (bytes):	6004
Entropy (8bit):	7.820560280332178
Encrypted:	false
SSDEEP:	96:0eE7m7MZSrQ6TsmIKscdWDkWjrfzX1fWxs11G+cKiw8DZ4sIV0gSnbntcKzlR3iN:P8mbrYml7cdWDkKr7RWxaFriw8DZGV0Q
MD5:	68FBA20A36F68AD97FE54282477743A5
SHA1:	FFCB8B9F5108D1123D9EE6B91DCA2298AFD41F61
SHA-256:	AA87E903FD217B167EFDBFDA12A7FF8E223D5F9AE8E9BC4E38960101C4514A69
SHA-512:	4ADF97F137026CE45E568F94954D4922B592057ACC6ADAA1E5574FCEB4BFE2A0AC3B894D2BFB49EAB87C7D6653D31F6A05E2F129DAD41668DFFB2E89594E28C
Malicious:	false
Reputation:	low
Preview:	JFIF.....Exif..II*.....V.....^.....i.....f.....8c.....8c.....0210.....0100.....r.....C.....%...#... , #&)*)...-0-(0%)(...C.....(.....((r.....j...<2..@!.....~..\\..@.5 .H...62UY..1.X..J.;E..."...*@>u...P.9.%..T..7.^.]...WVV..6...rX.....X.#..C...sN...6*Mo.Y@..W.u[3.q.v.B...ld .Z...g..C...{..D'..6.J..C.....X..8K.....u..b..Z.. yJ....[*..]r..`p..+FD.rb.....f..bb...Cw..as....l.T...p.z..w...]A.{~/E..+gr.....q++.&{;.s"...5...3O..z..3..L.bJ.tV.../q..{..8..J..H.....U.Z.hy,v.,k.e..}2...1]..n..t(S..1g.9]h..W.....ns*[*..g.....).e>.N.{..f[.n....1.Y...m#..g*O.Ol..y~.Kz~.....">.Y..PC,....y..8..:V...;\$. /s...Y.1

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\conductAllInScope[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:H:H
MD5:	99914B932BD37A50B983C5E7C90AE93B
SHA1:	BF21A9E8FBC5A3846FB05B4FA0859E0917B2202F
SHA-256:	44136FA355B3678A1146AD16F7E8649E94FB4FC21FE77E8310C060F61CAAFF8A
SHA-512:	27C74670ADB75075FAD058D5CEAF7B20C4E7786C83BAE8A32F626F9782AF34C9A33C2046EF60FD2A7878D378E29FEC851806BBD9A67878F3A9F1CDA4830763F
Malicious:	false
Reputation:	low
Preview:	{}

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\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):	104899
Entropy (8bit):	5.512173643045497
Encrypted:	false
SSDEEP:	1536:/kEv0CvhaUfvXms/fMYzMIVFPNPakN0IF/U2yCSE3N7Ly+BQ5:/xhZf5UPFN5U2yCSIQ5
MD5:	157EBD10600AA2A14AF91D185CE5CD6F
SHA1:	4C308496992F469E34F90FC55A88B8454D7C4910
SHA-256:	7297CD03A47F0FC09F5EBCDE2658C5715AD0FA4B782AE189CC242BDAF8178137
SHA-512:	71C414DF8E262959C4A2DFBBF9BF214940B56B92493D6524F0893CA374D767CBB734CAC071A5C6F49A4EB548BF35CB7838796038F4631E2BC9000244FE59FA5A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/unpkg/santa-core-utils@1.2685.0/dist/coreUtils.js

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\E\IMEEXW4H4\coreUtils[1].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=(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]={r:r,i:1,exports:{}};return e.call(o.exports,o,o.exports,n).o=!0,o.exports}return n.m=e,n.c=t,n.d=function(e,t,r){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.__esModule)return e;var r=Object.create(null);if(n.r(r),Object.definePropert

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEEXW4H4\current-user[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\explore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	4
Entropy (8bit):	1.5
Encrypted:	false
SSDEEP:	3:s:s
MD5:	37A6259CC0C1DAE299A7866489DFF0BD
SHA1:	2BE88CA4242C76E8253AC62474851065032D6833
SHA-256:	74234E98AFE7498FB5DAF1F36AC2D78ACC339464F950703B8C019892F982B90B
SHA-512:	04F8FF2682604862E405BF88DE102ED7710AC45C1205957625E4EE3E5F5A2241E453614ACC451345B91BAFC88F38804019C7492444595674E94E8CF4BE53817F
Malicious:	false
Reputation:	low
IE Cache URL:	https://engage.wixapps.net/_api/chat-web/v1/display-data/current-user?chatToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VySWQiOiIzODg0ZWRjNS1mZTM0LTRjOGMtYjQyZC04M2MzMjZhODEyOTQiLCJwYXJ0aWNpcGFudElkcyl6YWlyZODg0ZWRjNS1mZTM0LTRjOGMtYjQyZC04M2MzMjZhODEyOTQiXSwidXNlclR5cGUioiJB250YWN0IiwiaGlzdG9yeURpc2Fsbg93ZWQioMZhbHNILCJoaxNX0b3J5u2luY2Vuaw1lc3RhbnXAiOm51bGwslmNoYXRyb29tRmlsdGVyljpudWxsLClJ0ZW5hbnRJZC04M2MzMjZhODEyOTQiLCJleHAiOjE2MDg0MDczODIsImhhdCI6MTYwODMyMDk0Mn0.I6oIMRPKdwyAr46gbWcEz7UnVdxJOET5jXAmYXX7UiQ
Preview:	null

