ID: 324353
Cookbook: browseurl.jbs
Time: 14:05:29
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

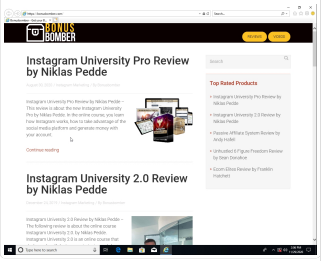
Analysis Report http://bonusbomber.com

Overview

General Information

Sample URL:	http://bonusbomber.com
Analysis ID:	324353

Most interesting Screenshot:



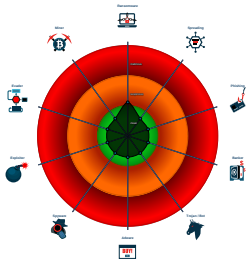
Detection

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

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6024 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6068 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6024 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

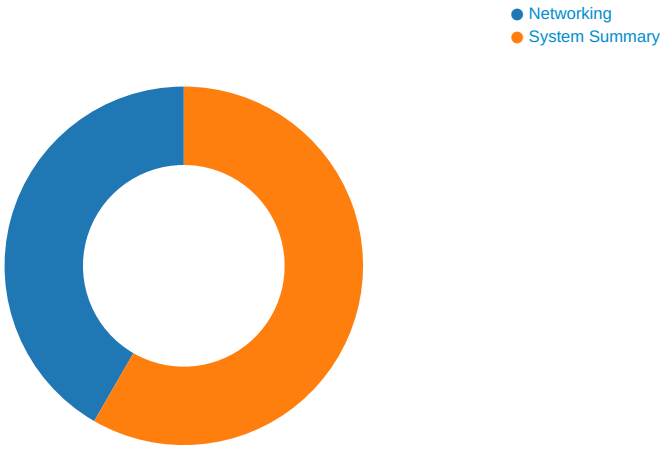
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



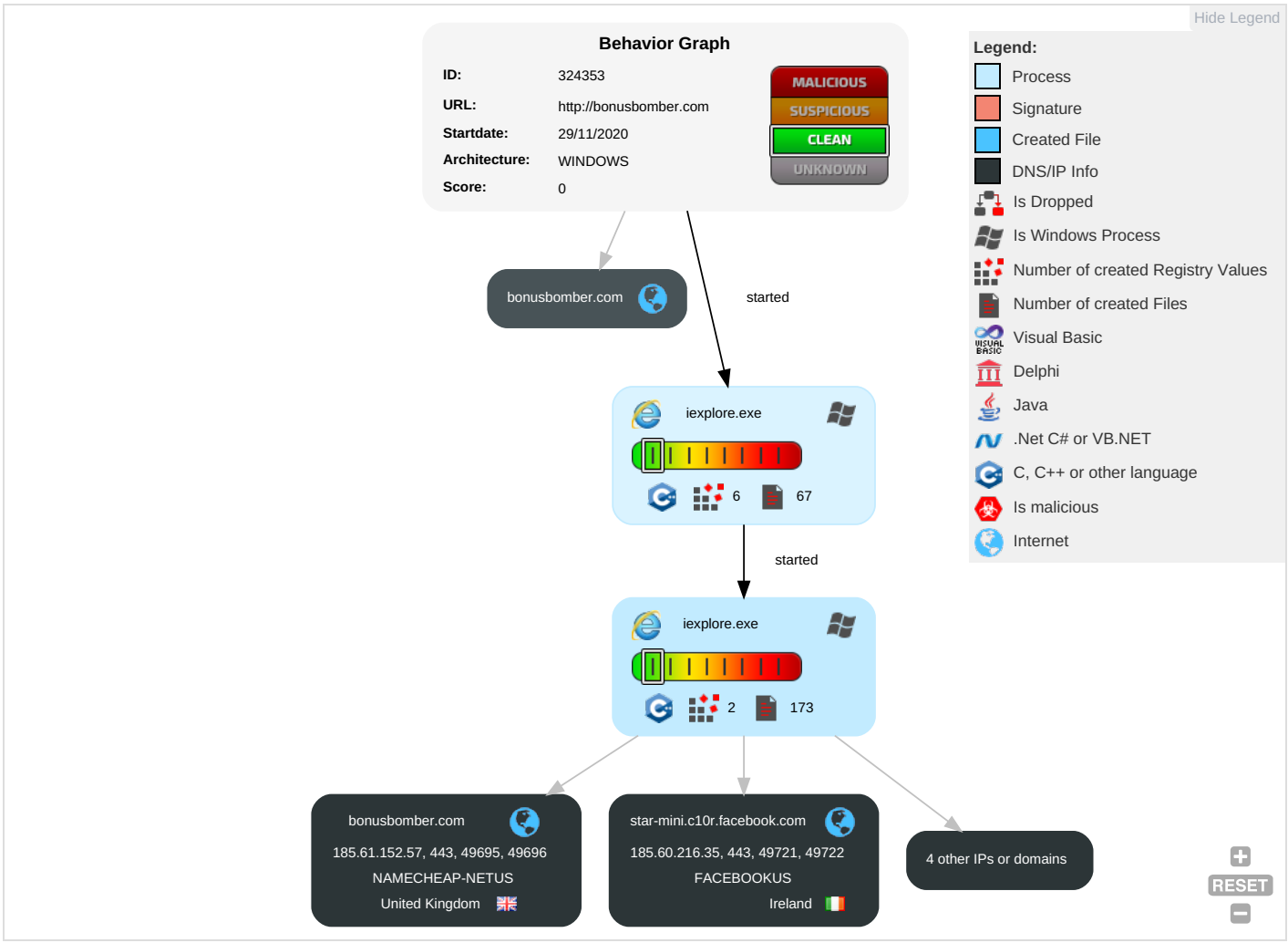
Click to jump to signature section

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	Impa
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 Partit
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 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
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 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Carri Billin Fraud

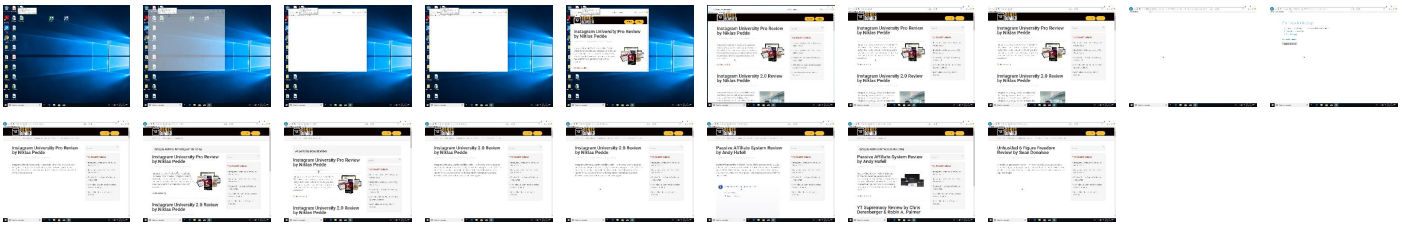
Behavior Graph

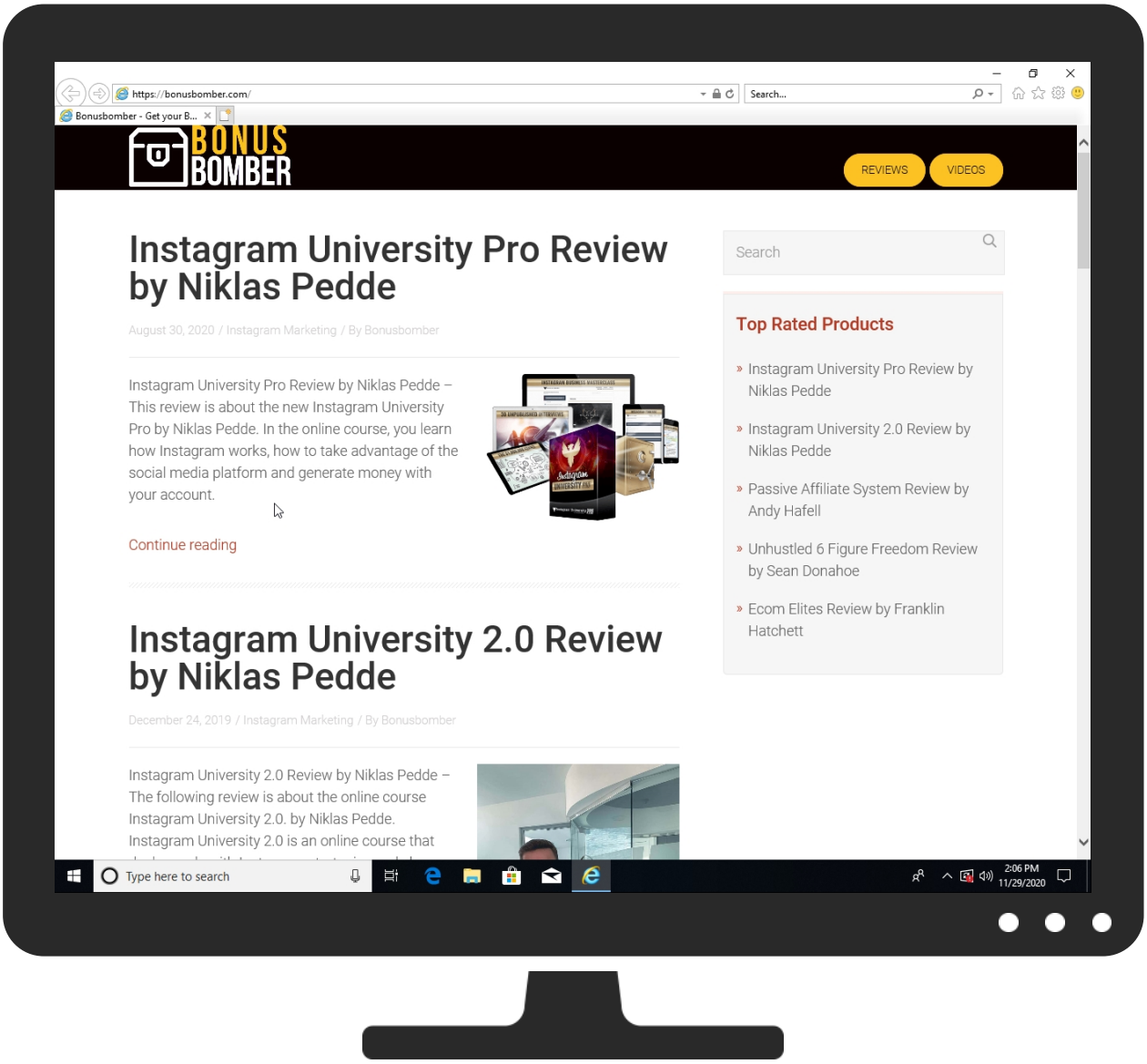


Screenshots

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://bonusbomber.com	0%	Virustotal		Browse
http://bonusbomber.com	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
bonusbomber.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://bonusbomber.com/wp-content/uploads/2019/08/Bonusbomber-1-50x28.png	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-includes/js/plupload/plupload.min.js?ver=2.1.9	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://bonusbomber.com/wp-content/uploads/2019/11/Bonusbomber-2-768x432.jpg	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/07/Bonusbomber-50x28.png	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/Root	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/first-launch-profits-review/	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/11/2969352_1546835250916bundle-1024x300.jpg	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/08/voicematic.png	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/07/VideoAppSuite.png	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/?p=473	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/03/facebook-group-strategy-768x498.png	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/6ff	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2020/08/WhatsApp-Image-2020-08-30-at-19.02.05-50x28.jpeg	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/instagram-university-2-0-review/feed/	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/07/Youtube-Affiliate-Hack.jpg	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-includes/js/jquery/jquery-migrate.min.js?v=1.500.1	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/themes/rise/css/reset.css?v=1.500.1	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/03/instagram-traffic-strategy-768x504.png	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/instagram-university-2-0-review/#primaryimage	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/yt-supremacy-review/	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/03/facebook-group-strategy.png	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/08/Bonusbomber-1-768x432.png	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/07/Bonusbomber-400x225.png	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/08/Bonusbomber-1-400x225.png	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/11/Bonusbomber-1.jpg	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/11/Bonusbomber-400x225.jpg	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/unhustled-6-figure-freedom-review/#primaryimage	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/03/traffic-booster.png	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/02/product-280x150.png	0%	Avira URL Cloud	safe	
http://https://www.youtube.co	0%	URL Reputation	safe	
http://https://www.youtube.co	0%	URL Reputation	safe	
http://https://www.youtube.co	0%	URL Reputation	safe	
http://https://bonusbomber.com/instagram-university-pro-review/#webpage	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/12/instagram-university-300x185.png	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/02/cropped-Download-300x300.png	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/11/Bonusbomber-2-400x225.jpg	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/#webpage	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/07/Youtube-Affiliate-Hack-50x28.jpg	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/category/instagram-marketing/feed/	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/12/weg-1.jpg	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/themes/rise/css/ie8.css	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/02/cropped-Download-32x32.png	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/instagram-university-pro-review/zInstagram	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/12/Foto-16.05.19_-14-53-45-1-1-232x300.jpg	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/plugins/tw-membership/assets/frontend/scripts/custom/global.js?ve	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/author/matl996/DBonusbomber	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/08/Bonusbomber-1.png	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-includes/wlwmanifest.xml	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/?p=444	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/03/instaglory-1.png	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/commission-hero-course-review/	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/12/instagram-university.png	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/chatterpal-review-by-paul-ponna/	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/#website	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/insta	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/ecom-elites-review-by-franklin-hatchett/	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/igpro	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-includes/css/dashicons.min.css?ver=4.9.16	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/plugins/tw-membership/assets/frontend/scripts/vendor/svg-convert.	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/12/Passive-Affiliate-System-50x33.jpg	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/themes/rise/js/html5/dist/html5shiv.js	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/themes/rise/style.css?ver=4.9.16	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/11/2969352_1546835250916bundle-50x15.jpg	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://bonusbomber.com/instagram-university-2-0-review/ub_confirmation=1Finstagram-university-pro-r	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/12/youtube-affiliate-hack-50x32.png	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/10/y3bsasezzq3jopbwtn0v.png	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/11/Bonusbomber.jpg	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/11/2969352_1546835250916bundle-150x150.jpg	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/xmlrpc.php?rsd	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/12/Foto-16.05.19_-14-53-45-1-1.jpg	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/instaglory-review/	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2020/08/WhatsApp-Image-2020-08-30-at-19.02.05-1024x576.jp	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-includes/js/imagesloaded.min.js?ver=3.2.0	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/12/weg-1-400x241.jpg	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/author/marcus-hauboldgmx-de/	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/category/instagram-marketing/w/ub_confirmation=1Finstagram-university-pro-re	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/themes/rise/css/ie7.css	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-includes/js/jquery/jquery.js?v=1.500.1	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/plugins/thrive-visual-editor/thrive-dashboard/js/dist/frontend.mi	0%	Avira URL Cloud	safe	
http://https://bonusbomber.com/wp-content/uploads/2019/11/Bonusbomber-768x432.jpg	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
star-mini.c10r.facebook.com	185.60.216.35	true	false		high
bonusbomber.com	185.61.152.57	true	false	• 0%, Virustotal, Browse	unknown
cdnjs.cloudflare.com	104.16.19.94	true	false		high
code.ionicframework.com	104.26.6.173	true	false		high
www.facebook.com	unknown	unknown	false		high
m.facebook.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://bonusbomber.com/category/online-marketing/	false		unknown
http://https://bonusbomber.com/	false		unknown
http://https://bonusbomber.com/category/instagram-marketing/	false		unknown

