



ID: 339437
Cookbook: browseurl.jbs
Time: 03:08:30
Date: 14/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report
https://clubfluent.com/sendy//l/WeciX0nqw9S20mfKVbMPsQ/viIp61hl1PT892Foz892SW4unA/MKroVFHPnG34QjG38Mb7Zg
Overview 33
General Information 3
Detection 3
Signatures 3
Classification 3
Startup 3
Malware Configuration 3
Yara Overview 3
Sigma Overview 3
Signature Overview 3
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 8
Contacted Domains 8
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 12
Public 12
General Information 12
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 14
ASN 14
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
Static File Info 47
No static file info 47
Network Behavior 47
Network Port Distribution 47
TCP Packets 48
UDP Packets 49
DNS Queries 51
DNS Answers 52
HTTPS Packets 55
Code Manipulations 64
Statistics 64
Behavior 64
System Behavior 65
Analysis Process: iexplore.exe PID: 5836 Parent PID: 792 65
General 65
File Activities 65
Registry Activities 65
Analysis Process: iexplore.exe PID: 5884 Parent PID: 5836 65
General 66
File Activities 66
Registry Activities 66
Disassembly 66

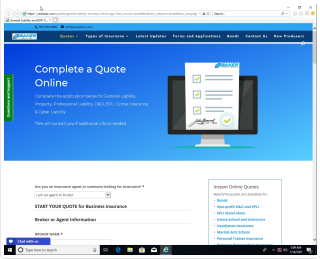
Analysis Report https://clubfluent.com/sendy//l/WeciX0n…

Overview

General Information

Sample URL:	http://https://clubfluent.com/sendy//l/WeciX0nqw9S20mfKVbMPsQ/vilp61hl1PT892Foz892SW4unA/MKroVFHPnG34QjG38Mb7Zg
Analysis ID:	339437

Most interesting Screenshot:



Detection

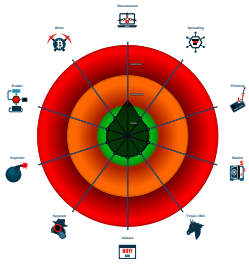


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5836 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5884 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5836 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

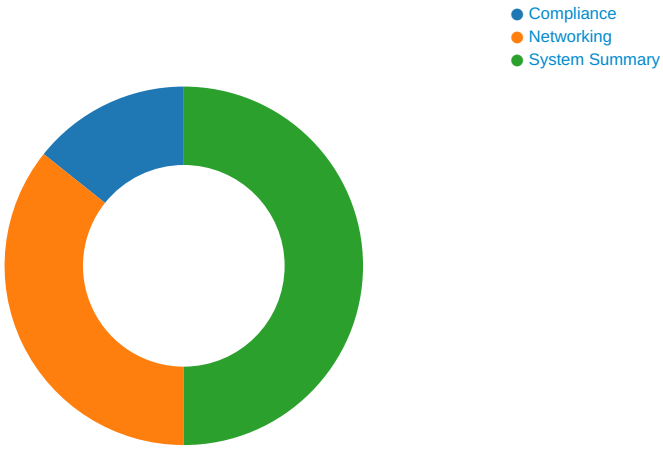
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



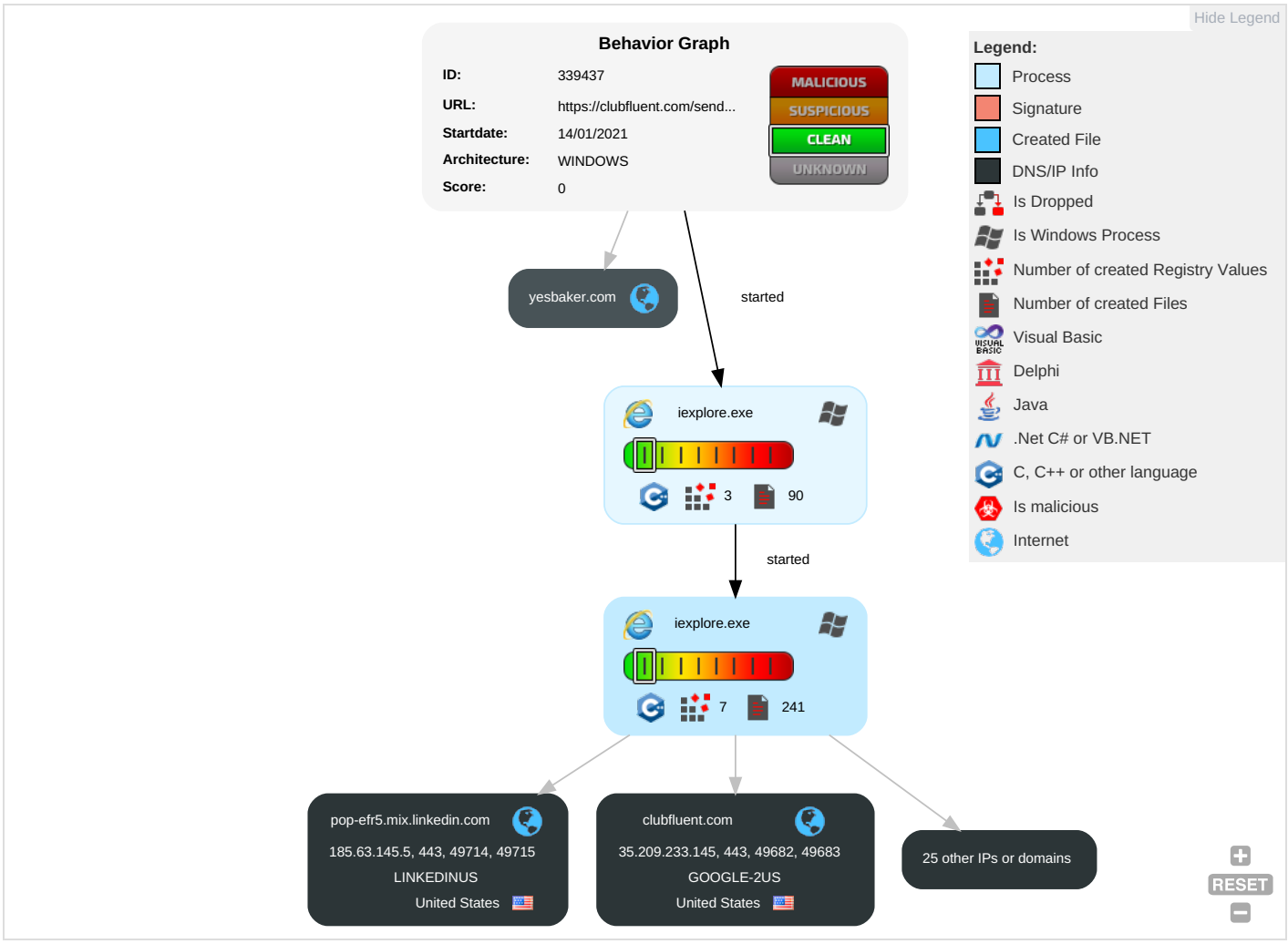
Click to jump to signature section

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

Mitre Att&ck Matrix

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

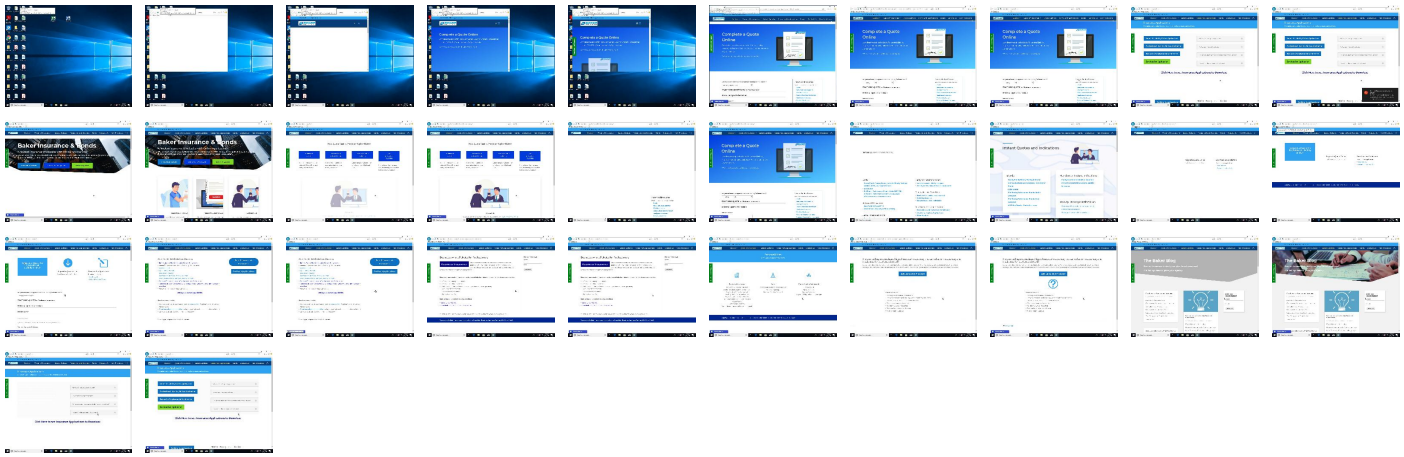
Behavior Graph

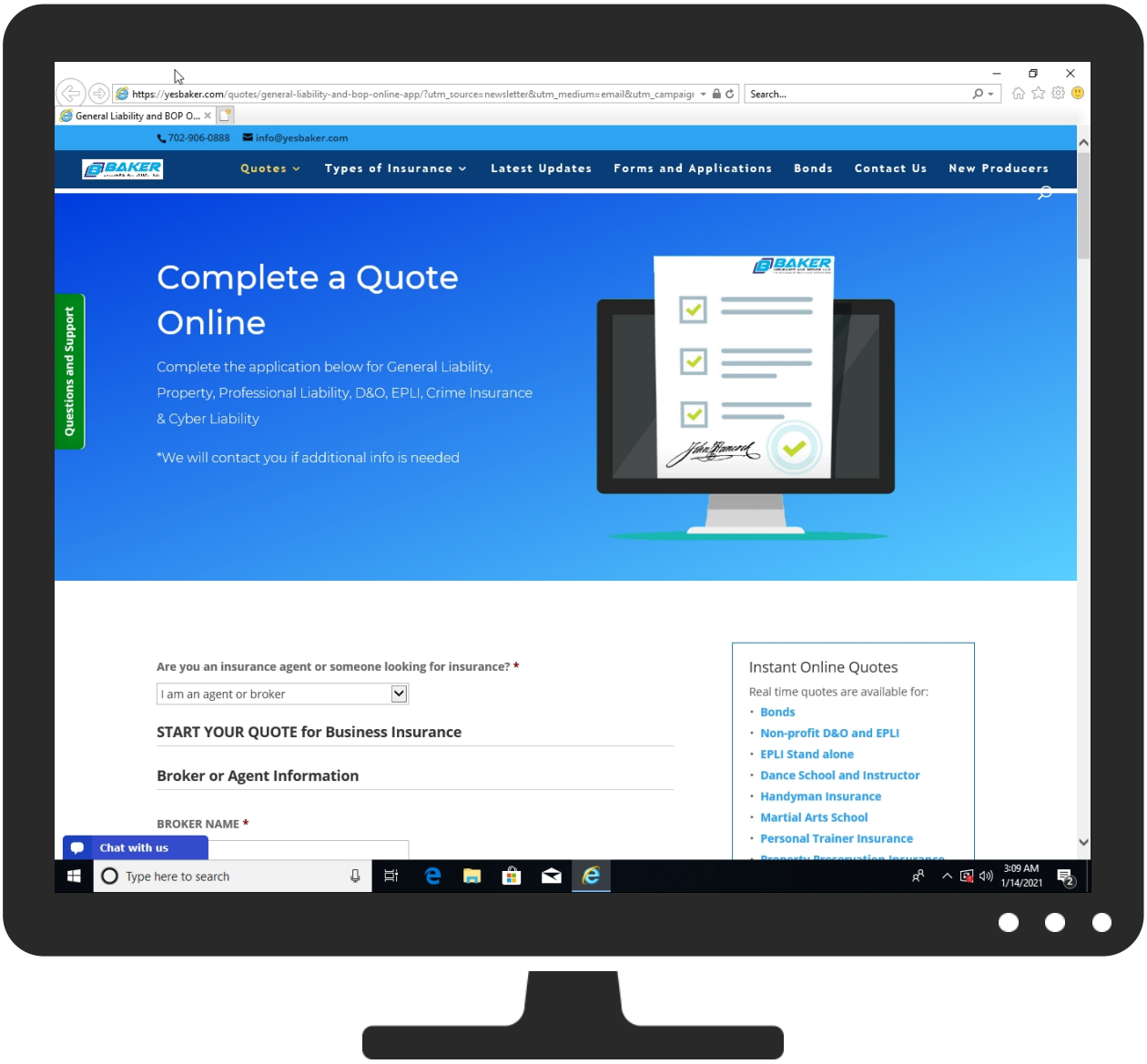


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http:// https://clubfluent.com/sendy//l/WeciX0nqw9S20mfKVbMPsQ/vilp61hl1PT892Foz892SW4unA/MKroVFHPnG34QjG38Mb7Zg	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
yesbaker.com	0%	Virustotal		Browse
clubfluent.com	0%	Virustotal		Browse
chimpstatic.com	0%	Virustotal		Browse
quora.map.fastly.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://robert-fleischmann.de)	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/sv.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/sv.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/sv.html	0%	URL Reputation	safe	
http://https://yesbaker.com/types-of-insurance/personal-lines/#primaryimage	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/types-of-insurance/classes-of-business/	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/wp-content/uploads/idea-min.png	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/types-of-insurance/businessowners-policies-for-professionals/#webpage	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/?p=99	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/wp-content/uploads/fast-response-min-768x760.png	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/wp-json/wp/v2/pages/59	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/?p=571	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/quotes/#webpage	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/wp-content/uploads/logo-b-social-mediasmall.png	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fyesbaker.com%2Fapplications%2F	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/?p=92	0%	Avira URL Cloud	safe	
http://https://yesbaker.com	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/types-of-insurance/sell-international-medical-and-trip-cancellation-insurance/f	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/#webpage	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/wp-content/uploads/insurance-12-300x225.png	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/quotes/gen	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fyesbaker.com%2Flatest-updates%2F	0%	Avira URL Cloud	safe	
http://https://quotebaker.com	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/dental-cancer-short-term-medical-insurance/	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/join-our-newsletter/	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/wp-content/uploads/business-02-768x542.jpg	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/?p=86	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/wp-content/uploads/insurance-14.png	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/wp-content/uploads/business-07-300x200.jpg	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/latest-updates/page/2/?et_blog	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/pl.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/pl.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/pl.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/fr.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/fr.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/fr.html	0%	URL Reputation	safe	
http://https://yesbaker.com/feed/	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/contact-us/	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/xmlrpc.php?rsd	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/wp-content/plugins/gravityforms/js/gravityforms.min.js?ver=2.4.15.1	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/wp-content/uploads/business-07.jpg	0%	Avira URL Cloud	safe	
http://https://help.yesbaker.com/loading.html?ver=2	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/wp-content/themes/Divi/core/admin/fonts/modules.ttf	0%	Avira URL Cloud	safe	
http://https://help.yesbaker.com/support/solutions/articles/26000041389-architects-engineers-and-inspector-	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/el.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/el.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/el.html	0%	URL Reputation	safe	
http://https://yesbaker.com/fire-sprinkler-contractor-insurance/	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fyesbaker.com%2Fquotes%2Fgeneral-liab	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/wp-json/wp/v2/pages/571	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/wp-content/uploads/insurance-12-1.png	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/wp-content/uploads/insurance-14-1-300x225.png	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/quotes/real-time-quotes/	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/types-of-insurance/feed/	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/types-of-insurance/personal-lines/olicies-for-professionals/	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/wp-content/uploads/fast-response-min.png	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fyesbaker.com%2Fquotes%2F&format	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/zh.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/zh.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/zh.html	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://www.hotjarconsent.com/fi.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/fi.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/fi.html	0%	URL Reputation	safe	
http://https://yesbaker.com/types-of-insurance/classes-of-business	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/wp-json/wp/v2/pages/181	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/applications/liability-and-bop-online-app/?utm_source=newsletter&utm_medium=ema	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/surety-bonds/	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/wp-content/plugins/gravityforms/css/formreset.min.css?ver=2.4.15.1	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/?p=59	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/wp-content/uploads/quote-online-min-300x297.png	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/applications/#webpage	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/insurance-agent-cyber-liability/	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/subdivision-bonds/	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/latest-updates/#webpage	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/wp-json/wp/v2/pages/92	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/sq.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/sq.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/sq.html	0%	URL Reputation	safe	
http://https://yesbaker.com/wp-content/uploads/idea-min-768x760.png	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/holiday-business-insurance/	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fyesbaker.com%2F&format=xml	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/it.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/it.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/it.html	0%	URL Reputation	safe	
http://https://yesbaker.com/?s=	0%	Avira URL Cloud	safe	
http://https://yesbaker.com/wp-includes/js/mediaelement/mediaelement-and-player.min.js?ver=4.2.16	0%	Avira URL Cloud	safe	
http://daneden.me/animate	0%	URL Reputation	safe	
http://daneden.me/animate	0%	URL Reputation	safe	
http://daneden.me/animate	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
yesbaker.com	104.21.19.250	true	false	• 0%, Virustotal, Browse	unknown
cf.zdassets.com	104.18.70.113	true	false		high
vars.hotjar.com	13.224.94.36	true	false		high
clubfluent.com	35.209.233.145	true	false	• 0%, Virustotal, Browse	unknown
s3.amazonaws.com	52.216.139.125	true	false		high
in-live.live.eks.hotjar.com	52.49.237.17	true	false		high
script.hotjar.com	13.224.94.39	true	false		high
chimpstatic.com	104.83.125.218	true	false	• 0%, Virustotal, Browse	unknown
widget-mediator.zopim.com	3.125.55.38	true	false		high
elb55.freshdesk.com	52.0.36.54	true	false		high
v2.zopim.com	104.16.104.139	true	false		high
pop-efr5.mix.linkedin.com	185.63.145.5	true	false		high
q.quora.com	3.213.100.238	true	false		high
s.w.org	192.0.77.48	true	false		high
static-cdn.hotjar.com	13.224.94.124	true	false		high
quora.map.fastly.net	151.101.1.2	true	false	• 0%, Virustotal, Browse	unknown
a.quora.com	unknown	unknown	false		high
in.hotjar.com	unknown	unknown	false		high
www.linkedin.com	unknown	unknown	false		high
help.yesbaker.com	unknown	unknown	false		unknown
px.ads.linkedin.com	unknown	unknown	false		high
static.zdassets.com	unknown	unknown	false		high
snap.licdn.com	unknown	unknown	false		high
static.hotjar.com	unknown	unknown	false		high
ekr.zdassets.com	unknown	unknown	false		high

Copyright null 2021

Name	IP	Active	Malicious	Antivirus Detection	Reputation
52718bdd550f7e11001c-3fe6492d1c83a22b9f69f88454beb1f4.ssl.cf5.rackcdn.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://yesbaker.com/types-of-insurance/	false		unknown
http://https://yesbaker.com/quotes/instant-quotes/	false		unknown
http://https://yesbaker.com/applications/	false		unknown

URLs from Memory and Binaries

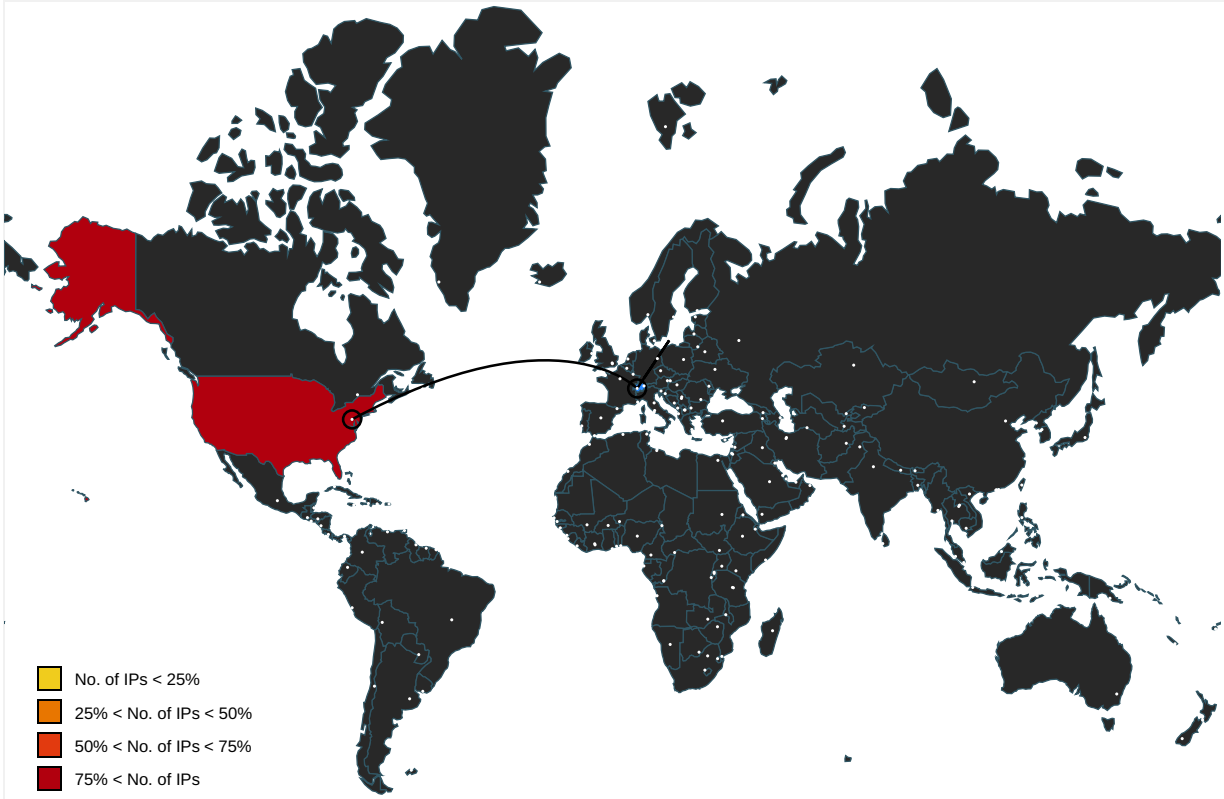
Name	Source	Malicious	Antivirus Detection	Reputation
http://robert-fleischmann.de)	custom.unified[1].js.2.dr	false	• Avira URL Cloud: safe	low
http://https://www.hotjarconsent.com/sv.html	modules.63d7c477e024dca70aae[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://yesbaker.com/types-of-insurance/personal-lines/#primaryimage	personal-lines[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/types-of-insurance/classes-of-business/	YUCJQHG8.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/wp-content/uploads/idea-min.png	YUCJQHG8.htm.2.dr, latest-updates[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/types-of-insurance/businessowners-policies-for-professionals/#webpage	businessowners-policies-for-professionals[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/?p=99	types-of-insurance[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/wp-content/uploads/fast-response-min-768x760.png	YUCJQHG8.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://bit.ly/raven-secret-key	widget_v2.329[1].js.2.dr	false		high
http://https://yesbaker.com/wp-json/wp/v2/pages/59	quotes[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/?p=571	general-liability-and-bop-online-app[1].htm0.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/quotes/#webpage	quotes[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/wp-content/uploads/logo-b-social-mediasmall.png	YUCJQHG8.htm.2.dr, latest-updates[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fyesbaker.com%2Fapplications%2F	applications[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/?p=92	professional-liability-quote-request[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com	YUCJQHG8.htm.2.dr, quotes[1].htm.2.dr, instant-quotes[1].htm.2.dr, applications[2].htm.2.dr, personal-lines[1].htm.2.dr, general-liability-and-bop-online-app[1].htm0.2.dr, types-of-insurance[1].htm.2.dr, professional-liability-quote-request[1].htm.2.dr, sell-international-medical-and-trip-cancellation-insurance[1].htm.2.dr, businessowners-policies-for-professionals[1].htm.2.dr, latest-updates[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/types-of-insurance/sell-international-medical-and-trip-cancellation-insurance/f	sell-international-medical-and-trip-cancellation-insurance[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/#webpage	YUCJQHG8.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://px.ads.linkedin.com/collect?	insight.min[1].js.2.dr	false		high
http://https://yesbaker.com/wp-content/uploads/insurance-12-300x225.png	YUCJQHG8.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/quotes/gen	~DF33282DA07EC74E7F.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://www.opensource.org/licenses/mit-license.php	custom.unified[1].js.2.dr	false		high
http://https://yesbaker.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fyesbaker.com%2Flatest-updates%2F	latest-updates[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://quotebaker.com	instant-quotes[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/dental-cancer-short-term-medical-insurance/	latest-updates[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/join-our-newsletter/	latest-updates[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.2.dr	false		high
http://https://yesbaker.com/wp-content/uploads/business-02-768x542.jpg	YUCJQHG8.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/quotes/instant-quotes/	~DF33282DA07EC74E7F.TMP.1.dr	false		unknown
http://https://yesbaker.com/?p=86	types-of-insurance[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown

Copyright null 2021

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://yesbaker.com/wp-content/uploads/insurance-14.png	YUCJQHG8.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://www.mediaelementjs.com/	mediaelement-and-player.min[1].js.2.dr	false		high
http://https://yesbaker.com/wp-content/uploads/business-07-300x200.jpg	YUCJQHG8.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/	~DF33282DA07EC74E7F.TMP.1.dr, latest-updates[1].htm.2.dr	false		unknown
http://https://yesbaker.com/latest-updates/page/2/?et_blog	latest-updates[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.hotjarconsent.com/pl.html	modules.63d7c477e024dca70aae[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.hotjarconsent.com/fr.html	modules.63d7c477e024dca70aae[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://html2canvas.hertzen.com	html2canvas[1].js.2.dr	false		high
http://https://www.zendesk.com/embeddables/?utm_source=webwidgetchat&utm_medium=poweredbyzendesk&utm_campai	widget_v2.329[1].js.2.dr	false		high
http://benalman.com/projects/jquery-hashchange-plugin/	custom.unified[1].js.2.dr	false		high
http://https://yesbaker.com/feed/	YUCJQHG8.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/contact-us/	YUCJQHG8.htm.2.dr, types-of-insurance[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/xmlrpc.php?rsd	YUCJQHG8.htm.2.dr, quotes[1].htm.2.dr, instant-quotes[1].htm.2.dr, applications[2].htm.2.dr, personal-lines[1].htm.2.dr, general-liability-and-bop-online-app[1].htm0.2.dr, types-of-insurance[1].htm.2.dr, professional-liability-quote-request[1].htm.2.dr, sell-international-medical-and-trip-cancellation-insurance[1].htm.2.dr, businessowners-policies-for-professionals[1].htm.2.dr, latest-updates[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/imakewebthings/waypoints/blog/master/licenses.txt	custom.unified[1].js.2.dr	false		high
http://https://schema.org	YUCJQHG8.htm.2.dr, quotes[1].htm.2.dr, instant-quotes[1].htm.2.dr, applications[2].htm.2.dr, personal-lines[1].htm.2.dr, general-liability-and-bop-online-app[1].htm0.2.dr, types-of-insurance[1].htm.2.dr, professional-liability-quote-request[1].htm.2.dr, sell-international-medical-and-trip-cancellation-insurance[1].htm.2.dr, businessowners-policies-for-professionals[1].htm.2.dr, latest-updates[1].htm.2.dr	false		high
http://https://yesbaker.com/types-of-insurance/	~DF33282DA07EC74E7F.TMP.1.dr	false		unknown
http://https://yesbaker.com/wp-content/plugins/gravityforms/js/gravityforms.min.js?ver=2.4.15.1	general-liability-and-bop-online-app[1].htm0.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/wp-content/uploads/business-07.jpg	YUCJQHG8.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://help.yesbaker.com/loading.html?ver=2	~DF33282DA07EC74E7F.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/wp-content/themes/Divi/core/admin/fonts/modules.ttf	YUCJQHG8.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://opensource.org/licenses/GPL-2.0	qevents[1].js.2.dr	false		high
http://https://help.yesbaker.com/support/solutions/articles/26000041389-architects-engineers-and-inspector-	general-liability-and-bop-online-app[1].htm0.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/types-of-insurance/personal-lines/	~DF33282DA07EC74E7F.TMP.1.dr	false		unknown
http://https://www.hotjarconsent.com/el.html	modules.63d7c477e024dca70aae[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://yesbaker.com/fire-sprinkler-contractor-insurance/	latest-updates[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fyesbaker.com%2Fquotes%2Fgeneral-liab	general-liability-and-bop-online-app[1].htm0.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/wp-json/wp/v2/pages/571	general-liability-and-bop-online-app[1].htm0.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/wp-content/uploads/insurance-12-1.png	latest-updates[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.zopim.com/privacy#cookie	widget_v2.329[1].js.2.dr	false		high
http://https://yesbaker.com/wp-content/uploads/insurance-14-1-300x225.png	instant-quotes[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.zopim.com/auth/$NAME/$KEY-$MID	widget_v2.329[1].js.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://yesbaker.com/quotes/real-time-quotes/	quotes[1].htm.2.dr, instant-quotes[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/types-of-insurance/feed/	types-of-insurance[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/types-of-insurance/personal-lines/olicies-for-professionals/	~DF33282DA07EC74E7F.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/wp-content/uploads/fast-response-min.png	YUCJQHG8.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fyesbaker.com%2Fquotes%2F&format	quotes[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.hotjarconsent.com/zh.html	modules.63d7c477e024dca70aae[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.hotjar.com	box-469cf41adb11dc78be68c1ae7f9457a4[1].htm.2.dr	false		high
http://www.elegantthemes.com	style[1].css.2.dr	false		high
http://https://www.hotjarconsent.com/fi.html	modules.63d7c477e024dca70aae[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://yesbaker.com/types-of-insurance/classes-of-business	types-of-insurance[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/wp-json/wp/v2/pages/181	sell-international-medical-and-trip-cancellation-insurance[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://use.typekit.net	widget_v2.329[1].js.2.dr	false		high
http://https://yesbaker.com/applications/liability-and-bop-online-app/?utm_source=newsletter&utm_medium=ema	~DF33282DA07EC74E7F.TMP.1.dr, {F358478D-5658-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/surety-bonds/	YUCJQHG8.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yoast.com/wordpress/plugins/seo/	YUCJQHG8.htm.2.dr	false		high
http://https://yesbaker.com/wp-content/plugins/gravityforms/css/formreset.min.css?ver=2.4.15.1	general-liability-and-bop-online-app[1].htm0.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/?p=59	quotes[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/wp-content/uploads/quote-online-min-300x297.png	YUCJQHG8.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/applications/#webpage	applications[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.amazon.com/	msapplication.xml.1.dr	false		high
http://https://yesbaker.com/insurance-agent-cyber-liability/	latest-updates[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/subdivision-bonds/	latest-updates[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/latest-updates/#webpage	latest-updates[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.twitter.com/	msapplication.xml5.1.dr	false		high
http://https://s3.amazonaws.com/assets.freshdesk.com/widget/freshwidget.js	YUCJQHG8.htm.2.dr	false		high
http://https://yesbaker.com/wp-json/wp/v2/pages/92	professional-liability-quote-request[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/types-of-insurance/businessowners-policies-for-professionals/	~DF33282DA07EC74E7F.TMP.1.dr	false		unknown
http://https://www.hotjarconsent.com/sq.html	modules.63d7c477e024dca70aae[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://yesbaker.com/wp-content/uploads/idea-min-768x760.png	YUCJQHG8.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/holiday-business-insurance/	latest-updates[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fyesbaker.com%2F&format=xml	YUCJQHG8.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.hotjarconsent.com/it.html	modules.63d7c477e024dca70aae[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://yesbaker.com/?s=	YUCJQHG8.htm.2.dr, quotes[1].htm.2.dr, instant-quotes[1].htm.2.dr, applications[2].htm.2.dr, personal-lines[1].htm.2.dr, general-liability-and-bop-online-app[1].htm0.2.dr, types-of-insurance[1].htm.2.dr, professional-liability-quote-request[1].htm.2.dr, sell-international-medical-and-trip-cancellation-insurance[1].htm.2.dr, businessowners-policies-for-professionals[1].htm.2.dr, latest-updates[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yesbaker.com/wp-includes/js/mediaelement/mediaelement-and-player.min.js?ver=4.2.16	latest-updates[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://daneden.me/animate	style[1].css.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.0.36.54	unknown	United States		14618	AMAZON-AESUS	false
185.63.145.5	unknown	United States		14413	LINKEDINUS	false
13.224.94.36	unknown	United States		16509	AMAZON-02US	false
13.224.94.39	unknown	United States		16509	AMAZON-02US	false
104.21.19.250	unknown	United States		13335	CLOUDFLARENETUS	false
52.216.139.125	unknown	United States		16509	AMAZON-02US	false
3.213.100.238	unknown	United States		14618	AMAZON-AESUS	false
192.0.77.48	unknown	United States		2635	AUTOMATTICUS	false
52.49.237.17	unknown	United States		16509	AMAZON-02US	false
104.18.70.113	unknown	United States		13335	CLOUDFLARENETUS	false
151.101.1.2	unknown	United States		54113	FASTLYUS	false
35.209.233.145	unknown	United States		19527	GOOGLE-2US	false
104.83.125.218	unknown	United States		16625	AKAMAI-ASUS	false
3.125.55.38	unknown	United States		16509	AMAZON-02US	false
104.16.104.139	unknown	United States		13335	CLOUDFLARENETUS	false
13.224.94.124	unknown	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339437
Start date:	14.01.2021
Start time:	03:08:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs