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\E\IMEEXW4H4\ld3470ec8ca26475da4b228f0199b5d3d[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 22 x 22, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	488
Entropy (8bit):	7.4150149562300545
Encrypted:	false
SSDEEP:	12:6v/76geHqnFfloJHycZx71H6RURaL0rPe9NNvPfqtVuewZfno:SxzUXzRHDq0q9wAeWno
MD5:	0463F01FFCB57DAB1464F3829D981991
SHA1:	C43093987542B9B6A9BAA59A6596C8103571499D
SHA-256:	EA2059B75DCFBAA5897F0E7976E25C9D448A474EB9AA4AACC6C459ED88F267AF
SHA-512:	F7E09BCD34CD9C1B9F72686FC584CF5F5B42B962D4EDAAB410474E42324AF212AB58DF78B05849CB8A7DC5F5D43A3B59A5E61B5A1000A84E5F47B4387072E60C
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....;.....pHYSt.....IDAT8....J.@.7.../..I.W..".].Gi.D.).@r_A...A...fuZ.J..vi...L.J.(...y.....Z...4..L.p.D..Y..<R....`..co...\$1.S....;....7...>..J+1.....^oLQp.56.S.....9...7j.EQ.8.U..\$.^..e.(c.s.&.x){S.g6.i.."}@.<.....+SA..L.S.b....*....q.J.&.....s.#.-H.....\$j.ts.....<F..F....%.R....._W].K.A..7^\$...X)....zQC<.*.....Z....ZBd.u.....m.b.n....`.....2S....8&.oC.5.i.v.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\E\MEEXW4H4\dataRefs.bundle.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\explore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2041
Entropy (8bit):	5.187952546384864
Encrypted:	false
SSDEEP:	48:xoznSHGdLNSxyAUwugTLHAqdLk0JNAfU0hC:4nrsUA/jjg0JN6C
MD5:	4395199113287A919FEE2901E715F886
SHA1:	E1E89ACDD2EC43E95EE68449FBF678BB7D426CA3
SHA-256:	435040DC25D4AA01CE75AEDB97F5237A70867CED605847D047315CD17AF5E188
SHA-512:	96ED4E022F4BD0F8CDB4A512B145605D639A5E3CFDDE32A9428BB8ACE14F4A0525874A99FFFD792D338E518A29894F349450E88595772E47E3FF82770F4AB2B2
Malicious:	false
Reputation:	low
IE Cache URL:	http://static.parastorage.com/unpkg/wix-ui-santa@2.0.214/dist/statics/dataRefs.bundle.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\dataRefs.bundle.min[1].js

Preview:	<pre>!function webpackUniversalModuleDefinition(e,r){"object"==typeof exports&&"object"==typeof module?module.exports=r():"function"==typeof define&&define.amd?define e([],r):"object"==typeof exports?exports.dataRefs=r():e.dataRefs=r()}("undefined"!=typeof self?self:this,(function(){return function(e){var r={}:function __webpack_require e__t){if(r[t])return r[t].exports;var __r[t]={i:t,l:!1,exports:{}};return e[t].call(__.exports,__,_.exports,__webpack_require__,___.l=!0,_.exports)}return __webpack_require__ __m=e.__webpack_require__.c=r,__webpack_require__.d=function(e,r,t){__webpack_require__.o(e,r) Object.defineProperty(e,r,{enumerable:!0,get:t})}.__webpack_requ ire__r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})}.__webpack_require__.t=function(e,r){if(1&r&&(e=__webpack_require__(e)),8&r)return e;if(4&r&&"object"==typeof e&&e.__esModule)return e;var t=Object.create(null</pre>
----------	---