URLs from Memory and Binaries

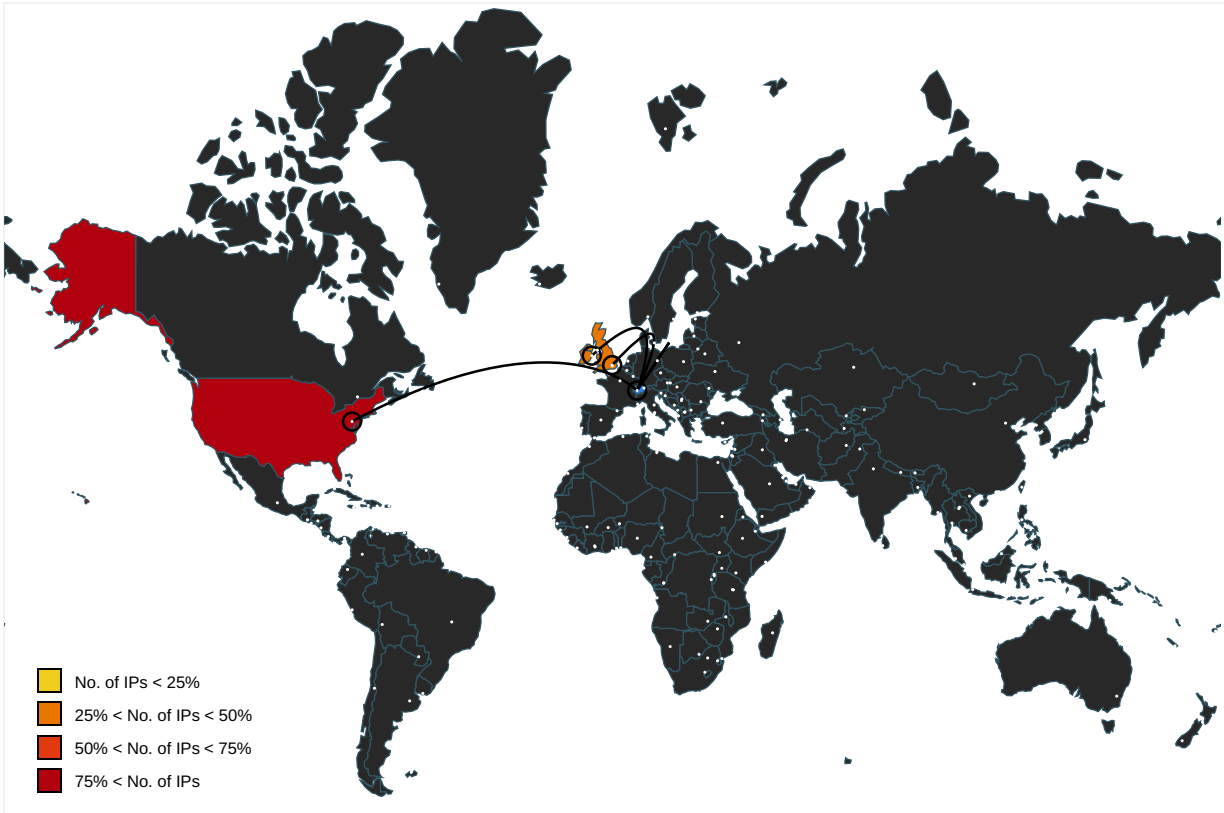
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://bonusbomber.com/wp-content/uploads/2019/08/Bonusbomber-1-50x28.png	unhustled-6-figure-freedom-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-includes/js/plupload/plupload.min.js?ver=2.1.9	00LZZJ6X.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/11/Bonusbomber-2-768x432.jpg	unhustled-6-figure-freedom-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/author/matl996/	matl996[1].htm.2.dr	false		unknown
http://https://bonusbomber.com/wp-content/uploads/2019/07/Bonusbomber-50x28.png	unhustled-6-figure-freedom-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/Root	{190FACD6-328F-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/first-launch-profits-review/	passive-affiliate-system-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/embed/	script[1].js.2.dr	false		high
http://https://bonusbomber.com/wp-content/uploads/2019/11/2969352_1546835250916bundle-1024x300.jpg	00LZZJ6X.htm.2.dr, unhustled-6-figure-freedom-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/08/voicematic.png	00LZZJ6X.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://twitter.com/benjsperry	ionicons.min[1].css.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://bonusbomber.com/wp-content/uploads/2019/07/VideoAppSuite.png	00LZZJ6X.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/embed/xhhlGOBCxJQ?rel=0&modestbranding=0&controls=1&showinfo=1&fs=1&wmode=tr	~DF2B4CE3B5C360B0D9.TMP.1.dr	false		high
http://https://bonusbomber.com/?p=473	instagram-university-2-0-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/instagram-university-pro-review/	instagram-university-pro-review[1].htm.2.dr, instagram-university-2-0-review[1].htm.2.dr	false		unknown
http://https://bonusbomber.com/wp-content/uploads/2019/03/facebook-group-strategy-768x498.png	unhustled-6-figure-freedom-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://thrivethemes.com/	style[1].css.2.dr	false		high
http://https://bonusbomber.com/6ff	unhustled-6-figure-freedom-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2020/08/WhatsApp-Image-2020-08-30-at-19.02.05-50x28.jpeg	instagram-university-pro-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0Copyright	Roboto[1].ttf.2.dr, RobotoCondensed[1].ttf.2.dr	false		high
http://https://bonusbomber.com/instagram-university-2-0-review/feed/	instagram-university-2-0-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/07/Youtube-Affiliate-Hack.jpg	unhustled-6-figure-freedom-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-includes/js/jquery/jquery-migrate.min.js?v=1.500.1	00LZZJ6X.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/themes/rise/css/reset.css?v=1.500.1	00LZZJ6X.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/embed/6ZOA5rekM-o?rel=0&modestbranding=0&controls=1&showinfo=1&fs=1&wmode=tr	~DF2B4CE3B5C360B0D9.TMP.1.dr	false		high
http://https://bonusbomber.com/wp-content/uploads/2019/03/instagram-traffic-strategy-768x504.png	instagram-university-pro-review[1].htm.2.dr, unhustled-6-figure-freedom-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/instagram-university-2-0-review/#primaryimage	instagram-university-2-0-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/yt-supremacy-review/	00LZZJ6X.htm.2.dr, passive-affiliate-system-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/03/facebook-group-strategy.png	unhustled-6-figure-freedom-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/08/Bonusbomber-1-768x432.png	unhustled-6-figure-freedom-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/07/Bonusbomber-400x225.png	unhustled-6-figure-freedom-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/08/Bonusbomber-1-400x225.png	unhustled-6-figure-freedom-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/11/Bonusbomber-1.jpg	unhustled-6-figure-freedom-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/11/Bonusbomber-400x225.jpg	unhustled-6-figure-freedom-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/unhustled-6-figure-freedom-review/#primaryimage	unhustled-6-figure-freedom-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/03/traffic-booster.png	unhustled-6-figure-freedom-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/02/product-280x150.png	passive-affiliate-system-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.co	{190FACD6-328F-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://bonusbomber.com/instagram-university-pro-review/#webpage	instagram-university-pro-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/12/instagram-university-300x185.png	instagram-university-2-0-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/02/cropped-Download-300x300.png	00LZZJ6X.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/11/Bonusbomber-2-400x225.jpg	unhustled-6-figure-freedom-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/#webpage	00LZZJ6X.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/07/Youtube-Affiliate-Hack-50x28.jpg	unhustled-6-figure-freedom-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://schema.org	00LZZJ6X.htm.2.dr, passive-affiliate-system-review[1].htm.2.dr, instagram-university-pro-review[1].htm.2.dr, online-marketing[1].htm.2.dr, matl996[1].htm.2.dr, instagram-marketing[1].htm.2.dr, instagram-university-2-0-review[1].htm.2.dr, youtube-marketing[1].htm.2.dr, unhustled-6-figure-freedom-review[1].htm.2.dr	false		high
http://https://bonusbomber.com/category/instagram-marketing/feed/	instagram-marketing[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/12/weg-1.jpg	passive-affiliate-system-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/themes/rise/css/ie8.css	00LZZJ6X.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://schema.org/ListItem	unhustled-6-figure-freedom-review[1].htm.2.dr	false		high
http://https://bonusbomber.com/wp-content/uploads/2019/02/cropped-Download-32x32.png	00LZZJ6X.htm.2.dr, imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.pinterest.com/js/pinit.js	script[1].js.2.dr	false		high
http://https://bonusbomber.com/instagram-university-pro-review/zInstagram	~DF2B4CE3B5C360B0D9.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/12/Foto-16.05.19_-14-53-45-1-1-232x300.jpg	instagram-university-2-0-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/plugins/tw-membership/assets/frontend/scripts/custom/global.js?ve	00LZZJ6X.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/author/matl996/DBonusbomber	~DF2B4CE3B5C360B0D9.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/08/Bonusbomber-1.png	unhustled-6-figure-freedom-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-includes/wlwmanifest.xml	00LZZJ6X.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/	unhustled-6-figure-freedom-review[1].htm.2.dr	false		unknown
http://https://bonusbomber.com/?p=444	passive-affiliate-system-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/03/instaglory-1.png	00LZZJ6X.htm.2.dr, instagram-university-pro-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/commission-hero-course-review/	00LZZJ6X.htm.2.dr, unhustled-6-figure-freedom-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/12/instagram-university.png	instagram-university-2-0-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/chatterpal-review-by-paul-ponna/	passive-affiliate-system-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/#website	unhustled-6-figure-freedom-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/insta	instagram-university-2-0-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/ecom-elites-review-by-franklin-hatchett/	00LZZJ6X.htm.2.dr, unhustled-6-figure-freedom-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/igpro	instagram-university-pro-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yoast.com/wordpress/plugins/seo/	00LZZJ6X.htm.2.dr	false		high
http://https://bonusbomber.com/wp-includes/css/dashicons.min.css?ver=4.9.16	00LZZJ6X.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/plugins/tw-membership/assets/frontend/scripts/vendor/svg-convert.	00LZZJ6X.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/12/Passive-Affiliate-System-50x33.jpg	passive-affiliate-system-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/themes/rise/js/html5/dist/html5shiv.js	00LZZJ6X.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/themes/rise/style.css?ver=4.9.16	00LZZJ6X.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/11/2969352_1546835250916bundle-50x15.jpg	unhustled-6-figure-freedom-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/channel/UCHKg3UdCHrOfnckaZwgqC-g?sub_confirmation=1	~DF2B4CE3B5C360B0D9.TMP.1.dr	false		high
http://https://bonusbomber.com/instagram-university-2-0-review/ub_confirmation=1Finstagram-university-pro-r	~DF2B4CE3B5C360B0D9.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/12/youtube-affiliate-hack-50x32.png	instagram-university-pro-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://twitter.com/ionicframework	ionicons.min[1].css.2.dr	false		high
http://https://bonusbomber.com/wp-content/uploads/2019/10/y3bsasezzq3jopbwtn0v.png	00LZZJ6X.htm.2.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://bonusbomber.com/wp-content/uploads/2019/11/Bonusbomber.jpg	unhustled-6-figure-freedom-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/11/2969352_1546835250916bundle-150x150.jpg	unhustled-6-figure-freedom-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/xmlrpc.php?rsd	00LZZJ6X.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/12/Foto-16.05.19_-14-53-45-1-1.jpg	instagram-university-2-0-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/instaglory-review/	00LZZJ6X.htm.2.dr, instagram-university-pro-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2020/08/WhatsApp-Image-2020-08-30-at-19.02.05-1024x576.jp	instagram-university-pro-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-includes/js/imagesloaded.min.js?ver=3.2.0	00LZZJ6X.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/12/weg-1-400x241.jpg	passive-affiliate-system-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/author/marcus-hauboldgmx-de/	00LZZJ6X.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://platform.twitter.com/widgets.js	script[1].js.2.dr	false		high
http://www.thrivethemes.com/	frontend.min[2].js.2.dr	false		high
http://https://bonusbomber.com/category/instagram-marketing/w/ub_confirmation=1Finstagram-university-pro-re	~DF2B4CE3B5C360B0D9.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/themes/rise/css/ie7.css	00LZZJ6X.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/unhustled-6-figure-freedom-review/	unhustled-6-figure-freedom-review[1].htm.2.dr	false		unknown
http://https://bonusbomber.com/wp-includes/js/jquery/jquery.js?v=1.500.1	00LZZJ6X.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/plugins/thrive-visual-editor/thrive-dashboard/js/dist/frontend.mi	00LZZJ6X.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bonusbomber.com/wp-content/uploads/2019/11/Bonusbomber-768x432.jpg	unhustled-6-figure-freedom-review[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://secure.gravatar.com/avatar/c24c4556e9f1e75ef933dffa6277a518?s=96&d=mm&r=g	passive-affiliate-system-review[1].htm.2.dr, instagram-university-pro-review[1].htm.2.dr, matl996[1].htm.2.dr, instagram-university-2-0-review[1].htm.2.dr, unhustled-6-figure-freedom-review[1].htm.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.26.6.173	unknown	United States		13335	CLOUDFLARENETUS	false
185.61.152.57	unknown	United Kingdom		22612	NAMECHEAP-NETUS	false
185.60.216.35	unknown	Ireland		32934	FACEBOOKUS	false
104.16.19.94	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324353
Start date:	29.11.2020
Start time:	14:05:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://bonusbomber.com
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	13
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@3/148@6/4
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://bonusbomber.com/ • Browsing link: https://www.facebook.com/sharer/sharer.php?u=https://bonusbomber.com/instagram-university-pro-review/ • Browsing link: https://www.youtube.com/channel/UCHKg3UdCHrOfnckaZwgqC-g?sub_confirmation=1 • Browsing link: https://bonusbomber.com/instagram-university-pro-review/ • Browsing link: https://bonusbomber.com/category/instagram-marketing/ • Browsing link: https://bonusbomber.com/author/matl996/ • Browsing link: https://bonusbomber.com/instagram-university-2-0-review/ • Browsing link: https://bonusbomber.com/passive-affiliate-system-review/ • Browsing link: https://bonusbomber.com/category/youtube-marketing/ • Browsing link: https://bonusbomber.com/unhustled-6-figure-freedom-review/ • Browsing link: https://bonusbomber.com/category/online-marketing/

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, ielowutil.exe, SgrmBroker.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 104.83.120.32, 216.58.215.234, 172.217.168.3, 152.199.19.161, 92.122.144.200, 93.184.221.240 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wu.azureedge.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, fonts.googleapis.com, fs.microsoft.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, wu.ec.azureedge.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, cs9.wpc.v0cdn.net • 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\Recovery\High\Active\RecoveryStore.{190FACD4-328F-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8616962311315133
Encrypted:	false
SSDEEP:	192:rsZHZd2b9WytYfefYD4M6XMoDIytrDDcfrjJQfrjNMjnX:rs5UbUKji0egC
MD5:	CDEB85B042CD1F2B3D2C2CD1395840F2
SHA1:	1E173617241BC6094A5FA88E6EAC6C59E05A549C
SHA-256:	67E59FE8A3CF0C9E34261666CD8FC455D44FA754EEB49DD1430B618033C20C6A
SHA-512:	259DCACBB236D5AD4194C587BDD70C394264AF855AB51C7DD42B6B233B4E77A99186865C7C38060EFFBBCEF588A9BEC22058A57629B1379FB3B525C12116467
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\{190FACD6-328F-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	528030
Entropy (8bit):	2.721756265942507
Encrypted:	false
SSDEEP:	3072:8iW4YA9HlkLjhIohEzXdx3Ac1whvW440QsZSUotgRYrfGLP460MNYMMHsc7uU:AsW
MD5:	3B27B68B1C15B11FA26D5BDB1CB7EB88
SHA1:	D018C7BBDC0E246A1C4817BF4166DCAF9EB77B77
SHA-256:	404A0BF5E027CB1DEB3C350B44CFE93D3BEF8C4D2E2906F1AE3B81949EF4B90D
SHA-512:	506500BC9DB7F788E25B5B148C968E502621B9B548635F4AA7A6F5DA5CBDB906BF29057D98EBC31CFDD5ADFDCABAB6F42FA886D1CA01531AF35BDB7BAB98AC46
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\{1F95BE08-328F-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5659758696428474
Encrypted:	false
SSDEEP:	48:Iw5GcprEGwpa57G4pQJGrapbSFrGQpKmG7HpRusTGIpG:rfZ8Q5d6pBSFFARTu4A
MD5:	C0BD5427647A48B8CB156846A415C842
SHA1:	ECC2ED5C4E4E341A8646268CB8D82B2FEEF899C7
SHA-256:	4DD667B40E1E475A6625124FE054E14D76F184C6ACB95D5B8800C49A49D0065D
SHA-512:	5B629E6EFCFE5D7081EE95D26E0EDBC1A2186D05D8BDAC4EE7A44205CBC246B0977B49EF49AF63CEC45AA48DF3D8B39B1ACC5DCF70664584806C75A846B2AE21
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	880
Entropy (8bit):	6.372795248190278
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
SSDEEP:	12:m8SEkz5XjfSv/7sq93CEgKGWsCnZ/xrMZiyy7wSTYL2zkupysRu5X1J4Vnbe6wDu:m8BYfJw3CrWqZ8cSbznQXN16o6cAi/y
MD5:	1141954A19F41C0669CE56F5A77BFA61
SHA1:	988C36557ACF9B19232C7A57AE404653354B0DF2
SHA-256:	70719B073A37103689ABD122F767861751E9B8D366446D394E7936851E83A1F1
SHA-512:	C88770F8942A7197D93C7DD19A411589E2BF38E4F72C41858F8B6B0D88C0052D2BF5D35EB4AFDEF0CC1EB72E01836186B4D7A729D9123646D2A54FFF0614A77
Malicious:	false
Reputation:	low
Preview:	M.h.t.t.p.s.:././.b.o.n.u.s.b.o.m.b.e.r...c.o.m./.w.p.-.c.o.n.t.e.n.t./.u.p.l.o.a.d.s./.2.0.1.9./.0.2./.c.r.o.p.p.e.d.-.D.o.w.n.l.o.a.d.-.3.2.x.3.2...p.n.g.....PNG.....IHDR... ... .D .....PLTE]]]^^^]]]^^^^^]]]eeeccccbjjjLiq]]]]]]]]]]]]]]]]]hhh]]]]]]]]]bb`vvvggg]]]]]]]]]]]]^^^ddddddfff]]]]]]]]]]]^^^xxx]]]^^^]]]nnn^^^]]]aaa__^]]]]]]]]]^^^]]]]]]]]]]]]]^^^]]]iii]]]]]]]]]www]]]]]]]]]^^^___]]][>.{...CtRNS. ..".....=*....8.....0..... +...../..#....Ay...!..Id....7..;.m....PIDATx...v.0..m.mVb.$@.N.....2&..@{.."2G..$.~U.Y\.....a) &fEdR..v.t._..)@.,..~..... }vy.$..k.h;z..q{s:..6i?t..q..xw....3..v..Og..i..F.C[..x.A..s..:.x.d+.3.....t..d..T.2.2.i..^.R.Eb(r.v.-.."s.Eb.....R.... #H."4.4.....`$..I...E...<.C..$[..^..7.....t..5.._....@.B.n..45U.FW ....T.....Ad.....Z.....I.#.....IEND.B`. ... .]..._....]..._....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\00LZZJ6X.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:	dropped
Size (bytes):	59440
Entropy (8bit):	5.284897375899777
Encrypted:	false
SSDEEP:	1536:oKMKhbtprXmZriZiof0Xycl0uYTPtv4Fnxf6:fhbtprXmZriZiofWycl0NTPZ4Vxf6
MD5:	9AA8EB768D28738579593F5D58A4D156
SHA1:	8AEA3F8CAEB4CB22B66FD64743C8A6DA80ABB050
SHA-256:	1CE62E3D2BDD8DEBB438C420AEF9E38CC34846775F08CA76DA607D19FDA64F29
SHA-512:	EE9CCC4A3787138B5852F9697EE54A6A2772CEEC9F107F34DCBB7AD2574AFF4D135B2DD23A297635FDDDAB05AE305DD117033DEDD14D6CF3A66216590BDBD B9B
Malicious:	false
Reputation:	low
Preview:	.<!DOCTYPE html>.<html lang="en-US">.<head>... [if lt IE 9]>..<script src="https://bonusbomber.com/wp-content/themes/rise/js/html5/dist/html5shiv.js"></script>..<script src="//css3-mediaqueries-js.googlecode.com/svn/trunk/css3-mediaqueries.js"></script>..<![endif]-->.. [if IE 8]>..<link rel="stylesheet" type="text/css" href="https://bon usbomber.com/wp-content/themes/rise/css/ie8.css"/>..<![endif]-->.. [if IE 7]>..<link rel="stylesheet" type="text/css" href="https://bonusbomber.com/wp-content/themes/ris e/css/ie7.css"/>..<![endif]-->..<meta name="viewport" content="width=device-width, initial-scale=1.0"/>..<meta charset="UTF-8">.....<title>Bonusbomber - Get your Bonus ...</title>.. This site is optimized with the Yoast SEO plugin v11.3 - https://yoast.com/wordpress/plugins/seo/ -->.<meta name="description" content="Get your Bonus ..."/>. <link rel="canonical" href="https://bonusbomber.com/" />.<link rel="next" href="https://bonusbomber.com/page/2/" />.<meta property="og:loc

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Bonusbomber[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, 960x540, frames 3
Category:	downloaded
Size (bytes):	41740
Entropy (8bit):	7.935375243742369
Encrypted:	false
SSDEEP:	768:AMX7ZEwFa76Ab3sSytZ9/kWQY1lzHPH1ulxk1OFmPDmZvHz1v075Ej6s/LYkS+lz:/XNEJ+AAhtZtHdVOFEDkrx07a+cUkSYz
MD5:	16F592D41603C46A705E4B91DC32BBDA
SHA1:	9D8E1A1C8D0889A572C25A3765904A7D4AABA48B
SHA-256:	12A482EDA795B3F44C956BAC40CBB1EDD22FF3387743DC9569A05C9EEF2BDD25
SHA-512:	D97BF0DA8CE38BB00F18ACF58F01A50365F580234C3C06155C7F0CA13D6297AAB0C10F2B0C61A11982CEA4F74B6F299E4817FF615AB49E461313B29A31FBE5C E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2019/11/Bonusbomber.jpg
Preview:	......JFIF..... $.' ",#..(7),01444.'9=82<.342.....2!.!2222222222222222222222222222222222222222222222222222..... ....9..5..I....b.[...9..g>....}.c.e...[...._.....3..{..b.kX.f...v.8l...>.1.....3...S~S<.P.9n/..}.Yz....h.1....C.!..)....\|E.....h....V.n. n.V..L..W.L*..!>!X.....s:o.7.3...c..5..W.U.....V.-dQ.5..z....R....M.^.ep.\....>b.m...l^.^....Yh./.q..y.~m.m..N.M.h.n\|.+...W.....u..o.g.*$.*.V+;_qV^..cHk'ka8..7j..,2d.jT.$..K;\4.6?. ZlNF..Mn..%n..<5j...A.....{.[u,....3..U.....,TI.@.&.....Vq.KY.F....U)ff.s,.R.../.M..Msc.p..A6.Z..M[..O.Z.:...V.I....m<7.y|s..U..b.....,TI.@.2..}.Yv....-a..3..T.....-J...Gn.\4.6? q|W.".kU..+u...U.@....WL+w.5.R..r..'.....#.....w....1H...../...-3)k#=.....R.fj.2.*o.cY..\4.6?..N^..i....d...D...V.a.u..w.5.R..x.H.`...>..8.....']....yb.LR.k..U..e..cS.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Foto-16.05.19_-14-53-45-1-1-280x150[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 116x150, frames 3
Category:	downloaded
Size (bytes):	3391
Entropy (8bit):	7.84912103248119
Encrypted:	false
SSDEEP:	96:PdUOtArMnQhXt/b0g5e8YcRvNcKTOlOstxj7x:PdGCQjIJ8YMoMsTF
MD5:	0FA8E9C65B89EAB2728EA3B07338CD85