Copyright null 2021

Sample URL:	http://https://clubfluent.com/sendy//l/WeciX0nqw9S20mfKVbMPsQ/vilp61hl1PT892Foz892SW4unA/MKroVFHPnG34QjG38Mb7Zg
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:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@3/166@21/16
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://yesbaker.com/ • Browsing link: https://yesbaker.com/quotes/ • Browsing link: https://yesbaker.com/quotes/general-liability-and-bop-online-app/ • Browsing link: https://yesbaker.com/quotes/instant-quotes/ • Browsing link: https://yesbaker.com/quotes/professional-liability-quote-request/ • Browsing link: https://yesbaker.com/types-of-insurance/ • Browsing link: https://yesbaker.com/types-of-insurance/classes-of-business/ • Browsing link: https://yesbaker.com/types-of-insurance/personal-lines/ • Browsing link: https://yesbaker.com/types-of-insurance/sell-international-medical-and-trip-cancellation-insurance/ • Browsing link: https://yesbaker.com/latest-updates/ • Browsing link: https://yesbaker.com/applications/

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, ielowutil.exe, wermgr.exe, SgrmBroker.exe, backgroundTaskHost.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): 88.221.62.148, 108.177.126.95, 2.20.85.119, 108.177.127.97, 108.177.127.94, 2.20.85.242, 108.177.127.113, 108.177.127.100, 108.177.127.102, 108.177.127.139, 108.177.127.101, 108.177.127.138, 13.107.42.14, 2.20.84.85, 152.199.19.161, 67.27.234.126, 67.27.157.126, 8.253.95.120, 67.27.158.254, 8.248.113.254, 13.88.21.125, 52.147.198.201 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, e11290.dspg.akamaiedge.net, e9706.dscg.akamaiedge.net, iecvlist.microsoft.com, l-0005.l-msedge.net, go.microsoft.com, www.googletagmanager.com, audownload.windowsupdate.nsatc.net, auto.au.download.windowsupdate.com.c.footprint.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.google-analytics.com, www-linkedin-com.l-0005.l-msedge.net, cf5.rackcdn.com.edgekey.net, fonts.googleapis.com, fs.microsoft.com, www-google-analytics.l.google.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, www-googletagmanager.l.google.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, e6923.g.akamaiedge.net, skypedataprdcoleus16.cloudapp.net, wildcard.licdn.com.edgekey.net, go.microsoft.com.edgekey.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\2OLSYT59\yesbaker[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	512991
Entropy (8bit):	4.777383283409861
Encrypted:	false
SSDEEP:	768:HhBzpBPbJ6z2GPit4MhBzpBPbJ6z2GPit4LhBzpBPbJ6z2GPit4FhBzpBPbJ6z2l:h
MD5:	1DAF13C6300636D545F6DC73BA457EF0
SHA1:	C373A9241532C2B50EE40964EE063F119FF13527
SHA-256:	6B118CD28F47674BC86174FFCFA87390097F15510EC15117D9D823FF3BEED5CA
SHA-512:	B8614F8E814B9A9116832A2C97DBD0FA718334945BAAF2F9CA805411DACC2934581CD9F27C8AECC24502BF0B42B58F1B0B6AD9104FDA2EE23117DB684FE4108 1
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root><item name="_hjid" value="980498b5-1a8b-4ee2-8837-282ea2edefde" ltime="3123185200" htime="30861925" /></root><root><item name="_hjid" value="980498b5-1a8b-4ee2-8837-282ea2edefde" ltime="3123185200" htime="30861925" /><item name="__storejs__" value=""__storejs__"" ltime="3135195200" htime="30861925" /></root><root><item name="_hjid" value="980498b5-1a8b-4ee2-8837-282ea2edefde" ltime="3123185200" htime="30861925" /></root><root><item name="_hjid" value="980498b5-1a8b-4ee2-8837-282ea2edefde" ltime="3123185200" htime="30861925" /><item name="__zlcstore" value="{"2aAG4Yaujk60E8bjImgY6dLCXCaOop7z":{"last_host":"widget-mediator.zopim.com","timestamp":1610622582164}}" ltime="3255075200" htime="30861925" /></root><root><item name="_hjid" value="980498b5-1a8b-4ee2-8837-282ea2edefde" ltime="3123185200" htime="30861925" /><item name="__zlcstore" value="{"2aAG4Yaujk60E8bjImgY6dLCXCaOop7z":{"account_stat

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\NTI5R0OA\vars.hotjar[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Reputation:	low
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{F358478B-5658-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8567954711084484
Encrypted:	false
SSDEEP:	48:IwbGcprCGwpLlG/ap8w4rGIpcw51GvnZpvw5lGogqp9w5BWGo4xpmw5MGWuO9w5g:rBZqZB2B9W8yt8bf8fxM8m8M8qf8zMX
MD5:	57E81F5D6A3BBB0CDD9F85A183B09A1F
SHA1:	88BC9D1DC3A0E7106DFE3BAEB4C406EE62243695
SHA-256:	9CA1E2BEB3B326BC64C0CEB4DFD34A28E96A5AEB17DC32D807855279C1D58321
SHA-512:	8C33292A7AD8E8DEAE8973E0C9B1516B3D69FBDF112EE53ADAE39BB574A0DBBDAB432E23BDB48AC88039F5E508DFDE833B5E0DD1695771C51DC462D415747 21F
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{F358478B-5658-11EB-90E4-ECF4BB862DED}.dat	
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F358478D-5658-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	384804
Entropy (8bit):	2.911598666183763
Encrypted:	false
SSDEEP:	1536:mrAHX76mzKKwmLKg23/e6ryXekHz+ysQ1:mrAHWmvVLZr1
MD5:	1B683C6609B7B17318FEA01E239E68E2
SHA1:	B5F1291A222ECCD2E433B2C17B380512F5C02135
SHA-256:	948B6DF354987C4F66CE5EF3146884453762A98AAB569D657F1A9B4CBA94EFF5
SHA-512:	6704E3BF669C4EEAD73F7DE9328197C8AF1BE418B292469CF19598F54FB270583FA63C2872856FB71647A15D5B841B8A3494BCDC697CAF25F01B016734C6100B
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{FC166633-5658-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5632968250238792
Encrypted:	false
SSDEEP:	48:IwqGcprDGwpaCG4pQuGrapbSYrGQpKeG7HpRBsTGIpG:rOZdQy6gBSYFAZTB4A
MD5:	A78705D273E5F389392C0C7E4E73FA50
SHA1:	D8824C5B7149465ABF7036B073437024399FB73D
SHA-256:	3431A3745E5179551642B94D26BDD5FB690212F8AE6CC57C99745E58679B876B
SHA-512:	E5210E12AB25B8E8A1AE69FA16574688221DF4881B635448ED0BFE880A6AF6F3133E50115085CD8065515D8F305564707BA57AA838A30896218049596505 5E65
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.0733286592660285
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEMDSYEPDS6nWiml002EtM3MHdNMNxOEMDSYEPDS6nWiml00ObVbkEty:2d6NxOdS5S6SZHKd6NxOdS5S6SZ76b
MD5:	179E0B15AD29E35AE5FBE6C6F2C316D0
SHA1:	7843787EDDE64D483BD1FA03C47B0331C684D462
SHA-256:	AFD9C481A424338C2630F96841CB96257E9C85FE833232863965959092A8BC2B
SHA-512:	70B46DD72623D063C125D4781850024B691F6E2E5FA9F3CBA29B4982907F0AD2E1F5DC9DEE278C16FD55EDD666AA2F866B6D94E0CC4F8738EE41028E957628C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xe81ac4f7,0x01d6ea65</date><accdate>0xe81ac4f7,0x01d6ea65</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>0xe81ac4f7,0x01d6ea65</date><accdate>0xe81ac4f7,0x01d6ea65</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):	5.088560980611857
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kgcJmE5cJMnWimI002EtM3MHdNMNxe2kgcJmEsUtnWimI00Obkak6t:2d6NxrsI6SZHKd6NxrsBSZ7Aa7b
MD5:	CBA245EA7F123C992E6D95A710FD2020
SHA1:	60BC10895ABE52438F8792A02D146F1777DC45DF
SHA-256:	D00E3E6E90671E66C1C07867658B13C9A958B6F82C97ECC676070A924C42E3DE
SHA-512:	18E818ACDB7AF0C9FE8689B48B8220D073629EA10DF8E7285A0C3B546914B8F829A186D0316D9AB36C315C07C93722672F37678A0F3959912F5514682527CAC8
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xe7a97cd9,0x01d6ea65</date><accdate>0xe7a97cd9,0x01d6ea65</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>0xe7a97cd9,0x01d6ea65</date><accdate>0xe7fcef10,0x01d6ea65</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):	5.116180622565726
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL2E1nWimI002EtM3MHdNMNxvL2E8KnWimI00ObmZEtMb:2d6Nxv1SZHKd6Nxv8KSZ7mb
MD5:	4AAF763C6FA08BB92F5F8B9963FECCAF
SHA1:	DB8CCEE90AD563A7EDE5C697BE067CCB997A8EE2
SHA-256:	7CA359F8DA8BE44641522E9D72D494B566FED670EFFE59BADA08D75C070AAC22
SHA-512:	ACAE2F1E8C5B970A69D1E00FAF76F13AD060C4BA4C2DE5EC85F36DE502FDF02161CC081184EAD2A79A3314149F2A64961EF427CFE1B62F9D466ADC27971A1F7
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xe81b612b,0x01d6ea65</date><accdate>0xe81b612b,0x01d6ea65</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>0xe81b612b,0x01d6ea65</date><accdate>0xe81c99a5,0x01d6ea65</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):	5.108001042701358
Encrypted:	false
SSDEEP:	12:TMHdNMNxiOEJnWimI002EtM3MHdNMNxiOEJnWimI00Obd5EtMb:2d6NxuSZHKd6NxuSZ7Jjb
MD5:	80C8DDCAD340F0540095D95E9A93E98A
SHA1:	AF78D869E63AED2F737D2E7561C6FB04E544596D
SHA-256:	4E2BFDF152929BD655DF53647964CF3F1CED9190496433F14CEB5BED7EA6FE54
SHA-512:	ED7BE495CF0A4E2A79FCA1196CAE7E2DE76F0F6E275FB66D3125F727D03722E429A4B673683B6E73711033430B2392D66DC3EA641A19C3518F60141AB29B12E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xe814c691,0x01d6ea65</date><accdate>0xe814c691,0x01d6ea65</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>0xe814c691,0x01d6ea65</date><accdate>0xe814c691,0x01d6ea65</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):	5.103347922472131

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGw4EnnWimI002EtM3MHdNMNxhGw4EnnWimI00Ob8K075EtMb:2d6NxQISZHKd6NxQISZ7YKajb
MD5:	3749ADE29791CC368253D1075E5C5B22
SHA1:	FD46E3B9D73E8A7D711BF89B790563579F388105
SHA-256:	8B5BF112EFC1326B14F8A59784F519CCE2F0B4C6D73C8B465F7E4FA02B6C4174
SHA-512:	41CFD03F750A40614BF0C24D4F3CD8AB49554736BA2D8EA13D422A07BE2F09D835E32DB28EB60F818017C540C08C7ED250B5BCB15F440A8C8B05E756B756B2(
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xe81d35f5,0x01d6ea65</date><accdate>0xe81d35f5,0x01d6ea65</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>0xe81d35f5,0x01d6ea65</date><accdate>0xe81d35f5,0x01d6ea65</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):	5.118095136269265
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n/I5+jEoI5+DnWimI002EtM3MHdNMNx0n/I5+jEocGnWimI00ObxEty:2d6Nx0LzDSZHKd6Nx0LGGSZ7nb
MD5:	FC3BB071093BB7A1B055A75B93C5BE56
SHA1:	963AF898E84D1F81ACB05858D2AAFC319E4C0D81
SHA-256:	7DB3FF6BBBA407801F785BE831466609E95625FA0043EB5BD6625FFE7E5E97ED
SHA-512:	849F0F44787E3C0D8BED85C91ECA94A40600B07577D80732B370A0CD5BE6C7928C7A38C1FB4678F8CDFBC5BEC32C02A082630AA09A62C44C58C6DADEC2C7B1B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xe8172904,0x01d6ea65</date><accdate>0xe8172904,0x01d6ea65</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>0xe8172904,0x01d6ea65</date><accdate>0xe81a28a2,0x01d6ea65</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.13269448783472
Encrypted:	false
SSDEEP:	12:TMHdNMNxxOEJnWimI002EtM3MHdNMNxxOEJnWimI00Ob6Kq5EtMb:2d6NxnSZHKd6NxnSZ7ob
MD5:	DB51B8B43FA3B470165A21DC003CA585
SHA1:	8B3B32F1C97A68D554ACB54F71C642F06A2EFB1E
SHA-256:	ECD4C8051F92BC599615D9CFADDD31B0AA0F18C5B50C040939104C44E5F79B73
SHA-512:	F55D4AE433D16B56AB092CBBFAC5E5E8813BF18636EFAEC907E6DD7142238567B347F73ABF6FD2F09318760BFFDD1CC299D4A181E7EB9C75A9F9069246E929F3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xe814c691,0x01d6ea65</date><accdate>0xe814c691,0x01d6ea65</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>0xe814c691,0x01d6ea65</date><accdate>0xe814c691,0x01d6ea65</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):	5.115308788875993
Encrypted:	false
SSDEEP:	12:TMHdNMNxcHJEatnWimI002EtM3MHdNMNxcHJEatnWimI00ObVEtMb:2d6Nx+SZHKd6Nx+SZ7Db
MD5:	512FC7B9085D1983D65C980C665C60E3
SHA1:	A017C979EB1ABB916A65DB2712AA7C00A6457D8D

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
SHA-256:	B2BB12D8EC73206EDC7C8D0F200A301E62D80C37F72539D206CBAB75BCB1F9E3
SHA-512:	EFE0E82134B973D46A6C4E449CC4C12930AB9B0B2081819DA33E2531A834BC075954398B6D5967FF084562F6CF41956015E0B14BF19A4EA2EAAA53187011353E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xe80d9fb2,0x01d6ea65</date><accdate>0xe80d9fb2,0x01d6ea65</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>0xe80d9fb2,0x01d6ea65</date><accdate>0xe80d9fb2,0x01d6ea65</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):	5.093693300747267
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnOEJnWimI002EtM3MHdNMNxfnOEJnWimI00Obe5EtMb:2d6NxVSZHKd6NxVSZ7ijb
MD5:	8F233A45DF71111B9E2688B65CE1554B
SHA1:	9B0A40439E009FBCC9CA4CB727455DEADBA1B89C
SHA-256:	55B6A4A8021110A8AD62F1049D70981CBF204938452D8EFF45D78FC883609955
SHA-512:	57C0D3B357613F960FF228C0A2A35B1E38B7124E7E72B583C087228C109748D291CE76FF1148E04DAF78EA9817CC22FB7FD55DD21727496B61F291B2CD9CA37(
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xe814c691,0x01d6ea65</date><accdate>0xe814c691,0x01d6ea65</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>0xe814c691,0x01d6ea65</date><accdate>0xe814c691,0x01d6ea65</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):	7077
Entropy (8bit):	7.6913826418791365
Encrypted:	false
SSDEEP:	192:McTQj3iyRR8gTnnJcsmIYsssssEYEEUecBZ3fh7:Mcc7HUOnnJUIYsssssbEE8B1h7
MD5:	A7F18227B016D7ECCE4642647BCA2EFD
SHA1:	32DCCFA144FCAB08C1BE30D9FC401B5EEF4A0942
SHA-256:	22079BA2D40A3390473500FB34FEE0785697696386E2FFC5A6B28058F9F29C14
SHA-512:	66C7E902ECA87F9B3999DD97DEBE86D664327423208432BCE9BEC1DD70D146C209795E99756B1D4D283A3823BEB6B88DC07488F84198767E28491C0308567672
Malicious:	false
Reputation:	low
Preview:	3.h.t.t.p.s.:././.y.e.s.b.a.k.e.r...c.o.m./.w.p.-.c.o.n.t.e.n.t./.u.p.l.o.a.d.s./.f.a.v.i.c.o.n...j.p.g.....JFIF.....".."..+"+.F26262FjBNBBNBj^r]V]r^..vv.....".."..+"+.F26262FjBNBBNBj^r]V]r^..vv.....".....Zlh...Z,....%GP.../2.....p@...g.v.....r.....N....G.O.....#W..\g@..9+`..>...DU.=.... b.....X... ....T....3.i..{...+q.X.....<.P..@.sS..3.....q..^.....i..uO.....-.5..I.....T.G}. .W....k..f.....`...,...y.....5L.....6.8....pP.....fbi.....8z.X.U.".5U...ON85..]`ea.....3..Vp.z..X....}...&.....@.7H8.....>..P..F..*.t.....i.....u.g....P.r..<....~:...K....V~..@.g.v.j..#."j.^.....u..O.....r..[.lj...@..eh...1a...r..<.6z4|.....p....W...p.-.....k.....CC....H...,...\.Y*....^r.....+$...c..... .H..fj^...i.d0.#hbr.U.....R.pWn .W.....%.8...8k

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\2aAG4Yaujk60E8bjImgY6dLCXCaOop7z[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	194
Entropy (8bit):	5.051713702832791
Encrypted:	false
SSDEEP:	6:Y9KXW/+k87hCh/izyHv0ngRKrvEE2e2ddw//1V:YoG2kKJyP0gsriZdqj
MD5:	9440C7C0F0D960E3CB0B55BEC6757C88
SHA1:	6053BD14F71D4D42504DC1CF95184E0D4BEDE3D6
SHA-256:	7E339C965603BEB0239409336F47EEFAA23CAD316B68C3497D197EC38495D3BA
SHA-512:	6B38F6EA1841750D944F6B848BED5A9179EEA2FD30FEF71D10FF8043662EC85E4229BD6708C9F14952DCC55A8775E2EA45034BA9675A217C5D6E0E81EDF9898
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ekr.zdassets.com/compose/zopim_chat/2aAG4Yaujk60E8bjImgY6dLCXCaOop7z

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\2aAG4Yaujk60E8bjImgY6dLCXCaOop7z[1].json	
Preview:	{"products":[{"name":"zopim_chat","id":"2aAG4Yaujk60E8bjImgY6dLCXCaOop7z","features":[],"url":"https://ekr.zdassets.com/compose_product/zopim_chat/abc123?deprecated_features=true","assets":{}}]}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\7711889ed56448a780eeab83a[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	50
Entropy (8bit):	4.296174630069641
Encrypted:	false
SSDEEP:	3:2LGffO9SMpsE:2LGXO9SMpsE
MD5:	104D46A3208B40E8DED389332F5A78A3
SHA1:	4AB55CCB2972E9A3CB62C65C97308C2450A682BB
SHA-256:	F6E4F5EDB3194334A199F0BF80B38D92A0B7388330FBCE94C8C0FB2F852C171F
SHA-512:	06FF914285DE322A565F5A66989653255369F6869320735ECE16696F7C2A3BC01BD3661F3FC2F99E9245E542ABE020C367132CF8C8C75D69E71E9EBFF8C46934
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://chimpstatic.com/mcjs-connected/js/users/dca38e5da8e69f33b4ef3814b/7711889ed56448a780eeab83a.js
Preview:	(function(){if(!window.$mcSite){$mcSite={};}})();.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\JTUOjIg1_i6t8kCHKm459WxZqi7g[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 65852, version 1.1
Category:	downloaded
Size (bytes):	65852
Entropy (8bit):	**7.9927317327762495**
Encrypted:	**true**
SSDEEP:	1536:QTzYcvQuJpIF8ZEAktOxhPcazKeVTHB+2kqnqwNBuYRIXYU4d21:QTUcvQuwCZEAQ8lZhVE2k4lC4d21
MD5:	8FEFF27599A7D5F35297D003B193C0E5
SHA1:	5CFBA2B9DBDF693E0FB4DB5C77CA20A6ED6319D9
SHA-256:	48A6C66B235C35F1FB383289F9E37CEFA4F20A59DC1D503869BDBA80F0F50DBE
SHA-512:	9FD490B36C1CD0C85C283BCACCE522104F802AFAA02DBAA159CBAE9819ABE99D8DAE6A2D0EF0C104A2E84EA3948291B23FC7D503412E0F9F24CCB7BD5B6F3D81
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTUOjIg1_i6t8kCHKm459WxZqi7g.woff
Preview:	wOFF.....<.....0`.....GDEF.....+.....1GPOS.....8....'.bGSUB..;X.....OS/2..@d...Q...`U..'cmap..@.....7cvt ..H....\....,...fpgm..I,...F...mM$.\|gasp..Ot.....glyf..O\|.....h#)xhead...p...6...6.<]ghhea.....#...$...khmtx.....Z;.loca.....q....N...maxp..... ... ...fname...4.....$/.KVpost...(...U..(.rZCIprep.....K..x...3.XQ.....m..m..&.m....\4k.{.....Yy..E.....fkp...v.....f?....K...b.....n....._...''^.[x.?.W..DO.dO...0W)....T...*VW.....DM...a...Vj.....U_..8R.p.&....9Z.....k3n.6...W.....Q...:..t....^....[xG.....S=..z./....=~.7....K...b..1CY..\|.....9l....'j`!..M.`...].?!..C.{9!.<....xOE..Q7.x.V.h.W.=..e.....j.2,.....h.....+Kp7..-PQ.*b.....R.a..,a.K.DJX,%,e.,a.J?. .x=....b..xw.{s.}.....;..l.....?t.. ...?=.7....`..k..NQ..idQ@.....f\.....;.904...8.....=.....(.....o8.$..:XS..z.....&l%...n..ss..fY.,....f.w!.].=x...0j{...h.=.....n.z.(...S.*...../ul/.m..|.''....F.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\JTUPjIg1_i6t8kCHKm459WxZOg3D-A[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 69316, version 1.1
Category:	downloaded
Size (bytes):	69316
Entropy (8bit):	**7.993692051214259**
Encrypted:	**true**
SSDEEP:	1536:+eXE+ksP2D7F8EaPnZbccYqsRI2CE+rYbPhLv6ENIkwPog21:+A2/CEaPnzRsWNE+MbNZN+Pb21
MD5:	7CE40DD1F5239AA322734490524EBC6A
SHA1:	5C008CB3E1E08F3FD75E70DF4326D5509A3CAA4A
SHA-256:	00FDDD54A15B722C05B226AB3260C7FEC6D1DE5CFAE3117EFED1DC1386072527
SHA-512:	7076A5148280AC70B1CC4C2F31B1022C133A6323A8A83F363BC90C62F96887FA24A6DE4F2A15DFA313082C09367565B13B6406DC8BA969A6FAC0F88DA4ECDB9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTUPjIg1_i6t8kCHKm459WxZOg3D-A.woff
Preview:	wOFF.....3@.....GDEF.....+.....1GPOS.....?....Z...GSUB..B<.....OS/2..GH...S...`V..Icmap..G.....7cvt ..O....b....0...fpgm..P....F...mM$.\|gasp..V`.....glyf..Vh...T..*..s.?head.....6...6.z].hhea.....#...$....hmtx.....loca.....u.....Nkmaxp..... ... ...fname.....41.L.post.....U..(.rZCIprep.....K..x...3.XQ....m..m...&.m....\4k.{.....Yy..E.....fkp...v.....f?....K...b.....n....._...''^.[x.?.W..DO.dO...0W)....T...*VW.....DM...a...Vj.....U_..8R.p.&....9Z.....k3n.6...W.....Q...:..t....^....[xG.....S=..z./....=~.7....K...b..1CY..|.....9l....'j`!..M.`...].?!..C.{9!.<....xOE..Q7.x...p#...?.e....|:.O.....<ffffff..33s.....(.Q../.n.....>..>..u7...Q....}w:t..H..;...y..lf.....v...5+....}xo..g.}X;+.<..y2.5z(.P...r...}.;._}.W>G>t.j,.l[.....M.....kl&e....-..y..{..'.....W.c.....,.>.b.....o ..o..x.+...k.....45OX.!h..gI.z=..m].!$.....K....G.....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\JTUPjIg1_i6t8kCHKm459WxZSgnD-A[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 69604, version 1.1
Category:	downloaded
Size (bytes):	69604
Entropy (8bit):	**7.991805556687666**
Encrypted:	**true**
SSDEEP:	1536:kNXWiWF8oEMFtUcb4gVMI2LeuWZMzn+D1ilia21:VbCoLT/XKeuWq7+DEIr21
MD5:	7578E1126B41D63AE7B7B458B2ECF2DD
SHA1:	1732DDE9777C0FB6189DE0C3628EF22BB297B1E6
SHA-256:	F6AA7C70644DC846F5B1E81AFDCAF84C12557C71E3E1DE07A4671C65A062E00D
SHA-512:	710FD0843AC7C4EA4D089E4A4DBB06189A1A44BA018BE2D8FB78ECE25D31932C3F9FFBC7DCAADFA7FE3D57DDDB97A2F7DAFDADB199A17C2E23F0DF6D5A3CDD7B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTUPjIg1_i6t8kCHKm459WxZSgnD-A.woff
Preview:	wOFF.....S.....GDEF.....+.....1GPOS.....9.....N.GSUB..<0.....OS/2..A<...S...`W..~cmap..A.....7cvt ..I....e....6..`fpgm..J....F...mM$.\|gasp..PX .....glyf..P`...f..R..0.head.....6...6..].hhea.....#...$....hmtx...$.....sk+loca...0.....3]maxp..... .. ...Pname...../.Lppost.....U..(.rZClprep...(.....K..x...3.XQ.. .....m..m...&.m....\4k.{.....Yy..E.....fkp...v.....f?....K...b.....n...._...''^.[x.?.W..DO.dO...0W)....T...*VW.....DM...a...Vj.....U_..8R.p.&....9Z.....k3n.6...W.....Q...:..t...^....[xG.....S=..z ./....=~.7....K...b..1CY..|.....9l....'j`!..M.`...].?!..C.{9!.<....xOE..Q7.x..W..UY.....9..i..U...y..i..XQ.n.....&. %*i.V[+X.Z..0...SL.Ka...Y.e.....3..v...:.;.?.....[.a.H...8.U'..:.... ..0.....A.....8...'.v.....hh..b1.L..O,....&..&..'..8|.....v.*#..A....v&=1....I.P...O..o.)?.p~.?..O.58j".Mz..W.o.<-.`~.....?. a...>../.B.....Y5....Z.|3<E.<.M

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\JTUPjIg1_i6t8kCHKm459WxZYgzD-A[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 68736, version 1.1
Category:	downloaded
Size (bytes):	68736
Entropy (8bit):	**7.993591033871696**
Encrypted:	**true**
SSDEEP:	1536:ni6cEWzGdF/mF81GdvoSJgkCr1NsnxbYb6B3nIfsOOzcf5f21:ikqGqC1GuIMr1NsnxOE3nDOOYRf21
MD5:	5DD75E5EBC71DE2903F3BE66B2BBF3E2
SHA1:	4E3741AFF6C7E782837388519A5A959D66CCF96C
SHA-256:	9A6021BC1E9FA77DE340F03237BDF9F4B32421288026F4206A29B7C09913FF97
SHA-512:	4AC579CBD0D1177907C82AAA4B30EBA06444C5E6B32BBD73C32249308DDEFFC68FF23CBCE2FB5FD2C2DE5B7383C952FA46ED2249474BCBCA75A9841D6F7C2452
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTUPjIg1_i6t8kCHKm459WxZYgzD-A.woff
Preview:	wOFF.....0d.....GDEF.....+.....1GPOS.....?q...<. .QGSUB..B .....OS/2..G,...S...`U@.4cmap..G.....7cvt ..O....b.....7.Efpgm..O....F...mM$.\|gasp..VD .....glyf..VL...O..'RD..head.....6...6.U]shhea.....#...$....hmtx.....'loca.....o....PY. maxp...X... ... ...ename...x.....,0.L.post...l...U..(.rZClprep.....K..x...3.XQ.. .....m..m...&.m....\4k.{.....Yy..E.....fkp...v.....f?....K...b.....n...._...''^.[x.?.W..DO.dO...0W)....T...*VW.....DM...a...Vj.....U_..8R.p.&....9Z.....k3n.6...W.....Q...:..t...^....[xG.....S=..z ./....=~.7....K...b..1CY..|.....9l....'j`!..M.`...].?!..C.{9!.<....xOE..Q7.x..et#.....:N..L&..x7.....u.....>...N..T.j..U...X..%.Za.*.....a.=vb.RB.1.(..I..s..M.P.~:..vb...q..g.....\^.. .y2R..(.L..+.w8i./...O.^..(.-..1...3Hh.....$.z<.....=e.)S...[].O..w...g...C.....L1..0;.....T..h.....?(S...I..U.K.%E.U.1}k6$tK..sAh...Na!a...$.VE..1..,I..Y@..H..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\JTUPjIg1_i6t8kCHKm459WxZcgvD-A[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 69760, version 1.1
Category:	downloaded
Size (bytes):	69760
Entropy (8bit):	**7.992307857451354**
Encrypted:	**true**
SSDEEP:	1536:fLHIJil37cMquF81yGhjT/7DyCNPACpdu2Qm59N21:fLoJWBfC1yGZXX4ou2QY/21
MD5:	8197DAF6E2226D6F7A935D17C86DB624
SHA1:	F7F47DE582E1AB0A50C47B3846C102EAE4FECD7D
SHA-256:	87DA1E1954D361586D3E3982BD0FA91179B5DC78A5CE2BEA6B8963E64A9D89DC
SHA-512:	8F5D535168CCE6B807E6BA85F16846A32D53D5D590412EB7566415E0683D77324BC5E67CA104911EE82F571CAEAD169CDD293F9CE03719881DDBE086C577E6E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTUPjIg1_i6t8kCHKm459WxZcgvD-A.woff
Preview:	wOFF.....7.....GDEF.....+.....1GPOS.....?.....[&d{GSUB..B.....OS/2..G....T...`V..cmap..G.....7cvt ..P....c....3..Afpgm..Pp...F...mM$.\|gasp..V.. .....glyf..V.....-.8E(.head...l...6...6..].hhea.....#...$....hmtx.....>..Aloca.....o.....:maxp...P... ... ...Qname...p.....$/.K.post...l...U..(.rZClprep.....K..x...3.XQ.. .....m..m...&.m....\4k.{.....Yy..E.....fkp...v.....f?....K...b.....n...._...''^.[x.?.W..DO.dO...0W)....T...*VW.....DM...a...Vj.....U_..8R.p.&....9Z.....k3n.6...W.....Q...:..t...^....[xG.....S=..z ./....=~.7....K...b..1CY..\|.....9l....'j`!..M.`...].?!..C.{9!.<....xOE..Q7.x..W.....}.^.t+<{..E.....I.v..c.3.2].y.j.....7.f...r.b.....=..S.\.7^.M.....Aq...Q.w.v!.;@.Et]s.._.=..5.....} .k...Y.p>...d.k.....9...~._...K.....sK_.2B....S...f.~.....W.....g.d.....:.Mk9.....0.1xFa.....r.+_...s7.....E..$..r.@.He.....}+.3 ..I.(EP.....K.F..A..E_z..SW