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\dataRefs.bundle[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	5342
Entropy (8bit):	5.0848714515233775
Encrypted:	false
SSDEEP:	96:UpMvR8dtyEvEWIEmcfXGunhXWlrKBKcvdr8:SkefyEvEW6mcfXGunhXP\rvodr8
MD5:	B8E3ABCA408C93651353D61BE04BDACD
SHA1:	877BBD5A5983F77513313C5B391D5FEBC39870D95
SHA-256:	700C9510C8FFABF84E3782EABF36042BCDE3E358EEF784E8A06A2A6BA31D79AF
SHA-512:	98AE8E8CFC00F1373C74A6D39366FE7A794F199524ECF17494583E2C5F081C78747A55C803F1DFCFEFCB020DE14F57DEB05EB09A856EEB8E25A0C7259C0828FE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/unpkg/wix-ui-santa@2.0.214/dist/statics/dataRefs.bundle.js
Preview:	<pre>(function webpackUniversalModuleDefinition(root, factory) {..if(typeof exports === 'object' && typeof module === 'object')...module.exports = factory();..else if(typeof define === 'function' && define.amd)...define([], factory);..else if(typeof exports === 'object')...exports["dataRefs"] = factory();..else...root["dataRefs"] = factory();})(typeof self !== 'undefined' ? self : this), function() {..return /*****/ (function(modules) { // webpackBootstrap./*****/ // The module cache./*****/ .var installedModules = {};./*****/.*****/ // The require function./*****/ .function __webpack_require__(moduleId) {./*****/.*****/ // Check if module is in cache./*****/ ..if(installedModules[moduleId]) {./*****/ ..retu rn installedModules[moduleId].exports;./*****/ ..}.*****/ // Create a new module (and put it into the cache)./*****/ ..var module = installedModules[moduleId] = {./*****/ .. i: moduleId,./*****/ ...i: false,./*****/ ...exports: {},./*****/ ..};./*****/.*****/</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\displayer.min[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	67102
Entropy (8bit):	5.352417346196783
Encrypted:	false
SSDEEP:	768:+KxFGqv1kt2j1K7CZrE6QceQxjIEG4jvavNrkJ0YN9uKn3C9u0msIzaGwlcF:+KxM2jRmwXj134jcNw9IKkOGWcF
MD5:	D539FEA485EDC5FAFB8969DEC255423B
SHA1:	0B703D06C9B0C3C472A9481CAB5DA8E38AE68524
SHA-256:	D3496F0BDF745CDCBEED10FFCB9D6A14B100E7FD33FEAA648AB93274231AA3F3
SHA-512:	85C74F93EDB11845E0B1D99844728A1B34AA68310DD1B2F5B6BE89EEB297E0EEC16EFF18B576FB6E33078079EDA570CF72E592488E1C13594AD894AE2039884C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.parastorage.com/services/wix-bolt/1.6850.0/node_modules/wix-santa/dist/packages-bin/displayer/displayer.min.js
Preview:	<pre>define(["displayer",["lodash","coreUtils","santa-components","componentsCore","prop-types","skins","reactDOM"],"image-client-api"],(function(t,e,i,r,o,a,p,n){return function(t) {var e={};function i(r){if(e[r])return e[r].exports;var o=e[r]={i:r,l:!1,exports:{}};return t[r].call(o.exports,o,o.exports,i),o.l=!0,o.exports}return i.m=t,i.c=e,i.d=function(t,e,r){i.o (t,e) Object.defineProperty(t,e,{enumerable:!0,get:r})},i.r=function(t){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(t,Symbol.toStringTag, {value:"Module"}),Object.defineProperty(t,"__esModule",{value:!0})},i.t=function(t,e){if(1&e&&(t=i(t)),8&e)return t;if(4&e&&"object"==typeof t&&t.__esModule)return t;var r=Object.create(null);if(i.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:t}),2&e&&"string"!=typeof t)for(var o in t)i.d(r,o,function(e){return t[e]}.bind(null,o));return r},i.n=function(t){var e=t&&t.__esModule?function(){return t.default}:function(){return t};return i.d(e,"a",e),e},i.o=f</pre>

Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 100

- 53 (DNS)
- 443 (HTTPS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 18, 2020 20:49:33.357769966 CET	49703	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.358537912 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.389118910 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.389154911 CET	443	49703	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.389241934 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.389341116 CET	49703	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.401611090 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.401838064 CET	49703	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.432552099 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.432904005 CET	443	49703	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.435733080 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.435775995 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.435812950 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.435851097 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.435878992 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.435882092 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.435925007 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.435939074 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.435945034 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.435947895 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.436417103 CET	443	49703	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.436465979 CET	443	49703	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.436515093 CET	443	49703	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.436516047 CET	49703	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.436548948 CET	49703	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.436553955 CET	443	49703	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.436568975 CET	49703	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.436588049 CET	443	49703	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.436619997 CET	49703	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.436641932 CET	49703	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.489073992 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.489486933 CET	49703	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.494990110 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.495130062 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.495173931 CET	49703	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.519804955 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.519937038 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.520467043 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.520555973 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.520831108 CET	443	49703	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.521018982 CET	443	49703	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.521025896 CET	49703	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.521110058 CET	49703	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.523036957 CET	49703	443	192.168.2.3	35.246.6.109