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Foto-16.05.19_-14-53-45-1-1-280x150[1].jpg</th></tr>
<tr><td>SHA1:</td><td>E308DBA5A24927694E57B1B1794069E42843F80B</td></tr>
<tr><td>SHA-256:</td><td>C64C217420D40FBAC90D748CEF4D8BECDD5F2F1C4D2BB4768DCB65B6887BA206</td></tr>
<tr><td>SHA-512:</td><td>22017F3E3B027497332A61E71AB555B66AD93FC3ABF7DE142A210F5FC804FD3449CBBB93CD6FF350C05FC042204BBCD39C784C6BF9769FFE40D71757CE2F11F
E</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://bonusbomber.com/wp-content/uploads/2019/12/Foto-16.05.19_-14-53-45-1-1-280x150.jpg</td></tr>
<tr><td>Preview:</td><td>......JFIF.............C......................$....+&-,*&))/5D:/2@3));Q<@FILML.9TZSJYDKLI...C.......#..#I1)1IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII........t.."....................................:..........
...............!1AQa.."2q........#BRb.$Cr3...!1.A.Qa............?.pEy.x.T.U....L.....-[..TU.)..m".K...q..Fm.f.t..p..56..V.!..(.....?......*...../.....n..V}t........l.
.)..].A'<.j6C.pu....c.....AI=.....}N......C.}q'...1V..m..>}..?..JNA'$...@n^.x...O.i....TYt..+w..E...J1.VFh..T"A.5.P:.^..rA...<.w$...h..G,R.s..q..U..[...N....@Kp.c.WE.o..RH......|Y....[.......
<}(i.[..H.;..`\r3UD9.I}s19}...O.......!O..&..l}*.+H..$....-E8.b.T-.....;X...|...X....dD.J..G.JV3Q'J..\.C..*..H.v..wj.of.#m%..4...5..iul .E.LJ.XT.d~T...}.......-bN.E....Q}>...[...~...!..bm..
Oy...S.h....#.\..8)..&.. .. .H..........x.t..3.G.S!.WI.``P.3..cN.}.....f.!.s..H.,H........Hx.A[#.J.h..#.E..Z..l./.P.d.5,.`..$WE.^.(.V.(.f.*V.</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\KFOlCnqEu92Fr1MmEU9fBBc-[1].woff</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>Web Open Font Format, TrueType, length 20464, version 1.1</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>20464</td></tr>
<tr><td>Entropy (8bit):</td><td>7.969622511404751</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>384:edA/1eSg82dg1kGeF2BFDEE+/adkuouo34TjkWqTExYOYg/c1iuHotcO:ey/1eSnLkGeWFQECadcLIc/TEfYr1RO</td></tr>
<tr><td>MD5:</td><td>87284894879F5B1C229CB49C8FF6DECC</td></tr>
<tr><td>SHA1:</td><td>FB1BD3BAF122D5D350EB387F0536C20DA71F09DF</td></tr>
<tr><td>SHA-256:</td><td>BA98F991D002C6BFAAF7B874652FFDCDE9261A86925DB87DF3ED2861EA080ADF</td></tr>
<tr><td>SHA-512:</td><td>663BA95BBBC6F7E65D7B1293E4A044C9111438A03B16664FC38A2B2F2C1A4CE96991C847B36691388AB322525A83DB2724CB4D1B9BF0440727F0B5CA7073AB8C</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://fonts.gstatic.com/s/roboto/v20/KFOlCnqEu92Fr1MmEU9fBBc-.woff</td></tr>
<tr><td>Preview:</td><td>wOFF......O........D........................GDEF.......G...d....GPOS............~..GSUB.......'......r.OS/2.......Q...`t...cmap...\..........W.cvt ...T...\...\1..Kfpgm.......2......$.gasp................glyf..
....;...l..(.4hdmx..H....l....."..head..I<...6...6...rhhea..It.......$....hmtx..I....x.....gO.loca..L........_.C|maxp..M.... ... .(..name..N...........:.post..N........ .m.dprep..O........S...)x...1.
.P......PB..U.=l.@..B)..w.......Y.e.u.m.C.s...x.h.~R....R...A.J.x....dK...{....?..F?.|.~.m...ms.{.Z..;......U.]7s......\.=D.=.7...>....x...D..O|.U:...|o..3.x.j.r"B............../.)x$.'"j...
..1LGmaGxQxG....~.:'.A..hd.z,.k..KO.....^.}H|#z_.O......R..A...9..A..!.(./..."..:.Iq1.r..s..r.7r.7s..q.wr....nz..]...2..d4c..c....d....T.1...d....\...,c9k.g..Yv.#O."%...... ...t"uM..%......
.j.#^.....}\c.q.i...<jy.D...C.01.2.r.....V..z.W.7b..L.S.41]..kUs.X/6..b.........(..(...K..{.^..'........`#./..B......N+p.m`...].lQ....Drg.M..Kx.^.S.*..........h ..$.k.'Hy.I.ze..4z.-T.....</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\KFOlCnqEu92Fr1MmSU5fBBc-[1].woff</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>Web Open Font Format, TrueType, length 20348, version 1.1</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>20348</td></tr>
<tr><td>Entropy (8bit):</td><td>7.971548837012925</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>384:sSRPUR1eEsGitLcRtdt6S1PvpjwY9O1V6LTFY88fFFEagMR3SAFNE/A:saP+1eBX4Rtdt6EJjwY9O1V6Pm82lR39</td></tr>
<tr><td>MD5:</td><td>B00849E00F4C2331CDDD8FFB44A6720B</td></tr>
<tr><td>SHA1:</td><td>5B7820FEC8F9810E291E1EB98764979830ED6621</td></tr>
<tr><td>SHA-256:</td><td>76B05400FFF9DA5B43862E3713099E3913916A629560265ED24B19D031227CBF</td></tr>
<tr><td>SHA-512:</td><td>64F2BB1D16525CB5435CC3AA253D83669C321D68695CDF14218EEE43B5347DD6BC67B23D6F5E359971B1FFA72857C2C9DCEC0370535F12EDC20AF42CF41CF6</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://fonts.gstatic.com/s/roboto/v20/KFOlCnqEu92Fr1MmSU5fBBc-.woff</td></tr>
<tr><td>Preview:</td><td>wOFF......O|..............................GDEF.......G...d....GPOS...............GSUB.......'......r.OS/2.......P...`t6..cmap...$..........W.cvt ....X...X/...fpgm...t...4......".gasp................glyf..
....;...lxRn..hdmx..Hl...l........head..H....6...6.Y.ihhea..I........$....hmtx..I0.........._Gloca..K.........k.N.maxp..M.... ... .(.\name..M........|..9.post..N........ .m.dprep..N........:z/.Wx...1.
.P......PB..U.=l.@..B)..w.......Y.e.u.m.C.s...x.h.~R....R...A.J.x.l..h.a........l.m.6.1+.X....i...y....&...._..63..5....2>...x|D...ct.Kx..H@b.3..l..#u.....L.*.....^.*.4.....rP..{.*......Q...
JT.:Xu>..T./>...oq...........~..@.....lq../.... ..#..".&.8.H$..r...J)..jj...&..f.=.9..N9.....'F..8.4.....m...m...m.m..n..&.X..}....S.|.....n........PHaE...J*...4..MjJ.*..nW)..rn3'/.....ks5zY
5c...Mgg.5..p..rR{c...p..t\.8.c=..p...X.(.......7....=.........!...H ....(.0...(.q.JT?.b..z].'T...m..vNi.....t....:P.R..H....t.........&?.:.j.51+.S.":j.SK'I.^....}S.i.</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\KFOmCnqEu92Fr1Mu4mxM[1].woff</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>Web Open Font Format, TrueType, length 20268, version 1.1</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>20268</td></tr>
<tr><td>Entropy (8bit):</td><td>7.970212610239314</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>384:LyfRPUY1e32pJd75q1DzPjsnouCrZsZtetWFNFfIP0cIWvdzNcrm:uJPb1em3dSPjKrZYtWntk0wvdzh</td></tr>
<tr><td>MD5:</td><td>60FA3C0614B8FB2F394FA29944C21540</td></tr>
<tr><td>SHA1:</td><td>42C8AE79841C592A26633F10EE9A26C75BCF9273</td></tr>
<tr><td>SHA-256:</td><td>C1DC87F99C7FF228806117D58F085C6C573057FA237228081802B7D8D3CF7684</td></tr>
</table>

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\OpenSans[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, digitally signed, 19 tables, 1st "DSIG", 26 names, Macintosh, Digitized data copyright \251 2010-2011, Google Corporation.Open SansRegular1.10;1ASC;OpenSans-R
Category:	downloaded
Size (bytes):	217276
Entropy (8bit):	6.419567239266024
Encrypted:	false
SSDEEP:	6144:GLpzdD/rIJXiQTutgCNktQFvmnoxXTS4u8sl:c9FrIJJaqCNktA+SXfJsl
MD5:	D7D5D4588A9F50C99264BC12E4892A7C
SHA1:	513966E260BB7610D47B2329DBA194143831893E
SHA-256:	13C03E22A633919BEB2847C58C8285FB8A735EE97097D7C48FD403F8294B05F8
SHA-512:	CE9F98208CD818E486A12848B2D64BD14E12D42D84B2E47436A3C4420A242583EEFC4A9B42401B51CC204146C6133645975682E4BB5D48527B3796770EFA3397
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/themes/rise/thrive-dashboard/css/font/OpenSans.ttf
Preview:	...........0DSIG..D...;H...tGDEF.&....7(....GPOS.7.7..7H...8GSUB.+=...7.....OS/2.6.........`cmap...........cvt .M..........fpgm~a.....<....gasp...#..7.....glyft8.K..$.../.head..cp...<...6hh ea...s...t...$hmtx.5<.........kernT+.~..T....6loca)..........Vmaxp.C......... nameH.B.........post.C.l......&+prepC..................Ww.(_.<..........51......+.........b.........................{........... ....V......./.\......................3.......3.....f.................@. [...(....1ASC.@. ....X ....H..... ....#...5...+.3.......h...q.....^.R.^.=.j.V...h...?...T.!.........f.......d...^.. .+.......u...^...h...j.!...!.?...h...w...h.o...1.y...../.....}.....s...!.....}.......T.#.`.....'...9.......;.}.....;.}.....d.j.m...........h.......{.....R...........3.V.1.........s.^.......s...s.}.s.....b.'.............3.......q.. ....s.......s.D.....j.............9...1.'.......R...=.h.....H...h.....#.........?...{.....h...!.{...5...d...F...R...h...T...d.....m.....h

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Passive-Affiliate-System[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, progressive, precision 8, 525x350, frames 3
Category:	downloaded
Size (bytes):	11230
Entropy (8bit):	7.892840530367724
Encrypted:	false
SSDEEP:	192:gR3G1YEA1+/e8fC0XeyIDbUUVPHjrVp5xz4SUiok0MiafoSwP06XfmKE:gR3G1Y1Ce8pXYLVbrtN4SXok0Mii4PXI
MD5:	8EC7A13ECFEEBFC5CBC50E46C237689F
SHA1:	41018CC2D9D0FD6401A377D211922C6AE077391D
SHA-256:	01C04E1A02E78D3B8406F7D937546550E4640DD511174847312927284B39A2A7
SHA-512:	7FF35626AE93B26A0A59D4A8C378E8B1C341E2E4681B5D75AD65EF28A95C0D71F4A79365C3AB789A90D3BB7B68EE9B1153C3B37628D9F3D9C6B42EEE5DAD3E 1D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2019/12/Passive-Affiliate-System.jpg
Preview:	......JFIF.....`.`...%...#... , #&')*)..-0-(0%()(...........(...((......^...."... ....~......lwz.....n..^....=....i...l....D.L.g.U.. .....s.$AZ...*,.........i...D..P...[.a........i..A)....DAU.Ha...d....{.}...3.k"fb.. ....i.wH..-kJ.R!H.. ..n.....4.];.ekZ.^.Z.DV%..a...n.....4.]{.. .L..o..Eb+1J.B...p6@...l...@.6..<...%.iR!H..Z..........K.........2..&H.L.rp...-kX.b........Q.Z.B`.DN.~x..k.&H._..0c..l}..y.R..V!.......[.10.D ...~vr2..l.#.d."....ZV..V.=N.l..8_..h...j..w...[e.$EiZR..k..c.Y...R.#.y..9..+.V!.?......&ID."+J..b....DEq.j...A..4.....P.....ng'>\...fH.kZR..W..1.....n=.g.^u..-ZDV+.1.7....g.m...Z..+Z.0""k...y35...1y.^kX..Ef.D..5y...r.K...+..)JV.." ...... =.g.^y.rEQZ.v[..NnN.F.yr..kL.S.,x....k......G.....4./.X.p.|<......_>{6\..K..U..,x.<.1X.F....D=.h.^{.5.}...>..<E...>o..>\...1....:9w.b".S

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Roboto[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 18 tables, 1st "GDEF", 26 names, Macintosh, Copyright 2011 Google Inc. All Rights Reserved.RobotoRegularVersion 2.137; 2017Roboto-RegularRo
Category:	downloaded
Size (bytes):	171676
Entropy (8bit):	6.461076726743102
Encrypted:	false
SSDEEP:	3072:Jyz4u0oy2goL/sAQRuzzlPrvRwhRFUzMWlYfxJVBxV+aYT3qPXZ10uNOIOU7og2i:JahOmCeu+bqPp1hWUMxFnI
MD5:	3E1AF3EF546B9E6ECEF9F3BA197BF7D2
SHA1:	DD1B1DB13FF1F72138C134C62F38FEF83749F36A
SHA-256:	79E851404657DAC2106B3D22AD256D47824A9A5765458EDB72C9102A45816D95

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Roboto[1].ttf	
SHA-512:	81A9260AA3597C02C40AB4642C565D7584D99DDCB8A59ADDC92C15BA93F96F05F2C94DC77C2D5C11C1805F593D84E5E9C62373ECC6CA43A76D15C05C1B1D1E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/themes/rise/thrive-dashboard/css/font/Roboto.ttf
Preview:	..... GDEF.B....(....bGPOS.....+@..].GSUB..Y.....OS/2.....`cmap.wX....X...Fcvt +.....0....Tfpgmw.`...-.....gasp.....(.....glyf&.....;...lhdmxUz`z...@....head.j.z...,...6hhea.....d...$hmtx.r.....8loca.w....0.....maxp.>..... name.....$....&post.m.d..(... prep.f....Λ...I.....#...pH_.<.....R.....0.s.....I....I...J.0.....T.....$.....3.....3....f.....P. [... ....GOOG.@.....f.... .....:.. . ....d.....w.~.n...i...e.e.g.....&.r.....N.....5.%.....L...~.s.~...~.].~.^.~.5.~...~...~.M.~.p.~.d.....)...H.d.....K./.j.8.....5.w.?.....I...s.z.....-...j.5.....N.....v.....m.....P...1.0.....=...9.....V.....H.(.....X.@.....y.9.Z.m.}...0.\..._.=.]...<.}.`.h.....j.....[.}....._..... ._.....i.....!...+...).....X...@.....q.....`.i...[...i.3.....Z.X.e.I.[.....f.n...J.Z.....F.a...B...>...{.....C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Unbenannt[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1608 x 668, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	94548
Entropy (8bit):	7.961332407034617
Encrypted:	false
SSDEEP:	1536:jzEIui3mHxGBKWO/P2qacklwqcTQs1uIhSlBq+qTq7Y6EAzDbdE:3Ebs1Kh2Tc4lBQTq06zbdE
MD5:	AB9EEF13C5EF45B9A084CB099BBB0C96
SHA1:	517A32BF5D39C7DD809278AACC9086A47340BDAE
SHA-256:	76846AD0447A5A51936CF51A6109C56160536A351680E546C2C78973D5D56F83
SHA-512:	BF537077731CB44A4D3C34B0F2A8CB4A13CB928AAF520FBEBF1A186C95ED9B1805CA74B0C53B87CF2F75FA53E7A292A0042B8B24A01EB37E475A646F2AD7EA17
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2019/11/Unbenannt.png
Preview:	.PNG.....IHDR...H.....&....PLTE.....TTT.....RRR...fff.....%.....#. .....=77.....633)&'...1--.....[[...,.....E@@Q...A;<...SKL...ZQR..u...jaa.....kU....z..t....r[.}.....~eS....z.....wuu.....{c.w_.....g....krhf....}~~ooo_`bu]J..m.....LEE.....T...kVE.....Q.....$.....QO;-...$4.s.bN>D0"...T...5#.....vs...Q..YE6...9...f.....jc....n.....i...;@H.....~`L.....5ay.....Q..*1:NYcrx.....nbV.....}w_A.)Ul...u..*n.N....bkw.....KLL....S0.....rJ%r.....BKW:w..T46...}....h.....O..!.....Hb...%7K-.....o.m.._>R..}...k\Q.^...Z....T...._$...p...{.3).s0.....C.....n.IDATx..mL.Y..i;.....m^.m...v`..$..L....", #H.&..B....t.p/..Ajg.....l2-.z.d.Q.b".Z..Vz[.....J..Cz.....z.....\u.T.].'...y.9d.R.J.*U.T.R.J.*U.T.R.J.*U.T.R.J.*U.T.R.J.*

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Webp.net-resizeimage__9_-removebg-preview-1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 587 x 425, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	64863
Entropy (8bit):	7.969960690477109
Encrypted:	false
SSDEEP:	1536:V7UYXP6f+2zph0Y4e9VazgaRQ6qce+PQGiQ31GWw7Y2v:tP6fN4erUfPqFeQgG97R
MD5:	5851DD5654454CE840157BAD6EE16E77
SHA1:	840CDBCF72E33B68CF0B18626F5637D1790A21F1
SHA-256:	1263C8CDAA7611FE796EFFCB6F53A63844E94D1A40F68164E4D39AA9487B2DE8
SHA-512:	B8F6572AEC7D5C78EBEA7F14AAD36240B920CACA1D94AC635FE6EE7CE25890EC78C873C8AA7232899C30771226D9C6D0D1D1EF3A6B4C306F7D974F128A1FAAD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2020/08/Webp.net-resizeimage__9_-removebg-preview-1.png
Preview:	.PNG.....IHDR...K.....$....PLTEGpL5%3...x`Z.....VGF.....vf..]T\DCJ...'"+v\Azx{317.....223.....--0...()*..... .....468.....%$#.....t...m..h.....,..F.....s.....xb..9:<.}...DDF.....IJL.....T..>?A<..'. '.-.....:. .....NOR...,..%5J....e... #(..anv...`UE..IA4..].....@7+f\N(...._.C.....=.5.....$.>b..P.#.....UTVZZ\.....neXTL@aP9...w.V...}W0.Kfgi.xU...db_.....rQ.....txmb....wi...qbMWG3.t_..y...w.9.lM6,"k.....rvjW..AnW>.....eGuSs..4.....wx^A>K\.+'utu.....mmn..kh.".~`.....zz{.{een{.lS.1..uZS^mG 1s|.f>`..mE.N.]g...>8`-7w.x.n.]2R.We..e...r9G.4.....].i.5'vcr.do.x.. .kSe.....NZh...9B....QP.?X...=.`X...O7F...rmU0q.`|.my.....ISb...b>.T..|..}q..F\.dO.....Z...vIaZk...]eu.....qx.....$....tRNS.*Lct.....Q.`....IDATx..}.O..gz..9.....1.Q..#.;..B E4.xp?p`.;dv.='.E....X.r..%.....R.5.....i.I.[=..::..y...~...-....K....=dT..j].....U.....~r.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\WhatsApp-Image-2020-08-30-at-19.02.05[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, 1280x720, frames 3
Category:	downloaded
Size (bytes):	88539
Entropy (8bit):	7.956274016794077
Encrypted:	false
SSDEEP:	1536:Bs+CEDeDSJvbtz5gqGvmWOmtvZu8RDUHwVLhetkeQ:BRCEDjx5K1tstTt0
MD5:	DFC1FCB36BBF0FA25B59AF153C57393C
SHA1:	D654AB78AD716BA9F86ADD0B31DD515228F89420
SHA-256:	8F8C8DCC6D6BD59E957ECEE65409CDD8F30C2F9FEB70E6381DABD29A5CF6EC67

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\WhatsApp-Image-2020-08-30-at-19.02.05[1].jpg	
SHA-512:	212885124C89668DE99D32129D54DFA39F98F943EA32F8BB7DF39E601C03A09E42BA5892249BEF5DF6831ED8028C14F32775BDF0CD07FF612D682EDC313798AF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2020/08/WhatsApp-Image-2020-08-30-at-19.02.05.jpeg
Preview:	......JFIF....."..... ....t\.U.U...z.....-{.....>...W...o.E.i.o.yz.....va...4W.1..@.....-K.".:l.3.....#:.....Y.....4.h..m...+.M..@.....:.1(=.d.#U...|.j,a\3...G..d.:..'...).....#.....S.....ri...%;.i.'.. X..v.....l....Q..;."^6..'....${.k`....S.{...=\|...=..Q.cw.....,.....R1..;\|NM..;./$"|4..4{.F...olt..pI.2.a....~.8..i<..9.id.....)...q.2]..O.....Ort..g.'...g2..19.:tL.....H.D..96...4...F.\.h4{.F ...n.....|{...l.fi.....E..lLiif.I..E.....C..;.]..=..]J.M.}m...s/8z.r..1..@.....7.F5.'o....a...gMY.)4.h.....g.....~.8..)...<.)w.....[..$...F.j$].d...Ro<.....lG.s.y.....R1..;|NM. .;./:.....y(.!..6}...2.I...[U~K....J.~..-....-*...$...F.j

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\admin-ajax[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):	92739
Entropy (8bit):	5.07585598384244
Encrypted:	false
SSDEEP:	1536:O5Tqf3pVcLvkkVWRQP5Tqf3pVcLvkkVWRQP5Tqf3pVcLvkkVWRQC:p
MD5:	BFB2AE2AC90D3E0B49089F6CB07A9A50
SHA1:	56D7003C3BD1FDCA69A2D96795FD0C445567F84E
SHA-256:	DBDED4125F0B5EBDE9DB41F070CEDDA5BAE1C7A5A5DC8BE7B142F4DF7393F7D3
SHA-512:	563E9BB95C56D73E52C68AFA10969244CB354DBEEAD5F66FC9EF85811F0654E6F623E6F22D9481CD8A0E4DF5CF1B7CADCD683F1EAC93901CA356CEA82898D C2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-admin/admin-ajax.php?action=twm-css&file=global&ver=3.0.5
Preview:	@import url('https://fonts.googleapis.com/css?family=Roboto:100,100i,300,300i,400,400i,500,500i,700,700i,900,900i');@import url('https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css');@import url('https://code.ionicframework.com/ionicons/2.0.1/css/ionicons.min.css');.theme__sm-6 .mw-elements-wrapper__link{color:white;}[data-toggle~="collapse"]{cursor:pointer;}.bt{box-shadow:0 0 0 1px #000 inset;}.list-none ul,.list-none li{margin:0;padding:0;list-style:none;}.fntWN{font-weight:normal;}.fntB{font-weight:500;}.fntBB{font-weight:bold;}.txtUp{text-transform:uppercase;}.txtDecorNoneAlways{text-decoration:none;}.txtDecorNoneAlways:hover,.txtDecorNoneAlways:active{text-decoration:none;}.bgOk{background:#4ebb74;color:#fff;}.clear:after{content:" ";display:block;clear:both;}.mw-content--editor{overflow:hidden;}.mw-content--editor img{max-width:100%;height:auto;}.mw-content--editor iframe{max-width:100%;margin:10px 0;}.mw-content--editor .alignleft{float:left;margin:5px

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\background_gradient[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 1x800, frames 3
Category:	downloaded
Size (bytes):	906
Entropy (8bit):	5.019973044227213
Encrypted:	false
SSDEEP:	12:V/XPYhiPRd8j7+9LoIrobtHTdbKs/XPYhiPRd8j7+9LoIrobtHTdbKi:dkiPoj7+XrobPbNkiPoj7+XrobPbX
MD5:	65B40239A269922CC6DB52BB57B142CB
SHA1:	C2B0F017A39CADE113A2F3E1E12C229E72A6E134
SHA-256:	13C0147E89DEF62D785AB0C6F772C7A01298DECC8F756DE5A7E7897C6FB84672
SHA-512:	122C07B70BC963D5DCC438E45DE0B31F0D4A3A9D1E3D8C91176A80247CD3FBD13E3C6F3D3F13EC2327CDCE4A8C78D113BA95DC76B3FC80D1ADB3931F57DF 5A8
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/background_gradient.jpg
Preview:	......JFIF.....d.d.....Ducky.....P.....Adobe.d..... .....W..... .....Qa.....?.....%.....x.....s...Z.....j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.....p.....A.....BP..qD.(.....ntH.@.....h?.....JFIF .....d.d.....Ducky.....P.....Adobe.d..... .....W..... .....Qa.....?.....%.....x.....s...Z.....j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.....p.....A.....BP..qD.(.....ntH.@.....h?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bullet[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	894
Entropy (8bit):	7.304718288205936
Encrypted:	false
SSDEEP:	24:/yBJNTqsSk9BTwE05su+xyBJNTqsSk9BTwE05su+R:CssSk7d0wIssSk7d0wR
MD5:	74698D2CCDCD04C5841AA1667204A064
SHA1:	43A2F38051ACBD4C5D722113DB6F8C6A5041DB54
SHA-256:	ADA75B96D514D0011CA905239089F72CF779C8ED5EBA55700C192870880EAF14