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\JTURjIg1_i6t8kCHKm45_cJD7g0[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\JTURjIg1_i6t8kCHKm45_cJD7g0[1].woff	
File Type:	Web Open Font Format, TrueType, length 66760, version 1.1
Category:	downloaded
Size (bytes):	66760
Entropy (8bit):	**7.992566869086574**
Encrypted:	**true**
SSDEEP:	1536:rFLrJF8VoDzqofN6KN+iS9LtqXwSGs/VwpQSU:h9CVoDzqo16KKRS3d6m
MD5:	605B1955F137C5A0F5C8BB9EF8E159A0
SHA1:	7D18B0663855A3B69CB9C96CB0CD12F8E4B6FA0A
SHA-256:	2CFE51BC6374D398DF02878552212424C127BF52D72E67FB3A1CF637AF984046
SHA-512:	D375D1665B2C4CAA0E466B3999A572338F04EF3D61CE4AD9E9BBA451AE0DC1364112A96615514DFB0877245EB58DF5A6A78DA6F0A21DF8CFB17F7EEFAFC0C4E6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTURjIg1_i6t8kCHKm45_cJD7g0.woff
Preview:	wOFF.....+`.....GDEF.....2....X.|GPOS.....>O....J.i.GSUB..A.....OOS/2..F....Q...`U?.:cmap..F\.....3cvt ..Np...b.....:.Gfpgm..N....F...mM$.\|gasp..U.....glyf..U$...G..#.M.Ahead...l...6...6.<.ehhea..... ...$....hmtx.....~.....V6bloca...D...o.....,.maxp..... ... ...Zname.....)!Etpost.....L..(....prep.....K..x.....XQ...s_m.6..v\.V..V..m.E\.\.....Yi..U.....l+q...Sv...=\|`...}./...Y..y.s..5..w.....R\.'._....._..xL.dLS.s.SI,.2XN.*beU.j.....6Q.I...J.z`o.....5.'j"N.d..i8K.p...Rm.....wj'.....xP....Q..:..t.....]....P...s.....'....U2f(.s.o..P.7...2\|...Eu,D..I.LV....-$cj.`/+d.G..4...F.S...x..W.t#I..mu.v.....-33333.....y....,.....z.V..j...UF. ...(.#.;..K.....\..1..$w.....lj.A.r.._..1...?u..u...a....2.. O&.F.....S..x...?..w\.k.u.2.(c.....(..=.....<.c....Xe.Q@.x..s>.7..7...~._.....o.v.Ob....v.?A.B.-.A=..&.NJy....0.....@.:v....h...!.d....D.m.b.....\.....]..-..V

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\JTURjIg1_i6t8kCHKm45_epG7g0[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 67412, version 1.1
Category:	downloaded
Size (bytes):	67412
Entropy (8bit):	**7.993450426954292**
Encrypted:	**true**
SSDEEP:	1536:vpUdhLGRrmF8WfSbBbaWCShX2pjB1AcEZpwpXssK/bg9SU:vgl8KCWfSbBbaWCSh6jB1UZpQc9/w
MD5:	0E813A2AA235DEC42E57B2528E706E6E
SHA1:	2C60C82DD360D8B0ABC0E95235E01054851F3387
SHA-256:	C680AD34448FA46EDA0C53281F2CDEC64CB508D636E21608E551B7716C026C7A
SHA-512:	DFB17A1FA40C2102F4D9ECEFA98FA85AC1676CEA752726CC6B8EFC44792E29383C14F8437F227859791D72F418D43E71628D1D1E4733021BE76B942D60561A56
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTURjIg1_i6t8kCHKm45_epG7g0.woff
Preview:	wOFF.....T.....O.....GDEF.....2....X.|GPOS.....7.....L...GSUB..:L.....OOS/2..?P...Q...`W...cmap..?.....3cvt ..G....e....6..Xfpgm..H ...F...mM$.\|gasp..Nh.....glyf..Np.....P@.2%.head.....6...6....hhea...(... ...$...uhmtx...H...r.....loca...../.maxp...@... ... ...Pname...`.....(.EWpost...L...L..(....prep.....K..x.....XQ..s_m.6..v\.V..V..m.E\.\.....Yi..U.....l+q...Sv...=|`...}./...Y..y.s..5..w.....R\.'._....._..xL.dLS.s.SI,.2XN.*beU.j.....6Q.I...J.z`o.....5.'j"N.d..i8K.p...Rm.....wj'.....xP....Q..:..t.....]...P...s.....'....U2f(.s.o..P.7...2|...Eu,D..I.LV....-$cj.`/+d.G..4...F.S...x..V...Y...;.{..7.....,Km..j....JSU.d%H.J.l.[+X.Z..0.0.L1a.....,.....~..7..5.%..y.{...9.....6o.....3G..FD.....:C.#Xg.C.....'!.9rn.....a....}...d.k..G.....C.~7uglt..7...B7.G....V..n..2..t1...M..1..U...5.....p~..i.'I5...)M...j.F....1..O..@..IS.b.S..q...B.....bq.V.r.,.I.V

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\conditional_logic.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):	7482
Entropy (8bit):	5.152122157418057
Encrypted:	false
SSDEEP:	192:rm04k/c0ap42mvmCZIMXHfdHCYtLm6N24u:rmBKt2muCBvxC0/u
MD5:	CCC8C4F2006EC4C58083C63DA6F0757C
SHA1:	6B2F58A6F4B35ABF369E90B2E632BE2FC9ADC42C
SHA-256:	15A67EA47EC12C84FCF1A63B7D6F9FA2B1D76017E08968BBEFFDC7B7CF3A0BFA
SHA-512:	2F3B94CF3E96B135103FC0D5CB53A53D8784398A92B2DA654F70A422D1AA4C2DA02C5DBBA4F5CD4A53CD4657939F49724A4375435C869581D85D7D01ECE5788
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-content/plugins/gravityforms/js/conditional_logic.min.js?ver=2.4.15.1
Preview:	var __gf_timeout_handle;function gf_apply_rules(e,t,i){var a=0;jQuery(document).trigger("gform_pre_conditional_logic",[e,t,i]);for(var n=0;n<t.length;n++)gf_apply_field_rule(e,t[n],i,function(){++a==t.length&&(jQuery(document).trigger("gform_post_conditional_logic",[e,t,i]),window.gformCalculateTotalPrice&&window.gformCalculateTotalPrice(e))})}function gf_check_field_rule(e,t,i,a){if(!window.gf_form_conditional_logic||!window.gf_form_conditional_logic[e]||!window.gf_form_conditional_logic[e].logic[t])return"show";var n=window.gf_form_conditional_logic[e].logic[t],r=gf_get_field_action(e,n.section);return"hide"!=r&&(r=gf_get_field_action(e,n.field)),r}function gf_apply_field_rule(e,t,i,a){var n=gf_check_field_rule(e,t,i,a);gf_do_field_action(e,n,t,i,a);var r=window.gf_form_conditional_logic[e].logic[t];r.nextButton&&gf_do_next_button_action(e,n=gf_get_field_action(e,r.nextButton),t,i)}function gf_get_field_action(e,t){if(!t)return"show";for(var i=0,a=0;a<t.rules.length;a++){gf_is_match(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\css[1].css	
Category:	dropped
Size (bytes):	3832
Entropy (8bit):	5.218030373982794
Encrypted:	false
SSDEEP:	96:nOYgS0aKOYg6aUuOYg1aAuOYgEaXOYgXaoOYgxMa4OYgpaNOYgwhacOYgbalOOS9:b3pqAhn7OLNYEorhCsxcpvnLsNLBve
MD5:	5E5B11109E8FA7B0414F304CB3D4CE71
SHA1:	857CE2C460DFBEDAE8C9765B173B900BFF74C0F7
SHA-256:	CFD11DD81E0A46CA8F652BDC4531B78AD423BF4B031449F4659642785A3C4AC0
SHA-512:	FF9781196ADF997077BD0AF60C366B3C1A6ECA808C25E38A8DA269DCC7C4922ED0C7E117B3E49F4DC3439403B1C22D3C26373DB197F000BD442BB3850907B7 A
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Montserrat';. font-style: italic;. font-weight: 100;. font-display: swap;. src: url(https://fonts.gstatic.com/s/montserrat/v15/JTUOjIg1_i 6t8kCHKm459WxZqi7g.woff) format('woff');.}.@font-face {. font-family: 'Montserrat';. font-style: italic;. font-weight: 200;. font-display: swap;. src: url(https://fonts.gstati c.com/s/montserrat/v15/JTUPjIg1_i6t8kCHKm459WxZBg_D-A.woff) format('woff');.}.@font-face {. font-family: 'Montserrat';. font-style: italic;. font-weight: 300;. font-d isplay: swap;. src: url(https://fonts.gstatic.com/s/montserrat/v15/JTUPjIg1_i6t8kCHKm459WxZYgzD-A.woff) format('woff');.}.@font-face {. font-family: 'Montserrat';. font- style: italic;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/montserrat/v15/JTUQjIg1_i6t8kCHKm459WxhzQ.woff) format('woff');.}.@font-face {. font-family: 'Montserrat';. font-style: italic;. font-weight: 500;. font-display: swap;. src: url(https://fonts.gstatic.com/s/m

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\email-decode.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1239
Entropy (8bit):	5.068464054671174
Encrypted:	false
SSDEEP:	24:ch63Cf5W8QPIHRZ3hwVFS39bYGwNef1yTZsNUkQ1sZmSuLqNWRco5Jcn5IKM6cuY:C6SQnw/x+SR8ZZkQbp1RZ5JwiKMm7Zc
MD5:	9E8F56E8E1806253BA01A95CFC3D392C
SHA1:	A8AF90D7482E1E99D03DE6BF88FED2315C5DD728
SHA-256:	2595496FE48DF6FCF9B1BC57C29A744C121EB4DD11566466BC13D2E52E6BBCC8
SHA-512:	63F0F6F94FBABADC3F774CCAA6A401696E8A7651A074BC077D214F91DA080B36714FD799EB40FED64154972008E34FC733D6EE314AC675727B37B58FFBEBEBE E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/cdn-cgi/scripts/5c5dd728/cloudflare-static/email-decode.min.js

Preview:	!function(){"use strict";function e(e){try{if("undefined"==typeof console)return;"error"in console?console.error(e):console.log(e)}catch(e){}}function t(e){return d.inner
	HTML='',d.childNodes[0].getAttribute("href")||""}function r(e,t){var r=e.substr(t,2);return parseInt(r,16)}function n(n,c){for(var o="",a
	=r(n,c),i=c+2;i<n.length;i+=2){var l=r(n,i)^a;o+=String.fromCharCode(l)}try{o=decodeURIComponent(escape(o))}catch(u){e(u)}return t(o)}function c(t){for(var r=t.querySelec
	torAll("a"),c=0;c<r.length;c++)try{var o=r[c],a=o.href.indexOf(l);a>-1&&(o.href="mailto:"+n(o.href,a+l.length))}catch(i){e(i)}}function o(t){for(var r=t.querySelectorAll(
	u),c=0;c<r.length;c++)try{var o=r[c],a=o.parentNode,i=o.getAttribute(f);if(i){var l=n(i,0),d=document.createTextNode(l);a.replaceChild(d,o)}}catch(h){e(h)}}function a(t){
	for(var r=t.querySelectorAll("template"),n=0;n<r.length;n++)try{i(r[n].content)}catch(c){e(c)}}function i(t){try{c(t),o(t),a(t)}catch(r){e(r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\favicon[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 477x434, frames 3
Category:	downloaded
Size (bytes):	6937
Entropy (8bit):	7.730618378000938
Encrypted:	false
SSDEEP:	192:ccTQj3iyRR8gTnnJcsmIYsssssEYEEUecBZ3fX:ccc7HUOnnJUIYsssssbEE8B1X
MD5:	F24D54AF9AC9794089DF045A2F770102
SHA1:	578A67E0332D109FDB3D5BACC9E7CF4FB714483B
SHA-256:	D2246208B79E2F678CC0597BA07C43445C59A259B67CBECB7F30B5EF38AFECED
SHA-512:	24EFB904FF5B96FA7EE299D86C669F5EEAB95F5897CB4293D51A6F143FFE138A7E00846215490D13E7BC8C7243EBC5B4FEBA93C33BEBF26374C3132F6E7ADA0 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-content/uploads/favicon.jpg
Preview:	......JFIF.....".".+"+.F26262FjBNBBNBj^r]V]r^..vv.....".".+"+.F26262FjBNBBNBj^r]V]r^..vv....."..... .....Zlh...Z,....%GP.../2.....p@...g.v.....r.....N....G.O.....#W..\g@..9+`..>...DU.=.... b.....X... ....T....3.i..{...+q.X.....<.P..@.sS. .3.....q..^.....i..uO.....-.5..I.....T.G}. .W....k..f.....`.....,...y.....5L.....6.8....pP.....fbi.....8z.X.U.".5U...ON85..]`ea.....3..Vp.z..X....}...&.....@.7H8.....>..P..F..*.t.....i .....u.g....P.r..<....~:...K....V~..@g.v.j..#."j.^.....u..O.....r..[.Ij...@..eh...1a...r..<.6z4|.....p....W...p.-.....k.....CC....H...,...\.Y*....^r.....+$...c..... .H..fj^...i.d0.#hbr.U.....R.pWn .W.....%.8...8k....}..$.....l.....q.....3a....\B.].n.....3.y.....c.....>.&:2..<2.2.'m.. ..>..t.}d...*.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\freshwidget[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\freshwidget[1].css	
Category:	downloaded
Size (bytes):	6615
Entropy (8bit):	5.079113238180744
Encrypted:	false
SSDEEP:	192:1D9L5LgOagOqgOXPbYLOMLOyLOSRBWlmXG:1DkRBWs2
MD5:	1BB44301BAECCCB5D9219A27128D1682
SHA1:	1BA8CDACF93033358F00E0AB0F0D12199993B4BD
SHA-256:	E6F651226B57C89F7894CDB853DCDEA4B7036A445BC38861EF1B404CD3C0A8EE
SHA-512:	8B53ADCC85F87F089A716C5E4351F0BBADBD6043D44EB802C748A17A7439C11A9033EAF5AE0253B009FC780B4302D5B5C23166B034DE2A2C67117AAF77C6D12 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s3.amazonaws.com/assets.freshdesk.com/widget/freshwidget.css?ver=2
Preview:	.freshwidget-button a:hover,.freshwidget-theme{text-decoration:none}.widget-ovelay{filter:alpha(opacity=50);opacity:.5;background-color:#fff}.freshwidget-container,.widget-ovelay{position:fixed;left:0;top:0;width:100%;height:100%;z-index:90002}.fd-btn-left a{left:-2px}.fd-btn-left a:hover{left:0}.fd-btn-right{right:-2px}.fd-btn-right:hover{right:0} .ie8.fd-btn-right,.ie9.fd-btn-right{right:35px}.ie8.fd-btn-right:hover,.ie9.fd-btn-right:hover{right:33px}.fd-btn-top{top:-2px}.fd-btn-top:hover{top:0}.fd-btn-bottom{bottom:0}.fd-btn-bottom a{bottom:-2px}.fd-btn-bottom a:hover{bottom:0}.freshwidget-theme{text-shadow:rgba(0,0,0,.2),-1px,-1px,1px;padding:8px 16px;background-color:#015453;color:#fff;font-size:14px;font-weight:700;outline:0}.freshwidget-theme:hover{color:#f3f3f3}.freshwidget-customimage{overflow:visible}.fd-btn-right .freshwidget-customimage{right:0}.freshwidget-button{position:fixed;display:block!important;width:0;height:0;z-index:90000;margin:0;outline:0}.freshwidget-button a{p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\freshwidget[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):	9037
Entropy (8bit):	5.191428216939456
Encrypted:	false
SSDEEP:	96:n4GR00j0m9us7Xc7yq7pp3O6hf8+yumyds97CzlukfZU11ysr+Ut44SAImcrtsnH:nR0e0mns7ya4+y6M1y3Uthahpdl
MD5:	896B5B9298B5C168646778D81DD962FC
SHA1:	63A967F6430B5398DC4CFC686059F729177C07A0
SHA-256:	A126FC513B831F8460DC9733C023000D5A0EEE394D33787BAE7C9F7362D58A66
SHA-512:	0BD2916C854813945CA106AC537E821B872D2BFB9E5359A44D899DEECD551AE64A5D5D0145FF689EE6C1EE33F47A3E8B98F46361B41783776B221C727E81E54(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s3.amazonaws.com/assets.freshdesk.com/widget/freshwidget.js
Preview:	!function(){function e(e){try{return e()}catch(t){window.console&&window.console.log&&window.console.log.apply&&window.console.log("Freshdesk Error: ",t)}}function t(e){return e&&!L.test(e)?B.location.protocol+"//"+e:e}function i(e){var t=B.createElement("link");t.setAttribute("rel","stylesheet"),t.setAttribute("type","text/css"),t.setAttribute("href",e),"undefined"!=typeof t&&B.getElementsByTagName("head")[0].appendChild(t)}function o(e){var t=B.createElement("script");t.setAttribute("type","text/javascript"),t.setAttribute("src",e),"undefined"!=typeof t&&B.getElementsByTagName("head")[0].appendChild(t)}function n(e,t,i){e&&e.addEventListener?e.addEventListener(t,i,!1):e&&e.attachEvent&&e.attachEvent("on"+t,i)}function r(e){var i;for(i in e)C.hasOwnProperty(i)&&("url"===i||"assetUrl"===i?C[i]=t(e[i]):C[i]=e[i])}function a(e){var t=e.src,i=window.navigator&&window.navigator.appVersion.split("MSIE"),o=parseFloat(i[1]);return o>=5.5&&7>o&&B.body.filters&&(e.style.filter="progid:DXImageTr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\general-liability-and-bop-online-app[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	534395
Entropy (8bit):	5.103716191964961
Encrypted:	false
SSDEEP:	3072:9hVLYPwkO97BTW3qUK55nEQ5+RRRd+daMEfPiTwQ4iAquW3qUK55nKQs+aRRd+dw:9dUf7fOfU+ocwwEaff
MD5:	B246FB3EEE54E62A5A9B2DD5D7123FC8
SHA1:	C946317539B46AD1C60E9B3E6A9BAC7B2ABFA200
SHA-256:	79826C993441899250E529E86F6270BBB4D276B3F901DB4FDED0D74A5C1A2DCC
SHA-512:	55013CB2885FEDCDD88D6FF609417D92DDB4F7CA023E412E57BDF458F1CC0A4731C08F79AAD22F8AE9BFD6AE0FCCD525C488BE6DD05C0CC59657555F749A3 FD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/quotes/general-liability-and-bop-online-app/
Preview:	<!DOCTYPE html>.<html lang="en-US">.<head>..<meta charset="UTF-8" />.<meta http-equiv="X-UA-Compatible" content="IE=edge">..<link rel="pingback" href="https://yesbaker.com/xmlrpc.php" />...<script type="text/javascript">...document.documentElement.className = 'js';..</script>...<script>var et_site_url='https://yesbaker.com';var et_post_id='571';function et_core_page_resource_fallback(a,b){"undefined"===typeof b&&(b=a.sheet.cssRules&&0===a.sheet.cssRules.length);b&&(a.onerror=null,a.onload=null,a.href?a.href=et_site_url+"/?et_core_page_resource="+a.id+et_post_id:a.src&&(a.src=et_site_url+"/?et_core_page_resource="+a.id+et_post_id))}.</script>. Google Tag Manager for WordPress by gtm4wp.com -->.<script data-cfasync="false" data-pagespeed-no-defer>//<![CDATA[..var gtm4wp_datalayer_name = "dataLayer";..var dataLayer = dataLayer || [];.// .</script>. End Google Tag Manager for WordPress by gtm4wp.com -->.. This site is optimized with the Yoast SEO plugin v15.5 - https://yoast.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\gtm4wp-form-move-tracker[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	1487
Entropy (8bit):	4.869728653314726
Encrypted:	false
SSDEEP:	24:zmqiMKahpf6p5ExpXvvMLhWX2nxFvo7HfpAYu+p+eFiMKahpf6p5ExpXvvMLhWXX:xiLGx6H6NvOs2xVoDe+FiLGx6H6NvOsX
MD5:	B554A878CD1C765DECEDC9AABCB7B103
SHA1:	431C26AB8BF86E3497397B44FB2774A4CA1F79AA
SHA-256:	BC71C403DC6113C8597E111A99D6A6A197DD2F2355402F8392CA4812DCA57D3D
SHA-512:	5507CBEA615699C3AAEF288ED87A6DC9574C56006D35016FBF05E3238B3D0FA420B298B3E498DE31097E2277793626AAE816D7A50ED27CFE7424CE0A67C479C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-content/plugins/duracelltomi-google-tag-manager/js/gtm4wp-form-move-tracker.js?ver=1.11.6
Preview:	jQuery(function() {..jQuery(":input")....on("focus", function() {....var input = jQuery(this);....var inputID = input.attr("id") || "(no input ID)";....var inputName = input.attr("name") || "(no input name)";....var inputClass = input.attr("class") || "(no input class)";.....var form = jQuery(this.form);....var formID = form.attr("id") || "(no form ID)";....var formName = form.attr("name") || "(no form name)";....var formClass = form.attr("class") || "(no form class)";.....window[gtm4wp_datalayer_name].push({.. ...'event' : 'gtm4wp.formElementEnter',.....'inputID' : inputID,.....'inputName' : inputName,.....'inputClass': inputClass,.....'formID' : formID,.....'formName' : formName,.....'formClass': formClass....});...})..... on("blur", function() {....var input = jQuery(this);....var inputID = input.attr("id") || "(no input ID)";....var inputName = input.attr("name") || "(no input name)";....var inputClass = input.attr("class") || "(no input cla

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\html2canvas[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	36985
Entropy (8bit):	5.357082903661818
Encrypted:	false
SSDEEP:	768:INzP8E2ElaXh1tgdXUp66O9+VwXE3LeoXUfYpEWfOjLz7tMfv:yzNj2n4jtpaeoYqEWfULXtMfv
MD5:	5330312B84E884012C526A60437BA7F3
SHA1:	BB20CA86B627499DCA1BCC9E24D11996746C27E4
SHA-256:	737473B145A0FB2D97963BA71104B42EA59D434E17D43DE3DB67DDFFC24200AC
SHA-512:	B3F5CAE2F6155D319E512BF86D13CEBB148398395379D129304700424D2DFC531DF55E9FB7C897770481C55D1E0FAD1CEB0FED8E8B5294ABBD2760005B57244
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s3.amazonaws.com/assets.freshdesk.com/widget/html2canvas.js?ver=2
Preview:	/*. html2canvas 0.4.1 <http://html2canvas.hertzen.com>. Copyright (c) 2013 Niklas von Hertzen.. Released under MIT License.*/.(function(t,e,n){"use strict";function r(t,e,n){var r,a=t.runtimeStyle&&t.runtimeStyle[e],o=t.style;return!/^-?[0-9]+\.?[0-9]*(?:px)?$/i.test(n)&&/^-?\d/.test(n)&&(r=o.left,a&&(t.runtimeStyle.left=t.currentStyle.left),o.left="fontSize"===e?"1em":n||0,n=o.pixelLeft+"px",o.left=r,a&&(t.runtimeStyle.left=a)),/^(thin\|medium\|thick)$/i.test(n)?n:Math.round(parseFloat(n))+"px"}function a(t){return parseInt(t,10)}function o(t,e,a,o){if(t=(t||"").split(","),t=t[o||0]||t[0]||"auto",t=u.Util.trimText(t).split(" "),"backgroundSize"!==a||t[0]&&!t[0].match(/cover|contain|auto/)){if(t[0]=-1===t[0].indexOf("%")?r(e,a+"X",t[0]):t[0],t[1]===n){if("backgroundSize"===a)return t[1]="auto",t;t[1]=t[0]}t[1]=-1===t[1].indexOf("%")?r(e,a+"Y",t[1]):t[1]}else;return t}function i(t,e,n,r,a,o){var i,l,s,c,d=u.Util.getCSS(e,t,a);if(1===d.length&&(c=d[0],d=[],d[0]=c,d[1]=c),-1!==(""+d[0]).

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\idea-min[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 779 x 771, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	24465
Entropy (8bit):	7.915182359447715
Encrypted:	false
SSDEEP:	384:L8JLR30kP02/0FzeXMnvCkdv0vM8l0JiXONdqy02Zx3MKD8YKiWpqmuerjlH4J:LmLpvP071FnniXkLvZL/KieRjx4J
MD5:	9E574ACDC2902A95D78AF21827CF268F
SHA1:	B41FC21B31D1A964968F2D6E74C333CA6D82CEA6
SHA-256:	2656CB96C0FE01589B99C0927C2B67C1657FA3BEBBF5240660642FC16D3AE824
SHA-512:	34351C6CBAD474FF59E2382991D9EB268FB0ED3AA090A814452418E76DA7ED9B457309E2FF20C65B2A711E111BE2482A4F2E02A8B9362CD9502682029E7EE556
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-content/uploads/idea-min.png
Preview:	.PNG.....IHDR.....+y....KPLTEU..U..L..5cw8i.<q.Az.E..H..Q..r..Y....X..W.....Y....._.IDATx...b.:...93{...i.....I.....:g..^r.....,$.B!.H...B.B(.,.B.B(.,.B.B(.,.B.B(.,.B.B(.,.B.B(.,.B.B(.,.B.B(.,.B.B(.,.B.B(.,.B.B(.,.B.B(.,.B.B(.,.B.B(.,.B.B(.,.B.B(.,.B.B...P.....P.....P.....P.....P.....P.....P.....P.....P.....,..,..B..! @..B..H...`..(..3.K.,.....0....`../I.pT...6.....i...$.0....aVu.n.3(^.`...{..]k....q.4s..z7..D..,.5^...j.wU.../J.pH.Z\....I.`!X....`!X..B.B.....P.,...`!.,...`!X....B(X..B.B.....P.,...`!.,...`!X....B(X..B.B.....P.,...`!.,...`!X....B(X..B.B.....P..,...`!.,...`!X....B(X..B.B.....P..,...`!.,...`!X....B(X..B.B.....P..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\instant-quotes[1].htm	
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	49039
Entropy (8bit):	5.485529035363543
Encrypted:	false
SSDEEP:	768:KzxCP+EVM14sZ4Ox4FMPkPS2BB9APCcWLhvTvGh9glRKDBG3oe5N6/OgRL:KsP+EVM14syOxWZqQByq5vGh9g3KDBGw
MD5:	1E05364C821DB2A1E82A234DA2D71180
SHA1:	443127719A7FE3466F1727262FB23421C4019E90
SHA-256:	5601FD4D8DBD58A31235860DF8AD2172BE03F87EC8F48670E51CC4F8F94957DE
SHA-512:	EE118F054E7E42DD59B9111F54C90C2E69C846C258E141651251F79857F3A14EC244CF61C15ADAC05A3E781BA52F204ECC0E33206AF62719F8C879F579F35509
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/quotes/instant-quotes/
Preview:	<!DOCTYPE html>.<html lang="en-US">.<head>..<meta charset="UTF-8" />.<meta http-equiv="X-UA-Compatible" content="IE=edge">..<link rel="pingback" href="https://yesbaker.com/xmlrpc.php" />...<script type="text/javascript">...document.documentElement.className = 'js';..</script>...<script>var et_site_url='https://yesbaker.com';var et_post_id='206129';function et_core_page_resource_fallback(a,b){"undefined"===typeof b&&(b=a.sheet.cssRules&&0===a.sheet.cssRules.length);b&&(a.onerror=null,a.onload=null,a.href?a.href=et_site_url+"/?et_core_page_resource="+a.id+et_post_id:a.src&&(a.src=et_site_url+"/?et_core_page_resource="+a.id+et_post_id))}.</script>. Google Tag Manager for WordPress by gtm4wp.com -->.<script data-cfasync="false" data-pagespeed-no-defer>//<![CDATA[..var gtm4wp_datalayer_name = "dataLayer";..var dataLayer = dataLayer || [];.// .</script>. End Google Tag Manager for WordPress by gtm4wp.com -->.. This site is optimized with the Yoast SEO plugin v15.5 - https://yoa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\insurance-14-1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 400 x 300, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	6277
Entropy (8bit):	7.880813328936925
Encrypted:	false
SSDEEP:	96:v+g/48gv04/2i2ssxSKQrbT31kXiOiVxdXPdMFYtIrlqkgMb1LIXVADlX:Hn8r2tSKoT1NVLPtWXgGRX
MD5:	1EDF126923864B68714FFAC859591CBA
SHA1:	6C31EEE52B011BA52995482C2A329904DDD071A5
SHA-256:	19B0C01F18A344AE23D4BEF795F6A84931DF71A8E45AFFBDE17F548107203244
SHA-512:	18ED52157BDEAF8F0C9AC4108377665A4F4CD6391A9DA610C817F6B91A40833958AB530E8BA1B655040B32D6AE9847A946FB1E329F6D2681546AC0B2E5B4A4F8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-content/uploads/insurance-14-1.png
Preview:	.PNG.....IHDR.....,.....i.....PLTEwq....g.....f..K?iM?l[PrF<k[Qu.....bV{l`.[Ox;2_9-UA5bH:hYl.%..]..... .....{.....tRNSnj.....K....+3K.....ID ATx...z....`5...xc...`.$....X.....3_o.....l.....b.\.V.u5._..t....D.e(...HdF..|.yl.&....AaTT..D.9%F.2.@.....Ff2.....r.5.&`..QM....c-(FC".d.Z.....p$1.^.F.1.$...Hl...3[.....c.....Z.$l...s.]D,.r. .XN jT.....[;.az.zF...C...2_...: ..<.*.FY.r..D.r5../.i.....E.H.G....Q.cp+.<A..1../.....@..z....{.....T....X+..W.Q.cHm.....x.....i#.E<..F.A.....H../.1....2...0..x!.A.}.@...r. ...B.b.Y ..c.E.....5....P..x1...-.r=.X.....S.....M...h...m @w]...^+.v*Z.A.<L.MBK...{0.-. X..<-. ..Vp.....]..).eNE.;H...8*.0..#...R...Z..`.FV.\].4.7.UFZ..Y.8t.,T.Q.h....H9.....-@_....0.j. e.25w. ..-@Y..<T.Q.h..e...Y..d.....hq.)..piA.kNE..HY.4Z.M...E..d.fN...j.-....PQ.....;..... .zE..wtcL ..-@. ..K5... N...C.a..E..vt...N..x...Z....ZE..&.+.X.'..5..8.,... .}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\insurance-35-1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 482 x 398, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	5641
Entropy (8bit):	7.920514027892909
Encrypted:	false
SSDEEP:	96:Fx25Yd/aXxmTM6Iu1bJiFlY0udLNgxLiXOuSaAMXwJVdw2MRdwJBNfR/:FuYVaXx/6tb2O0GpgifPAMXknMRKdx
MD5:	C61330C505A0D3F72585B194D5DDBB38
SHA1:	0DA152B2CD7F75019E98CD5ED5D91298E46714F3
SHA-256:	EF3A4B3A26912A0818A5FBBAC311800F7EC56946BA8F4437B00F435EE3F4DFFF
SHA-512:	8F926B2EB6E11542DE29987043C3F90AB0E91B898F74C5ABBD7DED0915ECBA1316A4038BEA1B2BED481038C804D53F2BB95F3ED5589867EFC2FD629F32BCCA 5B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-content/uploads/insurance-35-1.png
Preview:	.PNG.....IHDR.....|.....PLTE.....?e.H....._....h..eeU.....tRNS)33333333..*.....IDATx....z...`D.....{....X-...f.M.G.f.....G.....scbnE..xzb..f..yjb....8.K.?C)..IY..... R).).M.wk..#.RJ...E....8...N'.27E...R...2c.t..E../.....:g...%>+.....uR.....$^.4.....Z...s.42t....1..E.....O.d.Whd..b.e.8U_Y..r...=.....{..7C..%u...uA..{...K.H.X4..@..G_C,..@.. n..\|..V9.....)[...7..*.b/H..q.c/1..!#a..\|.....w...D..X..c./...pm...W...d11..[..&.....1..x.....3.h..A.#._).6.....8.E....b,.#\|....&...d.....c.....+.0..Bh..R.....?lq.G*....k<.1....T..<~-.. X..+..Y$A.S..a.=...7..%.$...2Md,..i..8.YA..D.7...L..''~l.y....<.....}...[R.U..h=0.9'....&[_7..i.../....k{....V.....p.[u.....l./P"n0....#M..p..D.w7..Xe.ge...'og.L...-..1.WhI....e.e...j.@ .q_.8&\(.:k.H.YD<W..Y.B!...H.,"{....&a....]5i.0..d,J...1s g...(>'.B!la.....d..'A.....\..(.!.]"N.!.\|....(...#_..''.E..k..]C..l-J...(k7...\|2...O.t.06.s...o.d....?.$`.x|z....o..r.'.....B..K...