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 18, 2020 20:49:33.523395061 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.525554895 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.525860071 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.525998116 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.526748896 CET	443	49703	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.526849985 CET	49703	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.595113039 CET	443	49703	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.595571995 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.655647993 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.655694962 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.655872107 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.677357912 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.677454948 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.677495003 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.677536964 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.677541018 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.677570105 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.677577972 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.677602053 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.677619934 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.677658081 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.677695990 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.677710056 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.677788973 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.687444925 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.687628031 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.687628031 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.687670946 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.687716007 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.687721014 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.687768936 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.687830925 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.710745096 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.710788965 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.710828066 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.710829020 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.710851908 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.710869074 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.710890055 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.710907936 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.710927010 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.710946083 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.710964918 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.710997105 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.711002111 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.711040020 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.711052895 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.711077929 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.711102009 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.711126089 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.711143017 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.711163998 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.711179972 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.711199999 CET	443	49704	35.246.6.109	192.168.2.3
Dec 18, 2020 20:49:33.711216927 CET	49704	443	192.168.2.3	35.246.6.109
Dec 18, 2020 20:49:33.711246014 CET	443	49704	35.246.6.109	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 18, 2020 20:49:27.013752937 CET	50200	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:49:27.026694059 CET	53	50200	8.8.8.8	192.168.2.3
Dec 18, 2020 20:49:28.027560949 CET	51281	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:49:28.040632963 CET	53	51281	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 18, 2020 20:49:29.196652889 CET	49199	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:49:29.209331989 CET	53	49199	8.8.8.8	192.168.2.3
Dec 18, 2020 20:49:30.577155113 CET	50620	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:49:30.590563059 CET	53	50620	8.8.8.8	192.168.2.3
Dec 18, 2020 20:49:31.627855062 CET	64938	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:49:31.640348911 CET	53	64938	8.8.8.8	192.168.2.3
Dec 18, 2020 20:49:32.221863031 CET	60152	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:49:32.253994942 CET	53	60152	8.8.8.8	192.168.2.3
Dec 18, 2020 20:49:32.913876057 CET	57544	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:49:32.927128077 CET	53	57544	8.8.8.8	192.168.2.3
Dec 18, 2020 20:49:33.283221960 CET	55984	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:49:33.343322992 CET	53	55984	8.8.8.8	192.168.2.3
Dec 18, 2020 20:49:33.756262064 CET	64185	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:49:33.769844055 CET	53	64185	8.8.8.8	192.168.2.3
Dec 18, 2020 20:49:33.926593065 CET	65110	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:49:33.941220045 CET	53	65110	8.8.8.8	192.168.2.3
Dec 18, 2020 20:49:34.845864058 CET	58361	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:49:34.866848946 CET	53	58361	8.8.8.8	192.168.2.3
Dec 18, 2020 20:49:35.967619896 CET	63492	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:49:35.980187893 CET	53	63492	8.8.8.8	192.168.2.3
Dec 18, 2020 20:49:36.146606922 CET	60831	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:49:36.173248053 CET	53	60831	8.8.8.8	192.168.2.3