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bullet[1]	
SHA-512:	4A09647CDAF0E8D0E7B890F2A7E45C8E848BA697DE49B900419E23EFF2319F7EAA7809FF0874DB670F36A0CBC3DDBF147C986AE0DDBA14456AE7CDF5C18753 70
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.;j.;l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`..PNG.....IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.;j.;l.Zj.\l.5o.7q. <..aw.<..dz.E.....1..@.7..~.....9..:.....A..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`... ....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. ..[U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\cropped-Download-32x32[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	688
Entropy (8bit):	6.648965145437188
Encrypted:	false
SSDEEP:	12:6v/7sq93CEgKGWsCnZ/xrMZiyy7wSTYL2zkupysRu5X1J4Vnbe6wDAixJkc:hw3CrWqZ8cSbznQXN16o6cAi/1
MD5:	E19C22ED5CBB62A3AD1851CE19EC0110
SHA1:	277A110853CD7BBA9803FEBD6E18D51E98DB4164
SHA-256:	2222CCBF6B577B543CAACE492F5964785765D5CB4394F3745A2A39138ADC2945
SHA-512:	052769DF062158D58BA3A6A3098149959A64FA8E7179D7666E4910272E089F2311DEB464FD836FE94EB580E7C960340C96F78FD2FF31FC1C54FF6FDDF6CD33E6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2019/02/cropped-Download-32x32.png
Preview:	.PNG.....IHDR... ... .D.....PLTE]]]^^^]]]^^^^^^]]]eeeccccbjjjLiq]]]]]]]]]]]]]]]]]]hhh]]]]]]]]]bb`vvvggg]]]]]]]]]]]^^^ddddddfff]]]]]]]]]]]^^^xxx]]]^^^]]]nnn^^^]]]aaa__^]]]]]]]]]^^^]]]]]]]]^^^]]]iii]]]]]]]]]]www]]]]]]]]^^^____]]][>.{...CtRNS. ..".....=*....8.....0..... +...../..#....Ay...!..Id....7..;.m....PIDATx...v.0..m.mVb.$@.N.....2&..@{.."2G..$.~U.Y\.....a) &fEdR..v.t._...)@.,,.~.....}vy.$..k.h;z..q{s:..6i?t..q..xw....3..v..Og..i..F.C[..x.A..s..:.x.d+.3.....t..d..T.2.2.i..^.R.Eb(r.v.-.."s.Eb.....R.... #H."4.4.....`$..I...E...<.C..$[..^..7.....t..5 ..._....@.B.n..45U.FW....T.....Ad.....Z.....I.#.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Reputation:	low
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\fiverr-arbitrage[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 756 x 492, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	26540
Entropy (8bit):	7.969814680997281
Encrypted:	false
SSDEEP:	768:n0EOQh6hJ53ft0FCuuGCr+MseTp3nw0g+:0zQh6hJ5l0F7E+Yp3w1+
MD5:	47EAF917B3E301723BF2B8716AD252D5
SHA1:	6D4A765D1889F09B2110F7F5679609D5BBD67895
SHA-256:	F932729D53BD6EE4164FCFDF05C2ED1CD02F7A0EF9CCB25D4FA35A9E22E3B684
SHA-512:	06F85938FE3DCFD31BD6C3C484BFC045DC2507493706BF6CAE8C1EF72F6FEBDC9DF8CC3632107A337D2A4084BCFBC5F3D8B64A45A8AB6ECE369BA3A394E8F A07
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\fiverr-arbitrage[1].png	
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2019/12/fiverr-arbitrage.png
Preview:	.PNG.....IHDR.....o.O....PLTE...```]E.J5.....L6.---iii.....7'....A.....9(.....WA.....C2.(((.....###...K6.$...jkQ.=+.T>.....(.....???.....d.\\\..,.....{`.1!.....G3.....i.eM. ..bM.....som...NNN...}....WWW.....vZ.5%.P<.JJJ222i.....777iko.j.....`I....DDD.r....i..j.....I6.....ivwwu.....RSR.....mk.m.....}}~.....jk.....\.h.....t8.J1]..x.....E>.....q...oBC....*h.....t.....nv.....I:....#.9x.....w..kj..j....o.}...u.....O.]rw.m..8R.!u..y.....=K....w..m.K9.....}.....yn.....y...mx..mk.|q.....v.u.....us.....j|.....y..~.z.....z.....b..dmIDATx...j.....Z.X0b..F.J..h....J+zK)..n\HApa.0<.W.=.....5..Lb..{z..w...d>..kf.....'MI.Z..W.:).N.z....^..W.:).N.z....^..W.:).N.z....^..W.:).N.z...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\font-awesome[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	troff or preprocessor input, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	37414
Entropy (8bit):	4.82325822639402
Encrypted:	false
SSDEEP:	768:mmMtI+A4CSIDqvnI+YTBrFPvVrJjhiRAiiEL:mXtI+A4GDUI+Y9rpVljhiIEL
MD5:	C495654869785BC3DF60216616814AD1
SHA1:	0140952C64E3F2B74EF64E050F2FE86EAB6624C8
SHA-256:	36E0A7E08BEE65774168528938072C536437669C1B7458AC77976EC788E4439C
SHA-512:	E40F27C1D30E5AB4B3DB47C3B2373381489D50147C9623D853E5B299364FD65998F46E8E73B1E566FD79E97AA7B20354CD3C8C79F15372C147FED9C913FFB10
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css
Preview:	/*!. * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome. * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License). */./* FONT PATH. * -------------------------- */.@font-face {. font-family: 'FontAwesome';. src: url('../fonts/fontawesome-webfont.eot?v=4.7.0');. src: url('../fonts/fontawesome-webfont.eot?#iefix&v=4.7.0') format('embedded-opentype'), url('../fonts/fontawesome-webfont.woff2?v=4.7.0') format('woff2'), url('../fonts/fontawesome-webfont.woff?v=4.7.0') format('woff'), url('../fonts/fontawesome-webfont.ttf?v=4.7.0') format('truetype'), url('../fonts/fontawesome-webfont.svg?v=4.7.0#fontawesomeregular') format('svg');. font-weight: normal;. font-style: normal;.}..fa {. display: inline-block;. font: normal normal normal 14px/1 FontAwesome;. font-size: inherit;. text-rendering: auto;. -webkit-font-smoothing: antialiased;. -moz-osx-font-smoothing: grayscale;.}./* makes the font 33% larger relative to the icon container */..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\google-ranking-secrets[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 764 x 487, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	34650
Entropy (8bit):	7.973061374333719
Encrypted:	false
SSDEEP:	768:Ei2dQ3aqM0W/8FW7GZ3CJDIYosbXaaQqngVyKOA8s2:DCyM0WUFWaZyOYXaaRgVxu
MD5:	E4A37BE161067639A322F333E12D1EDA
SHA1:	12E8FB7446AC516BFF5EF1BC7FA974E0B6705EF2
SHA-256:	1DFDD88A1FBE227CF237C81C411CEF4E4144B6A2D0614E0FE6ACFEBB28E2C782
SHA-512:	DC8DA508D6FAD077A2364B1C376CF48E468B6CAF49A736BD0C356E8AE245D8E70321D1DDD6DF1AA3431DE0377A93C03770324CF662F12E3FBA612BB32E9165F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2019/12/google-ranking-secrets.png
Preview:	.PNG.....IHDR.....yx....PLTE...4~...<..:.7 .8!^D.....___.6....3|.iij.....0001z...9.....4./w..5...4..7..-.....6pS. ....1,q.....2.n$-..[B.P:..t..3...J5.....6%..+...'f...$c....*m.,.....x)....}+)i...#`.....j.h!.-.... [.....e.....1.....0..G..W.....2.>+..a."^.D0..).....t'...hM..o...(((`..###.....WWW.(.....y[..P..a.....T..[.....4n."..$.....B..%..!.....j.PPP.t.....$T.....AAAe...=~.N....L.t...S.,,,.{.555.....III...,`.<.k...t.rss.....T>..x..k...k...A...4...8.B..I.U.....<<<+...-..%.....Eln.....*....i.aG.....zzz.mj.....ms.....k..u...t..n...o....umi.....o.....q.....m.n...|....j....v.....xv....lv..vl....q..y.....jk\z..ii.R..BW.V..in.4+6c..W....8A..k...c.....IDATx..?..>...c.... ... .....`BX..q.$.L.....=.i{..H.}Ps..w9..hi.i..j.SR...J... _..R.+.V.~..J....."..Ro..W...J... _..R.+.V.~..J...[)..z+..Ro..W...5.N.eY.<.H....7....."..Jm..J:.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\httpErrorPagesScripts[1]	
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\imagesloaded.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):	7994
Entropy (8bit):	5.110035708360205
Encrypted:	false
SSDEEP:	192:Jiryv7A3goz0aForCrK7r2zjqwr5s2gc/y66DOP:JiuvMtz0aForCrK7r+Vr5sO/y6B
MD5:	D0C2C0D7E37652E66657C8C8D6376442
SHA1:	F26118A43E9999E34BFBA542DB365F123F6EBAD2
SHA-256:	854D677B850907CD851EAC7E3F02F05A1E056F05BD5563199C5D93044FF16840
SHA-512:	353885B5502C4AE3530D863A47F3DF228402F5BA0B76D072D6F662D3D253970343C9230E772E44609EB0CA47A0D664E7F6C134491CA45BB78755727F19066A4D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-includes/js/imagesloaded.min.js?ver=3.2.0
Preview:	(function(){"use strict";function a(){}function b(a,b){for(var c=a.length;c--;)if(a[c].listener===b)return c;return-1}function c(a){return function(){return this[a].apply(this,arguments)}}var d=a.prototype,e=this,f=e.EventEmitter;d.getListeners=function(a){var b,c,d=this._getEvents();if("object"==typeof a){b={};for(c in d)d.hasOwnProperty(c)&&a.test(c)&&(b[c]=d[c])}else b=d[a]||(d[a]=[]);return b},d.flattenListeners=function(a){var b,c=[];for(b=0;b<a.length;b+=1)c.push(a[b].listener);return c},d.getListenersAsObject=function(a){var b,c=this.getListeners(a);return c instanceof Array&&(b={},b[a]=c),b||c},d.addListener=function(a,c){var d,e=this.getListenersAsObject(a),f="object"==typeof c;for(d in e)e.hasOwnProperty(d)&&-1===b(e[d],c)&&e[d].push(f?c:{listener:c,once:!1});return this},d.on=c("addListener"),d.addOnceListener=function(a,b){return this.addListener(a,{listener:b,once:!0})},d.once=c("addOnceListener"),d.defineEvent=function(a){return this.getListeners(a),this},d.defineEvents=f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC134
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.../...0.....#.....IDATx^...pUU..{....KB.....!....F.....jp.Q.....Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{.....[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po.....X..;.=.P...../...+...9./..s.....9..\|.....*.7v.`..V.....-^.$S[[[.....K..z.....3..3....5 ...0..."/n/.c...&.{.ht..?....A..I{.n.....|....t.....N}..%.v...:.E..i...`....a.k.mg.LX..fcFU.fO-..YEfd.}...~."......}l$....^.re..'^X..*}.?.^U.G..... .30...X.....f[.l0.P`..KC...[..[..6....~..i..Q.|;x..T .....s.5...n+.0..;...H#.2..#.M..m[^3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..l[..a...N,,.h.....5...f*.y...}...BX{.G^...?.c.....s^..P.{..G...t.0.:.X.DCs.....]vf...py).....x..>-..Be.a...G...Y!...z...g.{....d.s.o.....%.x.....R.W.....Z.b,....!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a)..t..e.j.W.....C<.1.....c..l1w....]3%....tR;,..3..-.NW.5...t..H..h..D..b.....M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery.masonry.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1819
Entropy (8bit):	5.047296238035306
Encrypted:	false
SSDEEP:	24:aUTV//j2ew8p/xnqy8VLF8Xlm7uEQGe1dLpDXzRRvCpx+zVfDpnOKLJWbqQApIsi:HgQBq5LYlm71TopDaW1ObqhuqVcPf
MD5:	CD0EB3406096FF80266E7C9D7D419186
SHA1:	0E3709691BF96233766DE30E2FD473B84166C5B6
SHA-256:	C2E606E1FC82EA3A554AAD5D0520E25D2677B89A891DC5C49E7ACE08FCE92E25
SHA-512:	3CAF5308CDBC5F42F1ECCF5944E8CA785AC086B85954765C1F40D91BD9CC9F3FE6EB816AD821B534F9AD36395F4B6B5D361BEA24EB272E94CAD2824F03FAAC6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-includes/js/jquery/jquery.masonry.min.js?v=1.500.1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery.masonry.min[1].js	
Preview:	/*!. * Masonry v2 shim. * to maintain backwards compatibility. * as of Masonry v3.1.2. *. * Cascading grid layout library. * http://masonry.desandro.com. * MIT License. * by David DeSandro. */.!function(a){"use strict";var b=a.Masonry;b.prototype._remapV2Options=function(){this._remapOption("gutterWidth","gutter"),this._remapOption("isResizable","isResizeBound"),this._remapOption("isRTL","isOriginLeft",function(a){return!a});var a=this.options.isAnimated;if(void 0!==a&&(this.options.transitionDuration=a?this.options.transitionDuration:0),void 0===a||a){var b=this.options.animationOptions,c=b&&b.duration;c&&(this.options.transitionDuration="string"==typeof c?c:c+"ms")}},b.prototype._remapOption=function(a,b,c){var d=this.options[a];void 0!==d&&(this.options[b]=c?c(d):d)};var c=b.prototype._create;b.prototype._create=function(){var a=this;this._remapV2Options(),c.apply(this,arguments),setTimeout(function(){jQuery(a.element).addClass("masonry")},0)};var d=b.prototype.layout;b.prototype.la

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\lightbox[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	3091
Entropy (8bit):	5.185727344848934
Encrypted:	false
SSDEEP:	96:rmFBI6NIPYyEc/NSaDqJ7LVWGa0mf6m6x:M7dc12p
MD5:	0AAEFCBC0BA3BE7DB23E7EBE45974FC1
SHA1:	3E6BD0BB958098539A8C2B2A9791CED88580E695
SHA-256:	0A2B1C4321710752A2874A4703D2B2E00164B062C631E9E24DF3DC72A841FBB9
SHA-512:	C69C3F6123068578A2ECC3DF6D2497BF38C1F5488327BB8CF0C74B970AA7AC61DFAE5A96811613E4C2F4CA1666EE579A277CD07EF9E8EF52C5897E762169B99
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/plugins/wp-product-review/assets/css/lightbox.css?ver=3.7.11
Preview:	/* Preload images */.body:after {..display: none;..content: url(../img/close.png) url(../img/loading.gif) url(../img/prev.png) url(../img/next.png);.}...lightboxOverlay {..display: none;..position: absolute;..z-index: 9999;..top: 0;..left: 0;..opacity: 0.8;..background-color: black;...filter: progid:DXImageTransform.Microsoft.Alpha(Opacity=80);.}...lightbox {..position: absolute;..z-index: 10000;..left: 0;..width: 100%;..font-weight: normal;..line-height: 0;..text-align: center;.}...lightbox .lb-image {..display: block;..max-width: inherit;..height: auto;..border-radius: 3px;.}...lightbox a img {..border: none;.}...lb-outerContainer {..position: relative;..width: 250px;..height: 250px;..margin: 0 auto;..border-radius: 4px;..background-color: white;...*zoom: 1;.}...lb-outerContainer:after {..display: table;..clear: both;..content: "";.}...lb-container {..padding: 4px;.}...lb-loader {..position: absolute;..top: 43%;..left: 0;..width: 100%;..height: 25%;..line-height: 0;..text-align: cent

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\masonry.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	28954
Entropy (8bit):	5.18028295721513
Encrypted:	false
SSDEEP:	768:S9+z0BFXYKby+HvOqvevgOkYtkdEvWBzigMPIW:SgKbbO0IkdEvPgS
MD5:	5420B6516C14245B504E7240A8310F2C
SHA1:	BF6D46E754ECA13C3074F002ABB124E55EF4C3AA
SHA-256:	3CA3E467B7D4D6B403AA4619019D9250B11449C8EE9C91C90BCBC9ACDD64FEA2
SHA-512:	D072090BA5351427D1CD9113F00494FAA967FDEA3F6514FA66C5291907F1838B6FAC45ABD25DB1EF66519C0B0D0C39375628438AB3908689D41B704444C27A2D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-includes/js/masonry.min.js?ver=3.3.2
Preview:	/*!. * Masonry PACKAGED v3.3.2. * Cascading grid layout library. * http://masonry.desandro.com. * MIT License. * by David DeSandro. */..!function(a){function b(){}functio n c(a){function c(b){b.prototype.option||(b.prototype.option=function(b){a.isPlainObject(b)&&(this.options=a.extend(!0,this.options,b))})}function e(b,c){a.fn[b]=function(e) {if("string"==typeof e){for(var g=d.call(arguments,1),h=0,i=this.length;i>h;h++){var j=this[h],k=a.data(j,b);if(k)if(a.isFunction(k[e])&&"_"!==e.charAt(0)){var l=k[e].apply(k,g) ;if(void 0!==l)return l}else f("no such method '"+e+"' for "+b+" instance");else f("cannot call methods on "+b+" prior to initialization; attempted to call '"+e+"'")}return this}return this.each(function(){var d=a.data(this,b);d?(d.option(e),d._init()):(d=new c(this,e),a.data(this,b,d))})}}if(a){var f="undefined"==typeof console?b:function(a){console.error(a)};return a.bridget=function(a,b){c(b),e(a,b)},a.bridget}}var d=Array.prototype.slice;"function"==typeof define&&define.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\matl996[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):	54621
Entropy (8bit):	5.28904522785664
Encrypted:	false
SSDEEP:	768:Qg4xeJKhbtproEXWZrif1mN4+3dQl0uYTPtv4Fnxf6:Q1MKhbtprXmZrilxl0uYTPtv4Fnxf6
MD5:	A51FA03AB3002141DD3E6D72558D1998
SHA1:	5C14D15A029F772017F5483134D48221D67A4C80
SHA-256:	74349D545D94BADF3E6DDC6EF736E03B8DFBE86DA6D11503DBDE64EAD0FD1593
SHA-512:	12FC5A333877E4084B162C287C444373442A60E4D4787579CE9867F9FB5A61DBCBDD40C4AD0018561D71379DD28EB3636AE7265017C79F5FE30D321F69D16972
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/author/matl996/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\matl996[1].htm	
Preview:	<!DOCTYPE html>.<html lang="en-US">.<head>... [if lt IE 9]>..<script src="https://bonusbomber.com/wp-content/themes/rise/js/html5/dist/html5shiv.js"></script>..<script src="//css3-mediaqueries-js.googlecode.com/svn/trunk/css3-mediaqueries.js"></script>..<![endif]-->.. [if IE 8]>..<link rel="stylesheet" type="text/css" href="https://bonusbomber.com/wp-content/themes/rise/css/ie8.css"/>..<![endif]-->.. [if IE 7]>..<link rel="stylesheet" type="text/css" href="https://bonusbomber.com/wp-content/themes/rise/css/ie7.css"/>..<![endif]-->..<meta name="viewport" content="width=device-width, initial-scale=1.0"/>..<meta charset="UTF-8">.....<title>Bonusbomber, Author at Bonusbomber</title>.. This site is optimized with the Yoast SEO plugin v11.3 - https://yoast.com/wordpress/plugins/seo/ -->.<link rel="canonical" href="https://bonusbomber.com/author/matl996/" />.<meta property="og:locale" content="en_US" />.<meta property="og:type" content="object" />.<meta property="og:title" cont

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\moxie.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	89142
Entropy (8bit):	5.484603350034357
Encrypted:	false
SSDEEP:	1536:x1TKM+gLpJNTOL4VnexxK1oH6u7OvK4g96Ov+pEDCx:VHOLCnexxK1MjFDY
MD5:	68DEC65B1E80B2B66994F4700762B65C
SHA1:	51C480AEC2C1D961F17FC78805686F937EEC3C5F
SHA-256:	BFAF6009146BF2144A14820F24ECF368D2354FF337584BAD42A93FA606023CA4
SHA-512:	86FBE6FF515E8FDBEC2B36C5B1E576027EB5130AC7910F9C8A8A0A90C7EDB65B5B7F2C9CEC78D397CDE9A6DB77549E0289BEF0AEF2CD4A94235DAA98B99E3747
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-includes/js/plupload/moxie.min.js?ver=1.3.5
Preview:	var MXI_DEBUG=!1;!function(a,b){"use strict";function c(a,b){for(var c,d=[],f=0;f<a.length;++f){if(c=g[a[f]]||e(a[f]),!c)throw"module definition dependecy not found: "+a[f];d.push(c)}b.apply(null,d)}function d(a,d,e){if("string"!=typeof a)throw"invalid module definition, module id must be defined and be a string";if(d===b)throw"invalid module definition, dependencies must be specified";if(e===b)throw"invalid module definition, definition function must be specified";c(d,function(){g[a]=e.apply(null,arguments)})}function e(b){for(var c=a,d=b.split(/[.\/]/),e=0;e<d.length;++e){if(!c[d[e]])return;c=c[d[e]]}return c}function f(c){for(var d=0;d<c.length;d++){for(var e=a,f=c[d],h=f.split(/[.\/]/),i=0;i<h.length-1;++i)e[h[i]]===b&&(e[h[i]]={}),e=e[h[i]];e[h[h.length-1]]=g[f]}var g={};d("moxie/core/utils/Basic",[],function(){var a=function(a){var b;return a===b?"undefined":null===a?"null":a.nodeType?"node":{}.toString.call(a).match(/\s([a-z|A-Z]+)/)[1].toLowerCase()},b=function(d){var e;return