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\loading[1].htm	
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	19941
Entropy (8bit):	5.975122494815057
Encrypted:	false
SSDEEP:	384:B+ILbGKLkhwEi+ILbGKLkhwEi+ILbGKLkhwEu:B+ILbGVwJ+ILbGVwJ+ILbGVwf
MD5:	65D8D77D4846043A07E35E1DC473CD64
SHA1:	BCE670786D249633530662B61FBC7AC4B30FE985
SHA-256:	FB30F1D03A700B4AB9ADF2AB049BBF1D2FC9B318CB32291DD2AC69D86322568B
SHA-512:	325DB2DEC0DFCBBDAAED3F460F0F2608D4567D184628BAED537C83ECE1CA285747D1C50F1900B0F8981F67EC3FFAD8ED86246E7513DA82F564B6BB6BF8E58 A3
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">.<html xmlns="http://www.w3.o rg/1999/xhtml">..<head>. <meta http-equiv="content-type" content="text/html; charset=utf-8" />. <meta http-equiv="cache-control" content="max-age=0" />. <meta ht tp-equiv="cache-control" content="no-cache" />. <meta http-equiv="expires" content="0" />. <meta http-equiv="expires" content="Tue, 01 Jan 1980 1:00:00 GMT" />. <meta http-equiv="pragma" content="no-cache" />. <meta http-equiv="robots" content="noindex, noarchive">. <title>Freshwidget Loading...</title>.</head>..<body>. <style>. body {. background: transparent;. margin: 0;. overflow: hidden;. }. . .ct {. margin-left: 20px;. margin-right: 20px;. -webkit-box- shadow: 0 5px 10px rgba(0, 0, 0, 0.4), white 0 0 1px inset;. -moz-box-shadow: 0 5px 10px rgba(0, 0, 0, 0.4), white 0 0 1px inset;. bo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\logo-b-social-mediasmall-400x250[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 400 x 250, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	35083
Entropy (8bit):	**7.992029341183243**
Encrypted:	**true**
SSDEEP:	768:QsJDlK8Xbp/SS5UXBqx4nyyqkmMIWIp0X5vP694l4DXxvGP:Qqogl5iXB48TTIpk6940+
MD5:	EFD69BAFEF29A202709A24794C37A149
SHA1:	C19132ACD12E11D2FA60C9CCC9AA230BA753FC9E
SHA-256:	A4A4FC6CB5CA3B91CEB389FA0331F964163F082C2E53B9E1A4904A6316581BD5
SHA-512:	6528485D6398F0E14394B138B25168D1A01D13DEDAACCB8B940B83992BC520AC0DFBEDDC0D4C6063060756604F7087877E4E53CF3DB88ABBA330469D45FB441
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-content/uploads/logo-b-social-mediasmall-400x250.png
Preview:	.PNG.....IHDR.....y.v....PLTE.....}.....mn.g..6..J..'.....{.@Y.[\.lJ.@A.89.32.23.01.11.01.-1.-1./0./1./2./0 ..1..2../2./1./2./1.-0..1..0./1.01..1..2.,..-2.-1.-0..Ie.....IDATx..}.o...b....83A..x.MR@...%k.,....;....MR.....Qb[.n....S.4L..4F.xU...r...o...}..w.q.}..4.....jo0M...'6..n...{{....o.. ...v.O&K\&.....7..z.U.....p.N...g...x.|~^n....n.4.?.4..Am..Q<.....W..Y.0:.e....F....b..t.@o...".....b..7.rq?6.....e...O..(wm...Do).n6.....9_....{.N.Ln4.C(. :.....\.#.[..c[,..... .22.c...Az-.q.....#L...+...3/c.....Eo../.qq{.<..qp.s.....U....."/4....h1.n.....7.....S..O.*0.#.ej.T`&o..t.....q..].<l.....y.e...x....o.....O...v=:.....~.g...D.?.....^}.....o.....2..W..rv.. ..a..7*..G.....G..15.....om...i.....Y..68dtY.../....v<|Z>...{f.Y>....1..]x.T...x5.=.R./....]F2..}x.....e.oF...G..'.....~F_.C../[^.;Pr.r.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\mediaelement-migrate.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):	1193
Entropy (8bit):	5.031478294068194
Encrypted:	false
SSDEEP:	24:f4YRVssO7j2l2t3Sr+EqXGD3Djqds+1DPDLNDORZGbMDbhLM9yAf6CKyDn:Q6VssKKLt38qXqz0LblOLGbwbhM9yo6u
MD5:	52BEC302D465DD23422D9986AF7BFA3A
SHA1:	931D9C73364F045FB548938888B1C237313C2259
SHA-256:	B37A604B4ADD99725C3A9E6B0440FC4452F71139517E7D7DEB452ED98499068C
SHA-512:	F5A26323D377835CFBCA3CFDFEB398E017C2B20BD16398C69B235D29E46D8EE22E5F66107CDFEFF0C6C3F99A2364D0727A183A7E69EEF5BA376C3ED8EE796E 8F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-includes/js/mediaelement/mediaelement-migrate.min.js?ver=5.6
Preview:	!function(e,a){void 0===mejs.plugins&&(mejs.plugins={},mejs.plugins.silverlight=[],mejs.plugins.silverlight.push({types:[]})),mejs.HtmlMediaElementShim=mejs.Htm lMediaElementShim||{getTypeFromFile:mejs.Utils.getTypeFromFile},void 0===mejs.MediaFeatures&&(mejs.MediaFeatures=mejs.Features),void 0===mejs.Utility&& (mejs.Utility=mejs.Utils);var t=MediaElementPlayer.prototype.init;MediaElementPlayer.prototype.init=function(){this.options.classPrefix="mejs-",this.$media=this.$node=a(this.node),t.call(this)};var i=MediaElementPlayer.prototype._meReady;MediaElementPlayer.prototype._meReady=function(){this.container=a(this.container),this.cont rols=a(this.controls),this.layers=a(this.layers),i.apply(this,arguments)},MediaElementPlayer.prototype.getElement=function(e){return void 0!==a&&e instanceof a?e[0]:e},Me diaElementPlayer.prototype.buildfeatures=function(e,t,i,s){for(var r=["playpause","current","progress","duration","tracks","volume","fullscreen"],l=0,n=this.options.featu res.length;l<n;l++){

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\mem5YaGs126MiZpBA-UN8rsOXOhv[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\mem5YaGs126MiZpBA-UN8rsOXOhv[1].woff	
File Type:	Web Open Font Format, TrueType, length 25684, version 1.1
Category:	downloaded
Size (bytes):	25684
Entropy (8bit):	7.980108489133185
Encrypted:	false
SSDEEP:	384:sO53pt1aIuhEXTlbQYC2ZclfmLS7wNO0NgIP05zXSruDtfN9lEJcr472p9jm:75JaIiITpQYCnmtN5gP0FXSrM11tJm
MD5:	E0D4CCF8057DAA4F5A58E1FBD8038A80
SHA1:	ED15E37A95E9C380F74A4612F2FB5B5CF0F0B429
SHA-256:	6F4CD7829E0AB8267DAC9E610DB42E685C39674C45FBE7146CA107CAC41B80EC
SHA-512:	3E86D18B76B6609E132C0B3C14083CF7DF05C5848D888E852C99DEF5791CB66DF4AE22EEB4118AF4C67E24B8BC38CCA44C45DA99C5396E2780B840C6F314AE8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UN8rsOXOhv.woff
Preview:	wOFF.....dT.....GDEF.....6...:.z..GPOS.....GSUB.....$5"OS/2...X...^...`.."vcmap.....6.....cvt .....g.....o.[fpgm...X.....s.ugasp.....#glyf.....M...~f...1head..V....6...6....hhea..V.... ...$....hmtx..W....6...`.*tbloca..ZL.....2..yAmaxp..]d... ... .I..name..].....%.@cpost..^x.....y. .prep..cD.....1..Sx.c`d``.a..&.v..F..FFWFW ....$=...d.c%..fl.....]r.2.....x.U....P.E.}.....5.\A.kX..k..\.....v.c.1.p...X8../....n.C...\.%...Z..u...\.p.}.1\...z.#.....)..KB8.~.9...]]...Rg.~.1xT.jH.....3.....x.c`f.cV``e``..j...(.../2.11s01qs.1s.01.,``.g``..b.. 0t.vfp`P...M...C.G/S....|..K..6 .....x....]Q...o.....6..qm...~.....g..3..s. J..*.4o...>(.....|.76g;N.Ln....uFQM=..<6o.O.....m.M.#...T..bE..4...M..29-..r.j..5.....a...3....s.ge..y-sH1.....&.c.r.jR[....k.p*s.Tx. .h@_.>...Z.==....n.^.....k.....`.....^...us\/..us]]...rM]}/.{.=.....R..Q.(.7.%.....Bx..<.0.F8. .G..Y.u...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\memnYaGs126MiZpBA-UFUKWyV9hIIqU[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23520, version 1.1
Category:	downloaded
Size (bytes):	23520
Entropy (8bit):	7.975386943527894
Encrypted:	false
SSDEEP:	384:ZbQHZqpWCN460nc8SfOQNQEE5qkiEruS3ksB4sgqVF6/DpJPykba77vKlN80a6u:ZbT47cbfOQNQEEtiErdDSsJVS7C7TYzu
MD5:	30D2A28FBFCC4726F2C2DB9AAC45C702
SHA1:	E83E79783D8803444A215F78FE603D2A2CDF8972
SHA-256:	C8E3A41B0708CB6DFAB03178BEDEDCF12EDA48B48A9CF8CE682D9E5E9091C905
SHA-512:	37039AEF085D1B8A92FDD9BB0B7BA41E01FE8232A9747A8011E701E243C79D3E830BDEFB0BB9A6AAD7249B0F25835235199B46DFE5A12FE7E54867E8EBC882FD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKWyV9hIIqU.woff
Preview:	wOFF.....[.....GDEF.....6...:.z..GPOS.....GSUB.....$5"OS/2...X...]...`~...cmap.....6.....cvt .....^.....M..fpgm...P.....~a..gasp.....#glyf.....EJ..m....head..NH...6...6./{.hhea..N....#...$....hmtx..N....>...`P.}.loca..Q.....2H.+umaxp..T.... ... .H..name..U.....*.D9post..V.....y. .prep..Z.....$...Jx.c`d``.a..&.v..F..FFWFW ....$=...d.c%..fl.....]r.2.....x.U....P.E.}.....5.\A.kX..k..\.....v.c.1.p...X8../....n.C...\.%...Z..u...\.p.}.1\....z.#.....)..KB8.~.9...]]...Rg.~.1xT.jH.....3.....x.%..@P.@....O$Z._*$"...SjL`...4La..A.4...+0..jp.^.B,.h..E..%0.9@.....Q...,*S.....x....]Q...o.....6..qm...~.....g..3..s. J..*.4o...>(.....|.76g;N.Ln....uFQM=..<6o.O.....m.M.#...T..bE..4...M..29-..r.j..5.....a...3....s.ge..y-sH1.....&.c.r.jR[....k.p*s.Tx. .h@_.>...Z.==....n.^.....k.....`.....^...us\/..us]]...rM]}/.{.=.....R..Q.(.7.%.....Bx..<.0.F8. .G..Y.u...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\pixel[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	2.7374910194847146
Encrypted:	false
SSDEEP:	3:CU9yltxlHh/:m/
MD5:	DF3E567D6F16D040326C7A0EA29A4F41
SHA1:	EA7DF583983133B62712B5E73BFFBCD45CC53736
SHA-256:	548F2D6F4D0D820C6C5FFBEFFCBD7F0E73193E2932EEFE542ACCC84762DEEC87
SHA-512:	B2CA25A3311DC42942E046EB1A27038B71D689925B7D6B3EBB4D7CD2C7B9A0C7DE3D10175790AC060DC3F8ACF3C1708C336626BE06879097F4D0ECAA7F56701
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://q.quora.com/_/ad/931b253b90044bdd807d8902b5bfe759/pixel?j=1&u=https%3A%2F%2Fyesbaker.com%2Fapplications%2F&tag=ViewContent&ts=1610622584394
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\pixel[2].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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\pixel[2].gif	
Entropy (8bit):	2.7374910194847146
Encrypted:	false
SSDEEP:	3:CU9yltxlHh/:m/
MD5:	DF3E567D6F16D040326C7A0EA29A4F41
SHA1:	EA7DF583983133B62712B5E73BFFBCD45CC53736
SHA-256:	548F2D6F4D0D820C6C5FFBEFFCBD7F0E73193E2932EEFE542ACCC84762DEEC87
SHA-512:	B2CA25A3311DC42942E046EB1A27038B71D689925B7D6B3EBB4D7CD2C7B9A0C7DE3D10175790AC060DC3F8ACF3C1708C336626BE06879097F4D0ECAA7F5670 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://q.quora.com/_/ad/931b253b90044bdd807d8902b5bfe759/pixel?j=1&u=https%3A%2F%2Fyesbaker.com%2Ftypes-of-insurance%2Fpersonal-lines%2F&tag=ViewContent&ts=1610622633259
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\pixel[3].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	2.7374910194847146
Encrypted:	false
SSDEEP:	3:CU9yltxlHh/:m/
MD5:	DF3E567D6F16D040326C7A0EA29A4F41
SHA1:	EA7DF583983133B62712B5E73BFFBCD45CC53736
SHA-256:	548F2D6F4D0D820C6C5FFBEFFCBD7F0E73193E2932EEFE542ACCC84762DEEC87
SHA-512:	B2CA25A3311DC42942E046EB1A27038B71D689925B7D6B3EBB4D7CD2C7B9A0C7DE3D10175790AC060DC3F8ACF3C1708C336626BE06879097F4D0ECAA7F5670 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://q.quora.com/_/ad/931b253b90044bdd807d8902b5bfe759/pixel?j=1&u=https%3A%2F%2Fyesbaker.com%2Flatest-updates%2F&tag=ViewContent&ts=1610622639375
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\pixel[4].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	2.7374910194847146
Encrypted:	false
SSDEEP:	3:CU9yltxlHh/:m/
MD5:	DF3E567D6F16D040326C7A0EA29A4F41
SHA1:	EA7DF583983133B62712B5E73BFFBCD45CC53736
SHA-256:	548F2D6F4D0D820C6C5FFBEFFCBD7F0E73193E2932EEFE542ACCC84762DEEC87
SHA-512:	B2CA25A3311DC42942E046EB1A27038B71D689925B7D6B3EBB4D7CD2C7B9A0C7DE3D10175790AC060DC3F8ACF3C1708C336626BE06879097F4D0ECAA7F5670 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://q.quora.com/_/ad/931b253b90044bdd807d8902b5bfe759/pixel?j=1&u=https%3A%2F%2Fyesbaker.com%2Fapplications%2F&tag=ViewContent&ts=1610622643707
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\professional-liability-quote-request[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	525986
Entropy (8bit):	5.092719966027382
Encrypted:	false
SSDEEP:	3072:HqVLYPwkO9fBaW3qUK55nEQ5+RRRd+daMEfPiTwQ4iAquW3qUK55nKQs+aRRd+d4:HM7f7fOfU+Q+
MD5:	6471834F6BC5A04C77A760C2C809CA18
SHA1:	D3C39E213DABE852FBFCBDF99B85C46421534174
SHA-256:	3EBC6EED99E2259CA1DC7D9787EB70F985B7F5DDECD8F07E2A4740693419AA28

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\professional-liability-quote-request[1].htm	
SHA-512:	CE26E4F0D72B0E33A3230C926254EAFB5215A1B8496AD4298F89B16CC0555A6FF3A1DB4CBABC741C36D960D85686DA73F369A14B6F8B6ABC866413C9BD47A23
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/quotes/professional-liability-quote-request/
Preview:	<!DOCTYPE html>.<html lang="en-US">.<head>..<meta charset="UTF-8" />.<meta http-equiv="X-UA-Compatible" content="IE=edge">..<link rel="pingback" href="https://yesbaker.com/xmlrpc.php" />...<script type="text/javascript">...document.documentElement.className = 'js';..</script>...<script>var et_site_url='https://yesbaker.com';var et_post_id='92';function et_core_page_resource_fallback(a,b){"undefined"===typeof b&&(b=a.sheet.cssRules&&0===a.sheet.cssRules.length);b&&(a.onerror=null,a.onload=null,a.href?a.href=et_site_url+"/?et_core_page_resource="+a.id+et_post_id:a.src&&(a.src=et_site_url+"/?et_core_page_resource="+a.id+et_post_id))}.</script>. Google Tag Manager for WordPress by gtm4wp.com -->.<script data-cfasync="false" data-pagespeed-no-defer>//<![CDATA[..var gtm4wp_datalayer_name = "dataLayer";..var dataLayer = dataLayer || [];..// .</script>. End Google Tag Manager for WordPress by gtm4wp.com -->.. This site is optimized with the Yoast SEO plugin v15.5 - https://yoast.c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\quote-online-400x300[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 400x300, frames 3
Category:	downloaded
Size (bytes):	19013
Entropy (8bit):	7.95892919766676
Encrypted:	false
SSDEEP:	384:ya0a5YqXKbvuqOzqGOxUnJ2Q8WHg19b2Hb6s/lQClV/BpfByUmo:l0a5YqyvuqOzqGOwGX9b2H5/1lVfJyU/
MD5:	AFB4429C38D712C71AB07422446C60FF
SHA1:	C1DF4E0477D812A453047CEC08138870E5CB7E57
SHA-256:	8834D6DCC85284E53F9EDAF543779434777C8822A622A0DF593B28C49DFC1705
SHA-512:	0654900103895C3FF6BE693320BC48EE8E36C087E7EEB394C2DD777A27A64E1B2CC79A3117C100108B8C6A0F63974ED4BB4946C778C6211537B459E452CFE7E9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-content/uploads/quote-online-400x300.jpg
Preview:	.....JFIF.....Vf.....j.....[.....ff.....i.V.J.U..vf.<.S.P.....v.....Y...W5.JY.....J"-.Tv.;.Y..{...5/(..g. ..m.Y..M...T...U..8.S..f.....p...m....Je(..T...Vv|.3..|.`.....l/.|...PzV...q.....XvS.....e.@..#...e..Z"%.\j.....y..=....=....K..u."*.-.;..oD+"f.cX....mw4....3.,..DD..w...v%.....E..^..n....DK.{...w.%/v.`l....l/.....z.-."....q.."..q.....*iQ.9.g%Kh.....-...J16@.....2)..l.k....D.....G.....Yf^4. ..e2....^./....0DJ;.{..d.y..&.).....e}F...[.X...w`....=..G.....C.....f.;in....o.\.>....bY(..P.....|.r.....H....q.P.D..ow.-.....x. .....m-.....4.&V...d.+.....%.....gv+im.\.s...;.}3.....,..~p.....n....A.Z.....r.....#..a..s.O.18l.6...{&.Ti.+.Kc..N....#.....c,..?...C.....=I...'...vV.s.x....b.cv.'..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\readyclass.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	30175
Entropy (8bit):	4.888704624837673
Encrypted:	false
SSDEEP:	768:V3P5jAUUQEkkAYqSCosSCtrqFBVuKBGIl0O8kjtybVjXRSqGkj+8EplpS9eleSqy:g
MD5:	686C924878C7544F5A9D68E9A6FE7E12
SHA1:	CB8BF815000BCD344BE8B83E26899B5CBB23C108
SHA-256:	B36C610ADF667F8F1F228E6D2390947A81257CDAE72B98C1C07CBE50F9FF06D3
SHA-512:	FB22FF81B42C00C0CD403824A223184FC838AE46C683D7908C7B24ACBBF1935148BB0813A158A2EE436261DD5B7CFFD4A0B46F35F9159DE4EFA42E9D68502C06
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-content/plugins/gravityforms/css/readyclass.min.css?ver=2.4.15.1
Preview:	@media only screen and (min-width:641px){.gform_wrapper .top_label li.gfield.gf_inline{vertical-align:top;width:auto!important;margin:0;padding-right:16px;float:none!important;display:-moz-inline-stack;display:inline-block}.gform_wrapper .top_label li.gfield.gf_inline input[type=email].large,.gform_wrapper .top_label li.gfield.gf_inline input[type=email].medium,.gform_wrapper .top_label li.gfield.gf_inline input[type=email].small,.gform_wrapper .top_label li.gfield.gf_inline input[type=number].large,.gform_wrapper .top_label li.gfield.gf_inline input[type=number].medium,.gform_wrapper .top_label li.gfield.gf_inline input[type=number].small,.gform_wrapper .top_label li.gfield.gf_inline input[type=password].large,.gform_wrapper .top_label li.gfield.gf_inline input[type=password].medium,.gform_wrapper .top_label li.gfield.gf_inline input[type=password].small,.gform_wrapper .top_label li.gfield.gf_inline input[type=tel].large,.gform_wrapper .top_label li.gfield.gf_inline input[type=tel].me

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\style.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	51433
Entropy (8bit):	4.950848998116943
Encrypted:	false
SSDEEP:	384:FLBjc7HBZDO/KRUb4XMXib+d+AwlVHI+vg7Y3K0dXtNXTXlx:d8XMXib+d+AwlxI+vg7uJ/TVx
MD5:	27F5295CCF3AD9E0E85DCAC543630288
SHA1:	19810723999BADC836ECA3DEE977B4DE1BBCA8ED

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\style.min[1].css	
SHA-256:	5C2288CA7B324881FAAE5E368EB4D69457E2784E042E868DE335D3827BB90981
SHA-512:	FFA38A60E417B21083ED1A26301E0CE8AF712939D31FE1FC1CB3931844D9B0CAC8F998C6437FCEDADEA2A86A66BA286025A5FE1D9A411B057D12A357C68AA2B3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-includes/css/dist/block-library/style.min.css?ver=5.6
Preview:	:root{--wp-admin-theme-color:#007cba;--wp-admin-theme-color-darker-10:#006ba1;--wp-admin-theme-color-darker-20:#005a87}#start-resizable-editor-section{display:none}.wp-block-audio figcaption{margin-top:.5em;margin-bottom:1em}.wp-block-audio audio{width:100%;min-width:300px}.wp-block-button__link{color:#fff;background-color:#32373c;border:none;border-radius:1.55em;box-shadow:none;cursor:pointer;display:inline-block;font-size:1.125em;padding:.667em 1.333em;text-align:center;text-decoration:none;overflow-wrap:break-word}.wp-block-button__link:active,.wp-block-button__link:focus,.wp-block-button__link:hover,.wp-block-button__link:visited{color:#fff}.wp-block-button__link.aligncenter{text-align:center}.wp-block-button__link.alignright{text-align:right}.wp-block-button.is-style-squared,.wp-block-button__link.wp-block-button.is-style-squared{border-radius:0}.wp-block-button.no-border-radius,.wp-block-button__link.no-border-radius{border-radius:0!important}.is-style-outline>.wp-block-button__l

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\JTURjIg1_i6t8kCHKm45_ZpC7g0[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 67360, version 1.1
Category:	downloaded
Size (bytes):	67360
Entropy (8bit):	**7.991256054146273**
Encrypted:	**true**
SSDEEP:	1536:qBiuVt1A78krsF8ljNRptLBgrHKqZPpFEz9ZRcb3l2fJSU:1+168koCBjptL+rvZRuzRcb30
MD5:	E8B54199FBD144A34EFD02C31DFD0E66
SHA1:	CE483630F953303A4783D7CC9A1563E3015E912C
SHA-256:	58CA60FA247DD7D7CEE0103DCA4B6DFD6D676C03070F861F032BB309F00A6CFD
SHA-512:	252225BCE684E29A97720F2061390BEA22DB7245B7954F0666465617330039832247F5E36EA7E8849BB4DCF0098CFD407C2136898D2CD82E761C55AE258DCA80
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTURjIg1_i6t8kCHKm45_ZpC7g0.woff
Preview:	wOFF..... .....-L.....GDEF.....2....X.|GPOS.....>J....A[..GSUB..A.....OOS/2..F....Q...`V..Ncmap..FX.....3cvt ..Nl...b....0...fpgm..N....F...mM$.\|gasp..U .....glyf..U .....%.B...head.....6...6.P.xhhea..... ...$....hmtx.....W..loca.....i....f.Smaxp..... ... ...Wname...(.....*.EIpost.....L..(....prep...d.....K..x.....XQ... s_m.6..v\.V..V..m.E\.\.....Yi..U.....I+q...Sv...=|`...}./...Y..y.s..5..w.....R\.'._....._..xL.dLS.s.SI,.2XN.*beU.j.....6Q.I...J.z`o.....5.'j"N.d..i8K.p...Rm.....wj'.....xP....Q..:.t.....]....P...s.....'....U2f(.s.o..P.7...2|...Eu,D..I.LV....-$cj.`/+d.G..4...F.S...x..V.p+G.}R.....e.G..g..133....133.....Oeg#.:.^mm.....pO.....o..`.x...x...w.+..y.$...(.0..Zh.X...2...6v.{'....cxI....z..c.d.h...!..[.6.....q..<.3B.haue.....V.1.....-.....I..H....x..B.....y~.../.....L.5._.]....Z..>.....z..;n.`....QW...D..$j.X..D.u.....d}.....3.Y.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\JTURjIg1_i6t8kCHKm45_bZF7g0[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 67256, version 1.1
Category:	downloaded
Size (bytes):	67256
Entropy (8bit):	**7.993061921886421**
Encrypted:	**true**
SSDEEP:	1536:NqJo5xJ07m3VzrGTKroF8W0kkeg3Q7i8ZtqY+qkfjm6+E/TU+m9T37SU:NquJuWUCWkhQxeY+zC6+ErUfV3f
MD5:	3117C2D16F1E8CD7221D7C425A9B8C8E
SHA1:	A3609D878A602F65CAEDF4917DFB6B877450CA48
SHA-256:	E6EEF844F108468F293ACF079590DD050C8AC756C05463E3BE98CB0D8BF853B0
SHA-512:	C3ED06997E0B9A01A06B126FDD63AE9AB212E20E67AB2AA23F66E7DB21AA3AFEBC9BD437D317ACAFBA654BFF7810B3DA120AA265AD080583B473DFD7BD985A3C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTURjIg1_i6t8kCHKm45_bZF7g0.woff
Preview:	wOFF...../.....GDEF.....2....X.|GPOS.....=.....Y.GSUB..?.....OOS/2..D....N...`Vr.Zcmap..E.....3cvt ..M ...d....2...fpgm..M....F...mM$.\|gasp..S .....glyf..S....s..(.Av.2head...H...6...6.Z..hhea..... ...$...)hmtx.....K.}loca...,...q....q..Hmaxp..... ... ...Wname.....+.FOpost.....L..(....prep.....K..x.....XQ.. .s_m.6..v\.V..V..m.E\.\.....Yi..U.....I+q...Sv...=|`...}./...Y..y.s..5..w.....R\.'._....._..xL.dLS.s.SI,.2XN.*beU.j.....6Q.I...J.z`o.....5.'j"N.d..i8K.p...Rm.....wj'.....xP....Q..:.t.....]...P...s.....'....U2f(.s.o..P.7...2|...Eu,D..I.LV....-$cj.`/+d.G..4...F.S...x..V..I;.=3=.;.s..au..m.m..m.*}...m..S..?uj.V.....$.3.....:.ko.%.=.:...;w;..K"..s0._....{.4.(..c....._w.vp .V.Qwtu`}..h...<...=...hL.....y.e.\._q1..eP.....3iU.....I.~...7 .../...7.....=7.MC.}..t....I..Q[. ...X..'...m$n.=.7z.2...X.@3".....W..h.O.....D.~...8 kiX..W..z....UtY...v. ..kv...I.UO

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\JTUSjIg1_i6t8kCHKm45xW0[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 67496, version 1.1
Category:	downloaded
Size (bytes):	67496
Entropy (8bit):	**7.993595810257416**
Encrypted:	**true**
SSDEEP:	1536:OG0h7CMbXrJF8cKJjIl5QmNZ/dTt/OvUoSLvwkFlJiSU:OBTbXdCrjwnVtKiXJw
MD5:	7BF99C007ACD1BAA1F21903B6FDA4D65