Dec 18, 2020 20:49:37.067430019 CET	60100	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:49:37.080768108 CET	53	60100	8.8.8.8	192.168.2.3
Dec 18, 2020 20:49:37.399960995 CET	53195	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:49:37.412132025 CET	53	53195	8.8.8.8	192.168.2.3
Dec 18, 2020 20:49:38.514981985 CET	50141	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:49:38.528269053 CET	53	50141	8.8.8.8	192.168.2.3
Dec 18, 2020 20:49:41.563009977 CET	53023	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:49:41.576458931 CET	53	53023	8.8.8.8	192.168.2.3
Dec 18, 2020 20:49:42.028597116 CET	49563	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:49:42.041498899 CET	53	49563	8.8.8.8	192.168.2.3
Dec 18, 2020 20:49:44.479059935 CET	51352	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:49:44.491574049 CET	53	51352	8.8.8.8	192.168.2.3
Dec 18, 2020 20:49:51.195866108 CET	59349	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:49:51.208276033 CET	53	59349	8.8.8.8	192.168.2.3
Dec 18, 2020 20:49:52.516149998 CET	57084	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:49:52.529171944 CET	53	57084	8.8.8.8	192.168.2.3
Dec 18, 2020 20:49:55.838455915 CET	58823	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:49:55.851674080 CET	53	58823	8.8.8.8	192.168.2.3
Dec 18, 2020 20:49:56.790255070 CET	57568	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:49:56.817173958 CET	53	57568	8.8.8.8	192.168.2.3
Dec 18, 2020 20:49:58.635737896 CET	50540	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:49:58.649594069 CET	53	50540	8.8.8.8	192.168.2.3
Dec 18, 2020 20:49:58.735515118 CET	54366	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:49:58.761723995 CET	53	54366	8.8.8.8	192.168.2.3
Dec 18, 2020 20:50:02.237984896 CET	53034	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:50:02.251899958 CET	53	53034	8.8.8.8	192.168.2.3
Dec 18, 2020 20:50:02.493880033 CET	57762	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:50:02.512685061 CET	53	57762	8.8.8.8	192.168.2.3
Dec 18, 2020 20:50:02.907363892 CET	55435	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:50:02.920509100 CET	53	55435	8.8.8.8	192.168.2.3
Dec 18, 2020 20:50:03.236354113 CET	53034	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:50:03.249360085 CET	53	53034	8.8.8.8	192.168.2.3
Dec 18, 2020 20:50:03.910402060 CET	55435	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:50:03.923523903 CET	53	55435	8.8.8.8	192.168.2.3
Dec 18, 2020 20:50:04.090281963 CET	50713	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:50:04.103029013 CET	53	50713	8.8.8.8	192.168.2.3
Dec 18, 2020 20:50:04.241621017 CET	53034	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:50:04.255045891 CET	53	53034	8.8.8.8	192.168.2.3
Dec 18, 2020 20:50:05.014653921 CET	55435	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:50:05.027857065 CET	53	55435	8.8.8.8	192.168.2.3
Dec 18, 2020 20:50:06.509921074 CET	53034	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:50:06.523062944 CET	53	53034	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 18, 2020 20:50:07.139516115 CET	55435	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:50:07.152331114 CET	53	55435	8.8.8.8	192.168.2.3
Dec 18, 2020 20:50:07.754221916 CET	56132	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:50:07.774302006 CET	58987	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:50:07.788564920 CET	53	58987	8.8.8.8	192.168.2.3
Dec 18, 2020 20:50:07.793586969 CET	53	56132	8.8.8.8	192.168.2.3
Dec 18, 2020 20:50:09.559262991 CET	56579	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:50:09.573353052 CET	53	56579	8.8.8.8	192.168.2.3
Dec 18, 2020 20:50:10.151210070 CET	60633	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:50:10.164937973 CET	53	60633	8.8.8.8	192.168.2.3
Dec 18, 2020 20:50:10.305078983 CET	61292	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:50:10.331729889 CET	53	61292	8.8.8.8	192.168.2.3
Dec 18, 2020 20:50:10.507325888 CET	53034	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:50:10.520314932 CET	53	53034	8.8.8.8	192.168.2.3
Dec 18, 2020 20:50:11.139436007 CET	55435	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:50:11.152477026 CET	53	55435	8.8.8.8	192.168.2.3
Dec 18, 2020 20:50:17.091336966 CET	63619	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:50:17.153517962 CET	53	63619	8.8.8.8	192.168.2.3
Dec 18, 2020 20:50:17.194736004 CET	64938	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:50:17.215648890 CET	53	64938	8.8.8.8	192.168.2.3
Dec 18, 2020 20:50:46.240859032 CET	61946	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:50:46.253968954 CET	53	61946	8.8.8.8	192.168.2.3
Dec 18, 2020 20:50:47.242527962 CET	61946	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:50:47.255892992 CET	53	61946	8.8.8.8	192.168.2.3
Dec 18, 2020 20:50:48.337734938 CET	61946	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:50:48.350914001 CET	53	61946	8.8.8.8	192.168.2.3
Dec 18, 2020 20:50:50.388214111 CET	61946	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:50:50.401559114 CET	53	61946	8.8.8.8	192.168.2.3
Dec 18, 2020 20:50:54.427699089 CET	61946	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:50:54.440726995 CET	53	61946	8.8.8.8	192.168.2.3
Dec 18, 2020 20:51:07.198730946 CET	64910	53	192.168.2.3	8.8.8.8