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\plupload.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):	15742
Entropy (8bit):	5.3987636897505675
Encrypted:	false
SSDEEP:	192:mRbxuEw6h/6YH7iYLp1xhlzrmw2WZkzw+VKKzezUdpzCpBh1z4MOBrbu8ZNlwNVx:kkEw6h/9z7B57OblOY7bff8KRXI2FoN
MD5:	47D38D462D5FA882A92DBD2B54D5D747
SHA1:	C4D6E955A0CE86646CA98A14CDAB135D0C56A130
SHA-256:	EC04A17E8917687B7AB3B9FC9486F9A2263E43DF2D058190566D032BF3A7457B
SHA-512:	E08363026F5BEF7CB092582EDAAF1AFBB65578EAE1BA0445F9C0A376D0583785051F88C33078F400493EC001D9F5B2066E40A60CDA1EC59BDCA256966DDB5E94
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-includes/js/plupload/plupload.min.js?ver=2.1.9
Preview:	!function(a,b,c){function d(a){function b(a,b,c){var e={chunks:"slice_blob",jpgresize:"send_binary_string",pngresize:"send_binary_string",progress:"report_upload_progress",multi_selection:"select_multiple",dragdrop:"drag_and_drop",drop_element:"drag_and_drop",headers:"send_custom_headers",urlstream_upload:"send_binary_string",canSendBinary:"send_binary",triggerDialog:"summon_file_dialog"};e[a]?d[e[a]]=b:c||(d[a]=b)}var c=a.required_features,d={};return"string"==typeof c?g.each(c.split(/\s*,\s*/),function(a){b(a,!0)}):"object"==typeof c?g.each(c,function(a,c){b(c,a)}):c===!0&&(a.chunk_size>0&&(d.slice_blob=!0),!a.resize.enabled&&a.multipart||(d.send_binary_string=!0),g.each(a,function(a,c){b(c,!a,!0)})),a.runtimes="html5,html4",d}var e=a.setTimeout,f={},g={VERSION:"2.1.9",STOPPED:1,STARTED:2,QUEUED:1,UPLOADING:2,FAILED:4,DONE:5,GENERIC_ERROR:-100,HTTP_ERROR:-200,IO_ERROR:-300,SECURITY_ERROR:-400,INIT_ERROR:-500,FILE_SIZE_ERROR:-600,FILE_EXTENSION_ERROR:-601,FILE_DUPLICATE_ERROR:-602,IM

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\product-280x150[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 105 x 150, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	6758
Entropy (8bit):	7.9609477801007715
Encrypted:	false
SSDEEP:	192:WX9EwqQiGhjr+ADGL8uITETPO/lDXJajo:WX9EwuGhjyJdITE8DXJco
MD5:	99A788AE06B83537D51431AE13976CE0
SHA1:	3A4C9AEF7602F46934211CB29AFBBF5E53F8F134
SHA-256:	D144D7A9142CD165C52C8374798D1E5128B35DA6EF91D41AB68BE2312A489258
SHA-512:	16088305842EE9F6237E1FF12235D178984B3DAE13FEB203B300A988C752E1CBAF5DAFC2D04F93B14045A7A147C2AAE53A2E50AC0F9A10C30C972060F78908BD
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\product-280x150[1].png	
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2019/02/product-280x150.png
Preview:	.PNG.....IHDR...i.....V.....PLTELiq.....9.#5k%/PFO^.0...O....G...V.7.....)^#.....9.$?.....<..<.....+....;....2....L..O....4..3....4m....#....J.....y.ru...k{.q....1..0..=..5..<..<...O.:...R.5..9...Z">.....2.....-~%D.)D....$B..7..7..<.%F..9...U.]...+;q...$A.....3.....5..(b.4.....7.%6I....#a.4..0h'D.....#....M!?.4Bq.....K.....:Huh{...&)7g...IT}CPzp..6Q ..#Z@X.au.....1K....1>j...../aMc.AMs...<DjE^....T_.bi..+xNZ.SDqYn..KVSi.x..)>.)..Ze..h?...'M..OH.A...7dGj7P....6?.....OVr.....oH`'...q...W...m.....v.Y0X. .cn....A@}3.....&..3.....|WM.,....Hpv..z.+7|....f.D...+.~.....}..Z..k...t.{.w...&..-'v.....}J.-...0\.E....~..VN...*TnjdV..7.....4....?..$.....].....n.=.R.. !.jP.fo.....3.j...U.dJg...8.Y{.]N. o...c>....@ .....1tRNS...5...t.uX.....C..3.....ux..Yt.T.....}..u..KYr.....IDATx...TSW.....u:S....>..y..VE.B%....Z./y.L.$1O.1...(.!..W(*Ph.X..8Z[...^_....w...{.w...}.9.$'@.....`.....{..Z|!.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\traffic-booster[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 766 x 494, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	45128
Entropy (8bit):	7.908011474902313
Encrypted:	false
SSDEEP:	768:0e6sssE7Kd+dQZub39noVIsDYcdqpg/ak1ZzOL30Bg/3bw50d4YT7Y6DRb1fj/Z5:Wed7Z+Pskc8pYib0BUrS0d4YT7Yw5
MD5:	CAE209D7803472EEB7B43DA38DC0F0FE
SHA1:	62734E982665F59BC1D34324DF1502328183F684
SHA-256:	1C7CECDE9567235015E9C4DCA341BDC9359A2A7A7FE989BE2387268E6E0BEE4D
SHA-512:	FF760F69E8E1793C438F67DF56912EC3395E593805E31CB4251EAE9D3CCB30DF989EA88C9B0B9DF1E1558098817065169B967E3B938B8DABCD26E1155E532685
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2019/03/traffic-booster.png
Preview:	.PNG.....IHDR.....PLTE.....()=.....1.....!"501C.....(.. ...45H...9;L. 4.....$.....$%:23E..-...>?O...+,?```..3.u2.....A..'.....#]D.....K...iii..*,, ,.~A..!.....(79K.z:..,...x6.....%.....".s,.....ABQ.|>....."$8.....###.._.....F\\]...T>.(((.....>=>BBC...!.....VVV.....*..LLMvvw.....PPQ111...||}...I5.GGH.j889.....D5 %.....555.....ddf...j..jjo>,.....i.....|^.....ppqj.....h...%.....oT..^9.r.,&4.z....eL..p4.t2ks.....K0...jmy<5B6/=z.....G..nl]]iQ=A.....os..y.j..h-._/xE7....zo %.+...5..zmi...TUb..iK,/MNZ...YA...;&.^50.zF.dB.k....RC...ycB?.k....jD.Z...."..I..nr.;..b<.....l.y.....`D.qB...~u.....g4.}j.k.r(..Q....S.....k.R4..y.U2..y.....]....IDATx..k.H.. .$..S.....&6&..0lsE...#\.U.H.@.P'x.b.,.,...bQ.Fu...i53.<.i...4.}.v.k..<.<...HI.V....K./5`I...,...%...F.')..H./5`I...,..%...$.R..._j...K.X....K./5`I...,..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\unhustled-6-figure-freedom-review[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):	83130
Entropy (8bit):	5.287978867764342
Encrypted:	false
SSDEEP:	1536:oAMKhbtprbAypDg3Wz7tZVqYUnd+9Il0uETPtq4Fnxf6:LhbtprbFtg3Wz7DVqYUndqIl0jTPM4VY
MD5:	66EFC13C7539BD68367671C96ECFCBC2
SHA1:	05D38584721DE21F28239CF5F91C9156280B9EEB
SHA-256:	AA0CE31DA04B61F30560360C31CDDCBDF575CACF0CD92FF3983DC4C7BB605835
SHA-512:	459C0D3163F40FC7B9E509881A708D6EEDBFDE81A2FCAE87E0BF17830495957095A1B1398F5FD6C736652909070F398A9530377C29AC4A5E0AA24EFE9002A272
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/unhustled-6-figure-freedom-review/
Preview:	.<!DOCTYPE html>.<html lang="en-US">.<head>... [if lt IE 9]>..<script src="https://bonusbomber.com/wp-content/themes/rise/js/html5/dist/html5shiv.js"></script>..<script src="//css3-mediaqueries-js.googlecode.com/svn/trunk/css3-mediaqueries.js"></script>..<![endif]-->.. [if IE 8]>..<link rel="stylesheet" type="text/css" href="https://bonusbomber.com/wp-content/themes/rise/css/ie8.css"/>..<![endif]-->.. [if IE 7]>..<link rel="stylesheet" type="text/css" href="https://bonusbomber.com/wp-content/themes/rise/css/ie7.css"/>..<![endif]-->..<meta name="viewport" content="width=device-width, initial-scale=1.0"/>..<meta charset="UTF-8">.....<title>Unhustled 6 Figure Freedom Review by Sean Donahoe - Bonusbomber</title>.. This site is optimized with the Yoast SEO plugin v11.3 - https://yoast.com/wordpress/plugins/seo/ -->.<meta name="description" content="Unhustled 6 Figure Freedom Review . In this new course by Sean Donahoe called Unhustled 6 Figure Freedom, you learn the secret

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\y3bsasezzq3jopbwtn0v-280x122[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 280 x 114, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	5796
Entropy (8bit):	7.831992859367212
Encrypted:	false
SSDEEP:	96:WkwLOhHdZ+gv464Egp1rSa98AWV1bx9QlO1++cwXvsgO8c3CCVq9wXhdWlnoPT:oLOj7465K0iY1bxOUIcEgO8gF49wxUl2
MD5:	007418C6557EEF8BBFE0CB2A851A70E7
SHA1:	F59B77E2CCCA10CAA82CC147F9C2E0767D4E44CD
SHA-256:	924B9F1564A5D597F93DBF21676C341577FC6E325597839DA331857941D92472
SHA-512:	456828175DB8A24C0EF14295120EB21F794D4B812C44B2B5F913971294BEB44CD774762CCB964772B840F42389C3931B3C6A68B2D305F94EA37CBF0C3BD83829
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2019/10/y3bsasezzq3jopbwtn0v-280x122.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\y3bsasezzq3jopbwtn0v-280x122[1].png	
Preview:	.PNG.....IHDR.....r.....H>6....PLTELiq9...@".J, ...en%v..K0hf..x..F$"v..G$.w.ve.....I+!v. w..H(!v.7s. w.hf..G'Pl..w..F#Fn.%v..[[cg."v..F$.w.Co. w..G% w..G%=p..Rl.[d 5r..F$.w.<q..RJ.w..w..G&8r. w..F%!w.2s..US.F#!v..F"!w..O@.H*.F# w..F#/t..F#!v..F#.N<"v..F#"v..F#.w..w..G&.N<.w..O@.F#+t..F#.M; w..F# w..L4.F".F#!v..J- w..F#!v.. H(.w..F# w..F"!w. w..F#.J..w..F#.w.&u..L4.w..F#.w..I+ w..w..w..F# w..J/.w..F$.F# w..J, w..F".w..w..F#.J,.w..F#.w..H*.w..F#.w..F# w..w..F#.H).w..F$.w..F# w..w..w..F$.F#.I* .w..w..w..F#.H).F#.w..w..w..F#.w..H(.w..w..w..F#.w..F#.w..F#.F#.w..F#.w..F#.w..F#.w..F#.w..F#.w..F#.w..F#.w..F#.G&.w..F#.w..w..F#.w..F#.w..F#.w..F#.w..w..F#.w..w..F#.w..F#.w..F#. w..w..F#.w..F#.F#.w..w..F#.F#.w..F#.w..F#.w..w..w..F#.?.....tRNS..... ..... !##$%%&'))++,-./1245558888;;=>@@@CCEEFGIJKLMMOPQRTVVWXXZZ\]^^``bbfgijklooqssuuwwxy{}}}.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\youtube-affiliate-hack[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 758 x 486, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	47521
Entropy (8bit):	7.973345798502962
Encrypted:	false
SSDEEP:	768:RxluTIeNOa7L8Hp4DC9CUZPzco83vdkBpyYLOoHzWi91a/kCLV8sK3kZF4F:RxcIeNngSbU7TqW7yN+9pCLV8sL74F
MD5:	71C44F477C0F08B7E38E53C44792AC74
SHA1:	383AC65DE1AFB59E46004D0C8BBBA8BBAB426DBE
SHA-256:	599E608BC1C4DCF4EC50DDD02EB8C4265D1B1A0C678F4790EFC391EC2018BB3E
SHA-512:	C35493E442E3B0E57A7997390C295D4F22EC3FC719CF58DB07F1FC8C2340E75CA56137BCCED06A3D9184E6EE9030BF0E0DB3739898417412681A4AA2FE8AD51
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2019/12/youtube-affiliate-hack.png
Preview:	.PNG.....IHDR...../:.....PLTE..... .....1.....$..A..O.....)..%..`..6..'''''r..4#.(((...C(.000...?2.444Q0....K6....N>....???...U D....WG.VE#_E.....GGGdF.....dL....kO.RRRsV.sU.ZZZ.*y[.[].^^^.13.`.aaaddd.g..h%jij.l..@@ko..q+tts.nkym..w!.l..{1n{..TS.k..sm..... u..j....7..... .q..%..9.kl..j...~.....m...1..E.....rr...2....D....l....k.....3...L.....9.O....?.{.2.6.I.:.\...*.....I....%..%.....%.3....A..9..4....."...$.....#..0.."....."....+.....I..... ...../..$..9..C..*.. .. :..)..T..(..2..$..B.....e..5..J..(.....(...nIDATx...K.[.....L5...y...A.....}....H..6..=....*.A....."(.w01.ll.d&.d22.Wg 2&1.?.w.|.$.....eM....g...u....A.<`. .P....{(..?.=.C..>..%....S..o....=.....A~..._.....r.....r....k....=.^..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\youtube-marketing[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):	25061
Entropy (8bit):	5.417836485679635
Encrypted:	false
SSDEEP:	768:Qz4tuJKhbtproZc6mN4+2HidQl0uYTtv4Fnxf6:QA8KhbtprocY3Fl0uYTtv4Fnxf6
MD5:	F8F85572134735CFF1E6526C35D9FBD8
SHA1:	302D1C2F1B008B4F72378628D4E572F13005207F
SHA-256:	29691F7D8801F213805949805EC6EF1154E4B9959855FAF62147321B5CDEC978
SHA-512:	A6261BB8F19FBD790EFF808096211DC9BBD4CEE5871DABA082221878F6BF5DA04CA3F48F17C488CD108D6FB27683362430C6E8650BB7CED6AAC57F1F6BD900 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/category/youtube-marketing/
Preview:	<!DOCTYPE html>.<html lang="en-US">.<head>... [if lt IE 9]>..<script src="https://bonusbomber.com/wp-content/themes/rise/js/html5/dist/html5shiv.js"></script>..<script src="//css3-mediaqueries-js.googlecode.com/svn/trunk/css3-mediaqueries.js"></script>..<![endif]-->.. [if IE 8]>..<link rel="stylesheet" type="text/css" href="https://bonu sbomber.com/wp-content/themes/rise/css/ie8.css"/>..<![endif]-->.. [if IE 7]>..<link rel="stylesheet" type="text/css" href="https://bonusbomber.com/wp-content/themes/rise /css/ie7.css"/>..<![endif]-->..<meta name="viewport" content="width=device-width, initial-scale=1.0"/>..<meta charset="UTF-8">.....<title>Youtube Marketing Archives - B onusbomber</title>.. This site is optimized with the Yoast SEO plugin v11.3 - https://yoast.com/wordpress/plugins/seo/ -->.<link rel="canonical" href="https://bonusbomb er.com/category/youtube-marketing/" />.<meta property="og:locale" content="en_US" />.<meta property="og:type" content="object" />.<meta proper

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\2969352_1546835250916bundle-1024x300[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, 1024x300, frames 3
Category:	downloaded
Size (bytes):	68020
Entropy (8bit):	7.970124030372086
Encrypted:	false
SSDEEP:	1536:BrVQONhqMMS3rRb5B5QYbitgO+0dYBS09ucx5LFoY:BZtxM0XbOTd8S8uC9FP
MD5:	CF78AB171C565F1E8544C275EBD0D0C0
SHA1:	BBD366F6927BB23091D6174FF218F46BF8071EAE
SHA-256:	D7F7B30823D485EDFC82D67D780CB0597753B8316E2A6520C134CE7A5918C0FC
SHA-512:	076C6E3957515D755AB84322C0D324C1E952674A7EC1CFE48322BA64D249A74DB35B0316171807EBC4ACDEDB25AF5CF9599C4A8AC0C62D57B542F5A00EA5A6 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2019/11/2969352_1546835250916bundle-1024x300.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\2969352_1546835250916bundle-1024x300[1].jpg	
Preview:	......JFIF.....'!..%...".."%()+,+. /3/*2'*+*.....*...**********.....,.....&..... ....$MN.P.= .....<..q..T.E....mR@:.....'ju*}.....:.R.V.{.b.....g.....{...;nh..Yy.....H:.N...F.=Sd.+.J.J8..:...b....._#.g..@....^[5l.W...o@.....uJ.a.(i..].mZ. \m..1.^8.....G.t<....#}y&.3..V..i.m..+.....9.7.jw..2L.Xm.J....*f....).....y3..e.G...]..r....K..TI..'....._.l.....e,.v.Y.{..q.A....&8k....^.....y3.]7j....T....0.,.X.9.u....G..`...+.W1 ..v.....w.NO.<.T...$p....f8..>.l...8.Y.....8..&n.0..t..._c...9[lN..R^g.....1.E...53..Es.\d.....OR.....x..C.....s...fk..r.U.\.....&q..Q2..]M.be...UA.NF..+>f.....4x..BG..{=Zu9i.....5..y.l2 a.....jZ....>w.r&2.3.o..w.....K.W.....@...Q..Y.).c.....C6..lx.Zg.v.'&.Wl.,....u7n...%.2.....|6a.<....K>.&.....K.V....\.,.....Cs...3|S