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\JTUSjIg1_i6t8kCHKm45xW0[1].woff	
SHA1:	C7B424219F0681A8DD969CF5142DC1D49A96CEC9
SHA-256:	C04F4153C1FCA18DFC983F5998F324498A7F36FAB4FD072EC5B956F66D254F61
SHA-512:	4E1F30ECA483CD85D55C79A5711CDB665F6AFE88F008843E82F9450B2384C49E76B389FC56547E522A1082DF29FEA82FC40EF396186F0AFC7D61309AA52CAEF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTUSjIg1_i6t8kCHKm45xW0.woff
Preview:	wOFF.....4p.....GDEF.....2....X.|GPOS.....><....}.NLGSUB..@.....OOS/2..E....P...`U..Bcmap..FD.....3cvt ..NX...\..../R.Hfpgm..N....F...mM$.\|gasp..T .....glyf..U.....-"...head...4...6...6.F.nhhea...l... ...$....hmtx.....!.loca.....r.....maxp..... ... ...Yname.....-5H.post.....L..(....prep.....K..x.....XQ...s_m.6..v\.V. .V..m.E\.\.....Yi..U.....l+q...Sv...=|`...}./...Y..y.s..5..w.....R\.'._....._..xL.dLS.s.SI,.2XN.*beU.j.....6Q.l...J.z`o.....5.'j"N.d..i8K.p...Rm....wj'....xP....Q..:..t.....]....P...s.....'....U2 f(.s.o..P.7...2|...Eu,D..l.LV....-$cj.`/+d.G..4...F.S...x....$K....h.....c.l..7X.u..m<c.6..X...b...:.k..y2+32'"*2...I..8..`.....y.S.0k.UO_.T..c..^ZWb.(..j....8.<....9.k..p>'.G .* O&.F.:.R...? ~...}.;&..... .Y.>.T.o...-....^.s.?.H.....n.@..|...w.....x.....O....1.U...:.....Nv..@x.....$...R ..x`..N.o...n~7.@.u.....m.Y..F`xT.I.....W6...%q..../..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\business-02[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1024x722, frames 3
Category:	downloaded
Size (bytes):	59793
Entropy (8bit):	7.978394546629885
Encrypted:	false
SSDEEP:	1536:N3+ZoiwcthM/oF4xzIEvEOJgpKqi23FBf:N3+ZoiRt2QF4xzDEOJggqim
MD5:	8D85B71F48EEF203DB5D83AD0D4720F6
SHA1:	C6BEBC1A2D45BA60E72342ECF89D34589E48EEC8
SHA-256:	E80DA5EB607C46FD96984A0E6E958992FAD6D19AB0077A4251E568096ED24592
SHA-512:	B04B7E519A985B3FD36276E8CF73F4220C9791FB75A584906689722BEA03777866AFE17D45B6BA3026D0F1D23B99D5A0356E520F3198982F81FE03202CCC6DFD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-content/uploads/business-02.jpg
Preview:	......JFIF.....'.....'<%+%%+%<5@404@5_JBBJ_m\W\m.vv.....'.....'<%+%%+%<5@404@5_JBBJ_m\W\m.vv....."..... .....Z..w#h._e[.(._L..uo.[....v:....|...k....[.l4..+a...$...Q....."b[.3=..&+.)...]."..U.vf.mKy6]WY.,.-.R.....lA.+4.ek%].2.6. ....X....3..,...[#.$K...D.2S....YE...\.y..T..f.D....^....y... [A.JS`k.E;.S...Q2z9.6 ...5..g..c.JFed...(.>.....f.....q..f.iu..n..d.k.....8.....t..S..+5)....'.6...C...DL.....;..i.....~v...z...^.lS.Y.e..m..._J....i.....W...x*.%.E..K.9Id.r...8.Y.X.'...W.....~.F.].....nT.....".u.K=G.QN.2...a..n..v#.....04.A,:.K.xd.....!.Q.=..3.....N.kEcy[AV.....K....Q.z%f....6A.X...V.B.w..2....b8G...E.5.5.2}.q.3.#=.=...3.....M..*_.\vs...3..%..j..=.....O.Z.k2.} (}ku-.$]....._...$<....D....3...&:.;....{.-r..[-.t...c:..M67S.kfk...I.)i.]..5y..c...6..\h.^.s.b..".&.b.....t..4. .D.#.;..x.8.1.WV..J.V..\.k...x{y.x.z..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\businessinsurance[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 288x55, frames 3
Category:	downloaded
Size (bytes):	4708
Entropy (8bit):	7.800101108384317
Encrypted:	false
SSDEEP:	96:NaYoqCnoNqopuF3Qs+XdYjsQgS/224qSJmkXmARyuxWfnkONz:AYtN+Qs+XAkSe24q4mAEuxWfvN
MD5:	4FA294E8BDEB720E35B1751C16E8BE6D
SHA1:	971A87060470044952152B16AC15B741F8941158
SHA-256:	8F9FD598FCFAB2D569F8A4A2607F4035AC80EC7731B27FD36363DBEDEE3AD119
SHA-512:	DAC7D8E1259C17F0F3EC23BBFC1E6EC39D3D61D510EB4711E123FD4DEC362EB223E2A9C601FDE2EC82C2B4422FA14DE94A4D88359C13D541E5EC00805C2B3 73
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-content/uploads/2014/06/businessinsurance.jpg
Preview:	......JFIF.....7. .."....?;Vmc...sw.rl..'....I s6>7.Rh.~6Z.....Z[+...Y.S..z.U4.....eYy.c..g..Q..diw.u?..?....K.g... .....x.....=Ne..k.....b...i..;(.L.....`.....es..zN\.u ...i.6.....'.....!"`#36.....I.W.{..z...F.N...'....>.l..1....g...*.....k..#...%..m...,`..6;.%..d.*{*h.....E..#!....{...S...@".. ..I..D.....>k.sT...#%-K....h.1...Fd..$..x.....P.Fa.w. {...(.J...,..!oz^.....%.U.K..C.H..?5Va.....f.mh.eS...G....J.;@....oO)..qAh.6.k6.V.3'.\|....GO.~.O;7r.z5..I.V...I.....m#.K)?.f...#..[.Cs.....*t.....$a..n.Y.Hd/..t+g..=.....'..>..I.... k|k..ye...FT...8$...tL>}.m:.1..}.Z._..S...N..E.SA...D.H....r.^u...!.k.m...g}...#...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\chosen-sprite[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 52 x 37, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	538
Entropy (8bit):	7.511588515571485
Encrypted:	false
SSDEEP:	12:6v/7aoptiv9ji1KpCLg4CiehiKIQGy/wBWGu1YX2/1eMViiNc7:joiv9jilLhQi7Onj1YmDVi6c7
MD5:	8B55A822E72B8FD5E2EE069236F2D797
SHA1:	AC1C922EA07B1486F0215F62330C84F3FFE91828
SHA-256:	8AA69EE6B2376505578D758BFBBC52AEC88FA5E591F1A7CABD8ADFA80A7B613A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\chosen-sprite[1].png	
SHA-512:	4970ABCF8C68EA16F76C5A6612A4FAFB791F5ED95CD01186EB49BD6000FA5C09DAF769A5BF298B86B52A2FE4961EFB0D4173A067CF85488BE0BC9F3EAC41E088
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-content/plugins/gravityforms/css/chosen-sprite.png
Preview:	.PNG.....IHDR...4...%.....^....IDATH..kSQ....-.....=.$..b.o.$((T.Hw...*....."nup..A.@ P..Apq..J$p!P.....M1.....;...=...\D..Y.n0...@}.D..M.F....>Fb..1.....c..!.6.1r..b.%G.....I..J(v...fFy.O.....H4B c.1.}..^...4..5Fo..G.X..v.U.n.(.R.s.p....v..*...8s.P....*.c.O.TQW....j.1Q.H}.....T..+...}...d../....L.Lc.F.6...7..,9.1IkJ.(.dJj..Lc..^..z*"Hu.j).....,?<..._1.a.....x.../b.}.T.!.....i.?O.u...oc\.....e.N....c:..99.\@.s. uZ....q..|yp.k.a.....6..B|....1....G.....gq..u.....p..+....[.*y.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\chosen.jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	29121
Entropy (8bit):	4.91438965646394
Encrypted:	false
SSDEEP:	768:+Otj9+umwo0XCITm9HNfhvwITdNWb0DvHrqgtV:+ORjgF9HNfh1TdNWb0DPugtV
MD5:	3E9F1DCB9CC75169765265133FB815A7
SHA1:	7678293E0A0DF6F57AEA34E07B7E0392EBBA2234
SHA-256:	73881513A7E7F8944A311BEA8E80E9FAD946E256AE74D62B5C8D469DC6DF0186
SHA-512:	ACC186178C20D51EF77A1B67C5706DE666D47CDF49509C1B936D4A3259CB643261EC190F99EA2F06E75D64210D25D7476183240A1F613C59CF992F6CB29922F2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-content/plugins/gravityforms/js/chosen.jquery.min.js?ver=2.4.15.1
Preview:	/* Chosen v1.8.7 | (c) 2011-2018 by Harvest | MIT License, https://github.com/harvesthq/chosen/blob/master/LICENSE.md */..(function(){var t,e,s,i,n=function(t,e){return function(){return t.apply(e,arguments)}},r=function(t,e){function s(){this.constructor=t}for(var i in e)o.call(e,i)&&(t[i]=e[i]);return s.prototype=e.prototype,t.prototype=new s,t._super__=e.prototype,t},o={}.hasOwnProperty;(i=function(){function t(){this.options_index=0,this.parsed=[]}return t.prototype.add_node=function(t){return"OPTGROUP"===t.nodeName.toUpperCase()?this.add_group(t):this.add_option(t)},t.prototype.add_group=function(t){var e,s,i,n,r,o;for(e=this.parsed.length,this.parsed.push({array_index:e,group:!0,label:t.label,title:t.title?t.title:void 0,children:0,disabled:t.disabled,classes:t.className}),o=[],s=0,i=(r=t.childNodes).length;s<i;s++)n=r[s],o.push(this.add_option(n,e,t.disabled));return o},t.prototype.add_option=function(t,e,s){if("OPTION"===t.nodeName.toUpperCase())return""!==t.text?(null!=e&&(th

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\formsmain.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	73888
Entropy (8bit):	5.060181779823719
Encrypted:	false
SSDEEP:	1536:KN4IaD5j+wyTmIV+g1Qyr6gbl3Ye0/+M3IOhqk4Jyr:KN4IaD5j+wyTmIV+g1Qyr6gbl3Ye0/+y
MD5:	37B8C175FF36A0BA7715BD003D24899F
SHA1:	8630F2D4A8F8DFF8DF5920799147EC21D243D1B3
SHA-256:	C60AE330DAF54DF0403A0E23846EA0D084EF91D25FCFA9D76134C7AA93DE31FD
SHA-512:	DADA2E8AB51829CE42C37E05B5D9CB994CAD58B53DF287C6835F9D05E31ED3E7E2EF4EBB3335965C4E5CE922FBB256BB0843149325FB30B31B639ED0C7B96E41
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-content/plugins/gravityforms/css/formsmain.min.css?ver=2.4.15.1
Preview:	.gform_wrapper select,.gform_wrapper textarea{font-size:inherit;font-family:inherit;letter-spacing:normal}.gform_wrapper .gf_progressbar:after,.gform_wrapper ol.validation_list:after{content:""}.gform_wrapper{margin:16px 0;max-width:100%}.gform_wrapper form{text-align:left;max-width:100%;margin:0 auto}.gform_wrapper *,.gform_wrapper :after,.gform_wrapper :before{box-sizing:border-box!important}.gform_wrapper h1,.gform_wrapper h2,.gform_wrapper h3{font-weight:400;border:none;background:0 0}.gform_wrapper input:not([type=radio]):not([type=checkbox]):not([type=submit]):not([type=button]):not([type=image]):not([type=file]){font-size:inherit;font-family:inherit;padding:5px 4px;letter-spacing:normal}.gform_wrapper input[type=image]{border:none!important;padding:0!important;width:auto!important}.gform_wrapper textarea{padding:6px 8px;line-height:1.5;resize:none}.gform_wrapper select{line-height:1.5}.gform_wrapper .ginput_container_multiselect select{background-image:none!important;-webkit-app

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\hotjar-1405306[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	3503
Entropy (8bit):	5.2406619943425525
Encrypted:	false
SSDEEP:	48:Be1f+BPr4DGrnCpDuMY6wRQAQl07krGMfr4U4R5UEyledehtwWNmQ4XTnOFom34D:dEensnIQKa4U4bULqOj4bKoD
MD5:	215B7571094A2AEEEDF2E9117B8BE121
SHA1:	478F99BD1D60BE7B76BA192BFFCF4952B0D1846E
SHA-256:	E3ADDD7AFD6E0AF05ED3E7BC6748D264A772ED9DE1280354EDBBFF591FFF59A1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\hotjar-1405306[1].js	
SHA-512:	B53E6AF6E4EF60ED8CDA65A5909EC0B34D7C9B1E93E852B1EAD18F35A636FEAD5A71447C84895BD61A543D5EC1E5EB1A598EE357FBBF2226F6B894FAAE79457A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.hotjar.com/c/hotjar-1405306.js?sv=7
Preview:	window.hjSiteSettings = window.hjSiteSettings || {"site_id":1405306,"r":1.0,"rec_value":1.0,"state_change_listen_mode":"automatic","record":false,"continuous_capture_enabled":false,"recording_capture_keystrokes":false,"anonymize_digits":true,"anonymize_emails":true,"suppress_all":false,"suppress_text":false,"suppress_location":false,"user_attributes_enabled":false,"legal_name":null,"privacy_policy_url":null,"deferred_page_contents":[],"record_targeting_rules":[],"feedback_widgets":[],"forms":[],"heatmaps":[],"polls":[],"integrations":{"optimizely":{"tag_recordings":false}},"features":["funnels.disable_traffic_log_capture","recordings.filter_new_user","recordings.page_content_ws","settings.billing_v2","heatmap.continuous_capture"]};..!function(e){var t={};function n(o){if(t[o])return t[o].exports;var r=t[o]={i:o,l:!1,exports:{}};return e[o].call(r.exports,r,r.exports,n),r.l=!0,r.exports}n.m=e,n.c=t,n.d=function(e,t,o){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:o})},n.r=funct

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\insurance-12[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 400 x 300, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	9190
Entropy (8bit):	7.922125532085358
Encrypted:	false
SSDEEP:	192:UBaf9uACKwHO5La/OKmYdKhZLm02mvm1fgOBrllHSTQF:UEluAgHKardKhZV2vBBrllF
MD5:	DD5FE4DCCE421E34754A425F7688C733
SHA1:	5A0EDF9F0519F3CE18F42CB4FB2B88CF0FAF397D
SHA-256:	CD9FF933BCDD3513A7E63C2151055E7DF0C7975F67118B2B7EF8B9F452E65378
SHA-512:	37A6F838F2404A2568531397937D8E386379D929D1346EFCF67764E750F56EFA7F5A0AB781DB78E44FF60017E5C8D4FDF08D64A825253025C1F94F47B19B4AEE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-content/uploads/insurance-12.png
Preview:	.PNG.....IHDR.....,.....i.....PLTEH:gz.....o.....z..~..q..v..m..g..[..]..u..N..Dy.@t.<a.Lj.2T.>H.>E.H:hw^z9.....tRNS.....W9"...v.....".IDATx..{W.K..9gs.Y ..$G !0d...A.j\K..':sa`.....A..y..v._~>.TU.2..j.T+.....s..\|>_,.J.j.?].K.(;$.[.pd.bz\...R1/BAa..A.k.....,BT..T.@t.b....]*.....7r....s.)..n..''[.U.@....12M=Lv.....UG. z..... qq...dSW....k.u"u... 2.....II.B....{V^.'(./s..@P=y.'0..I.....8[..16?..O...g..X..HJ. Xy.&.....Ug%$...*..`.>.D\$.....]g...bfk.d.:.#A.8VR>.A..;.....:].X.(_O.....a}w9K...x <..\|..4.Q....Q..V"..\|q .L...b.*_.H./.;...-}Y ...Ug..]D..A..v".Q.....<v:?..>,.r.....d2...7...l=.....c...LE....+.u.[..@...0...HxC..H....2h..H..0%....G."..%09...Sr.5kO.....K<?.m.J$.....cw.....G....~p..'..o.#.xS.A.S.V".D2...[F...7..'.I.<Tx8..-....z...I.H.....1]}...".I+[e.b..NR....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\insurance-14[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 400 x 300, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	6277
Entropy (8bit):	7.880813328936925
Encrypted:	false
SSDEEP:	96:v+g/48gv04/2i2ssxSKQrbT31kXiOiVxdXPdMFYtIrlqkgMb1LlXVADlX:Hn8r2tSKoT1NVLPtWXgGRX
MD5:	1EDF126923864B68714FFAC859591CBA
SHA1:	6C31EEE52B011BA52995482C2A329904DDD071A5
SHA-256:	19B0C01F18A344AE23D4BEF795F6A84931DF71A8E45AFFBDE17F548107203244
SHA-512:	18ED52157BDEAF8F0C9AC4108377665A4F4CD6391A9DA610C817F6B91A40833958AB530E8BA1B655040B32D6AE9847A946FB1E329F6D2681546AC0B2E5B4A4F8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-content/uploads/insurance-14.png
Preview:	.PNG.....IHDR.....,.....i.....PLTEwq....g.....f..K?iM?l[PrF<k[Qu.....bV{l`.[Ox;2_9-UA5bH:hYl.%..]..{.....tRNSnj.....K....+3K.....IDATx...z....`5...xc...`.$....X.....3_o.....l.....b.\.V.u5._..t....D.e(...HdF..|.yl.&....AaTT..D.9%F.2.@.....Ff2.....r.5.&`..QM....c-(FC".d.Z.....p$1.^.F.1.$...Hl...3[.....c.....Z.$l...s.]D,.r..XN jT.....[;.az.zF...C...2_...: ..<.*.FY.r..D.r5../.i.....E.H.G....Q.cp+.<A..1../.....@..z.....{.....T....X+..W.Q.cHm.....x.....i#.E<..F.A.....H../.1....2...0..x!.A.}.@...r. ...B.b.Y..c.E.....5....P..x1...-.r=.X.....S.....M...h...m @w]...^+.v*Z.A.<L.MBK...{0.-. X..<.. ..Vp.....]..).eNE.;H...8*.0..#...R...Z..`.FV.\].4.7.UFZ..Y.8t.,T.Q.h....H9.....-@_....0.j. e.25w...-@Y..<T.Q.h..e...Y..d.....hq.)..piA.kNE..HY.4Z.M...E..d.fN...j.-....PQ.....;..... .zE..wtcL ..-@. ..K5... N...C.a..E..vt...N..x...Z....ZE..&.+.X.'..5..8.,... .}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jquery-migrate.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	11224
Entropy (8bit):	5.2603128465032745
Encrypted:	false
SSDEEP:	192:JrprDNvD66fPP/+I6OP1fQP0Olr96DB6MHXcwr1RF:JrprxG6fPP3P1fQMOIsDsMMS
MD5:	79B4956B7EC478EC10244B5E2D33AC7D
SHA1:	A46025B9D05E3DF30D610A8AEF14F392C7058DC9
SHA-256:	029E0A2E809FD6B5DBE76ABE8B7A74936BE306C9A8C27C814C4D44AA54623300
SHA-512:	217F86FEE871FA36ECA4F25830E3917C7BF57A681140B135C508AA32F2A1E3EFF5A80661F3B5BA46747D0C305AF10B658D207F449550F3D417D9683216FEEA8F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jquery-migrate.min[1].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2
Preview:	/*! jQuery Migrate v3.3.2 | (c) OpenJS Foundation and other contributors | jquery.org/license */."undefined"==typeof jQuery.migrateMute&&(jQuery.migrateMute=!0) ,function(t){"use strict";"function"==typeof define&&define.amd?define(["jquery"],function(e){return t(e,window)}):"object"==typeof module&&module.exports?modul e.exports=t(require("jquery"),window):t(jQuery,window)}(function(s,n){"use strict";function e(e){return 0<=function(e,t){for(var r=/^(\d+)\.(\d+)\.(\d+)/,n=r.exec(e)||[],o=r.exec(t)||[],i=1;i<=3;i++){if(+o[i]<+n[i])return 1;if(+n[i]<+o[i])return-1}return 0}(s.fn.jquery,e)}s.migrateVersion="3.3.2",n.console&&n.console.log&&(s&&e("3.0.0")||n.console. log("JQMIGRATE: jQuery 3.0.0+ REQUIRED"),s.migrateWarnings&&n.console.log("JQMIGRATE: Migrate plugin loaded multiple times"),n.console.log("JQMIGRATE: Migrate is installed"+(s.migrateMute?"":" with logging active")+", version "+s.migrateVersion));var r={};function u(e){var t=n.console;s.migrateDeduplicateWarnings&&r[e]|| (r[e]=!0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jquery.json.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):	1848
Entropy (8bit):	5.399901834592819
Encrypted:	false
SSDEEP:	48:dtqPLuDUfgCdiThE+NbhYh5aE6BHMlSqPz9SqPz9RYf4JQvdE1e:dcPKAfgCdiVLs6xMVPx/PxRpJQae
MD5:	827FDE8D0DE0BA40AB12406EB78B4908
SHA1:	6705762130B2EB5F505FF924B8203CE4F8FD585D
SHA-256:	172314FF74044B918766ED4763279B5E8798622087C0A2930F59C9D44662213D
SHA-512:	A528D35B5051FB167ED507EB56D440C88919AA7844B014634D6CD75BA54280545BD4B6E916260C35285DC546DAEF108819CD8FAE70121B2ADBD10708A9640B5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-content/plugins/gravityforms/js/jquery.json.min.js?ver=2.4.15.1
Preview:	!function($){"use strict";var escape=/["\\\x00-\x1f\x7f-\x9f]/g,meta={"\b":"\\b","\t":"\\t","\n":"\\n","\f":"\\f","\r":"\\r",'"':'\\"',"\\":"\\\\"},hasOwn=Object.prototype.hasOwnProperty;$.t oJSON="object"==typeof JSON&&JSON.stringify?JSON.stringify:function(t){if(null===t)return"null";var e,r,n,o,i=$.type(t);if("undefined"!==i){if("number"===i||"boolean"===i)return String(t);if("string"===i)return $.quoteString(t);if("function"==typeof t.toJSON)return $.toJSON(t.toJSON());if("date"===i){var f=t.getUTCMonth()+1,u=t.getUTCDate (),s=t.getUTCFullYear(),a=t.getUTCHours(),l=t.getUTCMinutes(),c=t.getUTCSeconds(),p=t.getUTCMilliseconds();return f<10&&(f="0"+f),u<10&&(u="0"+u),a<10&& (a="0"+a),l<10&&(l="0"+l),c<10&&(c="0"+c),p<100&&(p="0"+p),p<10&&(p="0"+p),""+s+"-"+f+"-"+u+"T"+a+":"+l+":"+c+"."+p+'Z"'}if(e=[],$.isArray(t)){for(r=0;r<t.length;r++)e .push($.toJSON(t[r])||"null");return"["+e.join(",")+"]"}if("object"==typeof t){for(r in t)if(hasOwn.call(t,r)){if("number"===(i=typeof r))n=""+r+'"';

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	89496
Entropy (8bit):	5.289738088208255
Encrypted:	false
SSDEEP:	1536:AjExXUqrnxDjoXEZxkMV4SYSt0zvDD6ip3h8cApwEjOPrBeU6QLiTFbc0QlQvakU:AYh8eip3huuf6lidlrvakdtQ47GKE
MD5:	B6F7093369A0E8B83703914CE731B13C
SHA1:	D1889F5C173C2A4B20288F1F84758599AFD346EF
SHA-256:	60240D5A27EDE94FD35FEA44BD110B88C7D8CFC08127F032D13B0C622B8BE827
SHA-512:	D6AA7835D7B256B94DDD2F9D8DB84484F0413EBC502762C1BA21CBA7A392C6F550DB2418CDC8BD6D1DA6ED2CEA55BF22473C778493D416B1A1C38E6FFDB8(79D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-includes/js/jquery/jquery.min.js?ver=3.5.1
Preview:	/*! jQuery v3.5.1 | (c) JS Foundation and other contributors | jquery.org/license */.!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports? module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery requires a window with a document");return t(e)}:t(e)}("undefined"!=typeof window? window:this,function(C,e){"use strict";var t=[],r=Object.getPrototypeOf,s=t.slice,g=t.flat?function(e){return t.flat.call(e)}:function(e){return t.concat.apply([],e)},u=t.push,i=t.ind exOf,n={},o=n.toString,v=n.hasOwnProperty,a=v.toString,l=a.call(Object),y={},m=function(e){return"function"==typeof e&&"number"!=typeof e.nodeType},x=function(e) {return null!=e&&e===e.window},E=C.document,c={type:!0,src:!0,nonce:!0,noModule:!0};function b(e,t,n){var r,i,o=(n=n||E).createElement("script");if(o.text=e,t)for(r in c) (i=t[r]||t.getAttribute&&t.getAttribute(r))&&o.setAttribute(r,i);n.head.appendChild(o).parentNode.removeChild(o)}function w(e){return null==e?e+"":"o

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\loading[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):	13294
Entropy (8bit):	5.975122494815057
Encrypted:	false
SSDEEP:	192:UyfmiZ+/fRILbcxNRULVCyLwxzhwE3yfmiZ+/fRILbcxNRULVCyLwxzhwEu:B+ILbGKLkhwEi+ILbGKLkhwEu
MD5:	59E3DE1B634D6079D6EB4773C5B61954
SHA1:	20CABE14319C507C115354BD4D131B27219A3FD1
SHA-256:	E7128243603FB91EB2B7927A511050DAC2D3599D83E1A709D1A4AC1010066BB2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\loading[1].htm	
SHA-512:	DC3B3764134FC88CC1EA684C6E4D04BE1120BA2BBCD83CEDD9C245DAFD73F64A0262234CCA423BAA01947C0E99A5CEC347B630C2488C24600B0DA5BAFA62C A36
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">.<html xmlns="http://www.w3.o rg/1999/xhtml">..<head>. <meta http-equiv="content-type" content="text/html; charset=utf-8" />. <meta http-equiv="cache-control" content="max-age=0" />. <meta ht tp-equiv="cache-control" content="no-cache" />. <meta http-equiv="expires" content="0" />. <meta http-equiv="expires" content="Tue, 01 Jan 1980 1:00:00 GMT" />. <meta http-equiv="pragma" content="no-cache" />. <meta http-equiv="robots" content="noindex, noarchive">. <title>Freshwidget Loading...</title>.</head>..<body>. <style>. body {. background: transparent;. margin: 0;. overflow: hidden;. }. . .ct {. margin-left: 20px;. margin-right: 20px;. -webkit-box- shadow: 0 5px 10px rgba(0, 0, 0, 0.4), white 0 0 1px inset;. -moz-box-shadow: 0 5px 10px rgba(0, 0, 0, 0.4), white 0 0 1px inset;. bo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\mediaelementplayer-legacy.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	11256
Entropy (8bit):	5.010537766861896
Encrypted:	false
SSDEEP:	192:xthsVmeDXDanvgZenjAJKdXSMpNO96hDIzL79V1QVSD1CNxn6fR31r:czDanvuenjAkNBhDInSwh31r
MD5:	2B0DD7EECEA03B4BDEDB94BA622FDB03
SHA1:	703BECBA85161118DD6FC66AF465428EF43F561C
SHA-256:	B7908A015A567EC2363011DF2475368DBFF34360E9DA3FDFF50604D6395FB646
SHA-512:	FE64CFF950921BDF83EC09FE79CA5CE52DE40F5B8788697EB1D7B28055F2817778347D5D3C81A324801C7EC7151B3EE0EEE99B2882C3C3B10BD760342D3BF3E 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-includes/js/mediaelement/mediaelementplayer-legacy.min.css?ver=4.2.16
Preview:	.mejs-offscreen{border:0;clip:rect(1px,1px,1px,1px);-webkit-clip-path:inset(50%);clip-path:inset(50%);height:1px;margin:-1px;overflow:hidden;padding:0;position:absolute;w idth:1px;word-wrap:normal}.mejs-container{background:#000;font-family:Helvetica,Arial,serif;position:relative;text-align:left;text-indent:0;vertical-align:top}.mejs-conta iner,.mejs-container *{box-sizing:border-box}.mejs-container video::-webkit-media-controls,.mejs-container video::-webkit-media-controls-panel,.mejs-container video::-web kit-media-controls-panel-container,.mejs-container video::-webkit-media-controls-start-playback-button{-webkit-appearance:none;display:none!important}.mejs-fill-container ,.mejs-fill-container .mejs-container{height:100%;width:100%}.mejs-fill-container{background:transparent;margin:0 auto;overflow:hidden;position:relative}.mejs-container:f ocus{outline:none}.mejs-iframe-overlay{height:100%;position:absolute;width:100%}.mejs-embed,.mejs-embed body{background:#000;height:100%;margin:0;over

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\mem5YaGs126MiZpBA-UN_r8OXOhv[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 25004, version 1.1
Category:	downloaded
Size (bytes):	25004
Entropy (8bit):	7.978903570057148
Encrypted:	false
SSDEEP:	384:NQHZMrOEzGv0FkfCvQIW/HCt7oQy/u2NSXAF7Q57vRTVOq1SQgnYfScZfSmB7Mjr:lrzzGMFgCvLnt8Zuh2Q5VUCRZOr
MD5:	D2C6A4B3918B50C5F1854BB9C5D1DE0E
SHA1:	8DE0F3B153BE6114D55DAC6E69CE7AEF9CC98DB2
SHA-256:	6D764A8FFCF6DB322C1F2FB36473FBA60135B7AB93BE5969120152C0538C5EE4
SHA-512:	FC4E9632C1A6764A4C817DD0FEFF5E1FA70160FDCA8918ECA3B04BD351762E4BB93D4CC8CB2465BA0474766A48B23007432C985991047CC1B30E7605B536DD4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UN_r8OXOhv.woff
Preview:	wOFF.....a.....D.....GDEF.....6...:z..GPOS.....GSUB.....$5"OS/2...X...^...`}...cmap.....6.....cvt .....].....fpgm…P.....~a..gasp.....#glyf.. ....KK..}`.4.ahead..TH...6...6..F.hhea..T.... ...$....hmtx..T.....`....loca..W.....22..Kmaxp..Z.... ... .X..name..Z....."c?Jpost..[.....y. .prep..`.....:..]x.c`d``.a..&.v..F..FFWFW ....$=...d.c%..fl.....]r.2.....x.U....P.E.}.....5.\A.kX..k..\.....v.c.1.p...X8../....n.C...\.%...Z..u...\.p.}.1\....z.#.....)..KB8.~.9...]]...Rg.~.1xT.jH.....3.....x.c`fig.a`e``..j...(.../2.1..` b.ffcfeabbY.....@`...../..?....^..... 9.{.m@J....u.....x....]Q...o.....6..qm...~.....g..3..s. J..*.4o...>(.....|.76g;N.Ln....uFQM=..<6o.O.....m.M.#...T..bE..4...M..29-..r.j..5.....a ...3....s.ge..y-sH1.....&.c.r.jR[....k.p*s.Tx. .h@_.>...Z.==....n.^.....k.....`.....^...us\/..us]]...rM]}/.{.=.....R..Q.(.7.%.....Bx..<.0.F8. .G..Y.u...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\mem8YaGs126MiZpBA-UFW50d[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 24364, version 1.1
Category:	downloaded
Size (bytes):	24364
Entropy (8bit):	7.9780064341168915
Encrypted:	false
SSDEEP:	384:3QHZZt4XLVDTVvAN+dDVaBflEY45pxDJfYiDuRA2qbCsksxqHfE5fDB5Z1iEj9:c4XLbvAN8DkBlC5nDhYiDQ8bCshA/E5/
MD5:	B7B7C77B83E9D67F6756AA2716F35EBA
SHA1:	67FE3DC0A0C49F305D6B3BD63F4F8A10CEB6A38F
SHA-256:	191DBBA54729AA43F2C5C2F118971963758D7F0DF2CC2F28F91B86A03DEE83EC