Dec 18, 2020 20:51:07.228631973 CET	53	64910	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 18, 2020 20:49:33.283221960 CET	192.168.2.3	8.8.8.8	0x213	Standard query (0)	www.305cov idtest.com	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:33.756262064 CET	192.168.2.3	8.8.8.8	0xfe63	Standard query (0)	static.par astorage.com	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:33.926593065 CET	192.168.2.3	8.8.8.8	0x5415	Standard query (0)	frog.wix.com	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:34.845864058 CET	192.168.2.3	8.8.8.8	0x67f8	Standard query (0)	siteassets .parastorage.com	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:35.967619896 CET	192.168.2.3	8.8.8.8	0x12ba	Standard query (0)	static.wix static.com	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:37.399960995 CET	192.168.2.3	8.8.8.8	0xcd90	Standard query (0)	browser.sentry- cdn.com	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:41.563009977 CET	192.168.2.3	8.8.8.8	0xa7e1	Standard query (0)	sentry.wix press.com	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:42.028597116 CET	192.168.2.3	8.8.8.8	0xe389	Standard query (0)	engage.wix apps.net	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:55.838455915 CET	192.168.2.3	8.8.8.8	0xa805	Standard query (0)	www.youtub e.com	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:58.635737896 CET	192.168.2.3	8.8.8.8	0x12e4	Standard query (0)	googleads. g.doubleclick.net	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:58.735515118 CET	192.168.2.3	8.8.8.8	0x886	Standard query (0)	static.dou bleclick.net	A (IP address)	IN (0x0001)
Dec 18, 2020 20:50:07.754221916 CET	192.168.2.3	8.8.8.8	0x5453	Standard query (0)	i.ytimg.com	A (IP address)	IN (0x0001)
Dec 18, 2020 20:50:07.774302006 CET	192.168.2.3	8.8.8.8	0xcb6a	Standard query (0)	yt3.ggpht.com	A (IP address)	IN (0x0001)
Dec 18, 2020 20:50:09.559262991 CET	192.168.2.3	8.8.8.8	0x600e	Standard query (0)	wix-engage- visitors-prod-20.fi rebaseio.com	A (IP address)	IN (0x0001)
Dec 18, 2020 20:50:10.151210070 CET	192.168.2.3	8.8.8.8	0xb870	Standard query (0)	static.wix static.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 18, 2020 20:51:07.198730946 CET	192.168.2.3	8.8.8.8	0xbc34	Standard query (0)	d8ec26b2-28d6-41f2-b06e-8c76091f9420.static.pub.wix-code.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2020 20:49:33.343322992 CET	8.8.8.8	192.168.2.3	0x213	No error (0)	www.305covidtest.com	www253.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Dec 18, 2020 20:49:33.343322992 CET	8.8.8.8	192.168.2.3	0x213	No error (0)	www253.wixdns.net	balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Dec 18, 2020 20:49:33.343322992 CET	8.8.8.8	192.168.2.3	0x213	No error (0)	balancer.wixdns.net	5f36b111-balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Dec 18, 2020 20:49:33.343322992 CET	8.8.8.8	192.168.2.3	0x213	No error (0)	5f36b111-balancer.wixdns.net	td-balancer-euw2-6-109.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Dec 18, 2020 20:49:33.343322992 CET	8.8.8.8	192.168.2.3	0x213	No error (0)	td-balancer-euw2-6-109.wixdns.net		35.246.6.109	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:33.769844055 CET	8.8.8.8	192.168.2.3	0xfe63	No error (0)	static.parastorage.com	td-static-34-96-106-200.parastorage.com		CNAME (Canonical name)	IN (0x0001)
Dec 18, 2020 20:49:33.769844055 CET	8.8.8.8	192.168.2.3	0xfe63	No error (0)	td-static-34-96-106-200.parastorage.com		34.96.106.200	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:33.941220045 CET	8.8.8.8	192.168.2.3	0x5415	No error (0)	frog.wix.com	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 18, 2020 20:49:33.941220045 CET	8.8.8.8	192.168.2.3	0x5415	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		54.87.207.230	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:33.941220045 CET	8.8.8.8	192.168.2.3	0x5415	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		54.87.109.87	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:33.941220045 CET	8.8.8.8	192.168.2.3	0x5415	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		50.16.239.72	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:33.941220045 CET	8.8.8.8	192.168.2.3	0x5415	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		34.202.131.150	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:33.941220045 CET	8.8.8.8	192.168.2.3	0x5415	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		3.212.73.210	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:33.941220045 CET	8.8.8.8	192.168.2.3	0x5415	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		54.156.212.234	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:33.941220045 CET	8.8.8.8	192.168.2.3	0x5415	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		54.209.210.115	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:33.941220045 CET	8.8.8.8	192.168.2.3	0x5415	No error (0)	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com		54.224.154.27	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:34.866848946 CET	8.8.8.8	192.168.2.3	0x67f8	No error (0)	siteassets.parastorage.com	static.parastorage.com		CNAME (Canonical name)	IN (0x0001)
Dec 18, 2020 20:49:34.866848946 CET	8.8.8.8	192.168.2.3	0x67f8	No error (0)	static.parastorage.com	td-static-34-96-106-200.parastorage.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2020 20:49:34.866848946 CET	8.8.8.8	192.168.2.3	0x67f8	No error (0)	td-static-34-96-106-200.parastorage.com		34.96.106.200	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:35.980187893 CET	8.8.8.8	192.168.2.3	0x12ba	No error (0)	static.wixstatic.com	gcp.media-router.wixstatic.com		CNAME (Canonical name)	IN (0x0001)