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\2969352_1546835250916bundle[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, 1733x507, frames 3
Category:	downloaded
Size (bytes):	141960
Entropy (8bit):	7.96385434121153
Encrypted:	false
SSDEEP:	3072:2vxrZpV5kmqwLxxlATCZc9xh6oOdVSLy4VQW6zvdhCgokU854:cJfV57LxxlA+KxTaYLy4MhhCgo/854
MD5:	6DDAB159BB92226A485420578B816814
SHA1:	E97438DF779EFD1865432FCAB1903D759519FDBF
SHA-256:	52D4A71D7209A06C90A8DA986C667D6B74093888BB1DAD2138A0323F5B45C8AC
SHA-512:	832BD97268F1D766258931F23032EDBB8BBDB82B432E0A75F18431B8762D0850AF3EB85F7E493D5199D2C8085E17A6D0E6C5BA7420308D4C0B000F58C6647486
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2019/11/2969352_1546835250916bundle.jpg
Preview:	......JFIF.....'!..%...".."%()+,+. /3/*2'*+*.....*...**********.....D..... .....5.~O.}.....P..)Z..+@UJ.....V.d..@.....8...|.+.s.1.....)P....*...gP.....1...'.EN.1...7..yx.6..m...|.....7..AJ.*...@.@.*...J.....`.n_...e.[.^..".^_..R.[f;,..... .....a..L...in..f..(V...i5.'...../e.7s.;.9.P....59.c..qX..+q....)...|.n,jUm.c.JR.\...S.....s?..w.}....z9....TU..>|.Y.....5.C..R...:R...&>w..9h..b.....-...+_W.<.....g.7..]{N.q.%-...@.. .X.....-..6O.-..4.....#..c..e.)m.b..-.?..^w[..m|.c.kmiZc.....~.....5.]\.....v*...U+J.ZT.;...gK.....I.....3.9.m.{9...V.....:...._.m2.v,t.....nL.F..S.....-.K....kd.....o.....xw!..= ..s..Ku.Q.y.....o.{Ve.....[..nY..=3.....6,.e1/....Ym..l...t_e.....".K.....JU..1..._..q7....y'.{.-.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\KFOiCnqEu92Fr1Mu51QrEzAdKQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 21704, version 1.1
Category:	downloaded
Size (bytes):	21704
Entropy (8bit):	7.973226712101604
Encrypted:	false
SSDEEP:	384:wRRPUc1eNeMm6IbAOqBx9ybZoVdpnL5Q9Evdah83CTyTwyjP/J71FenyIw9:wnPv1eNeMm6eLEHyAdhL5QE0cwOP11YM
MD5:	F9E8E590B4E0F1FF83469BB2A55B8488
SHA1:	E90B097A67B069E35C13D4D481D259C35BF0A8B7
SHA-256:	5A3A9840414768FA2EC988B33C9E966FDFFE2DB7E560A270B3A9C6BA01F17718
SHA-512:	3E00FEA12DD63B19F97ACC765D1EED6810EFFFEDE185F8F37D56A827BF1FCB5DCACFE2F92F9031125B262B6E96120319481B4208A349D01DC8707AEAB6F7C3 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v20/KFOiCnqEu92Fr1Mu51QrEzAdKQ.woff
Preview:	wOFF.....T.....GDEF.....G...d....GPOS.....GSUB.....'.....r.OS/2.....O...`t..'cmap...$.....W.cvt .....H...H.2..fpgm...d...3...._...gasp.....glyf.. ....AD..t..1..hdmx..M....o.....head..NX...6...6.\|.hhea..N...."...$.}.Ohmtx..N....n.....M.loca..Q$.....Amaxp..S.... ... .(..name..S(..... G= post..T..... .a.dprep..T.....+6 .x...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R...A.J.x.l..h.a.....l.m.6.1+.X....i...y....&...._..63..5....2>...x\|D...ct.Kx..H@b.3..l..#u.....L.*....^.*.4.....rP..{.*.....Q...JT. :Xu>..T./>...oq.....~..@.....lq../.... ..#..".&.8.H$..r...J)..jj...&..f.=.9..N9....'F..8.4.....m...m...m.m..n..&.X..}....S.|.....n.....PHaE...J*...4..MjJ.*..nW)..rn3'/.....ks5zY5c...Mgg.5..p ..rR{c...p..t\.8.c=..p...X.(.....7....=.....!...H .....(.0...(.q.JT?.b..z].'T...m..vNi.....t....:P.R..H....t.....&?.:.j.51+.S.":j.SK'I.^....}S.i.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\KFOjCnqEu92Fr1Mu51TzBic6Csl[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 21588, version 1.1
Category:	downloaded
Size (bytes):	21588
Entropy (8bit):	7.973550860004932
Encrypted:	false
SSDEEP:	384:9do1erd5msN48bPbceGykR88v9yGLRkcl46tW6amtMQSJCo:9+1erd5vCfRzluCSJV
MD5:	81F57861ED4AC74741F5671E1DFF2FD9
SHA1:	AC3993E9EDC4C30C97FE670AA1E8A7088AA69E31
SHA-256:	EEC142608E8B417E2ACB6E5301A750047A04E2C5A6563223CAAE499E19EA08EE
SHA-512:	F23A7D58BE44E474CB65C368B048EB68AA1B6FEF4A12797A4A19C8D9E2F1BB7AB6FCEAE2AD17C59283616503107C332EA6245BF9F721BC49A676E8C92F46EC 4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v20/KFOjCnqEu92Fr1Mu51TzBic6Csl.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\KFOjCnqEu92Fr1Mu51TzBic6Csl[1].woff	
Preview:	wOFF.....TT.....GDEF.....G...d....GPOS.....~..GSUB.....'.....r.OS/2.....O...`u...cmap...X.....W.cvt ...P...J...J..,ofpgm.....3....c...gasp..... ....glyf.....@W..n.S...hdmx..M4...n.....head..M....6...6...`hhea..M....''...$....hmtx..N.....=-.loca..P.....maxp..Rh... ... .(..name..R..... .=$post..Sh..... .a.dprep..S. .....9..Bx...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R...A.J.x....dK...{....?..F?.|.~.m...ms.{.Z..;.....U.]7s.....\.=D.=.7...>....x...D..O|.U:...|o..3.x.j.r"B..... $.'"j.....1LGmaGxQxG....~.:'.A..hd.z,.k..KO.....^.}H|#z_.O.....R..A...9..A..!.(./..."..:.Iq1.r..s..r.7r.7s..q.wr....nz..]...2..d4c..c....d....T.1...d....\....,c9k.g..Yv.#O."%..... ...t"uM..%.....j .#^.....}\c.q.i...<jy.D...C.01.2.r.....V..z.W.7b..L.S.41]..kUs.X/6..b.....(..(...K..{.^..'.....`#./..B.....N+p.m`...].lQ....Drg.M..Kx.^.S.*.....h ..$.k.'Hy.I.ze..4z.-T.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\KFOlCnqEu92Fr1MmWUlfBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20356, version 1.1
Category:	downloaded
Size (bytes):	20356
Entropy (8bit):	7.972919215442608
Encrypted:	false
SSDEEP:	384:of+dt1ebKR28EPpAXxR5wthZZv4B8Te/h4+ctr5NH9NwZaUp4VsEgm:of+P1eeRcU8Hqdy+UHHbEw/
MD5:	ADCDE98F1D584DE52060AD7B16373DA3
SHA1:	0A9B76D81989A7A45336EBD7B48ED25803F344B9
SHA-256:	806EA46C426AF8FC24E5CF42A210228739696933D36299EB28AEE64F69FC71F1
SHA-512:	7B1D6CC0D841A9E5EFEC540387BC5F9B47E07A21FDC3DC4CE029BB0E3C74664BBC9F1BCCFD8FB575B595C2CC1FD16925C533E062C4C82EEE0C310FFD2B4C 927
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v20/KFOlCnqEu92Fr1MmWUlfBBc-.woff
Preview:	wOFF.....O.....GDEF.....G...d....GPOS.....~..GSUB.....'.....r.OS/2.....Q...`u...cmap...\.....W.cvt ...T...H...H+~..fpgm.....3...._...gasp..... ....glyf.....;...k....hdmx..H....m....!$..head..H....6...6...\hhea..I,.....$.&..hmtx..IL...y.....XF.loca..K.....`.C.maxp..M.... ... .(..name..M.....~..9.post..N..... .m.dprep..N.....)* v60x...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R...A.J.x....dK...{....?..F?.|.~.m...ms.{.Z..;.....U.]7s.....\.=D.=.7...>....x...D..O|.U:...|o..3.x.j.r"B..... .1LGmaGxQxG....~.:'.A..hd.z,.k..KO.....^.}H|#z_.O.....R..A...9..A..!.(./..."..:.Iq1.r..s..r.7r.7s..q.wr....nz..]...2..d4c..c....d....T.1...d....\....,c9k.g..Yv.#O."%..... ...t"uM..%..... j.#^.....}\c.q.i...<jy.D...C.01.2.r.....V..z.W.7b..L.S.41]..kUs.X/6..b.....(..(...K..{.^..'.....`#./..B.....N+p.m`...].lQ....Drg.M..Kx.^.S.*.....h ..$.k.'Hy.I.ze..4z.-T.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #00 0000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\SeanVertical-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, 1000x1000, frames 3
Category:	downloaded
Size (bytes):	63249
Entropy (8bit):	7.864968611221356
Encrypted:	false
SSDEEP:	1536:6m09kLsjyeH5fgFuVNCMKAWHleuhh5ivLcH2ztGDuDTG:D09VH5PCMKzHsuNq0u+
MD5:	EC850BEBE5173AB19AB3AF23A4C30CD4
SHA1:	B333C372F8BA774588A8CDDA0FB1F8ED7B3E3323
SHA-256:	350FA1C5E1B0D81567874E6E6E805DC897DFCE68D91E919E56B2EE3AF5AE1C03
SHA-512:	21B5092BDBFA57669415E0C4BB61DC8E42D9D31B6C7CFB355700586BE15C98BAEFB1435CB5877F4FE4F4A7FFD08C9F1276022055767AE5187C6D44AF5C3C844
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2019/11/SeanVertical-1.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\SeanVertical-1[1].jpg	
Preview:	.....JFIF.....%!'&$!$#).;2),8,#$3F48=?BCB(1HMH@M;AB?.....?*$*???.....~G..o...J@.....=..{.....o.....bme.....8.:...e.OFX..|y.=..G.KZ. .....9...'...M:..P.....t.....pZ]|.=c..=.\.....a..V.....w.g..\ .G5i.m.z)\..]....:7.....<..>...W..y1....g.4.....gWWF.L.....o....G'7Fv.}.>w.\..w.v.....#.O.....g.....)^NX.y.|.....W.....K.....^)..~....vk.>....y.W...;...I.....\. .....y.....=.[...V..y.....[.....[.....?.s.....Sk.j.a.q.Yy?+..8....{.zz4.....s.J.~..v....Z...Zg9.\\|../...w....wwgN.H.....W.W.....T..j3...?....}W.wg^.....z.s..{....{R.. kH.g.....S.....`.....~[.&.....oi...I+..)\.....k.?.v.v..m2.....2.m....k.k.....R.....?...~wg....;.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Webp.net-resizeimage__9_-removebg-preview-1-150x150[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 150 x 109, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	7663
Entropy (8bit):	7.970109374483929
Encrypted:	false
SSDEEP:	192:jv/TC4Iu2k/w8ou14iMQYvK52AjRDLYjWssLEBxWBlD+YNInpX3/:q4IuH/w61CJK5lRDLYjHswnE5+YNInp/
MD5:	51993C349BC9B7ADBEEF98B58525BF1D
SHA1:	7C41F5616534A709E40002F899B67A632F5A3CDE
SHA-256:	7153CF754885A47EA5DB7879AA420EF342BC0815361C114D95220D393A9BAD78
SHA-512:	937B4A4F27EE60396BB5B6F28AD306CE56F2CD97ABFDC78FF6B400FE5646B31C16AD44CE8A7F22EBE48D4FC8DE20FE1765D7060A39FFC77BE8A319C4A4CE0C18
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2020/08/Webp.net-resizeimage__9_-removebg-preview-1-150x150.png
Preview:	.PNG.....IHDR.....m.....t.h.....PLTEGpLE@B.....kX.....|oc.....435....{a...446.....+),...._^`..i.vU.....,+-...|gO..l..... ....}Z.....+...)..../(. '.,6.....6. *.AD.. ..5.8C.$...O. .F.3\..V.... +..<.R##$h..h..u..T.A(()P..D.)...,-g.Fr.-7-#Z.h001...~..234P$5w.Qh!$789u.mE8,a'K==?..>....$.S0f|..CBCO?7....Vs3@GHld3j..|TG?.%0e>Y.<)IM`NNP]N?rEI.0 .=W.=4NYhXWZfUA.7Jd[NnRj`_bn]KvPy.NH[dry`FreU}^jkjjvdw.[_fn|.V>ym\.kP.f{ust~uf.u]px..ku.uU.en.u..gY.|n.|e|~..}x.dC.re.s~..i.....].....v.wh.....b..o.....}..f.wL.....x.....j... .....v.u..o.....v.....z.....i.....~.....z...$tRNS. ..!38KUYb{.....!.P....zIDATx..il].....=.=w#)..HI.e.m..g.Ib..&M.....t....0mQ...A2(P.h..S`Z..0-.e..L.v..d..vb;..%..Iq.....$..U....s.....;.fe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\YTSupremacy[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 530 x 233, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	24478
Entropy (8bit):	7.983907438410961
Encrypted:	false
SSDEEP:	384:AlvVeDnU7uNsfsZ9cj6K/angd18Qk+lL1FWUl8JLYIMSBw+GXmAOSoapNTtOkyPz:8N7uN4tT/angdRlLyUlALwSG+umlSowO
MD5:	A3F747286C9CE93485530D2318EFA836
SHA1:	BEFB882C714B2D967869E5A0740FEA6D574E245D
SHA-256:	22C7C61C1A77B9F716779D41F3B001F72FAB50518C4962B084370B269DECE316
SHA-512:	10AA5021DE36E3002AC1156FE1F19F0772A5C13CEFF1AFD61C0DD81CCE761752CD8CDCE60C2A8AB70DE03C0FB400DC227E326078029AE4E11CE7D5A6406B691
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2019/07/YTSupremacy.png
Preview:	.PNG.....IHDR.....F).~....PLTELiq.....(..$...CU..).Le..#.....v.....2O..,K.....Sj.C^.)G.>W.....>...Qh.x..<W...4Q..bx.....4Q...%E..*..4.Ib.Um.i~.?Z.h}.f{..5.ez..?._u.[q.f{.>Z.Xo.F`.<V.h|.....'.....kkk...655..'.....-75..%$$$165.....(..'.....977..'.....iii677..'.....(95...sss.....222)))).....)955--- .....#544lll365ccc..'....'.....on n...000.....<77.....'.....)75.....h....*.....<==...BBB..0....(`'2...B14...U*2..%..81..#.....L.3v..i$1...O.....IFG.....$C...^^^...\..>24..)...MMM.....!SSS...D.....{.....>..t 0. .,.....zzz.....-.....+....2O.....XXX..%.....-.....cx.....,.Of....Xl....3N.....s..}.....1i..,.....+....,C...v=F.....dl.....J[.KU..s...>tRNS.....2."..Cj2....}.Z...O(.NEc*= .....b..z...d..q.9V>....\.IDATx..].O..6OC ....<..i..4.>.....[~!l....~.....@...).)T....."!. .....)..._.Z{...H...N.O.xl<.g.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\admin-ajax[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	92739
Entropy (8bit):	5.07585598384244
Encrypted:	false
SSDEEP:	1536:O5Tqf3pVcLvkkVWRQP5Tqf3pVcLvkkVWRQP5Tqf3pVcLvkkVWRQC:p
MD5:	BFB2AE2AC90D3E0B49089F6CB07A9A50
SHA1:	56D7003C3BD1FDCA69A2D96795FD0C445567F84E
SHA-256:	DBDED4125F0B5EBDE9DB41F070CEDDA5BAE1C7A5A5DC8BE7B142F4DF7393F7D3
SHA-512:	563E9BB95C56D73E52C68AFA10969244CB354DBEEAD5F66FC9EF85811F0654E6F623E6F22D9481CD8A0E4DF5CF1B7CADCD683F1EAC93901CA356CEA82898DC2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\admin-ajax[1].css	
Preview:	@import url('https://fonts.googleapis.com/css?family=Roboto:100,100i,300,300i,400,400i,500,500i,700,700i,900,900i');@import url('https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css');@import url('https://code.ionicframework.com/ionicons/2.0.1/css/ionicons.min.css');.theme__sm-6 .mw-elements-wrapper__link{color:white;}[data-toggle~="collapse"]{cursor:pointer;}.bt{box-shadow:0 0 0 1px #000 inset;}.list-none ul,.list-none li{margin:0;padding:0;list-style:none;}.fntWN{font-weight:normal;}.fntB{font-weight:500;}.fntBB{font-weight:bold;}.txtUp{text-transform:uppercase;}.txtDecorNoneAlways{text-decoration:none;}.txtDecorNoneAlways:hover,.txtDecorNoneAlways:active{text-decoration:none;}.bgOk{background:#4ebb74;color:#fff;}.clear:after{content:" ";display:block;clear:both;}.mw-content--editor{overflow:hidden;}.mw-content--editor img{max-width:100%;height:auto;}.mw-content--editor iframe{max-width:100%;margin:10px 0;}.mw-content--editor .alignleft{float:left;margin:5px

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bullet[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKIv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/bullet.png
Preview:	.PNG.....IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.:j.:l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\circle[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	1987
Entropy (8bit):	5.066469183369679
Encrypted:	false
SSDEEP:	48:oAIYprfvr6qMzrXEBVP+gsZr0aub6XXydqrx:oNYprrUrEjP+gsZ5ygV
MD5:	87CAD0B844F37988C7B7484E5603E06B
SHA1:	39B40C9CF4734448116B3B842F25E0494B55FA37
SHA-256:	4F6D4E9246E62595533595B7242EBBE933ADEB86F79B94B9E9E4478E34ACEA0B
SHA-512:	1A96AF309D6771002C9520B3E58DA5EF18FC3A1E3A2EC2EE38DA2E5732368BCA18B5DD25E63DC54F638717CBF9B8AF96E97C3738807DD1F413890F6687F86A9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/plugins/wp-product-review/assets/css/circle.css?ver=3.7.11
Preview:	/**********. *. * CSS Percentage Circle. * Author: Andre Firchow. *.**********/.. rect-auto,..wppr-c100.wppr-good .wppr-slice,..wppr-c100.wppr-very-good .wppr-slice {..clip: rect(auto, auto, auto, auto);.}...wppr-pie,..wppr-c100 .wppr-bar,..wppr-c100.wppr-good .wppr-fill,..wppr-c100.wppr-very-good .wppr-fill {..clip: rect(0em, 0.5em, 1em, 0em);..position: absolute;..box-sizing: border-box;..width: 100%;..height: 100%;..border: 15px solid #333;..border-radius: 50%;.}...wppr-pie-fill,..wppr-c100.wppr-good .wppr-bar:after,..wppr-c100.wppr-good .wppr-fill,..wppr-c100.wppr-very-good .wppr-bar:after,..wppr-c100.wppr-very-good .wppr-fill {..-webkit-transform: rotate(180deg);..-ms-transform: rotate(180deg);..transform: rotate(180deg);.}...wppr-c100 {..display: inline-block;..position: absolute;..top: 50%;..left: 50%;..width: 100%;..min-width: 100px;..max-width: 120px;..height: 100%;..min

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\close[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	280
Entropy (8bit):	6.264381543729851
Encrypted:	false
SSDEEP:	6:6v/lhPZmllQ9SoBcolgs4zHt7xDivIRQ6HarMKvuup:6v/7Rm/Q9Zpg7zHRxOQW6HarLvuc
MD5:	D9D2D0B1308CB694AA8116915592E2A9
SHA1:	3CA48361CFE0E41163023D03C26296F375BB3EAC
SHA-256:	5D62E6C90005BFB71F6ABB440F9E4753681CB23BBD5E60477AB6F442D2F0E69C
SHA-512:	AE70339EC05F19D698A319CC265DA583814711ACBEFD81DDCB7D6D5E59934B78B289E5A55C666AF62216A8F9CE5DE60AFD6F41C54EF7E4EA569D5458CEF78A F5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/plugins/wp-product-review/assets/img/close.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\close[1].png	
Preview:	.PNG.....IHDR.....g...<PLTE.....KKK.....JJJHHH.....n.....tRNS.J.....K.....|...xIDATx^}.I.. .DQ..Q...w....j...0T....W.~Y....hC,..W$....r.$.9. ...$".H"..;.. .x7{@b..(.).G.O&..H....}Q=..|.. ..H.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\dashicons.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	46360
Entropy (8bit):	6.055516422081972
Encrypted:	false
SSDEEP:	768:Jy79SeLdo/v4lcBBcX2MI6wuWASjxuKsbss0UjEhREyIPRQ:J2hoXmcBi9xwuSupbbJyIPe
MD5:	1C364E777CD2B874EA6CF09100861C6C
SHA1:	58BB8DABDB753287BE070AC2840C0FDBBD27F533
SHA-256:	D0DF2FF25FDED9E43A0CFA5159393D4482725BFB390E8CA94F34DA85B5304117
SHA-512:	7E5F18F12B56D711B70509EA80E5CAE14326558EBFF755A3D61A8D9156FFCDAD243274195D83FE27C6E295FECCC19A285AD358EBBCD720846820B51E22389F3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-includes/css/dashicons.min.css?ver=4.9.16
Preview:	/*! This file is auto-generated */.@font-face{font-family:dashicons;src:url(../fonts/dashicons.eot)}@font-face{font-family:dashicons;src:url(data:application/font-woff;charset=utf-8;base64,d09GRgABAAAAAGYMAA4AAAAAowAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAABGRlRNAAABRAAAABwAAAAcckwii0dERUYAAAFgAAAAHwAAACABMwAET1MvMgAAAYAAAABAAAAAYJYFacxjbWFwAAABwAAAAUEAAAKi6kAXkmdhc3AAAAMEAAAACAAAAAj//wADZ2x5ZgAAAwwAAFnuAACMgOFsk4doZWFkAABc/AAAAC4AAAA2DP0UgmhoZWEAAF0sAAAAGgAAACQPogeuaG10eAAAXUgAAAEHAAACFodAcgtsb2NhAABeUAAAAg4AAAIO/oLadm1heHAAAGBgAAAAHwAAACABWQC1bmFtZQAAYIAAAAGbAAADVi8qdoNwb3N0AABiHAAAA+cAAApGwPo//ndlYmYAAGYEAAAABgAAAayr1bhAAAAAQAAAADMPaLPAAAAANMHHI4AAAAA0wdjLXjaY2BkYGDgA2IJBhBgYmBkYGRkBZIsYB4DAASNADkAeNpjYGY/xTiBgZWBhVWEZQMDA8M0CM20h8GIKQLIB0phB6He4X4MDqp/vrqzXwDxgaQGkGJEUqLAwAgANrQKyHja3ZC9SwNBEMXnkqgcuzcGxOIgxYGkuO78JMHmNMQkoCKmkIhI/GhiFRshXRoLO1vBv0U7tdFGFAzWaqXO7o426nkkYGFv44N5w4Ph92AAIAm9yYAVO1jHcbK6OWW1470GIfRBJvtBNg2RSyPkU0BTlKcCFalMNdqgBrVoX1nKVq7yVV6Falbb2tW+zuuKqZgVUzN10zAtc2COOMU2u+z	

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\dashicons[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Dashicons family
Category:	downloaded
Size (bytes):	22449
Entropy (8bit):	7.968327336521213
Encrypted:	false
SSDEEP:	384:j0vkjXx0OZlDA5Pv3/yDimeZsSTN6iJnpKAXES2XVgVlsx1i:j0cVrU56OTLB2XylC1i
MD5:	30E410C715C6215FA7FAA1C979B6480C
SHA1:	C67CED157875CFA23222EE70F18A337BE2051957
SHA-256:	A55660C37AF5BBCC8C6C485C032E3D74D876946607E6C20148E3D3D5F37043B8
SHA-512:	F2D64FA18A777B52651A16EDB14379CF8178C7E40FFE119CBBE69FE915FFD8DB1F41FDC62EDE2960620D1D14B555A07F62B0BEBEC65AC146ADB383009A4C1F42
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-includes/fonts/dashicons.eot
Preview:	.W...V.....LP.....D.a.s.h.i.c.o.n.s.....R.e.g.u.l.a.r...x.V.e.r.s.i.o.n. .1...0.0.6.;.P.S. .0.0.1...0.0.6.;.h.o.t.c.o.n.v. .1...0...7.0.;.m.a.k.e.o.t.f...l.i.b.2...5...5.8.3.2.9...".D.a.s.h.i.c.o.n.s. .R.e.g.u.l.a.r.....BSGP.....Vw.V{.@I.....Y.D.M.F..x...>.....)[..1.H..-A)F...1..../.S?.U.'.&a....:f."K.K`lwR....".}..k....I...%.....Y..\5.r..-."^.eX[.^.../....z.t).K.T.....;.e...l....3X...I..5....&.....Z7..Qn9...IG2.aow.o. (.\^.....i.....&...i...[.a....@t..g..e..JH.....xa....?@.....|.....4RUB*B.,B.P.....A....0..0.JVT".#.I..)2.....2QH.%#.b...U.Q...4...c9.V...ExP.K..TK.n(..R.}..X.G5....=A..9&.'~d[.X../...".o...k{.Ao&....|5.S..yN.._K....&...u`.a.5V.xmc..2..Lig..._)a...3.....T%..p..h.z(...V$..g.JTWt.B..`.H..Au....4;?.....xN.W|..K.j..5.n..T......./.uL-..Qz/.....0.*.5.....F..F..2....)ZH...T]`...(..-z!..c.{y}...S!{...5+.^..pB74..0w...../.y.;.~.~.}n.A@