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\mem8YaGs126MiZpBA-UFW50d[1].woff	
SHA-512:	CA739EE8DFCFB8A060BC0BA10C246988DCBCE4024CEC24F5F37308048C96844C67724B033F68781E86A296DFC7468ED8E1667D930D9E8C70BE96F0D284ECCDC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem8YaGs126MiZpBA-UFW50d.woff
Preview:	wOFF....._,.....GDEF.....6...:.z..GPOS.....GSUB.....$5"OS/2...X...^...`~f..cmap.....6.....cvt .....Y.....M..fpgm...L.....~a..gasp.....#glyf.. ....H...v.6C..head..Q....6...6..cphhea..R.... ...$...hhmtx..R,.....`...loca..UD.....2..maxp..X`... ... .1..name..X.....&:A.post..Yp.....y. .prep..^<.....C...x.c`d``.a..&.v..F.. FFWFW ....$=...d.c%..fl.....]r.2.....x.U....P.E.}....5.\A.kX..k..\....v.c.1.p...X8../....n.C...\.%...Z..u...\.p.}.1\....z.#.....)..KB8.~.9...]]...Rg.~.1xT.jH.....3.....x.c`f..8.....u..1... <.f.....e...>...7.k0...c.3.....l..D.Z8z."....X<X..)..f.....x....]Q...o.....6..qm...~.....g..3..s. J..*.4o...>(.....|.76g;N.Ln....uFQM=..<6o.O.....m.M.#...T..bE..4...M..29-..r.j..5. .....a...3....s.ge..y-sH1.....&.c.r.jR[....k.p*s.Tx. .h@_.>...Z.==....n.^.....k.....`.....^...us\/..us]]...rM]}/.{.=.....R..Q.(.7.%.....Bx..<.0.F8. .G..Y.u...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\memnYaGs126MiZpBA-UFUKW-U9hIIqU[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23868, version 1.1
Category:	downloaded
Size (bytes):	23868
Entropy (8bit):	7.979638985615689
Encrypted:	false
SSDEEP:	384:a9YHfFZFePSGOLmI/WzYJb0u5XG2pyuLku5UtnK4yj1CPVkasY8C/EU0a6k:N/F2s7uY2q22pyptjVkasvCcjzk
MD5:	AEFF9F0AF1A6193B84B19ECA87EA4880
SHA1:	EF93A075CEFCF2A9ADB8C5F47F6E4073070B9210
SHA-256:	A97D00D68E7A6805D042116D737E92690809443E87F08085FCA52F78C6FABCCF
SHA-512:	D57FD22A73F5BDE931CEA3BFA8F2ED0D66B46EF108CDF8A800DF184505A53101E2CFFF8F221C6E78EDA813B04073675A5BF8946A71E68D2270DD329AB4BA281
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKW-U9hIIqU.woff
Preview:	wOFF.....]<.....GDEF.....6...:.z..GPOS.....GSUB.....$5"OS/2...X...]...`..!.cmap.....6.....cvt .....o.....fpgm...`.....s.ugasp.....#glyf... ...Fp..pn....head..O....6...6....hhea..O....#...$....hmtx..O....4...`l.=`loca..S.....2_\BFmaxp..V0... ... .]..name..VP.....8Gtpost..WL.....y. .prep..\ .....@..R.x.c`d``.a..&.v..F ..FFWFW ....$=...d.c%..fl.....]r.2.....x.U....P.E.}.....5.\A.kX..k..\.....v.c.1.p...X8../....n.C...\.%...Z..u...\.p.}.1\....z.#.....)..KB8.~.9...]]...Rg.~.1xT.jH.....3.....x.%..@0... ?.%.N.OJ.s&pJ...:[h-.a.{..(\....nw-..7...).L...'...T.M7..bz..~.)b.....\.....x....]Q...o.....6..qm...~.....g..3..s. J..*.4o...>(.....|.76g;N.Ln....uFQM=..<6o.O.....m.M.#...T..bE..4 ...M..29-..r.j..5.....a...3....s.ge..y-sH1.....&.c.r.jR[....k.p*s.Tx. .h@_.>...Z.==....n.^.....k.....`.....^...us\/..us]]...rM]}/.{.=.....R..Q.(.7.%.....Bx..<.0.F8. .G..Y.u...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\memnYaGs126MiZpBA-UFUKWiUNhIIqU[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23408, version 1.1
Category:	downloaded
Size (bytes):	23408
Entropy (8bit):	7.978409043250865
Encrypted:	false
SSDEEP:	384:j08SX8c0+xc6rxYT9FQkeKX1QG2BP2KFlVuaMYtsKqe3a9MMzjF5aSP2ZW0a6HZ:8Xf0++OqTTQgSFBP/lV+YOKKjMzHZ
MD5:	D7E0C8F45B667E66E0FA94D77D6B2F11
SHA1:	4A5442D59539782926397E807BA97441C55D66D1
SHA-256:	F461846EBDE06B126199AB1B219003C99009D9A40CAFDC0D3ABF86565B62E3E8
SHA-512:	E38C6D197138F9868A6B52E9BF463A3CBEF615CEDEDD78DDA54F385FE437C626699FCD75F66009AA8D83CF3E124F1BB1940A1896DDA5CF14C3AA99AB98AAC82
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKWiUNhIIqU.woff
Preview:	wOFF.....[p.....T.....GDEF.....6...:.z..GPOS.....GSUB.....$5"OS/2...X...]...`....cmap.....6.....cvt .....b.....g.ifpgm...T.....s.ugasp.....glyf... ...E...pBEN$Zhead..N....6...6..{.hhea..N<...#...$....hmtx..N`.....`..PSloca..Q.....2Il,+maxp..T.... ... .*..name..T.....)/C.post..U.....y. .prep..Z.....x.c`d``.a..&.v..F. .FFWFW ....$=...d.c%..fl.....]r.2.....x.U....P.E.}.....5.\A.kX..k..\.....v.c.1.p...X8../....n.C...\.%...Z..u...\.p.}.1\....z.#.....)..KB8.~.9...]]...Rg.~.1xT.jH.....3.....x.c`f9.....u..1... <.f.....A.(.....@`...../..?....^..... 9.8.m@J....}.....x....]Q...o.....6..qm...~.....g..3..s. J..*.4o...>(.....|.76g;N.Ln....uFQM=..<6o.O.....m.M.#...T..bE..4...M..29-..r.j..5... ...a...3....s.ge..y-sH1.....&.c.r.jR[....k.p*s.Tx. .h@_.>...Z.==....n.^.....k.....`.....^...us\/..us]]...rM]}/.{.=.....R..Q.(.7.%.....Bx..<.0.F8. .G..Y.u...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\modules[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), modules family
Category:	downloaded
Size (bytes):	92564
Entropy (8bit):	6.337482280506063
Encrypted:	false
SSDEEP:	1536:L2S6qLRqKELiXMjCs7VDmGWALXJ8jzxJ9OIgr26F9BEFDTs8/M/OuWhX5j63QWI/:L2S6qLRqKELiXMjCs7VDmGWAN8H79OIL
MD5:	AB43C4E3E2452CB3FE13DA5C75F55886
SHA1:	1086B2F4F2A5FE091FBCDBCA916B44D18050C2C2
SHA-256:	B41620417E9D7F07D82BB5375A9B5310A147B9D835CAB02DF078CBB16B0CC1B1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\modules[1].eot	
SHA-512:	A657C4B70CE80EBFDD172BC225B871658D20F22FE6855AFE24B504A26AF7F2DA9ED3049B38DF92A8EA8CFB8F8FCB5CBD9CA27DCE59252AFABD579BD27D10E84F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-content/themes/Divi/core/admin/fonts/modules.eot?
Preview:	.i...h.....LP.....[.x(.....m.o.d.u.l.e.s.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .2...4.....m.o.d.u.l.e.s.....0OS/2.....`cmap.....dgasp.....glyf4.v.....[.head.....],...6hhea.A....]d...$hmtxa.c...]....hloca...R..c....6maxp.....g(... name.X....gH....post.....h.... .....3.....@.....@...@.. ....H.....~...&..... ..... b.l.....79.....79.....79.....l.@...>.#..%265...2764/...'&"....0"1.....2?..... ....@...s.....I.B...@.#..."...'&".....021....27>.?.64'&"...4&. .....@.....s.....0.1..2764/.!2654&#!764'&"..0.1. .....18.1.....s.....(.....3!.....2?.>.7>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\online-application-2[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 400 x 352, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	10855
Entropy (8bit):	7.938165909414721
Encrypted:	false
SSDEEP:	192:pfshjTCW8LPErUHDK5PvYgeDwd9SSvL+h0x7tK5ZxShLZkZ+Lff2iTWWAoHG7Tv:pUh3MnG5Pggrd95i4QZ4kU1m/
MD5:	802DD38E637804C5859261E128E727C2
SHA1:	4552B7EA44E5F6B12E45C1524C0BFC060F3CE7C9
SHA-256:	5B50661F27DB5B337DD40D5B021DC97944E23504FBB949CFBECBEE420A488580
SHA-512:	404B950217F23E36F3401E760DA05341E2ECDFC6DF7072E3546A40DDF97E97FAE00EE709958EB0320CA26154427067341572 63B1E883296C47369C25FC0E8907
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-content/uploads/online-application-2.png
Preview:	.PNG.....IHDR.....`.....PLTE.....=.....(QS,NL,..>..,`\$$$#$"'&'$%%%%%%$# "!#! ....."!.)*!+, *+'--$41(11(211667<<8A@BEF9>>:@@:AA?CX@DZ69. DJ]WYYFKKGKLijj3.....v.....\|~...U..H../..b.....X....tRNS.....HH...".. .IDATx...s.F...i...c\c.a.3....qls.B.$F2.QF.. .....@...9VTo...D`...v...}&T.o+..7.-....vZ....@lu..m5o.x....mY..ePz..=.x...3..<;..G..'\.....<....L..<...Q.....+B.~.....o...o.....C.n&...o.F .-.1...<...{yy7..\....C..}....+...z....'....zk@r(.o..[ .1:..H).mk...}.! .h.....[L.[04.W._.am.....t.h.t...xF/...C6+.....K..=]am...x`..x.....5.u.....>99...^{....\.....YJ....U....K.b.u.... B..-..g<..$..5>.-q.7XA....#....v...@.}.d...K...bq.H" .. ...]..>.....D[t...7.. zt...1..\."..?I/..)...86J.{...n]^j...06..0.<.!.w.8....`J7c$.-.{a..6.5.....]}\.rB.....{}....k.v _]O.....g...r..?..tL.j.!..V `{@.....x~..@..%!...v.y.o.S...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\personal-lines[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	25955
Entropy (8bit):	5.446551816262722
Encrypted:	false
SSDEEP:	768:+78OP+SVs14sZ4OGV9/rTAk68CcWLhsTvGh9gf:+3P+SVs14syOWlTn68qmvGh9gf
MD5:	28224F0C87727BB0668730BC909E2D3D
SHA1:	738CB5066F344BD1647BFC32425DE96890C90B76
SHA-256:	81D68EB8456E1B7DB3BD7F4A23BC3E95ADDA57CD26F1CE6FCE81D5730EE3CC24
SHA-512:	08CD55CE182B75764C29A411D59C6AAF33B0923A2DC036F47C0674B564009E4EE5BAD264AA06D08FD3192B27DA2C5F5294943A5ECE2098A0A983A5358307E57
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/types-of-insurance/personal-lines/
Preview:	<!DOCTYPE html>.<html lang="en-US">.<head>..<meta charset="UTF-8" />.<meta http-equiv="X-UA-Compatible" content="IE=edge">..<link rel="pingback" href= "https://yesbaker.com/xmlrpc.php" />...<script type="text/javascript">...document.documentElement.className = 'js';..</script>...<script>var et_site_url='https://yesbaker .com';var et_post_id='731';function et_core_page_resource_fallback(a,b){"undefined"===typeof b&&(b=a.sheet.cssRules&&0===a.sheet.cssRules.length);b&&(a.onerror= null,a.onload=null,a.href?a.href=et_site_url+"/?et_core_page_resource="+a.id+et_post_id:a.src&&(a.src=et_site_url+"/?et_core_page_resource="+a.id+et_post_id))}. </script>. Google Tag Manager for WordPress by gtm4wp.com -->.<script data-cfasync="false" data-pagespeed-no-defer>//<![CDATA[..var gtm4wp_datalayer_name = "d ataLayer";..var dataLayer = dataLayer || [];.// .</script>. End Google Tag Manager for WordPress by gtm4wp.com -->.. This site is optimized with the Yoast SEO plugin v15.5 - https://yoast.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\pixel[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	2.7374910194847146
Encrypted:	false
SSDEEP:	3:CU9yltxlHh/:m/
MD5:	DF3E567D6F16D040326C7A0EA29A4F41
SHA1:	EA7DF583983133B62712B5E73BFFBCD45CC53736
SHA-256:	548F2D6F4D0D820C6C5FFBEFFCBD7F0E73193E2932EEFE542ACCC84762DEEC87

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\pixel[1].gif	
SHA-512:	B2CA25A3311DC42942E046EB1A27038B71D689925B7D6B3EBB4D7CD2C7B9A0C7DE3D10175790AC060DC3F8ACF3C1708C336626BE06879097F4D0ECAA7F5670 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://q.quora.com/_/ad/931b253b90044bdd807d8902b5bfe759/pixel?j=1&u=https%3A%2F%2Fyesbaker.com%2Fquotes%2Fgeneral-liability-and-bop-online-app%2F%3Futm_source%3Dnewsletter%26utm_medium%3Demail%26utm_campaign%3Dbib&tag=ViewContent&ts=1610622568162
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\pixel[2].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	2.7374910194847146
Encrypted:	false
SSDEEP:	3:CU9yltxlHh/:m/
MD5:	DF3E567D6F16D040326C7A0EA29A4F41
SHA1:	EA7DF583983133B62712B5E73BFFBCD45CC53736
SHA-256:	548F2D6F4D0D820C6C5FFBEFFCBD7F0E73193E2932EEFE542ACCC84762DEEC87
SHA-512:	B2CA25A3311DC42942E046EB1A27038B71D689925B7D6B3EBB4D7CD2C7B9A0C7DE3D10175790AC060DC3F8ACF3C1708C336626BE06879097F4D0ECAA7F5670 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://q.quora.com/_/ad/931b253b90044bdd807d8902b5bfe759/pixel?j=1&u=https%3A%2F%2Fyesbaker.com%2F&tag=ViewContent&ts=1610622601766
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\pixel[3].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	2.7374910194847146
Encrypted:	false
SSDEEP:	3:CU9yltxlHh/:m/
MD5:	DF3E567D6F16D040326C7A0EA29A4F41
SHA1:	EA7DF583983133B62712B5E73BFFBCD45CC53736
SHA-256:	548F2D6F4D0D820C6C5FFBEFFCBD7F0E73193E2932EEFE542ACCC84762DEEC87
SHA-512:	B2CA25A3311DC42942E046EB1A27038B71D689925B7D6B3EBB4D7CD2C7B9A0C7DE3D10175790AC060DC3F8ACF3C1708C336626BE06879097F4D0ECAA7F5670 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://q.quora.com/_/ad/931b253b90044bdd807d8902b5bfe759/pixel?j=1&u=https%3A%2F%2Fyesbaker.com%2Fquotes%2Fgeneral-liability-and-bop-online-app%2F&tag=ViewContent&ts=1610622610003
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\pixel[4].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	2.7374910194847146
Encrypted:	false
SSDEEP:	3:CU9yltxlHh/:m/
MD5:	DF3E567D6F16D040326C7A0EA29A4F41
SHA1:	EA7DF583983133B62712B5E73BFFBCD45CC53736
SHA-256:	548F2D6F4D0D820C6C5FFBEFFCBD7F0E73193E2932EEFE542ACCC84762DEEC87
SHA-512:	B2CA25A3311DC42942E046EB1A27038B71D689925B7D6B3EBB4D7CD2C7B9A0C7DE3D10175790AC060DC3F8ACF3C1708C336626BE06879097F4D0ECAA7F5670 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://q.quora.com/_/ad/931b253b90044bdd807d8902b5bfe759/pixel?j=1&u=https%3A%2F%2Fyesbaker.com%2Fquotes%2Finstant-quotes%2F&tag=ViewContent&ts=1610622615437
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\pixel[5].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	2.7374910194847146
Encrypted:	false
SSDEEP:	3:CU9yltxlHh/:m/
MD5:	DF3E567D6F16D040326C7A0EA29A4F41
SHA1:	EA7DF583983133B62712B5E73BFFBCD45CC53736
SHA-256:	548F2D6F4D0D820C6C5FFBEFFCBD7F0E73193E2932EEFE542ACCC84762DEEC87
SHA-512:	B2CA25A3311DC42942E046EB1A27038B71D689925B7D6B3EBB4D7CD2C7B9A0C7DE3D10175790AC060DC3F8ACF3C1708C336626BE06879097F4D0ECAA7F5670 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://q.quora.com/_/ad/931b253b90044bdd807d8902b5bfe759/pixel?j=1&u=https%3A%2F%2Fyesbaker.com%2Fquotes%2Fprofessional-liability-quote-request%2F&tag=ViewContent&ts=1610622619935
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\pixel[6].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	2.7374910194847146
Encrypted:	false
SSDEEP:	3:CU9yltxlHh/:m/
MD5:	DF3E567D6F16D040326C7A0EA29A4F41
SHA1:	EA7DF583983133B62712B5E73BFFBCD45CC53736
SHA-256:	548F2D6F4D0D820C6C5FFBEFFCBD7F0E73193E2932EEFE542ACCC84762DEEC87
SHA-512:	B2CA25A3311DC42942E046EB1A27038B71D689925B7D6B3EBB4D7CD2C7B9A0C7DE3D10175790AC060DC3F8ACF3C1708C336626BE06879097F4D0ECAA7F5670 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://q.quora.com/_/ad/931b253b90044bdd807d8902b5bfe759/pixel?j=1&u=https%3A%2F%2Fyesbaker.com%2Ftypes-of-insurance%2Fsell-international-medical-and-trip-cancellation-insurance%2F&tag=ViewContent&ts=1610622636020
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\quotes[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	31656
Entropy (8bit):	5.418439948883803
Encrypted:	false
SSDEEP:	768:YqFbP+EVm14sZ4Okbtg5a+DCcPWlfh7TvGh9gu5Sm:Y+P+EVm14syOkx3OEf5vGh9guP
MD5:	B13BB0457FB397C35C8340D9646E5B12
SHA1:	8647439EF5B107D88A58025F13E3A25C83D85BA4
SHA-256:	1440513F8976964219FDE2B1DA26017EA719B3C73FC9D3B078636A471EB6EFA9
SHA-512:	058F47B620348BF15CEF408B44B2C2E8ED63EC5E741D8F6511710BAC7E3C0FCF3DC6D7627C789EA3B2CD7A732FCAABEAF8F1D8775890218A12A801608B2668 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/quotes/
Preview:	<!DOCTYPE html>.<html lang="en-US">.<head>..<meta charset="UTF-8" />.<meta http-equiv="X-UA-Compatible" content="IE=edge">..<link rel="pingback" href="https://yesbaker.com/xmlrpc.php" />...<script type="text/javascript">...document.documentElement.className = 'js';..</script>...<script>var et_site_url='https://yesbaker.com';var et_post_id='59';function et_core_page_resource_fallback(a,b){"undefined"===typeof b&&(b=a.sheet.cssRules&&0===a.sheet.cssRules.length);b&&(a.onerror=null,a.onload=null,a.href?a.href=et_site_url+"/?et_core_page_resource="+a.id+et_post_id:a.src&&(a.src=et_site_url+"/?et_core_page_resource="+a.id+et_post_id))}.</script>. Google Tag Manager for WordPress by gtm4wp.com -->.<script data-cfasync="false" data-pagespeed-no-defer>//<![CDATA[..var gtm4wp_datalayer_name = "dataLayer";..var dataLayer = dataLayer || [];..// .</script>. End Google Tag Manager for WordPress by gtm4wp.com -->.. This site is optimized with the Yoast SEO plugin v15.5 - https://yoast.c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\style[1].css	
Size (bytes):	817873
Entropy (8bit):	4.844258343599798
Encrypted:	false
SSDEEP:	24576:6Ae7+im5gQIUl7I4GNZ4+B4Dzy0WHFgEcgXrMf28aVurwA4EszVSlIfU3vdMWLpE:6oim5gQIUl7I4GNZ4+B4Dzy0WHFgEcgZ
MD5:	4C8DD51C4A2753B61893C0E94C0FE24D
SHA1:	3CA12FA9866C7DED4EA0F6D74D86F2103E2202D7
SHA-256:	7670B72ADC45F883C8A50156462719D577055EFDE1861D50749E4D1D5F1C35E0
SHA-512:	3744637028D56928502F93970C3E227ADF614EA0054C4AEA9465F02B109EA2859383801B924E7B42DA5208E7ECC84055E054E21EF822FB35FBC8F132ECBB4542
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-content/themes/Divi/style.css?ver=4.7.7
Preview:	/*!.Theme Name: Divi.Theme URI: http://www.elegantthemes.com/gallery/divi/.Version: 4.7.7.Description: Smart. Flexible. Beautiful. Divi is the most powerful theme in our collection..Author: Elegant Themes.Author URI: http://www.elegantthemes.com.Tags: responsive-layout, one-column, two-columns, three-columns, four-columns, left-sidebar, right-sidebar, custom-background, custom-colors, featured-images, full-width-template, post-formats, rtl-language-support, theme-options, threaded-comments, translation-ready.License: GNU General Public License v2.License URI: http://www.gnu.org/licenses/gpl-2.0.html.*/../*! This minified app bundle contains open source software from several third party developers. Please review CREDITS.md in the root directory or LICENSE.md in the current directory for complete licensing, copyright and patent information. This file and the included code may not be redistributed without the attributions listed in LICENSE.md, including associate copyright notices and lic

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\subscribe-loader[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 16 x 16
Category:	downloaded
Size (bytes):	1422
Entropy (8bit):	6.988080119006123
Encrypted:	false
SSDEEP:	24:QGal1hnBWwjx82lY2T3JbV8EZayE1oyJ3VMTE1UEzGY8VrrOZGlNJhpXFrmP:QH1kNn2VKElEdJ3MEmEzL8V0G3pXFU
MD5:	70204EC0349400B426DB6B4FA99D24A0
SHA1:	6D894C606D3C329164CE589F8F15808EDD8FA6E1
SHA-256:	EC94DB5859FCEE150EB22E089FE0305E55FD528510578DE1B54646890A5C0F05
SHA-512:	FA392352F472A2B58743BBE166B9E40C175943C29BECBBE0ACAE0DB3DDFF1A1808BDB65DBB2245F5C66ED335B3CA201294CB93C0A43F4E4C0D05F64CC8AB06E9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-content/themes/Divi/includes/builder/styles/images/subscribe-loader.gif
Preview:	GIF89a.....!..NETSCAPE2.0.....!..XMP DataXMP<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.5-c021 79.155772, 2014/01/13-19:44:00 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CC 2014 (Macintosh)" xmpMM:InstanceID="xmp.iid:73E79A7D24BB11E485B4D9EAF70CB61C" xmpMM:DocumentID="xmp.did:73E79A7E24BB11E485B4D9EAF70CB61C"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:73E79A7B24BB11E485B4D9EAF70CB61C" stRef:documentID="xmp.did:73E79A7C24BB11E485B4D9EAF70CB61C"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.....~}|{zyxwvutsrqponmlkjihgfedcba`_

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\widget_v2.329[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):	1060227
Entropy (8bit):	5.358276095534078
Encrypted:	false
SSDEEP:	24576:daDrxEsHHjqHg51J2CnraPld0zh/59Xnp96V2AO9pTHdwmH/n7dV5uopI50pgBsy:davxEsHHjqHg51J2CnraPld0zh/59Xn6
MD5:	D602A3E049521CF85D88A115A9FA4617
SHA1:	9D532C120AF61798ECE02EE60CB589A86DB26964
SHA-256:	61369806BEC04E47C33A6B6CD94C9249A8F89EC2FD47C601D4DDB460F4A33F2C
SHA-512:	5135A72367F6BFD06B4436E6837C9EC86979569DBBC12EF6E80E76DED9FCA1060678D8F62E75464A2D3809A9BFA086D0C29F23B951EA7E7CC85BED92D2F9626D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://v2.zopim.com/bin/v/widget_v2.329.js
Preview:	!function(t) {.function e(n) {.if (i[n]) return i[n].exports;.var o = i[n] = {.i: n,.l: !1,.exports: {}.};.t[n].call(o.exports, o, o.exports, e);.o.l = !0;.return o.exports;.}.var i = {};.e.m = t;.e.c = i;.e.d = function(t, i, n) {.e.o(t, i) || Object.defineProperty(t, i, {.enumerable: !0,.get: n.});.};.e.r = function(t) {."undefined" != typeof Symbol && Symbol.toStringTag && Object.defineProperty(t, Symbol.toStringTag, {.value: "Module".});.Object.defineProperty(t, "__esModule", {.value: !0.});.};.e.t = function(t, i) {.1 & i && (t = e(t));.if (8 & i) return t;.if (4 & i && "object" == typeof t && t && t.__esModule) return t;.var n = Object.create(null);.e.r(n);.Object.defineProperty(n, "default", {.enumerable: !0,.value: t.});.if (2 & i && "string" != typeof t) for (var o in t) e.d(n, o, function(e) {.return t[e];.}.bind(null, o));.return n;.};.e.n = function(t) {.var i = t && t.__esModule ? function() {.return t.default;.} : function() {.return t;.};.e.d(i, "a", i);.return i;.};.e.o

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\wp-mediaelement.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\wp-mediaelement.min[1].css	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	4186
Entropy (8bit):	4.923675414240059
Encrypted:	false
SSDEEP:	48:wFfAeWkkqEsKO+TBxaBIIj+NqUFQW76d7JrOv2bN:wueWkkrLoI7U
MD5:	EA958276B7DE454BD3C2873F0DC47E5F
SHA1:	B143F6E8E8F79D8F104C26B0057EF5514D763219
SHA-256:	2E10D353FF038C2CAD3492FC17801AF3E6EF2669C9E9713BDB78B1DCB104C4FE
SHA-512:	2D40A1E713355EFF88FA3BBF5471B4DB5ACC48FA2B978A555C034F2E5C7F131FCAF48E849D5D048DF9D5DAE068C4B6467A97B1DDE99115E6B32F57E928569F 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-includes/js/mediaelement/wp-mediaelement.min.css?ver=5.6
Preview:	.mejs-container{clear:both;max-width:100%}.mejs-container *{font-family:Helvetica,Arial}.mejs-container,.mejs-container .mejs-controls,.mejs-embed,.mejs-embed b ody{background:#222}.mejs-time{font-weight:400;word-wrap:normal}.mejs-controls a.mejs-horizontal-volume-slider{display:table}.mejs-controls .mejs-horizontal-volume- slider .mejs-horizontal-volume-current,.mejs-controls .mejs-time-rail .mejs-time-loaded{background:#fff}.mejs-controls .mejs-time-rail .mejs-time-current{background:# 0073aa}.mejs-controls .mejs-horizontal-volume-slider .mejs-horizontal-volume-total,.mejs-controls .mejs-time-rail .mejs-time-total{background:rgba(255,255,255,.33)}.mejs- controls .mejs-horizontal-volume-slider .mejs-horizontal-volume-current,.mejs-controls .mejs-horizontal-volume-slider .mejs-horizontal-volume-total,.mejs-controls .mejs-t ime-rail span{border-radius:0}.mejs-overlay-loading{background:0 0}.mejs-controls button:hover{border:none;-webkit-box-shadow:none;box-shadow:none}.me-cannotpla y{width:au

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\1f389[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3153
Entropy (8bit):	4.321364335901197
Encrypted:	false
SSDEEP:	96:1gttasJDk5uXDd4Cm9rZGatWoUHJrX2cyTteR/eueAa:Kt/D96XidxRmBz
MD5:	B052A4BEF57C1AA73CD7CFF5BC4FB61D
SHA1:	3EFF89776B2A1D9AC207D0F62FD1FF7DBB4371F2
SHA-256:	194DE9942601B9A42CC9EA79663AACA170816CFC07CBE8B2A568852427FA7088
SHA-512:	7DD807177208CF6E27154EBE83D62422E86F14CDEB69FBE95AC75A7D6D63D0A646E43F0DA7A8CF745F2199326C2EBE5EDE370BD4332AA8ABFF1AF660E2B268 1F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s.w.org/images/core/emoji/13.0.1/svg/1f389.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 36 36"><path fill="#DD2E44" d="M11.626 7.488c-.112.112-.197.247-.268.395l-.008-.008L.134 33.141l.011.011c-. 208.403.14 1.223.853 1.937.713.713 1.533 1.061 1.936.853l.01.01L28.21 24.735l-.008-.009c.147-.07.282-.155.395-.269 1.562-1.562-.971-6.627-5.656-11.313-4.687-4.6 86-9.752-7.218-11.315-5.656z"/><path fill="#EA596E" d="M13 12L.416 32.506l-.282.635.011.011c-.208.403.14 1.223.853 1.937.232.232.473.408.709.557L17 17l-4-5z"/> <path fill="#A0041E" d="M23.012 13.066c4.67 4.672 7.263 9.652 5.789 11.124-1.473 1.474-6.453-1.118-11.126-5.788-4.671-4.672-7.263-9.654-5.79-11.127 1.474-1.473 6.454 1.119 11.127 5.791z"/><path fill="#AA8DD8" d="M18.59 13.609c-.199.161-.459.245-.734.215-.868-.094-1.598-.396-2.109-.873-.541-.505-.808-1.183-.735- 1.862.128-1.192 1.324-2.286 3.363-2.066.793.085 1.147-.17 1.159-.292.014-.121-.277-.446-1.07-.532-.868-.094-1.598-.396-2.11-.873-.541-.505-.809-1.183-.735-1.86 2.13-1.192 1.325-2.286 3.362-2.065.578.062.883-.05

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Copy-baker-logo2-1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1753x445, frames 3
Category:	downloaded
Size (bytes):	25504
Entropy (8bit):	7.8029176978245465
Encrypted:	false
SSDEEP:	768:uQdnUkZiDWl0sM2fGeike/l8FM1mlCeD6iP6U6w606GNcgPGq:tn1oDYVfFetV1ECeuiy7/bGN7
MD5:	D2788E7A36F75B9B82160F4BC258B850
SHA1:	26900A482DFAD472E52DEFC077688BB903557037
SHA-256:	53D36A1288F2FD70792436289E032E0D47D83023184999095ABC1B11F88FFE59
SHA-512:	6A6D7F24F72C3859E5B4927D17E818FA5C39D25D873F926C5C07BC01EA6EE85D2057880BAE6905EBD72423A72151BB681A6DD85A1AE5C0FE9E10F0366F02967
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-content/uploads/Copy-baker-logo2-1.jpg
Preview:	......JFIF.....".".."+"+.F26262FjBNBBNBj^r]V]r^..vv.....".".."+"+.F26262FjBNBBNBj^r]V]r^..vv....."..... .....Vp1.....c....- ..y..3...1.....t..... .....<.u/ ..2S..Es.....4.....e+7.....N.....<..`...>.....N{ .h.j.....D&.....-x.....f~O..L...m.m.....f.....s`.....g...E....e'=..F...16.....T.....*....= *.....=.`....,...._.`.S..g....=.OHhP...6.....2...E...g.2.3+:.._..v.. .....O!.g%CEQ....]VM.Uy..e.f.....i.....L.....^eC.^pg.p..0...@r.|...{.1S.....x.....1.k..Y.3#.....DA...350AS.~..8..-] 5...%a.]_N.F.e.....e.?...s.16.....: .....l.j.|w}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\JTUPjIg1_i6t8kCHKm459WxZFgrD-A[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 69448, version 1.1
Category:	downloaded
Size (bytes):	69448
Entropy (8bit):	**7.993164519460345**
Encrypted:	**true**
SSDEEP:	1536:VD++kLIidIpLiODLF8Vpmg1nxEpBLtaFDBc9cKhrJdEVd021:VqvLDQLvCtVe7taLc9ns021
MD5:	D0E4A30EB08D63A1631116362DE55430
SHA1:	4F4C421E8E0F5E34EEAD44665A0CEE4CCD2FEE06
SHA-256:	8F30735802195D9E66C20120F06CF737F25AD44C046D1122D66BB15806DF2D47
SHA-512:	55DB060B3E5758FA20AFA0E383265485D28D8C89BC9BE057DA3316E630B5688D1A54455E7A526234F40EB2A21CE97F0F811ADF918F0F1A63B57EFFE27C38950E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTUPjIg1_i6t8kCHKm459WxZFgrD-A.woff
Preview:	wOFF.....H.....7T.....GDEF.....+.....1GPOS.....>.....D.("GSUB..A4.....OS/2..F@...S...`Vs.Ucmap..F.....7cvt ..N....d....2...fpgm..O....F...mM$.\|gasp..UX .....glyf..U`.....-..5..head...D...6...6..].hhea...\|...#...$....hmtx.....:.{loca.....k....".Amaxp..... ... ...bname...8.....D3.N.post...4...U..(.rZClprep.....K..x...3.XQ. .....m..m...&.m....\4k.{.....Yy..E.....fkp...v.....f?....K...b.....n....._..."^.[x.?.W..DO.dO...0W)....T...*VW.....DM...a...Vj.....U_..8R.p.&....9Z.....k3n.6...W.....Q...:..t....^....[xG.....S=.. z./....=~.7....K...b..1CY..|.....9l....'j`!..M.`...].?!..C.{9!.<....xOE..Q7.x..W..$l....j...;=.w.m.m.m...g.....\..W1.....?... . .vx...f....3O:.].9....`s...My.....#..*.>.../.=...b..c..V..8.....#.. f.p.1....mn?...w.F..=...'{.g.....1...Q..#.=... ."^p%7.}.f...n...to...>q...w.D9.....ro.d...o.{3...."t=..X..E5...}..H.q.R.....e.....Z..a.t..2V..E.Vj|....,Y@I