Dec 18, 2020 20:49:35.980187893 CET	8.8.8.8	192.168.2.3	0x12ba	No error (0)	gcp.media-router.wixstatic.com		34.102.176.152	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:37.412132025 CET	8.8.8.8	192.168.2.3	0xcd90	No error (0)	browser.sentry-cdn.com		151.101.2.217	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:37.412132025 CET	8.8.8.8	192.168.2.3	0xcd90	No error (0)	browser.sentry-cdn.com		151.101.66.217	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:37.412132025 CET	8.8.8.8	192.168.2.3	0xcd90	No error (0)	browser.sentry-cdn.com		151.101.130.217	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:37.412132025 CET	8.8.8.8	192.168.2.3	0xcd90	No error (0)	browser.sentry-cdn.com		151.101.194.217	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:41.576458931 CET	8.8.8.8	192.168.2.3	0xa7e1	No error (0)	sentry.wixpress.com	sentry-nlb-e70282e8a06dcc98.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 18, 2020 20:49:41.576458931 CET	8.8.8.8	192.168.2.3	0xa7e1	No error (0)	sentry-nlb-e70282e8a06dcc98.elb.us-east-1.amazonaws.com		52.2.188.208	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:42.041498899 CET	8.8.8.8	192.168.2.3	0xe389	No error (0)	engage.wixapps.net	verticals.wix.com		CNAME (Canonical name)	IN (0x0001)
Dec 18, 2020 20:49:42.041498899 CET	8.8.8.8	192.168.2.3	0xe389	No error (0)	verticals.wix.com	180.verticals.sv5.wix.com		CNAME (Canonical name)	IN (0x0001)
Dec 18, 2020 20:49:42.041498899 CET	8.8.8.8	192.168.2.3	0xe389	No error (0)	180.verticals.sv5.wix.com		185.230.61.180	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:55.851674080 CET	8.8.8.8	192.168.2.3	0xa805	No error (0)	www.youtube.com	youtube-ui.l.google.com		CNAME (Canonical name)	IN (0x0001)
Dec 18, 2020 20:49:58.649594069 CET	8.8.8.8	192.168.2.3	0x12e4	No error (0)	googleads.g.doubleclick.net	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Dec 18, 2020 20:49:58.649594069 CET	8.8.8.8	192.168.2.3	0x12e4	No error (0)	pagead46.l.doubleclick.net		172.217.168.66	A (IP address)	IN (0x0001)
Dec 18, 2020 20:49:58.761723995 CET	8.8.8.8	192.168.2.3	0x886	No error (0)	static.doubleclick.net	static-doubleclick-net.l.google.com		CNAME (Canonical name)	IN (0x0001)
Dec 18, 2020 20:50:07.788564920 CET	8.8.8.8	192.168.2.3	0xcb6a	No error (0)	yt3.ggpht.com	photos-ugc.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Dec 18, 2020 20:50:07.788564920 CET	8.8.8.8	192.168.2.3	0xcb6a	No error (0)	photos-ugc.l.googleusercontent.com		216.58.215.225	A (IP address)	IN (0x0001)
Dec 18, 2020 20:50:07.793586969 CET	8.8.8.8	192.168.2.3	0x5453	No error (0)	i.ytimg.com		172.217.168.22	A (IP address)	IN (0x0001)
Dec 18, 2020 20:50:09.573353052 CET	8.8.8.8	192.168.2.3	0x600e	No error (0)	wix-engage-visitors-prod-20.firebaseio.com		35.201.97.85	A (IP address)	IN (0x0001)
Dec 18, 2020 20:50:10.164937973 CET	8.8.8.8	192.168.2.3	0xb870	No error (0)	static.wixstatic.com	gcp.media-router.wixstatic.com		CNAME (Canonical name)	IN (0x0001)
Dec 18, 2020 20:50:10.164937973 CET	8.8.8.8	192.168.2.3	0xb870	No error (0)	gcp.media-router.wixstatic.com		34.102.176.152	A (IP address)	IN (0x0001)
Dec 18, 2020 20:51:07.228631973 CET	8.8.8.8	192.168.2.3	0xbc34	No error (0)	d8ec26b2-28d6-41f2-b06e-8c76091f9420.static.pub.wix-code.com	cdn.wix-code.com		CNAME (Canonical name)	IN (0x0001)
Dec 18, 2020 20:51:07.228631973 CET	8.8.8.8	192.168.2.3	0xbc34	No error (0)	cdn.wix-code.com	d2rddclowni6h8.cloudfront.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2020 20:51:07.228631973 CET	8.8.8.8	192.168.2.3	0xbc34	No error (0)	d2rcdclown i6h8.cloud front.net		65.9.68.81	A (IP address)	IN (0x0001)
Dec 18, 2020 20:51:07.228631973 CET	8.8.8.8	192.168.2.3	0xbc34	No error (0)	d2rcdclown i6h8.cloud front.net		65.9.68.60	A (IP address)	IN (0x0001)
Dec 18, 2020 20:51:07.228631973 CET	8.8.8.8	192.168.2.3	0xbc34	No error (0)	d2rcdclown i6h8.cloud front.net		65.9.68.13	A (IP address)	IN (0x0001)
Dec 18, 2020 20:51:07.228631973 CET	8.8.8.8	192.168.2.3	0xbc34	No error (0)	d2rcdclown i6h8.cloud front.net		65.9.68.16	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
Dec 18, 2020 20:49:33.435882092 CET	35.246.6.109	443	192.168.2.3	49704	CN=305covidtest.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	Tue Dec 15 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	Tue Mar 16 00:59:59 CET 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	9e10692f1b7f78228b2d4e 424db3a98c
					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
Dec 18, 2020 20:49:33.436588049 CET	35.246.6.109	443	192.168.2.3	49703	CN=305covidtest.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	Tue Dec 15 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	Tue Mar 16 00:59:59 CET 2021 Mon Jan 01 00:59:59 CET 2029 Mon 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	9e10692f1b7f78228b2d4e 424db3a98c
					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		
Dec 18, 2020 20:49:33.944577932 CET	34.96.106.200	443	192.168.2.3	49707	CN=*.parastorage.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	Wed Sep 09 02:00:00 CEST 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	Tue Mar 09 00:59:59 CET 2021 Mon Jan 01 00:59:59 CET 2029 Mon 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	9e10692f1b7f78228b2d4e 424db3a98c
					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		
Dec 18, 2020 20:49:33.944994926 CET	34.96.106.200	443	192.168.2.3	49705	CN=*.parastorage.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	Wed Sep 09 02:00:00 CEST 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	Tue Mar 09 00:59:59 CET 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		
Dec 18, 2020 20:49:33.945770979 CET	34.96.106.200	443	192.168.2.3	49706	CN=*.parastorage.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	Wed Sep 09 02:00:00 CEST 2020 Thu Jan 01 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Tue Mar 09 00:59:59 CET 2021 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					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		
Dec 18, 2020 20:49:33.946420908 CET	34.96.106.200	443	192.168.2.3	49708	CN=*.parastorage.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	Wed Sep 09 02:00:00 CEST 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	Tue Mar 09 00:59:59 CET 2021 Mon Jan 01 00:59:59 CET 2029 Mon 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		