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=1460

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\dnserror[1]	
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMo reInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Reputation:	low
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\facebook-group-strategy[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 771 x 500, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	25325
Entropy (8bit):	7.963636102815299
Encrypted:	false
SSDEEP:	384:VxEilwycIp+OTk3APTXz2YUSgjdVACVH813yPfOTkTIRyzcnEhP8mR7Sus:Vu2+2k3gXZufAC5+bRFEl8jus
MD5:	52F2A11DE5E2A3D7CAA952B4D57743E2
SHA1:	B3D6128C0298C3ECE59C718D5A276DD0B5FE082F
SHA-256:	3BCF91A790D46D766313749CFEA0D7AA6025BBBC16408214079B11642736964C
SHA-512:	5AEDE530B36BA52AE497D3E92AA730A265DB4B977C451B939AFAA1E494853A3757DA91C9B6BBC1D08D484DB495C71E5AD2BF20FE57786257C34683A1231B557 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2019/03/facebook-group-strategy.png
Preview:	.PNG.....IHDR.....V.....PLTE...^E.iii000.....,,,```.....K6.4"....._.....i.....*++.|.O8.....G2.....W?.jO.....g.....7&..j...{\.. j.?,..v.dK.....j....NNNUUUS=.....41*#..!!!.....ii.....j....[[[.....jlp.....C0..p.DDC...aD....)....[B.yX.uuu...554.....>>>.....}....b.....mjjD:'.v.}}}(((.....sS.....&),;5(.....vil.M@$ ...ly.....III......./.*$$$t..;(.....i^^^...m..s....ddd...888.....F....b...y.....--....|o.....vmi.n.....&.....fUE"..p....vm^K!...kj..mi.ox.hQ.|.....l...i....oH.....qV....f.x..___..~... .\.z\..}l.....~w.....rk.....mw.....6.jl.j...t.....vn.....m...}.....~.....+)&...^._.IDATx....L..]).....)..le..Ed.S.....X.^.....1t..!...5~[.A4...Ng.....O..DD.-....0@..".}...D.... ..0@...DD."....0@.."..}...D.....0@.."..}...D.....0@.."....H..2T.b..4....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\httpErrorPagesScripts[1]	
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\image2-280x150[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 280 x 122, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	10874
Entropy (8bit):	7.956701631696734
Encrypted:	false
SSDEEP:	192:MJH5cmmCNc9LSsH7E0U+6sSwUT/3EiGZ0mwV1fd83/sSt5kvxJJyRSV9LdYidB:W+RCy7wPHdT/rGZ0VV4cvxJ4kLLdYGB
MD5:	B00CEBC86805463DF11ED299B86317B6
SHA1:	6D438E943E12A39A494FAD357C236E2E1DF08603
SHA-256:	2389ED4EEA10C9075E8433E90D6FA313DF87CB1764F47452339964BDE0A7217A
SHA-512:	F338F95D55ABAE7402B391B31B5C39D18B901A1F175E0687258CF3F987D85B56D8E17BF4E9389536DAC7223DA61AB39CF49694B6285AD2B2EC3E34D351F9311
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2019/02/image2-280x150.png
Preview:	.PNG.....IHDR.....z.....S..[....PLTE.....###&&&A..***---222777g&"L5-?>>DDDb<9KKKz9.QQQUUUhOE,W.]_aao.[Lfee.T@Ek.iix~ebnmlqq~utsTv.oX._.{zz.xm\}._~..~.mY=.....`...~i.f.....l.}...~j..zt..S..}Y....r.6.o.w...y...z...y#.~E.....0...h.....tN.~~.....p.....B.....a.....}....R.....~.....d.....u..... .....=..'5IDATx..}y.\G}..U.zW_.3.3....e[.....#K..@Bv..>l.9v...$.5!.'.I..H.z..p..@lp,l.e[.![']=}.....==.d...Iz>.....U}.W.....O..(./....R.;m..H.....~I^....}.^.....K]o..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC134
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.../...0.....#.....IDATx^...pUU..{....KB.....!....F.....jp.Q.....Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{.....[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po.....X..;.=.P...../...+...9./..s.....9..\|.....*.7v.`..V.....-^.$S[[[.....K..z.....3..3....5 ...0..''/n/.c...&.{.ht..?....A..I{.n...|....t.....N}..%.v...:.E..i....`....a.k.mg.LX..fcFU.fO-..YEfd.}...~.''.....}I$....^.re..'^X..*}.?.^U.G..... .30...X.....f[.l0.P`..KC...[..[..6....~..i..Q.|;x..T .....s.5...n+.0..;...H#.2..#.M..m[^3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..l[..a...N,,.h.....5...f*.y...}...BX{.G^...?.c.....s^..P.(..G...t.0.:.X.DCs.....]vf...py).....x..>-..Be.a...G...Y!...z...g.{....d.s.o.....%.x.....R.W.....Z.b,....!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a)..t..e.j.W.....C<.1.....c..l1w....]3%....tR;,..3..-.NW.5...t..H..h..D..b.....M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\instagram-university-2-0-review[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):	47486
Entropy (8bit):	5.361385511811207
Encrypted:	false
SSDEEP:	768:o147uJKhbtpr6En1t0c8wac5Aadc8kosGeon9/Ql0ubTtq4Fnxf6:oQ8KhbtprB1tt8+5Aadc8hsy9Il0ubT8
MD5:	6D2DF35D7CE265A8FAE1264529090A4D
SHA1:	3C7442A512A61D2179FAC0B35A3966204B16D09C
SHA-256:	E7D64A67CB3F4692790A17A685CEFBC43F6372D0D5A709AF65E0FE286655279C
SHA-512:	8C5CB8B07A36B5617D8709962EBA253681732E12CE91AADA20C5AB50169BDF81DBEDB9382B00E95264A974E7EBBCD87492D8B53C9DA29B4D5437ED07FBCC669
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/instagram-university-2-0-review/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\instagram-university-2-0-review[1].htm	
Preview:	.<!DOCTYPE html>.<html lang="en-US">.<head>... [if lt IE 9]>..<script src="https://bonusbomber.com/wp-content/themes/rise/js/html5/dist/html5shiv.js"></script>..<script src="//css3-mediaqueries-js.googlecode.com/svn/trunk/css3-mediaqueries.js"></script>..<![endif]-->.. [if IE 8]>..<link rel="stylesheet" type="text/css" href="https://bonusbomber.com/wp-content/themes/rise/css/ie8.css"/>..<![endif]-->.. [if IE 7]>..<link rel="stylesheet" type="text/css" href="https://bonusbomber.com/wp-content/themes/rise/css/ie7.css"/>..<![endif]-->..<meta name="viewport" content="width=device-width, initial-scale=1.0"/>..<meta charset="UTF-8">.....<title>Instagram University 2.0 Review by Niklas Pedde - Bonusbomber</title>.. This site is optimized with the Yoast SEO plugin v11.3 - https://yoast.com/wordpress/plugins/seo/ -->.<meta name="description" content="Instagram University 2.0 Review - The following experience report is about the online course Instagram University 2.0. by Niklas Pe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\instagram-university-pro-review[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):	73223
Entropy (8bit):	5.247496189215683
Encrypted:	false
SSDEEP:	1536:oWMKhbtprq4mzkY9Iy7ZyUxUnNkL1toKIUvVy6Zu+USA9Il0uhTPtq4Fnxf6:Zhbtprq5z79Iy4eUnNkLnoKIUvVyKu+0
MD5:	4220D5884BD519C068F71FC598E6B84E
SHA1:	C36A690BEB64C9D5491214944EF6ABD71E0E0B56
SHA-256:	FFBD0CFD6CFA4F84DC5A2F53DD2F00BF7A4BDB7C3C0252A3B08091326DCF7DAD
SHA-512:	D7AE9044287758981F26691E17C94B15E10A55750A2868AFCE0ECDE2F2F8BBBF95C5C2843DD1252816050A2B82E8B2FC6560419DAA69451285175983E7C6C48B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/instagram-university-pro-review/
Preview:	.<!DOCTYPE html>.<html lang="en-US">.<head>... [if lt IE 9]>..<script src="https://bonusbomber.com/wp-content/themes/rise/js/html5/dist/html5shiv.js"></script>..<script src="//css3-mediaqueries-js.googlecode.com/svn/trunk/css3-mediaqueries.js"></script>..<![endif]-->.. [if IE 8]>..<link rel="stylesheet" type="text/css" href="https://bonusbomber.com/wp-content/themes/rise/css/ie8.css"/>..<![endif]-->.. [if IE 7]>..<link rel="stylesheet" type="text/css" href="https://bonusbomber.com/wp-content/themes/rise/css/ie7.css"/>..<![endif]-->..<meta name="viewport" content="width=device-width, initial-scale=1.0"/>..<meta charset="UTF-8">.....<title>Instagram University Pro Review by Niklas Pedde - Bonusbomber</title>.. This site is optimized with the Yoast SEO plugin v11.3 - https://yoast.com/wordpress/plugins/seo/ -->.<meta name="description" content="Instagram University Pro Review - The following experience report is about the online course Instagram University Pro by Niklas Ped

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\instagram-university[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1138 x 703, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	124673
Entropy (8bit):	7.988222188416738
Encrypted:	false
SSDEEP:	3072:9t0IH/OD4prQn0gZ/Yt4jZ0VY4y6DB6R/hiF07Y:7oAQ1hA4eVY3U8Rwy7Y
MD5:	6C02DC9C5417710768232658A86F76AD
SHA1:	2722EF1921535B4A4F42DE702FE09449C3CA217A
SHA-256:	665B76F5677753CD25E67995666B05307F017BF9C7C765246425F71B06B40DA8
SHA-512:	EB3985CA0F8372C8097084D6E921F35EC1201670F4B15D63327B9E2DBAE28DBEB5EBB2B124FB1454AD1794465D730F53E5CCC82D765DE7A4A50E8065FA77E0D2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2019/12/instagram-university.png
Preview:	.PNG.....IHDR...r.....23.....PLTE.....M.....!.....N.....!..)... ..!.7..'!.%'. '"0$.+%!'*....*+*G#.3*#9*.02.-3171(?0#+0f174>4,39<E5)!5._..:=%U1.8<7...C:2L:-k,*:A?K>4Q@3@FD...MB<p9.GI2UD8..,f@(ELITG@...ZI<IQNzC.ZLD...^L?RPM..-UV?`PDdP@uJ3_RK.n.dSF.K%bWPfVK[ZViWGJ]z..r+g..Q.kZM...h[Qo]N.VBi_[.U2n_S.U.taRsbWffffjR.[9xdTue\ygZ.<.._>yj`.cN~j\}mc.dCsrm.n`ou..rf.g+.iL.K>.sd.uo.m\.vi6..yn.yi.\|vr~..qR.F..}q...ve....w...x..t.....v.....\|b..z.....~s...^.....q..~..... ..\|.R.....3.....~.{@.....o.....}y...k....w.....h.....N.....t..... .....8&iQ...IDATx...Qj.Q....!.O..f.I7..\@6.N.... e..TK+Q$.7.2....@&.~wf .....)..+...r. +...r....3..c...V.x..c..9...o.....?+.i...\.7.....<..]w..4...m.]9K...d.....5r.....z...8...B~.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ionicons.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	51284
Entropy (8bit):	4.573895834393703
Encrypted:	false
SSDEEP:	384:R48w+hhJhjRqFdtYRjJIjsjaHnNfc2C4741mf5HRzL:R4YhhjQFduRjJ7uHFcu7Smf5xzL
MD5:	1690997909AAE14B023A6580D4A2F33F
SHA1:	A4FD9551382A3B5C9C43E14ADB8C4C4149CD2352
SHA-256:	92AC508220F5BB60EC94E07650528EB66625F82A4740ADA068CDE05365781286
SHA-512:	617658DBE762B0F4C1A6433C90EA2FE21A0D27D431F00B2B216DE28636066FC4653A23D0B6CCCC53B9ABBD5A234E3416DCB8296B7F0DEE0CEBA1B45CE99A2CF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.ionicframework.com/ionicons/2.0.1/css/ionicons.min.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ionicons.min[1].css	
Preview:	@charset "UTF-8";/*!. Ionicons, v2.0.1. Created by Ben Sperry for the Ionic Framework, http://ionicons.com/. https://twitter.com/benjsperry https://twitter.com/ionicframework. MIT License: https://github.com/drifty co/ionicons.. Android-style icons originally built by Google.s. Material Design Icons: https://github.com/google/material-design-icons. used under CC BY http://creativecommons.org/licenses/by/4.0/. Modified icons to fit ionicon.s grid from original..*/@font-face{font-family:"Ionicons";src:url("../fonts/ionicons.eot?v=2.0.1");src:url("../fonts/ionicons.eot?v=2.0.1#iefix") format("embedded-opentype"),url("../fonts/ionicons.ttf?v=2.0.1") format("truetype"),url("../fonts/ionicons.woff?v=2.0.1") format("woff"),url("../fonts/ionicons.svg?v=2.0.1#Ionicons") format("svg");font-weight:normal;font-style:normal}.ion,.ionicons,.ion-alert:before,.ion-alert-circled:before,.ion-android-add:before,.ion-android-add-circle:before,.ion-android-alarm-clock:before,.ion-android-alert:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\main_orange[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	182318
Entropy (8bit):	5.187304757250811
Encrypted:	false
SSDEEP:	1536:GLUMqq0ibjCbRskmUDdlQdcYfLy5seVjJ9PZ9UJ:GLUMqq0inhcRseVXY
MD5:	19FCF59F618BFE9FE4E3A2D5D57B02EB
SHA1:	048D6222BEB9CDD571BD09253340086AEF5D4989
SHA-256:	E2A0B6DA49D370E715144D0FF0DB9CD8325AE18F360FC7C3AA1BAA581DD2B7AF
SHA-512:	14CE2124487C3FB92F8D05F59236CD4F689C605831052653600F9C5181DF5D64C0CE58828420696671920B63B7F7F447E74DE2038FC46043506AB2A91458DD87
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/themes/rise/css/main_orange.css?v=1.500.1
Preview:	@font-face{font-family:'Roboto';src:url("../thrive-dashboard/css/font/Roboto.ttf") format("truetype");font-weight:normal;font-style:normal}@font-face{font-family:'Open Sans';src:url("../thrive-dashboard/css/font/OpenSans.ttf") format("truetype");font-weight:normal;font-style:normal}@font-face{font-family:'Roboto Condensed';src:url("../fonts/RobotoCondensed.ttf") format("truetype");font-weight:normal;font-style:normal}@font-face{font-family:'rise-font';src:url("../fonts/rise-icomoon.eot?6xplcw");src:url("../fonts/rise-icomoon.eot?#iefix-6xplcw") format("embedded-opentype"),url("../fonts/rise-icomoon.woff?6xplcw") format("woff"),url("../fonts/rise-icomoon.ttf?6xplcw") format("truetype"),url("../fonts/rise-icomoon.svg?6xplcw#rise-font") format("svg");font-weight:normal;font-style:normal}@keyframes side-menu{from{top:100%}to{top:0}}@-webkit-keyframes side-menu{from{top:100%}to{top:0}}@keyframes progress-bar{from{width:0}to{width:100%}}@-webkit-keyframes progress-bar{from{width:0}to{width:1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\navcancl[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2713
Entropy (8bit):	4.1712007174415895
Encrypted:	false
SSDEEP:	24:r3avxU5hzsIVmVMeLmVMyHf63lboxMCLxvriN6LOAPAnQay78eLx5Tb87nVkEhML:upU0GVeLVGBXvrp4n/1a5TI7Ve/G79KX
MD5:	4BCFE9F8DB04948CDDB5E31FE6A7F984
SHA1:	42464C70FC16F3F361C2419751ACD57D51613CDF
SHA-256:	BEE0439FCF31DE76D6E2D7FD377A24A34AC8763D5BF4114DA5E1663009E24228
SHA-512:	BB0EF3D32310644285F4062AD5F27F30649C04C5A442361A5DBE3672BD8CB585160187070872A31D9F30B70397D81449623510365A371E73BDA580E00EEF0E4E
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/navcancl.htm
Preview:	.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html>.... <head>.. <link rel="stylesheet" type="text/css" href="res://ieframe.dll/ErrorPageTemplate.css" />.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />.... <title>Navigation Canceled</title>.... <script src="res://ieframe.dll/errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="res://ieframe.dll/httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:navCancelInit(); ">.... <table width="730" cellpadding="0" cellspacing="0" border="0">.... Error title -->.. <tr>.. <td id="infoIconAlign" width="60" align="left" valign="top" rowspan="2">.. <img src="res://ieframe.dll/info_48.png" id="infoIcon" alt="Info icon">..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\next[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 50 x 45, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1350
Entropy (8bit):	7.795826172553452
Encrypted:	false
SSDEEP:	24:OgMSVQogiW6rN55Wfj2byDoY6nn1SoPthAOy79jQC7tVcaKE028k:ZBCiWYNvGjWyDop1SoPMr9ECxUk
MD5:	31F15875975AAB69085470AABBFEC802
SHA1:	777E92C050F600B4519299C3D786B8F2F459FEA4
SHA-256:	15B869B02C6FBAA8C6C26445A2DD2D9BAD80FD27B1409F8179E5DD89DC89D90A
SHA-512:	EDC920DCD2F5AC9A6E08098C6A59F888A9CB135FF4EF3DC2183931E065B6531E00E2C8ACD3C329A3D90EB939EA3DB318A9B677B5AA78A227815373D7008D40A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/plugins/wp-product-review/assets/img/next.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\next[1].png	
Preview:	.PNG.....IHDR...2...-.....8.....IDATx..KL\U..3w.+0.b.gp.-a.Z.U.....Rjj.-.Z.va.i.....@.....HA...F.#a..C.M0. @x#e.O.|....9.'..2.Y..}..{y.4...@'..F<.....%..I?I....X.....#....=.".... .xA.8l..c ....r..J..D...u=j.....~.....T1],.N$.<.N.B...wvww.....7p...a.>.r.Ngdaaa6nZSSS..\|...S..e2N.Q...H..C+.....*.....eTWD.)..H....z.bMOO....>..R&..LS-..TWW..... Z.....z?..2&#..r....).-,,..2.....\|.*#....t../..h4....a%3666....e..p..h.DI .....d0..."3.....k.M2gAEiii.....F.].L.d..@..F2Nj3?.\(...X]]]....9...u....<.&.*..6.(((hA....,v...i.....3s.d..... .J..@..Ef.T..0..Q.M+....y.....,.Z6.....p.....Q..f... [...>.+ph.b...*.c. ..d.p..f.4....!..&...S ..}.@.-.e..x.\.D"_....2..2.....ZLW%...A..y....4.:..Y.3333.#W.....7'.....}.\|600.W\....;..G...TD .:...tN.....~.....\|.....4."...!.c ...k...?.*...9.}...v...;U..A...rMM.."....Q.J.9 .$I.a....."....d.@"..O.W.9.$..D.T655....[[[o.l.J.-..q.M...Kd.L\nll..lttt..}UL".$