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\JTUPjIg1_i6t8kCHKm459WxZbgjD-A[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 69504, version 1.1
Category:	downloaded
Size (bytes):	69504
Entropy (8bit):	**7.991446797381646**
Encrypted:	**true**
SSDEEP:	1536:bjEzKrCLJoJIdtF8yvrOsSNCFvejeviH+VC0uuwAwXwuAJF21:Uz7LJaIXCjNevaH+/R9uAz21
MD5:	DA8BDA5921E3FB5932A51AE7FBF0BF14
SHA1:	7AA715616F09B3E7E225C9CC0CC5E56FB4021B2A
SHA-256:	44DE5B4623A5F951564D0063A7FF88507A1BD1BEFD8A3C3EADF1AB680C39687D
SHA-512:	C401A238389C290DAFADDEF8D8186420FBA3209086D4C3E9A3F4DD859B05237EB7E2283E42EAC8042E7DF061C8E2C53CEAAFF8861887DEDDAF55C103CC593 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTUPjIg1_i6t8kCHKm459WxZbgjD-A.woff
Preview:	wOFF.....9(.....GDEF.....+.....1GPOS.....?....".YtQGSUB..B.....OS/2..G....S...`W@.ocmap..G.....7cvt ..O....e....5=..fpgm..Pd...F...mM$.\|gasp..V. .....glyf..V.....0....Bhead...`...6...6..].hhea.....#...$....hmtx.....e8..loca.....x.....Omaxp...P... ... ...Pname...p.....L3.O.post...l...U..(.rZClprep.....K..x...3.XQ... ....m..m...&.m....\4k.{.....Yy..E.....fkp...v.....f?....K...b.....n....._..."^.[x.?.W..DO.dO...0W)....T...*VW.....DM...a...Vj.....U_..8R.p.&....9Z.....k3n.6...W.....Q...:..t....^....[xG.....S=..z. /....=~.7....K...b..1CY..|.....9l....'j`!..M.`...].?!..C.{9!.<....xOE..Q7.x..W.t+9.....1....v.....Y....O.W.yo...JO=...#..j.....=.dT.z....W_...cgD .a.k6....K... F.U.....=m.w.....w. .L[.!k.(.).1b.9..}^..3_5...b.O~.!."..itv...U...N..Nb}..0.""}>...yT...O..._...@.#.;..W../.3.....8.o....j.....Hc..{.=...KT.z.....t..b.....4.g.....e.0.Xvs.sc.m.0...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\JTUQjIg1_i6t8kCHKm45_QphzQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 64348, version 1.1
Category:	downloaded
Size (bytes):	64348
Entropy (8bit):	**7.993537722902948**
Encrypted:	**true**
SSDEEP:	1536:aO0GNmWrknJxbtBY5XrJ+F8+yB09vPfJH4wddZKXs3gAvJ2A11CxbxVQSU:T02mWEtcXsC+j5PhRHZKXs3gW2AqnE
MD5:	1405DDA3ABCCD4D62E6BFD51B1B0195C
SHA1:	ACD0C7602DF3A1394E1DB9E0782FFFB7E9FDD75E
SHA-256:	51EDD7F81176C384FDEF0487E8E639285A047592B3DDAB3AA88156D71281AFB3
SHA-512:	2552EE5F87092D6A90CC4029A26763100B42EAF356E5926026CE821AA6A4A445A72D5654467A843DFBEBECB240C5373AA2CE499EB3DEBC4645CD57199726291
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTUQjIg1_i6t8kCHKm45_QphzQ.woff
Preview:	wOFF.....\.....,.....GDEF.....2....X.|GPOS.....8....8..<)GSUB..:.....OOS/2..?....O...`U..-cmap..@.....3cvt ..H$...\....,...fpgm..H....F...mM$.|gasp..N..... ...glyf..N....B..+..a.head.....6...6.0.Yhhea...L... ...$....hmtx...l...c...../S.loca.....v.....maxp...H... ... ...\name...h.....)JD.post...T...L..(....prep.....K..x.....XQ...s_m.6..v\. V..V..m.E\.\.....Yi..U.....l+q...Sv...=\|`...}./...Y..y.s..5..w.....R\.'._.....,..xL.dLS.s.SI,.2XN.*beU.j.....6Q.l...J.z`o.....5.'j"N.d..i8K.p...Rm.....wj'.....xP....Q..:..t.....]....P...s.....'.... U2f(.s.o..P.7...2\|...Eu,D..I.LV....-$cj.`/+d.G..4...F.S...x.V.hTW.=3wf..g..w..l.vXZ ...JAkk..j.+..qI"`e.EP..\.E.R.B...R...%."....,...a..A...p.3.O&j.....s.R.|....;..Fp..1..=..[...s0.-..w..id. {....(.....9:>.....=...`d$.9.....o~7C...%|...U.....}l.A....g.. ..p..k..[d....w.n.u..1.j...zkk...;z.h<..l..F.^...*n.!=...llm..K(.'..*...H

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\JTURjIg1_i6t8kCHKm45_aZA7g0[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\JTURjIg1_i6t8kCHKm45_aZA7g0[1].woff	
File Type:	Web Open Font Format, TrueType, length 66532, version 1.1
Category:	downloaded
Size (bytes):	66532
Entropy (8bit):	**7.9921992751304805**
Encrypted:	**true**
SSDEEP:	1536:TeEhZuE0S4CraF8aLdxxxhzTnqgFq4bq9k5MVo/s1SU:THArCGCaLPJzTnlbVMO0R
MD5:	030E8B9B5D28B64486D9F855FB74C135
SHA1:	400B6AF08962BDCEF3B58630993C0E8A6B4B4CCC
SHA-256:	EE76A91D22C4577D6638DE273E0540E21E05E9C189900F54F8993ED0C0043D7B
SHA-512:	EB1CFBC0409E26C2393E6BD2E68E73E0970E9B90E20AFAEE0A8EA0F28E2B9850235B776D4E9A091750B7329B25F69DDFEF55864AC7F4A08A5E04917A322E2C60
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTURjIg1_i6t8kCHKm45_aZA7g0.woff
Preview:	wOFF.....-.....GDEF.....2....X.|GPOS.....=....:....GSUB..@H.....OOS/2..EL...O...`U$.2cmap..E.....3cvt ..M....\....-P.mfpgm..N....F...mM$.|gasp..T T.....glyf..T\.....&..(.lhead...t...6...6.5._hhea..... ...$....hmtx.....F.loca...X...s....~..'maxp..... ... ...Zname.....-ZG.post.....L..(....prep...(.....K..x.....XQ...s_m.6..v \.V..V..m.E\.\.....Yi..U.....I+q...Sv...=\|`...}./...Y..y.s..5..w.....R\.'._....._..xL.dLS.s.SI,.2XN.*beU.j.....6Q.I...J.z`o.....5.'j"N.d..i8K.p...Rm.....wj'.....xP....Q..:..t.....]....P...s.....'.. ..U2f(.s.o..P.7...2\|...Eu,D..I.LV....-$cj.`/+d.G..4...F.S...x..Wep#I.}3..O...Y..333333.>ffffff.[..cf.e.l....15N.Q]..VK.Z...F. .H|.....yo{.0..>...%..a.{.0.8.).c.QE2t..G.s.....!...F.ph...." @.L~..+.....C.....~../...)+...K'.>J...#..Gv..;@...)G<.....1...?.wz.."......(..o...[s|.;v.s z.W.h.HFI.n.`s#6.0.....m|.Z.R..l.2DZ....[...A@..].r`C@....s..?z.d..T

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\YUCJQHG8.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	68892
Entropy (8bit):	5.348751709617085
Encrypted:	false
SSDEEP:	1536:mqP+EVK14syOo/F7y+1vGh9gnDB28CgwPQ0:mMVKBA729gj0
MD5:	F1E96572BE2B73FE1A1AB1F1DBF61BAD
SHA1:	09E360FA90056AB07AFD852CC0FA7A18ADD9D473
SHA-256:	08A5E272DC0697DB4AA7C45FE01675DC28D7656E9BE1A2243B81841DC50F5B8A
SHA-512:	123FA3585E39044877BF848B0BFAE8FC4C591C5E0BD88DE2CE62B0E1E76AD7082C49BAD37CA059E2D9429D4CDF7908238D9475BBE373B999C874DE3721EFD1B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/
Preview:	<!DOCTYPE html>.<html lang="en-US">.<head>..<meta charset="UTF-8" />.<meta http-equiv="X-UA-Compatible" content="IE=edge">..<link rel="pingback" href= "https://yesbaker.com/xmlrpc.php" />...<script type="text/javascript">...document.documentElement.className = 'js';..</script>...<script>var et_site_url='https://yesbaker .com';var et_post_id='205942';function et_core_page_resource_fallback(a,b){"undefined"===typeof b&&(b=a.sheet.cssRules&&0===a.sheet.cssRules.length);b&&(a.onerr or=null,a.onload=null,a.href?a.href=et_site_url+"/?et_core_page_resource="+a.id+et_post_id:a.src&&(a.src=et_site_url+"/?et_core_page_resource="+a.id+et_post_id))}. </script>. Google Tag Manager for WordPress by gtm4wp.com -->.<script data-cfasync="false" data-pagespeed-no-defer>//<![CDATA[..var gtm4wp_datalayer_name = "dataLayer";..var dataLayer = dataLayer || [];// .</script>. End Google Tag Manager for WordPress by gtm4wp.com -->.. This site is optimized with the Yoast SEO plu gin v15.5 - https://yoa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\box-469cf41adb11dc78be68c1ae7f9457a4[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2063
Entropy (8bit):	5.436376937609834
Encrypted:	false
SSDEEP:	48:v0zLZFaTlO5WLpCyYxfoR8OpWNNAc++JRJC62Cgr3ONu:xE5WLpCyYXOczrcriu
MD5:	469CF41ADB11DC78BE68C1AE7F9457A4
SHA1:	063CF0F9171176CF86ADAF36E88558472F6E1001
SHA-256:	66F396314193BFE4809457B6C8004D026E3C503BEFE550E29EA068667F84CE39
SHA-512:	DA8C219B6CD560605D9035575EBE64E7BF85E7AB095C6F3F4BC36FDFCFC75EC0F480970FF7259312FAA75A47D060512C9DC5B25F53E7E6DCB1B7C7BC04B21D88
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://vars.hotjar.com/box-469cf41adb11dc78be68c1ae7f9457a4.html
Preview:	<!DOCTYPE html>..<html lang="en">.<head>.<meta charset="utf-8"/>.<script>(function(){function h(a){return{get:function(b){var c=JSON.parse(a.getItem(b));return! c||Date.parse(c.expires)<=(new Date).getTime()?(a.removeItem(b),null):c.value},set:function(b,c,m){c={value:c,expires:m.toUTCString()};a.setItem(b,JSON.stringif y(c))},remove:function(b){a.removeItem(b)}}}function d(a,b,c,m,d){this.parseCommand=function(e,g){function h(){var a=JSON.stringify({messageId:k,value:n||!1});w indow.parent.postMessage(a,"*")}var p=s[a],q=e.action,r=e.key,k=e.messageId,f=e.siteId,f=m?r:r+.":"+f,n=e.value,l=e.expiresMinutes||1440*(e.expiresDays||365),t= function(){var a=new Date;a.setTime(a.getTime()+6E4*l);return a}();if(!function(){var a={_hjSet:c,_hjGet:b,_hjRemove:c}[q]||[];return 0<=a.indexOf("*")||0<=a.indexOf(g)}( ))throw Error("Command "+q+" not allowed on key: "+r);switch(q){case "_hjSet":p.set(f,n,t,d);break;case "_hjGet":n=p.get(f);h();break;case "_hjRemove":p.remove(f)}}function k(a){try{var b=J

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\business-07[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1024x684, frames 3
Category:	downloaded
Size (bytes):	28406
Entropy (8bit):	7.93834897101844
Encrypted:	false
SSDEEP:	768:39ASnudiKit6doHA4GSzfGisbBPJ2yuV46fVNAhmDZr:nu8ftl4GS6pbBPJlub9ehmZr
MD5:	ED0D5F57B6911F2B2F2E5F3F1728BDD5
SHA1:	911D7627CB6D3E41B6C98012B88534282833635C
SHA-256:	867F10F2787BA5B7B908FE6676F5C5E9267C328DF75EC24197F7305201B4F2CF
SHA-512:	0C579B42895A0F1AF530F8EDA255204772890E635F1494FA72EFCA9BC306B73FDFCDA22F4CCE72D8FCDB1B7CE180BF26ABB055C5AC796FD0E563E9ABB8581524
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-content/uploads/business-07.jpg
Preview:	......JFIF.....&# #&:*-*-*:X7@77@7XN_MHM_N.nbbn.....&# #&:*-*-*:X7@77@7XN_MHM_N.nbbn.....".....^~]....S.WY+.Vj.k.TQ+,u.)..k`.(`...p.*..*$F.i.Qn.>..\.L....TU]ry.....U..g'd\.fU..dk....5.vX.KF...P.....8&%[Q"..R..u....ed.M.....4d..w\g}K...\....a.d.e..m.D.^z,....]..0..9.9.4.....IF ./..*.....G,...)..d...K....u.pvn+..n.xUI'4;&.R.....).v.J.F.....q.....D.*.@..wJQ.rY.R.6*..G:.S..q..>..Bz.:..!..s.....u.+g%Up.~.0..0s...D.....{.....p`....k.....F...oOE...R.7+8.R.Y.`(6..I.....*....$..P...]....SDb...[d...h..a..U.@s0.y7]M4S=w./OE.z....fS....).BA.G}.q. ....0..0...i.A..IF!.$._9...].y|p..{..n95...2S.....].5.....nB.....CD..%.xy6.BQj.D..s.z.HC.&.....c9..._v..7t...V..y....S.lq..w..`F..U.8.-.d...!..4...bQQ@..E.@C..VK..r...pT.....hS...u.d.E.N.Uf.....f.Z,"B...:.*{..(b..W..N0.....d.....z\3h.N.^.`...../..;.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\comment-reply.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	3035
Entropy (8bit):	5.175892657328079
Encrypted:	false
SSDEEP:	48:Q7A4E/XN5NrU6ma9vQS5S65KATpwAuw1JhlzPnMxysBaOP0Uj11dJaGulyPEwU9b:L3OmmAiAJrPnMxyujjTzaGuJs2yzgUym
MD5:	6D5632A96B45B575263B8CA1751BABD7
SHA1:	A541258E96F7824506B1186B6F69C6E8E2484DB3
SHA-256:	A16DF2F75E04129B12A5FDE7311C7EA9131418080FD3F6BCB2B28CE1FAA2FE8E
SHA-512:	07C468EFF5CCD98EB6B09C31CB98EE50047EB13E26B242F9363323B18EB803A786241409A3DD205AF63D784A970E634D8D85BA69878D2ADD1ED9DBFAB393FC9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-includes/js/comment-reply.min.js?ver=5.6
Preview:	/*! This file is auto-generated */.window.addComment=function(f){var v,I,C,h=f.document,E={commentReplyClass:"comment-reply-link",commentReplyTitleId:"reply-title",cancelReplyId:"cancel-comment-reply-link",commentFormId:"commentform",temporaryFormId:"wp-temp-form-div",parentIdFieldId:"comment_parent",postIdFieldId:"comment_post_ID"},e=f.MutationObserver||f.WebKitMutationObserver||f.MozMutationObserver,i="querySelector"in h&&"addEventListener"in f,n=!!h.documentElement.dataset;function t(){d(),function(){if(!e)return;new e(o).observe(h.body,{childList:!0,subtree:!0})}()}function d(e){if(i&&(v=b(E.cancelReplyId),I=b(E.commentFormId),v)){v.addEventListener("touchstart",l),v.addEventListener("click",l);var t=function(e){if((e.metaKey||e.ctrlKey)&&13===e.keyCode)return I.removeEventListener("keydown",t),e.preventDefault(),I.submit.click(),!1};I&&I.addEventListener("keydown",t);for(var n,d=function(e){var t,n=E.commentReplyClass;e&&e.childNodes||(e=h);t=h.getElementsByClassName?e.getElements

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	2107
Entropy (8bit):	5.157416365408043
Encrypted:	false
SSDEEP:	48:SY3Q1aPY3QEazY3QxMah+Y3QpaBY3QwhaaO1aBOEaxOxMau/OpaiOwhas:SYg1aPYgEazYgxMah+YgpaBYgwhaaO1Q
MD5:	B51BEFB35AC46D7DB5302150AB24FBCB
SHA1:	245763C1414C398C37DA84FBDE17ADAD043C5360
SHA-256:	916880C9AADE8675656754B52744D1B51689B7EFC88D3F88B942BC5A926F8298
SHA-512:	3BACA8D07099994826332773900D63C17E472795ED750ADE3BCFDB4D623B7FCEE9F2CEA60B80B385184D20ED9BFDE2ABA761DBD5137023B247337C1CDECACB7
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 300;. font-display: swap;. src: url(https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKWyV9hlIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/opensans/v18/mem6YaGs126MiZpBA-UFUK0Xdcs.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 600;. font-display: swap;. src: url(https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKXGUdhlIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 700;. font-display: swap;. src: url(https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKWiUNhlIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 800;. font-display: swap;. src: url(https://fonts.gstatic.com/s/opensans

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\css[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	3832
Entropy (8bit):	5.218030373982794
Encrypted:	false
SSDEEP:	96:nOYgS0aKOYg6aUuOYg1aAuOYgEaXOYgXaoOYgxMa4OYgpaNOYgwhacOYgbalOOS9:b3pqAhn7OLNYEorhCsxcpvnLsNLBve
MD5:	5E5B11109E8FA7B0414F304CB3D4CE71
SHA1:	857CE2C460DFBEDAE8C9765B173B900BFF74C0F7
SHA-256:	CFD11DD81E0A46CA8F652BDC4531B78AD423BF4B031449F4659642785A3C4AC0
SHA-512:	FF9781196ADF997077BD0AF60C366B3C1A6ECA808C25E38A8DA269DCC7C4922ED0C7E117B3E49F4DC3439403B1C22D3C26373DB197F000BD442BB3850907B7 A
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Montserrat';. font-style: italic;. font-weight: 100;. font-display: swap;. src: url(https://fonts.gstatic.com/s/montserrat/v15/JTUOjIg1_i 6t8kCHKm459WxZqi7g.woff) format('woff');.}.@font-face {. font-family: 'Montserrat';. font-style: italic;. font-weight: 200;. font-display: swap;. src: url(https://fonts.gstati c.com/s/montserrat/v15/JTUPjIg1_i6t8kCHKm459WxZBg_D-A.woff) format('woff');.}.@font-face {. font-family: 'Montserrat';. font-style: italic;. font-weight: 300;. font-d isplay: swap;. src: url(https://fonts.gstatic.com/s/montserrat/v15/JTUPjIg1_i6t8kCHKm459WxZYgzD-A.woff) format('woff');.}.@font-face {. font-family: 'Montserrat';. font- style: italic;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/montserrat/v15/JTUQjIg1_i6t8kCHKm459WxhzQ.woff) format('woff');.}.@font-face {. font-family: 'Montserrat';. font-style: italic;. font-weight: 500;. font-display: swap;. src: url(https://fonts.gstatic.com/s/m

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\css[3].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	6625
Entropy (8bit):	5.28564245744198
Encrypted:	false
SSDEEP:	192:p3p7AQn/OiNRESryC7xup73zT0tEQMA2nfOEEwrSx6MahJV2:p3xV/hnP+QQ7Rf5/+L
MD5:	06E6AF577CC2B18A333B9169383C52DD
SHA1:	4FAF9D6BF69B7A1084A71AEDB35318369C52B9E4
SHA-256:	77F0754133657912F5F50084056DA6E04C6D920C155427D6C389F55DC0F75485
SHA-512:	188C326F018A84F55C32B0DFDC63BBCA3E67A81229C21D4443D7B0E2F62D95B50C5F4714749B39553857DB1305D9AC4466A70C5E3877ED890EF1318B1CAE40C
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Raleway';. font-style: italic;. font-weight: 100;. font-display: swap;. src: url(https://fonts.gstatic.com/s/raleway/v18/1Pt_g8zYS_SKggPN yCgSQamb1W0lwk4S4WjNPrc.woff) format('woff');.}.@font-face {. font-family: 'Raleway';. font-style: italic;. font-weight: 200;. font-display: swap;. src: url(https:// fonts.gstatic.com/s/raleway/v18/1Pt_g8zYS_SKggPNyCgSQamb1W0lwk4S4ejMPrc.woff) format('woff');.}.@font-face {. font-family: 'Raleway';. font-style: italic;. font- weight: 300;. font-display: swap;. src: url(https://fonts.gstatic.com/s/raleway/v18/1Pt_g8zYS_SKggPNyCgSQamb1W0lwk4S4TbMPrc.woff) format('woff');.}.@font-face {. f ont-family: 'Raleway';. font-style: italic;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/raleway/v18/1Pt_g8zYS_SKggPNyCgSQamb1W0lwk4S 4WjMPrc.woff) format('woff');.}.@font-face {. font-family: 'Raleway';. font-style: italic;. font-weight: 500;. font-display: swap;. src: url(https://fonts.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\css[4].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	6625
Entropy (8bit):	5.28564245744198
Encrypted:	false
SSDEEP:	192:p3p7AQn/OiNRESryC7xup73zT0tEQMA2nfOEEwrSx6MahJV2:p3xV/hnP+QQ7Rf5/+L
MD5:	06E6AF577CC2B18A333B9169383C52DD
SHA1:	4FAF9D6BF69B7A1084A71AEDB35318369C52B9E4
SHA-256:	77F0754133657912F5F50084056DA6E04C6D920C155427D6C389F55DC0F75485
SHA-512:	188C326F018A84F55C32B0DFDC63BBCA3E67A81229C21D4443D7B0E2F62D95B50C5F4714749B39553857DB1305D9AC4466A70C5E3877ED890EF1318B1CAE40C
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Raleway';. font-style: italic;. font-weight: 100;. font-display: swap;. src: url(https://fonts.gstatic.com/s/raleway/v18/1Pt_g8zYS_SKggPN yCgSQamb1W0lwk4S4WjNPrc.woff) format('woff');.}.@font-face {. font-family: 'Raleway';. font-style: italic;. font-weight: 200;. font-display: swap;. src: url(https:// fonts.gstatic.com/s/raleway/v18/1Pt_g8zYS_SKggPNyCgSQamb1W0lwk4S4ejMPrc.woff) format('woff');.}.@font-face {. font-family: 'Raleway';. font-style: italic;. font- weight: 300;. font-display: swap;. src: url(https://fonts.gstatic.com/s/raleway/v18/1Pt_g8zYS_SKggPNyCgSQamb1W0lwk4S4TbMPrc.woff) format('woff');.}.@font-face {. f ont-family: 'Raleway';. font-style: italic;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/raleway/v18/1Pt_g8zYS_SKggPNyCgSQamb1W0lwk4S 4WjMPrc.woff) format('woff');.}.@font-face {. font-family: 'Raleway';. font-style: italic;. font-weight: 500;. font-display: swap;. src: url(https://fonts.

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\dashicons.min[1].css	
Size (bytes):	59010
Entropy (8bit):	6.03688965162806
Encrypted:	false
SSDEEP:	768:oey/Z24B3P3aXOhUzSv16CAyLquqSfurIdUMbs73KO08QSJ2BQH02CRqxMWs5FJq:ox/ZvB/qPWMiquqioMUXQSJYIMW+FJq
MD5:	D5E6CE5103B482FE0A2D355D003E9FFD
SHA1:	504E8BE39E6CF2BA66BF8D80F2C6200E5FE7E6A4
SHA-256:	8273F0538929EDE9599E3CFEA8142A252A7D0CB6DBACB230BF188490DDE79D4B
SHA-512:	D198D458C7FAC95FB443FE4FD6199148BFB33B78184EFA4D8D998768F38C7C7BFC3EF6F992B2593F45A5FD232E9229692309C955DAE7A7E020200723F59432D3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-includes/css/dashicons.min.css?ver=5.6
Preview:	/*! This file is auto-generated */.@font-face{font-family:dashicons;src:url(../fonts/dashicons.eot?99ac726223c749443b642ce33df8b800);src:url(../fonts/dashicons.eot?99ac726223c749443b642ce33df8b800#iefix) format("embedded-opentype"),url("data:application/x-font-woff;charset=utf-8; base64,d09GRgABAAAAAHvwAAsAAAAA3EgAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAABHU1VCAAABCAAAADMAAABCsP6z7U9TLzIAAAE8AAAAQAAAAFZAuk8lY21hcAAAAXwAAAk/AAAU9l+BPsxnbHlmAAAKvAAAYwIAAKlAcWTMRWhlYWQAAG3AAAAALwAAADYXkmaRaGhlYQAAbfAAAAAfAAAAJAQ3A0hobXR4AABuEAAAACUAAAVQpgT/9mxvY2EAAG44AAACqgAAAqps5EEYbWF4cAAAcOQAAAAfAAAAIAJvAKBuYW1lAABxBAAAATAAAAIiwytf8nBvc3QAAHI0AAAJvAAAEhojMlz2eJxjYGRgYOBikGPQYWB0cfMJYeBgYGGAAJAMY05meiJQDMoDyrGAaQ4gZoOIAgCKIwNPAHicY2Bk/Mc4gYGVgYOBhzGNgYHBHUp/ZZBkaGFgYGJgZWbACgLSXFMYHD4yfHVnAnH1mBgZGIE0CDMAAI/zCGl4nN3Y93/eVRnG8c/9JE2bstLdQIF0N8x0t8w0pSMt0BZKS5ml7F32lrL3hlKmCxEQtzjAhQMRRcEJijhQQWV4vgNBGV4nl3+B/mbTd8+reeVJvuc859znvgL0A5pkO2nW3xcJ8qee02ej7/NNDOz7fHPTw/r/LnTo60ale4ooWov2orOYXXQXPWVr2V52lrPL3qq3WlmtqlZXx	

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\et-divi-customizer-global-16097187143931.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	9019
Entropy (8bit):	4.822508935624176
Encrypted:	false
SSDEEP:	192:B6F5f64/DM56miw5a2AEobxfLeC6eOybvIEK+HbX/4xP6zDmqGwHxoMKamTqjEXH:hvhDf
MD5:	4A1414EB01994D06B3A2456246E21C3C
SHA1:	EFEF716F3F21C0F4592862E75DA833EBA2C2D99F
SHA-256:	D876CE5A034BC3B9EB4DF02BCA5D08348A96B39F62547665FE4EB487AAF35FD2
SHA-512:	C1F63FEFBB807A4DD72AEA8B30227C0C350B38CD2FC779719117FFA52487F15E26921B8EF58025492E14027BBC2794E79A3BC4CDCFCD543F5E2368650C613C0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://yesbaker.com/wp-content/et-cache/global/et-divi-customizer-global-16097187143931.min.css
Preview:	.woocommerce #respond input#submit,.woocommerce-page #respond input#submit,.woocommerce #content input.button,.woocommerce-page #content input.button,.woocommerce-message,.woocommerce-error,.woocommerce-info{background:#2EA3F2!important}#et_search_icon:hover,.mobile_menu_bar:before,.mobile_menu_bar:after,.et_toggle_slide_menu:after,.et-social-icon a:hover,.et_pb_sum,.et_pb_pricing li a,.et_pb_pricing_table_button,.et_overlay:before,.entry-summary p.price ins,.woocommerce div.product span.price,.woocommerce-page div.product span.price,.woocommerce #content div.product span.price,.woocommerce-page #content div.product span.price,.woocommerce div.product p.price,.woocommerce-page div.product p.price,.woocommerce #content div.product p.price,.woocommerce-page #content div.product p.price,.et_pb_member_social_links a:hover,.woocommerce .star-rating span:before,.woocommerce-page .star-rating span:before,.et_pb_widget li a:hover,.et_pb_filterable_portfolio .et_pb_portfolio_filters li a.active

Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 102

- 53 (DNS)
- 443 (HTTPS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 03:09:23.121290922 CET	49682	443	192.168.2.3	35.209.233.145
Jan 14, 2021 03:09:23.121841908 CET	49683	443	192.168.2.3	35.209.233.145
Jan 14, 2021 03:09:23.274369001 CET	443	49682	35.209.233.145	192.168.2.3
Jan 14, 2021 03:09:23.274650097 CET	49682	443	192.168.2.3	35.209.233.145
Jan 14, 2021 03:09:23.277312994 CET	443	49683	35.209.233.145	192.168.2.3
Jan 14, 2021 03:09:23.277553082 CET	49683	443	192.168.2.3	35.209.233.145
Jan 14, 2021 03:09:23.288024902 CET	49682	443	192.168.2.3	35.209.233.145
Jan 14, 2021 03:09:23.288259983 CET	49683	443	192.168.2.3	35.209.233.145
Jan 14, 2021 03:09:23.441072941 CET	443	49682	35.209.233.145	192.168.2.3
Jan 14, 2021 03:09:23.443676949 CET	443	49683	35.209.233.145	192.168.2.3
Jan 14, 2021 03:09:23.443808079 CET	443	49682	35.209.233.145	192.168.2.3
Jan 14, 2021 03:09:23.443852901 CET	443	49682	35.209.233.145	192.168.2.3
Jan 14, 2021 03:09:23.443883896 CET	443	49682	35.209.233.145	192.168.2.3
Jan 14, 2021 03:09:23.443995953 CET	49682	443	192.168.2.3	35.209.233.145
Jan 14, 2021 03:09:23.444046974 CET	49682	443	192.168.2.3	35.209.233.145
Jan 14, 2021 03:09:23.447737932 CET	443	49683	35.209.233.145	192.168.2.3
Jan 14, 2021 03:09:23.447781086 CET	443	49683	35.209.233.145	192.168.2.3
Jan 14, 2021 03:09:23.447810888 CET	443	49683	35.209.233.145	192.168.2.3
Jan 14, 2021 03:09:23.447995901 CET	49683	443	192.168.2.3	35.209.233.145
Jan 14, 2021 03:09:23.448050976 CET	49683	443	192.168.2.3	35.209.233.145
Jan 14, 2021 03:09:23.486381054 CET	49682	443	192.168.2.3	35.209.233.145
Jan 14, 2021 03:09:23.486588955 CET	49683	443	192.168.2.3	35.209.233.145
Jan 14, 2021 03:09:23.491969109 CET	49682	443	192.168.2.3	35.209.233.145
Jan 14, 2021 03:09:23.492117882 CET	49683	443	192.168.2.3	35.209.233.145
Jan 14, 2021 03:09:23.492167950 CET	49682	443	192.168.2.3	35.209.233.145
Jan 14, 2021 03:09:23.640862942 CET	443	49682	35.209.233.145	192.168.2.3
Jan 14, 2021 03:09:23.640911102 CET	443	49682	35.209.233.145	192.168.2.3
Jan 14, 2021 03:09:23.640958071 CET	49682	443	192.168.2.3	35.209.233.145
Jan 14, 2021 03:09:23.641001940 CET	49682	443	192.168.2.3	35.209.233.145
Jan 14, 2021 03:09:23.641741991 CET	49682	443	192.168.2.3	35.209.233.145
Jan 14, 2021 03:09:23.644074917 CET	443	49683	35.209.233.145	192.168.2.3
Jan 14, 2021 03:09:23.644195080 CET	49683	443	192.168.2.3	35.209.233.145
Jan 14, 2021 03:09:23.644268036 CET	443	49683	35.209.233.145	192.168.2.3
Jan 14, 2021 03:09:23.644341946 CET	49683	443	192.168.2.3	35.209.233.145
Jan 14, 2021 03:09:23.644742966 CET	49683	443	192.168.2.3	35.209.233.145
Jan 14, 2021 03:09:23.644856930 CET	443	49682	35.209.233.145	192.168.2.3
Jan 14, 2021 03:09:23.647731066 CET	443	49683	35.209.233.145	192.168.2.3
Jan 14, 2021 03:09:23.647806883 CET	49683	443	192.168.2.3	35.209.233.145
Jan 14, 2021 03:09:23.650078058 CET	443	49682	35.209.233.145	192.168.2.3
Jan 14, 2021 03:09:23.650173903 CET	49682	443	192.168.2.3	35.209.233.145
Jan 14, 2021 03:09:23.734896898 CET	443	49682	35.209.233.145	192.168.2.3
Jan 14, 2021 03:09:23.735105991 CET	49682	443	192.168.2.3	35.209.233.145
Jan 14, 2021 03:09:23.825248003 CET	49684	443	192.168.2.3	104.21.19.250
Jan 14, 2021 03:09:23.826056957 CET	49685	443	192.168.2.3	104.21.19.250