Dec 18, 2020 20:49:34.150326967 CET	54.87.207.230	443	192.168.2.3	49709	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 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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		
Dec 18, 2020 20:49:34.151119947 CET	54.87.207.230	443	192.168.2.3	49710	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
Dec 18, 2020 20:49:34.942856073 CET	34.96.106.200	443	192.168.2.3	49712	CN=*.parastorage.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	Wed Sep 09 02:00:00 CEST 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	Tue Mar 09 00:59:59 CET 2021 Mon Jan 01 00:59:59 CET 2029 Mon 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		
Dec 18, 2020 20:49:35.016886950 CET	34.96.106.200	443	192.168.2.3	49711	CN=*.parastorage.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	Wed Sep 09 02:00:00 CEST 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	Tue Mar 09 00:59:59 CET 2021 Mon Jan 01 00:59:59 CET 2029 Mon 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		
Dec 18, 2020 20:49:36.012722969 CET	34.102.176.152	443	192.168.2.3	49713	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	Mon Sep 07 02:00:00 CEST 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	Sun Mar 07 00:59:59 CET 2021 Mon Jan 01 00:59:59 CET 2029 Mon 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		
Dec 18, 2020 20:49:36.012923002 CET	34.102.176.152	443	192.168.2.3	49714	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	Mon Sep 07 02:00:00 CEST 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	Sun Mar 07 00:59:59 CET 2021 Mon Jan 01 00:59:59 CET 2029 Mon 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					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		
Dec 18, 2020 20:49:36.014271021 CET	34.102.176.152	443	192.168.2.3	49715	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	Mon Sep 07 02:00:00 CEST 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	Sun Mar 07 00:59:59 CET 2021 Mon Jan 01 00:59:59 CET 2029 Mon 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		
					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	Tue Mar 12 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Mon Jan 01 00:59:59 CET 2029 Wed Jan 01 00:59:59 CET 2031		
Dec 18, 2020 20:49:36.014460087 CET	34.102.176.152	443	192.168.2.3	49716	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	Mon Sep 07 02:00:00 CEST 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	Sun Mar 07 00:59:59 CET 2021 Mon Jan 01 00:59:59 CET 2029 Mon 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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		
Dec 18, 2020 20:49:36.018650055 CET	34.102.176.152	443	192.168.2.3	49717	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	Mon Sep 07 02:00:00 CEST 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	Sun Mar 07 00:59:59 CET 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
Dec 18, 2020 20:49:36.019213915 CET	34.102.176.152	443	192.168.2.3	49718	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=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Mon Sep 07 02:00:00 CEST 2020	Sun Mar 07 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=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		
Dec 18, 2020 20:49:37.497536898 CET	151.101.2.217	443	192.168.2.3	49727	CN=v2.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	Mon Dec 14 15:10:21 CET 2020	Thu Apr 22 20:10:21 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=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
Dec 18, 2020 20:49:41.802220106 CET	52.2.188.208	443	192.168.2.3	49729	CN=*.wixpress.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=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Wed Sep 02 02:00:00 CEST 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	Tue Mar 02 00:59:59 CET 2021 Mon Jan 01 00:59:59 CET 2029 Mon 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		
Dec 18, 2020 20:49:41.803942919 CET	52.2.188.208	443	192.168.2.3	49730	CN=*.wixpress.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=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Wed Sep 02 02:00:00 CEST 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	Tue Mar 02 00:59:59 CET 2021 Mon Jan 01 00:59:59 CET 2029 Mon 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		
Dec 18, 2020 20:49:42.435563087 CET	185.230.61.180	443	192.168.2.3	49731	CN=*.wixapps.net 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 Sep 11 02:00:00 CEST 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	Thu Mar 11 00:59:59 CET 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		
Dec 18, 2020 20:49:42.439376116 CET	185.230.61.180	443	192.168.2.3	49732	CN=*.wixapps.net 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 Sep 11 02:00:00 CEST 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	Thu Mar 11 00:59:59 CET 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					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		

Code Manipulations

Statistics

Behavior

- iexplore.exe
- iexplore.exe

💡 Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5228 Parent PID: 792

General

Start time:	20:49:31
Start date:	18/12/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7f4520000
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: 5532 Parent PID: 5228

General

Start time:	20:49:31
Start date:	18/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5228 CREDAT:17410 /prefetch:2
Imagebase:	0x250000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEE8013E2AB58D5A
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