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 03:09:23.834975958 CET	443	49682	35.209.233.145	192.168.2.3
Jan 14, 2021 03:09:23.840832949 CET	443	49683	35.209.233.145	192.168.2.3
Jan 14, 2021 03:09:23.865590096 CET	443	49684	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:23.865714073 CET	49684	443	192.168.2.3	104.21.19.250
Jan 14, 2021 03:09:23.866079092 CET	443	49685	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:23.866169930 CET	49685	443	192.168.2.3	104.21.19.250
Jan 14, 2021 03:09:23.866389990 CET	49684	443	192.168.2.3	104.21.19.250
Jan 14, 2021 03:09:23.867476940 CET	49685	443	192.168.2.3	104.21.19.250
Jan 14, 2021 03:09:23.906567097 CET	443	49684	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:23.907486916 CET	443	49685	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:23.909178972 CET	443	49684	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:23.909221888 CET	443	49684	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:23.909311056 CET	49684	443	192.168.2.3	104.21.19.250
Jan 14, 2021 03:09:23.909362078 CET	49684	443	192.168.2.3	104.21.19.250
Jan 14, 2021 03:09:23.911052942 CET	443	49685	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:23.911102057 CET	443	49685	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:23.911123037 CET	49685	443	192.168.2.3	104.21.19.250
Jan 14, 2021 03:09:23.911174059 CET	49685	443	192.168.2.3	104.21.19.250
Jan 14, 2021 03:09:23.921829939 CET	49684	443	192.168.2.3	104.21.19.250
Jan 14, 2021 03:09:23.922236919 CET	49684	443	192.168.2.3	104.21.19.250
Jan 14, 2021 03:09:23.922451019 CET	49684	443	192.168.2.3	104.21.19.250
Jan 14, 2021 03:09:23.924309969 CET	49685	443	192.168.2.3	104.21.19.250
Jan 14, 2021 03:09:23.924628973 CET	49685	443	192.168.2.3	104.21.19.250
Jan 14, 2021 03:09:23.962281942 CET	443	49684	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:23.962331057 CET	443	49684	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:23.962358952 CET	443	49684	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:23.962397099 CET	443	49684	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:23.962414980 CET	49684	443	192.168.2.3	104.21.19.250
Jan 14, 2021 03:09:23.962426901 CET	443	49684	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:23.962465048 CET	49684	443	192.168.2.3	104.21.19.250
Jan 14, 2021 03:09:23.962488890 CET	49684	443	192.168.2.3	104.21.19.250
Jan 14, 2021 03:09:23.962563992 CET	443	49684	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:23.964432001 CET	443	49685	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:23.964586020 CET	443	49685	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:23.965064049 CET	443	49685	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:23.965094090 CET	443	49685	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:23.965132952 CET	49685	443	192.168.2.3	104.21.19.250
Jan 14, 2021 03:09:23.965178967 CET	49685	443	192.168.2.3	104.21.19.250
Jan 14, 2021 03:09:23.978748083 CET	49684	443	192.168.2.3	104.21.19.250
Jan 14, 2021 03:09:23.978864908 CET	49685	443	192.168.2.3	104.21.19.250
Jan 14, 2021 03:09:24.019117117 CET	443	49685	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:24.019171953 CET	443	49684	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:25.640331984 CET	443	49684	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:25.640386105 CET	443	49684	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:25.640417099 CET	443	49684	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:25.640438080 CET	443	49684	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:25.640476942 CET	443	49684	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:25.640516043 CET	443	49684	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:25.640543938 CET	443	49684	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:25.640589952 CET	443	49684	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:25.640633106 CET	443	49684	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:25.640661955 CET	49684	443	192.168.2.3	104.21.19.250
Jan 14, 2021 03:09:25.640671015 CET	443	49684	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:25.640707016 CET	49684	443	192.168.2.3	104.21.19.250
Jan 14, 2021 03:09:25.640712023 CET	443	49684	104.21.19.250	192.168.2.3
Jan 14, 2021 03:09:25.640712976 CET	49684	443	192.168.2.3	104.21.19.250

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 03:09:21.843089104 CET	51904	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:21.902811050 CET	53	51904	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:22.944227934 CET	61328	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:23.112231970 CET	53	61328	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 03:09:23.745858908 CET	54130	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:23.822630882 CET	53	54130	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:25.987453938 CET	56961	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:25.998631954 CET	59353	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:26.014602900 CET	52238	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:26.051857948 CET	53	56961	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:26.070725918 CET	53	52238	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:26.073196888 CET	53	59353	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:26.994606018 CET	49873	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:26.997210026 CET	53196	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:27.000761032 CET	56777	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:27.007852077 CET	58643	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:27.055648088 CET	53	53196	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:27.059648037 CET	53	49873	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:27.061135054 CET	53	56777	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:27.074924946 CET	53	58643	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:27.431196928 CET	60985	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:27.480423927 CET	53	60985	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:27.918989897 CET	50200	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:27.948237896 CET	51281	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:27.948721886 CET	49199	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:27.954062939 CET	50620	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:27.976717949 CET	53	50200	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:28.010464907 CET	53	51281	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:28.011235952 CET	53	50620	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:28.012501955 CET	53	49199	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:28.306406975 CET	64938	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:28.366729021 CET	53	64938	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:28.391819954 CET	60152	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:28.395975113 CET	57544	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:28.450545073 CET	53	60152	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:28.454330921 CET	53	57544	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:28.672813892 CET	55984	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:28.723609924 CET	53	55984	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:29.143764973 CET	64185	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:29.202166080 CET	53	64185	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:29.254476070 CET	65110	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:29.302273989 CET	53	65110	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:29.377796888 CET	58361	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:29.436702967 CET	53	58361	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:30.487988949 CET	63492	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:30.538652897 CET	53	63492	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:30.717384100 CET	60831	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:30.807003021 CET	53	60831	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:47.932384014 CET	60100	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:47.993128061 CET	53	60100	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:51.860797882 CET	53195	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:52.639834881 CET	50141	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:52.699125051 CET	53	50141	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:52.903315067 CET	53195	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:52.951138973 CET	53	53195	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:53.652623892 CET	50141	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:53.703459024 CET	53	50141	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:53.920527935 CET	53195	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:53.968601942 CET	53	53195	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:54.661634922 CET	53023	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:54.668334007 CET	50141	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:54.718297958 CET	53	53023	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:54.719011068 CET	53	50141	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:55.934286118 CET	53195	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:55.983236074 CET	53	53195	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:56.668371916 CET	50141	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:09:56.727902889 CET	53	50141	8.8.8.8	192.168.2.3
Jan 14, 2021 03:09:59.950830936 CET	53195	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 03:10:00.007261038 CET	53	53195	8.8.8.8	192.168.2.3
Jan 14, 2021 03:10:00.681968927 CET	50141	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:10:00.732690096 CET	53	50141	8.8.8.8	192.168.2.3
Jan 14, 2021 03:10:07.530255079 CET	49563	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:10:07.578190088 CET	53	49563	8.8.8.8	192.168.2.3
Jan 14, 2021 03:10:39.940541983 CET	51352	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:10:39.994538069 CET	53	51352	8.8.8.8	192.168.2.3
Jan 14, 2021 03:10:56.868294001 CET	59349	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:10:56.926875114 CET	53	59349	8.8.8.8	192.168.2.3
Jan 14, 2021 03:10:58.409872055 CET	57084	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:10:58.466155052 CET	53	57084	8.8.8.8	192.168.2.3
Jan 14, 2021 03:10:59.887723923 CET	58823	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:11:00.918324947 CET	58823	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:11:01.798785925 CET	53	58823	8.8.8.8	192.168.2.3
Jan 14, 2021 03:11:03.502825975 CET	57568	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:11:03.560570002 CET	53	57568	8.8.8.8	192.168.2.3
Jan 14, 2021 03:11:04.555740118 CET	50540	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:11:04.615164995 CET	53	50540	8.8.8.8	192.168.2.3
Jan 14, 2021 03:11:05.695971966 CET	54366	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:11:05.744100094 CET	53	54366	8.8.8.8	192.168.2.3
Jan 14, 2021 03:11:07.803446054 CET	53034	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:11:07.862066984 CET	53	53034	8.8.8.8	192.168.2.3
Jan 14, 2021 03:11:10.358455896 CET	57762	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:11:10.414985895 CET	53	57762	8.8.8.8	192.168.2.3
Jan 14, 2021 03:11:11.539604902 CET	55435	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:11:11.587335110 CET	53	55435	8.8.8.8	192.168.2.3
Jan 14, 2021 03:11:20.544790030 CET	50713	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:11:20.595668077 CET	53	50713	8.8.8.8	192.168.2.3
Jan 14, 2021 03:11:22.126482010 CET	56132	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:11:22.180268049 CET	53	56132	8.8.8.8	192.168.2.3
Jan 14, 2021 03:11:26.291150093 CET	58987	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:11:26.339131117 CET	53	58987	8.8.8.8	192.168.2.3
Jan 14, 2021 03:11:27.440299034 CET	56579	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:11:27.488343000 CET	53	56579	8.8.8.8	192.168.2.3
Jan 14, 2021 03:11:28.375327110 CET	60633	53	192.168.2.3	8.8.8.8
Jan 14, 2021 03:11:28.433839083 CET	53	60633	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2021 03:09:22.944227934 CET	192.168.2.3	8.8.8.8	0xeb14	Standard query (0)	clubfluent.com	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:23.745858908 CET	192.168.2.3	8.8.8.8	0x32fc	Standard query (0)	yesbaker.com	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:25.998631954 CET	192.168.2.3	8.8.8.8	0xdbaa	Standard query (0)	52718bdd550f7e11001c-3fe6492d1c83a22b9f69f88454beb1f4.ssl.cf5.rackcdn.com	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:26.014602900 CET	192.168.2.3	8.8.8.8	0x900b	Standard query (0)	s3.amazonaws.com	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:26.997210026 CET	192.168.2.3	8.8.8.8	0x41fd	Standard query (0)	v2.zopim.com	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:27.000761032 CET	192.168.2.3	8.8.8.8	0x81c	Standard query (0)	chimpstatic.com	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:27.431196928 CET	192.168.2.3	8.8.8.8	0x7bba	Standard query (0)	static.zdassets.com	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:27.918989897 CET	192.168.2.3	8.8.8.8	0x9e47	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:27.948237896 CET	192.168.2.3	8.8.8.8	0x12c5	Standard query (0)	static.hotjar.com	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:27.954062939 CET	192.168.2.3	8.8.8.8	0xa398	Standard query (0)	a.quora.com	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:28.306406975 CET	192.168.2.3	8.8.8.8	0xdb40	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:28.391819954 CET	192.168.2.3	8.8.8.8	0xa73f	Standard query (0)	q.quora.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2021 03:09:28.395975113 CET	192.168.2.3	8.8.8.8	0xf9f4	Standard query (0)	script.hotjar.com	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:28.672813892 CET	192.168.2.3	8.8.8.8	0x9bf3	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:29.143764973 CET	192.168.2.3	8.8.8.8	0x30a	Standard query (0)	vars.hotjar.com	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:29.254476070 CET	192.168.2.3	8.8.8.8	0x7804	Standard query (0)	ekr.zdassets.com	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:29.377796888 CET	192.168.2.3	8.8.8.8	0x3e2b	Standard query (0)	in.hotjar.com	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:30.487988949 CET	192.168.2.3	8.8.8.8	0x89d6	Standard query (0)	widget-mediator.zopim.com	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:30.717384100 CET	192.168.2.3	8.8.8.8	0x2c58	Standard query (0)	help.yesbaker.com	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:54.661634922 CET	192.168.2.3	8.8.8.8	0xbc71	Standard query (0)	yesbaker.com	A (IP address)	IN (0x0001)
Jan 14, 2021 03:10:39.940541983 CET	192.168.2.3	8.8.8.8	0xb472	Standard query (0)	s.w.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2021 03:09:23.112231970 CET	8.8.8.8	192.168.2.3	0xeb14	No error (0)	clubfluent.com		35.209.233.145	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:23.822630882 CET	8.8.8.8	192.168.2.3	0x32fc	No error (0)	yesbaker.com		104.21.19.250	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:23.822630882 CET	8.8.8.8	192.168.2.3	0x32fc	No error (0)	yesbaker.com		172.67.190.180	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:26.070725918 CET	8.8.8.8	192.168.2.3	0x900b	No error (0)	s3.amazonaws.com		52.216.139.125	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:26.073196888 CET	8.8.8.8	192.168.2.3	0xdbaa	No error (0)	52718bdd550f7e11001c-3fe6492d1c83a22b9f69f88454beb1f4.ssl.cf5.rackcdn.com	cf5.rackcdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 03:09:27.055648088 CET	8.8.8.8	192.168.2.3	0x41fd	No error (0)	v2.zopim.com		104.16.104.139	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:27.055648088 CET	8.8.8.8	192.168.2.3	0x41fd	No error (0)	v2.zopim.com		104.16.107.139	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:27.055648088 CET	8.8.8.8	192.168.2.3	0x41fd	No error (0)	v2.zopim.com		104.16.105.139	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:27.055648088 CET	8.8.8.8	192.168.2.3	0x41fd	No error (0)	v2.zopim.com		104.16.106.139	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:27.055648088 CET	8.8.8.8	192.168.2.3	0x41fd	No error (0)	v2.zopim.com		104.16.103.139	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:27.061135054 CET	8.8.8.8	192.168.2.3	0x81c	No error (0)	chimpstatic.com		104.83.125.218	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:27.480423927 CET	8.8.8.8	192.168.2.3	0x7bba	No error (0)	static.zdassets.com	cf.zdassets.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 03:09:27.480423927 CET	8.8.8.8	192.168.2.3	0x7bba	No error (0)	cf.zdassets.com		104.18.70.113	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:27.480423927 CET	8.8.8.8	192.168.2.3	0x7bba	No error (0)	cf.zdassets.com		104.18.71.113	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:27.976717949 CET	8.8.8.8	192.168.2.3	0x9e47	No error (0)	snap.licdn.com	wildcard.licdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 03:09:28.010464907 CET	8.8.8.8	192.168.2.3	0x12c5	No error (0)	static.hotjar.com	static-cdn.hotjar.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 03:09:28.010464907 CET	8.8.8.8	192.168.2.3	0x12c5	No error (0)	static-cdn.hotjar.com		13.224.94.124	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2021 03:09:28.010464907 CET	8.8.8.8	192.168.2.3	0x12c5	No error (0)	static-cdn .hotjar.com		13.224.94.96	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:28.010464907 CET	8.8.8.8	192.168.2.3	0x12c5	No error (0)	static-cdn .hotjar.com		13.224.94.45	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:28.010464907 CET	8.8.8.8	192.168.2.3	0x12c5	No error (0)	static-cdn .hotjar.com		13.224.94.98	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:28.011235952 CET	8.8.8.8	192.168.2.3	0xa398	No error (0)	a.quora.com	quora.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 03:09:28.011235952 CET	8.8.8.8	192.168.2.3	0xa398	No error (0)	quora.map. fastly.net		151.101.1.2	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:28.011235952 CET	8.8.8.8	192.168.2.3	0xa398	No error (0)	quora.map. fastly.net		151.101.65.2	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:28.011235952 CET	8.8.8.8	192.168.2.3	0xa398	No error (0)	quora.map. fastly.net		151.101.129.2	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:28.011235952 CET	8.8.8.8	192.168.2.3	0xa398	No error (0)	quora.map. fastly.net		151.101.193.2	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:28.366729021 CET	8.8.8.8	192.168.2.3	0xdb40	No error (0)	px.ads.lin kedin.com	mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 03:09:28.366729021 CET	8.8.8.8	192.168.2.3	0xdb40	No error (0)	mix.linkedin.com	pop-efr5.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 03:09:28.366729021 CET	8.8.8.8	192.168.2.3	0xdb40	No error (0)	pop-efr5.m ix.linkedin.com		185.63.145.5	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:28.450545073 CET	8.8.8.8	192.168.2.3	0xa73f	No error (0)	q.quora.com		3.213.100.238	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:28.450545073 CET	8.8.8.8	192.168.2.3	0xa73f	No error (0)	q.quora.com		3.214.152.179	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:28.450545073 CET	8.8.8.8	192.168.2.3	0xa73f	No error (0)	q.quora.com		3.227.227.165	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:28.450545073 CET	8.8.8.8	192.168.2.3	0xa73f	No error (0)	q.quora.com		3.217.219.88	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:28.450545073 CET	8.8.8.8	192.168.2.3	0xa73f	No error (0)	q.quora.com		3.230.50.184	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:28.450545073 CET	8.8.8.8	192.168.2.3	0xa73f	No error (0)	q.quora.com		50.17.2.180	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:28.450545073 CET	8.8.8.8	192.168.2.3	0xa73f	No error (0)	q.quora.com		3.225.115.141	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:28.454330921 CET	8.8.8.8	192.168.2.3	0xf9f4	No error (0)	script.hotjar.com		13.224.94.39	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:28.454330921 CET	8.8.8.8	192.168.2.3	0xf9f4	No error (0)	script.hotjar.com		13.224.94.37	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:28.454330921 CET	8.8.8.8	192.168.2.3	0xf9f4	No error (0)	script.hotjar.com		13.224.94.35	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:28.454330921 CET	8.8.8.8	192.168.2.3	0xf9f4	No error (0)	script.hotjar.com		13.224.94.93	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:28.723609924 CET	8.8.8.8	192.168.2.3	0x9bf3	No error (0)	www.linked in.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 03:09:29.202166080 CET	8.8.8.8	192.168.2.3	0x30a	No error (0)	vars.hotjar.com		13.224.94.36	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:29.202166080 CET	8.8.8.8	192.168.2.3	0x30a	No error (0)	vars.hotjar.com		13.224.94.108	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:29.202166080 CET	8.8.8.8	192.168.2.3	0x30a	No error (0)	vars.hotjar.com		13.224.94.30	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2021 03:09:29.202166080 CET	8.8.8.8	192.168.2.3	0x30a	No error (0)	vars.hotjar.com		13.224.94.105	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:29.302273989 CET	8.8.8.8	192.168.2.3	0x7804	No error (0)	ekr.zdassets.com	cf.zdassets.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 03:09:29.302273989 CET	8.8.8.8	192.168.2.3	0x7804	No error (0)	cf.zdassets.com		104.18.70.113	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:29.302273989 CET	8.8.8.8	192.168.2.3	0x7804	No error (0)	cf.zdassets.com		104.18.71.113	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:29.436702967 CET	8.8.8.8	192.168.2.3	0x3e2b	No error (0)	in.hotjar.com	in-live.live.eks.hotjar.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 03:09:29.436702967 CET	8.8.8.8	192.168.2.3	0x3e2b	No error (0)	in-live.live.eks.hotjar.com		52.49.237.17	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:29.436702967 CET	8.8.8.8	192.168.2.3	0x3e2b	No error (0)	in-live.live.eks.hotjar.com		52.19.70.84	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:29.436702967 CET	8.8.8.8	192.168.2.3	0x3e2b	No error (0)	in-live.live.eks.hotjar.com		34.252.74.75	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:29.436702967 CET	8.8.8.8	192.168.2.3	0x3e2b	No error (0)	in-live.live.eks.hotjar.com		52.18.148.102	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:29.436702967 CET	8.8.8.8	192.168.2.3	0x3e2b	No error (0)	in-live.live.eks.hotjar.com		52.51.23.49	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:29.436702967 CET	8.8.8.8	192.168.2.3	0x3e2b	No error (0)	in-live.live.eks.hotjar.com		63.33.16.37	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:29.436702967 CET	8.8.8.8	192.168.2.3	0x3e2b	No error (0)	in-live.live.eks.hotjar.com		18.203.1.140	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:29.436702967 CET	8.8.8.8	192.168.2.3	0x3e2b	No error (0)	in-live.live.eks.hotjar.com		54.171.249.106	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:30.538652897 CET	8.8.8.8	192.168.2.3	0x89d6	No error (0)	widget-mediator.zopim.com		3.125.55.38	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:30.538652897 CET	8.8.8.8	192.168.2.3	0x89d6	No error (0)	widget-mediator.zopim.com		54.93.73.12	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:30.538652897 CET	8.8.8.8	192.168.2.3	0x89d6	No error (0)	widget-mediator.zopim.com		18.195.130.25	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:30.538652897 CET	8.8.8.8	192.168.2.3	0x89d6	No error (0)	widget-mediator.zopim.com		18.159.81.166	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:30.538652897 CET	8.8.8.8	192.168.2.3	0x89d6	No error (0)	widget-mediator.zopim.com		18.196.236.175	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:30.538652897 CET	8.8.8.8	192.168.2.3	0x89d6	No error (0)	widget-mediator.zopim.com		3.120.194.189	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:30.538652897 CET	8.8.8.8	192.168.2.3	0x89d6	No error (0)	widget-mediator.zopim.com		52.29.215.52	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:30.538652897 CET	8.8.8.8	192.168.2.3	0x89d6	No error (0)	widget-mediator.zopim.com		35.158.236.168	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:30.807003021 CET	8.8.8.8	192.168.2.3	0x2c58	No error (0)	help.yesbaker.com	elb55.freshdesk.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 03:09:30.807003021 CET	8.8.8.8	192.168.2.3	0x2c58	No error (0)	elb55.freshdesk.com		52.0.36.54	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:30.807003021 CET	8.8.8.8	192.168.2.3	0x2c58	No error (0)	elb55.freshdesk.com		54.175.198.198	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:30.807003021 CET	8.8.8.8	192.168.2.3	0x2c58	No error (0)	elb55.freshdesk.com		35.175.28.23	A (IP address)	IN (0x0001)
Jan 14, 2021 03:09:54.718297958 CET	8.8.8.8	192.168.2.3	0xbc71	No error (0)	yesbaker.com		104.21.19.250	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2021 03:09:54.718297958 CET	8.8.8.8	192.168.2.3	0xbc71	No error (0)	yesbaker.com		172.67.190.180	A (IP address)	IN (0x0001)
Jan 14, 2021 03:10:39.994538069 CET	8.8.8.8	192.168.2.3	0xb472	No error (0)	s.w.org		192.0.77.48	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 14, 2021 03:09:23.443852901 CET	35.209.233.145	443	192.168.2.3	49682	CN=clubfluent.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Jan 03 19:43:49 CET 2021	Sat Apr 03 20:43:49 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
							Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Jan 14, 2021 03:09:23.447781086 CET	35.209.233.145	443	192.168.2.3	49683	CN=clubfluent.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Jan 03 19:43:49 CET 2021	Sat Apr 03 20:43:49 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
							Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Jan 14, 2021 03:09:23.909221888 CET	104.21.19.250	443	192.168.2.3	49684	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sun Aug 02 02:00:00 CEST 2020	Mon Aug 02 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
							Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 14, 2021 03:09:23.911102057 CET	104.21.19.250	443	192.168.2.3	49685	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sun Aug 02 02:00:00 CEST 2020	Mon Aug 02 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
							Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 14, 2021 03:09:26.330893040 CET	52.216.139.125	443	192.168.2.3	49690	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020	Mon Aug 09 14:00:00 CEST 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
							Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Jan 14, 2021 03:09:26.330929995 CET	52.216.139.125	443	192.168.2.3	49691	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Jan 14, 2021 03:09:27.293512106 CET	104.16.104.139	443	192.168.2.3	49703	CN=*.zopim.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sat May 30 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Mon May 31 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jan 14, 2021 03:09:27.293816090 CET	104.16.104.139	443	192.168.2.3	49702	CN=*.zopim.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sat May 30 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Mon May 31 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jan 14, 2021 03:09:27.374800920 CET	104.83.125.218	443	192.168.2.3	49700	CN=wildcardsan.us15.list-manage.com, OU=IT, O="The Rocket Science Group, LLC", L=Atlanta, ST=Georgia, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Nov 21 01:00:00 CET 2019 Fri Mar 08 13:00:00 CET 2013	Fri Feb 19 13:00:00 CET 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jan 14, 2021 03:09:27.394531965 CET	104.83.125.218	443	192.168.2.3	49701	CN=wildcardsan.us15.list-manage.com, OU=IT, O="The Rocket Science Group, LLC", L=Atlanta, ST=Georgia, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	Thu Nov 21 01:00:00 CET 2019	Fri Feb 19 13:00:00 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jan 14, 2021 03:09:27.565457106 CET	104.18.70.113	443	192.168.2.3	49704	CN=ssl911790.cloudflaressl.com CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Oct 28 01:00:00 CET 2020 Thu Sep 25 02:00:00 CEST 2014 Thu Jan 01 01:00:00 CET 2004	Fri May 07 01:59:59 CEST 2021 Tue Sep 25 01:59:59 CEST 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Sep 25 02:00:00 CEST 2014	Tue Sep 25 01:59:59 CEST 2029		
					CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jan 14, 2021 03:09:27.570060015 CET	104.18.70.113	443	192.168.2.3	49705	CN=ssl911790.cloudflaressl.com CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Oct 28 01:00:00 CET 2020 Thu Sep 25 02:00:00 CEST 2014 Thu Jan 01 01:00:00 CET 2004	Fri May 07 01:59:59 CEST 2021 Tue Sep 25 01:59:59 CEST 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Sep 25 02:00:00 CEST 2014	Tue Sep 25 01:59:59 CEST 2029		
					CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 14, 2021 03:09:28.108335972 CET	13.224.94.124	443	192.168.2.3	49708	CN=*.hotjar.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Dec 25 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jan 24 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 14, 2021 03:09:28.115055084 CET	151.101.1.2	443	192.168.2.3	49710	CN=quora.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Dec 27 18:16:54 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Sat Mar 27 18:16:54 CET 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Jan 14, 2021 03:09:28.122225046 CET	13.224.94.124	443	192.168.2.3	49711	CN=*.hotjar.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Dec 25 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jan 24 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 14, 2021 03:09:28.122628927 CET	151.101.1.2	443	192.168.2.3	49713	CN=quora.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Dec 27 18:16:54 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Sat Mar 27 18:16:54 CET 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Jan 14, 2021 03:09:28.488298893 CET	185.63.145.5	443	192.168.2.3	49714	CN=px.ads.linkedin.com, O=LinkedIn Corporation, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jan 06 01:00:00 CET 2021 Wed Sep 23 02:00:00 CEST 2020	Tue Jul 06 01:59:59 CEST 2021 Mon Sep 23 01:59:59 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
Jan 14, 2021 03:09:28.489229918 CET	185.63.145.5	443	192.168.2.3	49715	CN=px.ads.linkedin.com, O=LinkedIn Corporation, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jan 06 01:00:00 CET 2021 Wed Sep 23 02:00:00 CEST 2020	Tue Jul 06 01:59:59 CEST 2021 Mon Sep 23 01:59:59 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
Jan 14, 2021 03:09:28.550750971 CET	13.224.94.39	443	192.168.2.3	49718	CN=*.hotjar.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Dec 25 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jan 24 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 14, 2021 03:09:28.551461935 CET	13.224.94.39	443	192.168.2.3	49719	CN=*.hotjar.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Dec 25 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jan 24 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 14, 2021 03:09:28.706340075 CET	3.213.100.238	443	192.168.2.3	49716	CN=*.quora.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Dec 27 18:16:22 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Sat Mar 27 18:16:22 CET 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Jan 14, 2021 03:09:28.707135916 CET	3.213.100.238	443	192.168.2.3	49717	CN=*.quora.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Dec 27 18:16:22 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Sat Mar 27 18:16:22 CET 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 14, 2021 03:09:29.298796892 CET	13.224.94.36	443	192.168.2.3	49723	CN=*.hotjar.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Dec 25 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jan 24 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 14, 2021 03:09:29.298847914 CET	13.224.94.36	443	192.168.2.3	49722	CN=*.hotjar.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Dec 25 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jan 24 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 14, 2021 03:09:29.387779951 CET	104.18.70.113	443	192.168.2.3	49725	CN=ssl911790.cloudflaressl.com CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Oct 28 01:00:00 CET 2020	Fri May 07 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Sep 25 02:00:00 CEST 2014	Tue Sep 25 01:59:59 CEST 2029		
					CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jan 14, 2021 03:09:29.390183926 CET	104.18.70.113	443	192.168.2.3	49724	CN=ssl911790.cloudflaressl.com CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Oct 28 01:00:00 CET 2020	Fri May 07 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Sep 25 02:00:00 CEST 2014	Tue Sep 25 01:59:59 CEST 2029		
					CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jan 14, 2021 03:09:29.564188957 CET	52.49.237.17	443	192.168.2.3	49726	CN=*.hotjar.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sat Aug 29 02:00:00 CEST 2020	Tue Sep 28 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		

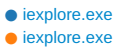
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 14, 2021 03:09:30.720494032 CET	3.125.55.38	443	192.168.2.3	49727	CN=*.zopim.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sat May 30 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Mon May 31 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-24-65281,29-23-24,0	57f3642b4e37e28f5cbe3020c9331b4c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jan 14, 2021 03:09:31.070094109 CET	52.0.36.54	443	192.168.2.3	49728	CN=fdus-55.freshdesk.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Dec 03 11:11:30 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Wed Mar 03 11:11:30 CET 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Jan 14, 2021 03:09:31.071407080 CET	52.0.36.54	443	192.168.2.3	49729	CN=fdus-55.freshdesk.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Dec 03 11:11:30 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Wed Mar 03 11:11:30 CET 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Jan 14, 2021 03:09:54.809556961 CET	104.21.19.250	443	192.168.2.3	49734	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sun Aug 02 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Mon Aug 02 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 14, 2021 03:10:40.104279995 CET	192.0.77.48	443	192.168.2.3	49745	CN=*.w.org CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Dec 19 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sun Dec 19 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jan 14, 2021 03:10:40.105130911 CET	192.0.77.48	443	192.168.2.3	49746	CN=*.w.org CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Dec 19 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sun Dec 19 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5836 Parent PID: 792

General

Start time:	03:09:21
Start date:	14/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff61c2d0000
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: 5884 Parent PID: 5836

Copyright null 2021

General

Start time:	03:09:21
Start date:	14/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5836 CREDAT:17410 /prefetch:2
Imagebase:	0x320000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly

Copyright null 2021