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\sharer[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	96160
Entropy (8bit):	5.473399833379101
Encrypted:	false
SSDEEP:	1536:fgZ/RNZEok6By4EUMozgmBpe1LnfyMnvWxplMhhkCyCjgGh7rekh3nH1hZO5p8Ge:MRpE
MD5:	BEB2C35FF4E7A0F40747D794CEFBCFEE
SHA1:	0F85658D36DA64EEC94BA11706D78401D45E172C
SHA-256:	5B106453A7A616D691936A5CFDF7DB411FD385625F93E2996C46BD016D7E7A15
SHA-512:	924E3D3C1A84A4673C48C69F1CA24467DB7BB9123330345207FCB7E787B8CABC0FFF493B7E969C14BE763EDEDACE499642598A4081CE0F6092BEE352F8C4A4E 9
Malicious:	false
Reputation:	low
Preview:	<html><head><title>Redirecting...</title><script type="text/javascript" nonce="5bFSRjhE">/*<![CDATA[*/(function(){function si_cj(m){setTimeout(function(){new Im age().src="https:\/\/error.facebook.com\/common\/scribe_endpoint.php?c=si_clickjacking&t=5949"+"&m="+m;},5000);}if(top!=self){try{if(parent!=top){throw 1;}var si_cj_d=["a pps.facebook.com","apps.beta.facebook.com"];var href=top.location.href.toLowerCase();for(var i=0;i<si_cj_d.length;i++){if (href.indexOf(si_cj_d[i])>=0){throw 1;}}si_cj("3 ");}catch(e){si_cj("1 \t");window.document.write("\u003Cstyle nonce=\"5bFSRjhE\">body * {display:none !important;}\u003C\/style>\u003Ca href=\"#\" onclick=\"top.location .href=window.location.href\" style=\"display:block !important;padding:10px\">Go to Facebook.com\u003C\/a>");/*iyRSNck2*/}}})()/* */</script><script nonce="5bFS RjhE">window.location.replace("https:\/\/m.facebook.com\/sharer\/sharer.php?u=https\u00253A\u00252F\u00252Fbonusbomber.com\u00252Finstagram-university-pro- review\u00252F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\sharer[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	94958
Entropy (8bit):	5.471767137145293
Encrypted:	false
SSDEEP:	1536:fB41/j9+xxQb0KrGIvTDMPeoVDmIFIkbJJYGFbgqioke9LNlkkyz48R30yAxfbDX:H
MD5:	A65B7FD395363C6086D050B5CCE4FD2F
SHA1:	ADF1C6F84A6ECCEA61F53487CA4754B54EEEA62D
SHA-256:	5E44D83C50062CECA6D85C8F9689545C357253E0901F7B63B915E9BE713372C6
SHA-512:	56527CD73458D0758823CE117DC6C3CA7FB306F6CDB2FA64A3377B6B7B9FB13D72E79D5895C040897DA06FFC0EC7EC22AF8A0DC4F79BCC4AB3A49C5B55E6A A3
Malicious:	false
Reputation:	low
Preview:	<html><head><title>Redirecting...</title><script type="text/javascript" nonce="KAEteZK5">/*<![CDATA[*/(function(){function si_cj(m){setTimeout(function(){new Im age().src="https:\/\/error.facebook.com\/common\/scribe_endpoint.php?c=si_clickjacking&t=5479"+"&m="+m;},5000);}if(top!=self){try{if(parent!=top){throw 1;}var si_cj_d=["a pps.facebook.com","apps.beta.facebook.com"];var href=top.location.href.toLowerCase();for(var i=0;i<si_cj_d.length;i++){if (href.indexOf(si_cj_d[i])>=0){throw 1;}}si_cj("3 https:\/\/www.facebook.com\/sharer\/sharer.php?u=https\u00253A\u00252F\u00252Fbonusbomber.com\u00252Finstagram-university-pro-review\u00252F");}catch(e) {si_cj("1 \thttps:\/\/www.facebook.com\/sharer\/sharer.php?u=https\u00253A\u00252F\u00252Fbonusbomber.com\u00252Finstagram-university-pro-review\u00252F");wi ndow.document.write("\u003Cstyle nonce=\"KAEteZK5\">body * {display:none !important;}\u003C\/style>\u003Ca href=\"#\" onclick=\"top.location.href=window.locatio n.href\" style=\"display:block

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\thrive_flat[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	648755
Entropy (8bit):	4.983993011989391
Encrypted:	false
SSDEEP:	3072:VjL3q8o2nmyfsF0A0hTjVrISStYlfXLFB9l3uFWCZipUNX1KBjiM/MxRUslulfsV:NT1nnA0RVc3YlfJ0rBulfMH0vC0185
MD5:	F86E1110F61A3AAB91C25F5CC997A81F
SHA1:	969796AC6F0B2DCC1DAF4D9D13E643254F259114
SHA-256:	B47087F6A82A55A8805D26BC51D40700D34EA823D10DD01889DC5CFC76816764
SHA-512:	207831F4E43113C4235D4A7409D123A4D6093CA4D6D8BF4ABEC7019E58FBF5B4EDDEF69CF01E023E82FEB425CD9F6E874A8C3BB6D668BBED0673092784CEC0 57
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/plugins/thrive-visual-editor/editor/css/thrive_flat.css?ver=2.5.8.2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\thrive_flat[1].css	
Preview:	@font-face{font-family:'thrvicomoon';src:url("fonts/thrvicomoon/icomoon.eot?jtzdu4");src:url("fonts/thrvicomoon/icomoon.eot?#iefixjtzdu4") format("embedded-open type"),url("fonts/thrvicomoon/icomoon.ttf?jtzdu4") format("truetype"),url("fonts/thrvicomoon/icomoon.woff?jtzdu4") format("woff"),url("fonts/thrvicomoon/icomoon.svg?jtzdu 4#thrvicomoon") format("svg");font-weight:normal;font-style:normal}[class^="thrv-icon-"],[class*=" thrv-icon-"]{font-family:'thrvicomoon' !important;speak:none;font-style :normal;font-weight:normal;font-variant:normal;text-transform:none;line-height:1;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}.thrv-icon-spinner:b efore{content:"\e97a"}.thrv-icon-spinner2:before{content:"\e97b"}.thrv-icon-spinner8:before{content:"\e981"}.thrv-icon-spinner9:before{content:"\e982"}.thrv-icon-cross:be fore{content:"\e605"}.thrv-icon-align-justify:before{content:"\e604"}.thrv-icon-uniE603:before{content:"\e603"}.thrv-icon-uniE602:before{content:"\e602"}.thrv-i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\voicematic[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 932 x 551, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	125606
Entropy (8bit):	7.967032398798433
Encrypted:	false
SSDEEP:	3072:m3qOJSlm5jTyHoSp2D62WCXZakb+f6l9asQn58Gm40xv84xJrQK:OVJSlm5jTmopXWCDH6aVCH40KKQK
MD5:	74E06700B54737493E6DAE6D62E8E82E
SHA1:	EB79DF78EEF8FDC9DFDEFB2640F1239CA4D29592
SHA-256:	4AA40F5F6B74A7F60111E9C6A4C2B7836B8780411C63DEB54C5160A6BC0E2443
SHA-512:	2EF0173F7DCA0D09D5AF25FFC2589A9A4CEB8746F226EFE39AA01C6E7BA16061D39F7A88D3E6E5067F8A8AA8B9303FE59C63E3CD0B2368381537F1D5B0D4A93 A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2019/08/voicematic.png
Preview:	.PNG.....IHDR.....'.....2d-....PLTE..=..#.....#.....).....z:.B...#...,..4..(..9..$..#.....,..$..6..>.....A..-..'..,..D.....1..'..1..(..3..#..K..9..5..<..1..1.....@..4..R..7..DVu.w@.9..7..P }....3..K..1..sE.D.....[n....>..pL.ad.J.....]-..C..kR....d^._i.$.....iY. ..).....ay....a.....}M.V|.S..tW.....O..hn....mc..U..~.....<.....e.Z.....}\....ly....H.....vj.M./..... #.C...fV.<...q..D....Y_.....N...>..F?a...!.g&8.B.....[J.-.3'JP!.&..<4\...Mj.).O[.|2..>p....C%..9gE!yt9.sm.=..~>.L@.4/.Dy.3.\...\-..mn...h.q&.7i3.....M|.....\...NS].QIeM...~*lf}....u. .`.}w.e^v.'RM..[Sp>.h..t.....A7P^J.....N.....S..X.....p..l.....g-c...3.....}}.y....Xf|..y0.k...W..E..e9P.{;.....+/....j.9wI...LDr.....z..m}....JQ.[.....yC+.....$P...b.3...0.bJ.w...aIDA Tx..].n.H...C.-.&!...h..-AV./0O.w0...&.e..E.}1...i.bz..6.E7...k...N...CE...b.H.)...:.T.W...juX..J.r..j...2..r.^eV.VE\-.qR..Kp&N+...sj8TC9.a.Tk.....#._.W.pd.Sq2...?.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\weg-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, 1152x695, frames 3
Category:	downloaded
Size (bytes):	67560
Entropy (8bit):	7.90862794655821
Encrypted:	false
SSDEEP:	1536:VqeY50250q/7DlgdtgQehzygI44bsy0RBOzjjdmwshQ:VqeY501qXlgbgup4J7MjlQQ
MD5:	D4123C6B09E03056E4EF88C4879420AE
SHA1:	8C0C90B5E4958D362214122322B69AE8F134F42C
SHA-256:	551DD4B94EE03654A3A6EBEF62D698E2919047D402E712404D24034664631A84
SHA-512:	49D4E69718BF5D1F379F6F1C557AFE51CE0774077124EEF993E98DB62DF4BA6D426519507AD3E38E4D58CE4DA3176FAF21CE8BAB12279F60860E1D0DF468B7B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2019/12/weg-1.jpg
Preview:	.....JFIF.....! ....#'2*#%/%..+;,/35888!*=A<6A2785.....5$.$55555555555555555555555555555555555555555555555555..... .....X.....D.....''@.#n.....(.....Cu..D..... ....,....7z.....,_.H.....?.].=...u.Q..;4....h.<r..@./....''.....F....'.s..7...n...{.p...9..G..''.....>..... .8.a.I. .....w.....Q(.$D.Q(..D.Q(.J%..D.Q(.J%...\.....D.-..~....R.w{.V...].F.^{...c...z...D.Q(.J%..D.Q(.I.5...`.....,.....,_...h.o.w>...,_..{.....|.[.../m.D.Q(.J%..D.Q(.H..... .....`.....S.K....w.....>.Of.}.Z2....g.v$D.1(.J%..D.Q(.H.....^.9....^.}V.}_-.|.J./O...y,...q_..-.$D.D.....0.LL&&&$..''a(L$._.|..o.....t..o.g...:.u..g8..?L.[B.@&$. J.....I.....`..... <uh.....?L.[a.....&..2.....97.t....C.w.z.5.....~.0.....7...h.g_..z..gVu....?L.[.....K.P.....]..al.....+.....0...D.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\wp-emoji-release.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	12026
Entropy (8bit):	5.144024560194641
Encrypted:	false
SSDEEP:	192:3IdCwIdZKx/4W+TJr3J//bEvAbWXXR6AooHyrOUlSY06KdpNfojt3gzQ5aY:35zw4W+TJr3J//bEl+XgA5UedpqtgM5N
MD5:	15D0C302DC74FD87BD9CFEAB513E13E4
SHA1:	D25B738415C1594C4F840904BB876055D96CF256
SHA-256:	D2458B9FD9089FDCB9DE317093E004EF3A65597DC68B9ADFDEB15A7C9968D0D5
SHA-512:	CD6489B36E49844A85EB0B2E168F05F3C5BEBB622395786B9324B32D85B10A4B4FD9AFBE786B2DEBA6ECEF0EFE1CD51F2C00D72E75578CF3FD5D59283E6E90 94
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-includes/js/wp-emoji-release.min.js?ver=4.9.16

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\wp-emoji-release.min[1].js	
Preview:	// Source: wp-includes/js/twemoji.min.js.var twemoji=function(){"use strict";function a(a,b){return document.createTextNode(b?a.replace(s,""):a)}function b(a){return a.replace(u,h)}function c(a,b){return"".concat(b.base,b.size,"/",a,b.ext)}function d(a,b){for(var c,e,f=a.childNodes,g=f.length;g--;)c=f[g],e=c.nodeType,3===e?b.push(c):1!==e||"ownerSVGElement"in c||v.test(c.nodeName.toLowerCase())||d(c,b);return b}function e(a){return o(a.indexOf(t)<0?a.replace(s,""):a)}function f(b,c){for(var f,g,h,i,j,k,l,m,n,o,p,q,s,t=d(b,[]),u=t.length;u--;){for(h=!1,i=document.createDocumentFragment(),j=t[u],k=j.nodeValue,m=0;l=r.exec(k);){if(n=l.index,n!==m&&i.appendChild(a(k.slice(m,n),!0)),p=l[0],q=e(p),m=n+p.length,s=c.callback(q,c)){o=new Image,o.onerror=c.onerror,o.setAttribute("draggable","false"),f=c.attributes(p,q);for(g in f)f.hasOwnProperty(g)&&0!==g.indexOf("on")&&!o.hasAttribute(g)&&o.setAttribute(g,f[g]);o.className=c.className,o.alt=p,o.src=s,h=!0,i.appendChild(o)}o||i.appendChild(a(p,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Bonusbomber-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, 960x540, frames 3
Category:	downloaded
Size (bytes):	35196
Entropy (8bit):	7.911523697205894
Encrypted:	false
SSDEEP:	768:LVnExQNMaUmONHNmOJJi3oJDENQUUOgluVXrdbMwTdx/:BEiVONHvbi3o1/BlufMedx/
MD5:	F812F3BFFC15A4D8983739D8FA5434E4
SHA1:	68EBCF74672DF97CD06B9CBDF70A4BCB640C0413
SHA-256:	075DFF06CE9A61351E6A7C496FB7ECF94D33EC86545A7238DFD9B96494B73A76
SHA-512:	C1B25096C469FBA8BEC4F0312D96388A9D2490096029C67165D99C08773CB81E8E963698125E25C2D5826B915DB6E329D060D333CCB327C29F26CB50FC7DD10
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2019/11/Bonusbomber-1.jpg
Preview:	......JFIF..... $.' ",#..(7),01444.'9=82<.342.....2!.!2222222222222222222222222222222222222222222222222.....".....9..]5_.O%..3X...a`...`..N0.^9.r..;#..o...q.}0.O.y..={O.Y.g...>8...\/.!..y...{.....e.&.^%.m.F....B.:4.$.UK#.y....|yk..6..q.Z.M..o.n.6.".z.F.e9...H".nu5J.j.%u.....X.....x.0o.j....Q..#_....C.6g!e.8.^.8h..h.%..a.-.DY[.....>s..[q..[u.:l.A1..:W..G...R@.^..v.....q]....].B....8....Hs.b.Y..LU.h.5.@..u.#.....-6..Z..{.ql-j.....C...9....v..w.....8^R....t.>sL.Q.L.W0n-f...R.....c.....>.,...,.U3h.u.A.....Es.O.....z....W....A..12.f..6+..c+..g4.....;V.'..kt.2.G...<..=^.....$.Xu.8.....\..3.....f.z.....z...8*...?h4o../...F....WR....:j.j"K.....Z...X..`....."O.....m!..}T..-.?.->...:.n..Z.....Wl....<&.*V.j..[..R>Ibg.a..(.D.;A..[.k<....F\.=.....D.k...V..b..E.....r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\ErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4336
Entropy (8bit):	5.207912016937144
Encrypted:	false
SSDEEP:	48:5Q5K5k5pvFehWrrarrZIrHd3FIQfOSCQ5K5k5pvFehWrrarrZIrHd3FIQfOS6:5GIydFPr81yHpBGvGIydFPr81yHpBGR
MD5:	6159ABD64336CBA0EE5B0E18D39005A8
SHA1:	878A28A13FC79E80457541D0D75A3713630959EC
SHA-256:	A152AFA43222B69350F261EFDF2D8C616FE143BAD398CA5C2B02AD8862005DD1
SHA-512:	4EA9DCCCBCD43CAEEB6DD67ECDFBA58CEFEA76BB3E8CA948E84FE301FCD77D6B84568E2BC59C6C22112FC2301E1B5146A2EE059651D93A1CCB37D72DC94E9F8
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/ErrorPageTemplate.css
Preview:	.body..{...font-family: "Segoe UI", "verdana", "arial";...background-image: url(background_gradient.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_gradient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...background-color: #F4F4F4;..}.. ..a..{...color: rgb(19,112,171);.font-size: 1em;...font-weight: normal;...text-decoration: none;...margin-left: 0px;...vertical-align: top;..}....a:link, a:visited..{...color: rgb(19,112,171);...text-decoration: none;...vertical-align: top;..}....a:hover..{...color: rgb(7,74,229);...text-decoration: underline;..}....p..{...font-size: 0.9em;..}.....h1 /* used for Title */..{...color: #4465A2;...font-size: 1.1em;...font-weight: normal;...vertical-align

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\First-Launch-Profits-Review-280x150[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 280 x 127, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	10154
Entropy (8bit):	7.9774982161155
Encrypted:	false
SSDEEP:	192:2MxlG38hh54fuxYe1zdlmiWB+0qLQfmFWiCVujK75Jlb789fCQOUeY8yZo8ou:2MLPv5WMYVnqL0aWiCVu6QCQObYrPou
MD5:	71949328247B0CD13D10CE82F808F1B5
SHA1:	15AD5E5A0D56B8571E31DA7618201B5DCB416794
SHA-256:	FF0965CEA6DA61F399056FF77B2C7487D480BAA4E37CBDB47165CA8F0B73E536
SHA-512:	C193C5D05138657750F9853B59FA956091E370AE906FE30BF5D40F00865E264E6D37083BD96FC83A8156312BCEFE7DFBE7AD125889978E77F4DFC2EA1A718FDD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2019/02/First-Launch-Profits-Review-280x150.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\First-Launch-Profits-Review-280x150[1].png	
Preview:	.PNG.....IHDR.....-.....PLTELiq^kv.. ...;h~...H..(+.-.....P`j/...../..z..Kdr..$...(.....f....(..Lgw.....$..,>U...).....Lt."........#...`.'7R%.. |....r.....(.....^.....^|...=~.38Tv.....(&.L...-z....IXl...g.....!/WGJO...";...b..lot.....67?..@..#...<..w~.'+].....Z.....LRW.....#...1c{j...../2`J..C.. ..T..y...:Jj..#(]JMs...,.....,..]..0Yv.....A..C.....O,,,&*S.I`<>h.Vn.`{.I.Y\u .v.X\.bbb.|..~..... .....gj....opq'..js."..".4..%..B..{]w{.#..8..$....R..+....;..(..+..O..v.....+..5...,..?.....f...,..Y..-..B..1...i..y..4..M.....C..W...b.....R.....]...h..v.....s..... .....W....stRNS..... &'),.689<ABEGJPPTWZ\\eeiloptttxz}..... .....&e...#.IDATx..y...y.....{..... .....%P.%..Ca(.J.TeZv.'..'U._.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\KFOjCnqEu92Fr1Mu51S7ACc6Csl[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22020, version 1.1
Category:	downloaded
Size (bytes):	22020
Entropy (8bit):	7.969254342778129
Encrypted:	false
SSDEEP:	384:OdR1e4g/v2pwEHXT4vHn5YHPGVubG85NtyZpe21oW4lDXLNXOEGV0u5YN4L5:Oz1e4TpT0/cPGVppl6RLNefY2L5
MD5:	288AD9C6E8B43CF02443A1F499BDF67E
SHA1:	96A90B4B2F04445CEE7091C257D9C7D905BF74B8
SHA-256:	6F2974A396DC0695D071E842551E7AF9C72F0EF8D2D076FE73A523B1A3C2D0E7
SHA-512:	C853526CE2743996089E573DE9D99C9E1B730C41FF3F8F32E316A8ED654EE48CA04A67731D3FBC5F3FB94DB309F99F29F3FA9AC739B1D126BC909858E13C615
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v20/KFOjCnqEu92Fr1Mu51S7ACc6CsI.woff
Preview:	wOFF.....V.....8.....GDEF.....G...d....GPOS.....~..GSUB.....'.....r.OS/2.....N...`t..dcmap...X.....W.cvt ...P...\...\1..Mfpgm.....2.....$.gasp..... ....glyf.....A...r....|hdmx..N....l..... ..head..OD...6...6...vhhea..O|..."...$....hmtx..O....w.....6Kloca..R.....Zs<.maxp..S.... ... .(..name..T.....!.>gpost..T..... .a.dprep..U.....X9 ..x...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R...A.J.x....dK...{....?..F?.|.~.m...ms.{.Z..;.....U.]7s.....\.=D.=.7...>....x...D..O|.U:...|o..3.x.j.r"B......./.)x$.'"j..... 1LGmaGxQxG....~.:'.A..hd.z,.k..KO.....^.}H|#z_.O.....R..A...9..A..!.(./..."...:.lq1.r..s..r.7r.7s..q.wr....nz..]...2..d4c..c....d....T.1...d....\....,c9k.g..Yv.#O."%..... ...t"uM..%.....j .#^.....}\c.q.i...<jy.D...C.01.2.r.....V..z.W.7b..L.S.41]..kUs.X/6..b.....(..(...K..{.^..'.....`#./..B.....N+p.m`...].lQ....Drg.M..Kx.^.S.*.....h ..$.k.'Hy.I.ze..4z.-T.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\KFOkCnqEu92Fr1MmgVxIlzQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20368, version 1.1
Category:	downloaded
Size (bytes):	20368
Entropy (8bit):	7.971898421780985
Encrypted:	false
SSDEEP:	384:OIRPUl1e5SYHXm+bzFN/ZBTq3j84ogy4+nSpTub5c/Pmbw2ML:OcPC1eQYHXthN/ZBTq3s7J2y2/PQa
MD5:	5CB7EDFCEB233100075DC9A1E12E8DA3
SHA1:	0BD90E5EF8C6650F6ECC41A11A46D3F66E5A898E
SHA-256:	C4EAD4DE9F7AFF237D06B530EAD8413D1357427F6A925944342BB4E2B1DCE6D0
SHA-512:	8C00FF1EEE085F346412E08CA937260B87340374ADDD9A97B1809FD76D4E412A0A4AC44EEEB539BF65693ACACB9A1AFAD7B4F42AC1B47447AEB385B3D7F623 3B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v20/KFOkCnqEu92Fr1MmgVxIlzQ.woff
Preview:	wOFF.....O.....GDEF.....G...d....GPOS.....GSUB.....'.....r.OS/2.....P...`t..{cmap...$.....W.cvt .....H...H.2..fpgm...d...3...._...gasp.....glyf.. ....<...p|#..hdmx..H....p.....head..I4...6...6.G..hhea..II.....$...khmtx..I....c....ef.loca..K.....maxp..M.... ... .(..name..M.....x..9.post..N..... .m.dprep..N.....+6.x...1..P. .....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R...A.J.x.I..h.a.....I.m.6.1+.X....i...y....&...._..63..5....2>...x|D...ct.Kx..H@b.3..I..#u.....L.*....^.*.4.....rP..{.*.....Q...JT. :Xu>..T./>...oq.....~..@.....lq../.... ..#..".&.8.H$..r...J)..jj...&..f.=.9..N9....'F..8.4.....m...m...m.m..n..&.X..}....S.|.....n.....PHaE...J*...4..MjJ.*..nW)..rn3'/.....ks5zY5c...Mgg.5..p ..rR{c...p..t\.8.c=..p...X.(.....7....=.....!...H .....(.0...(.q.JT?.b..z].'T...m..vNi.....t....:P.R..H....t.....&?.:.j.51+.S."j.SK'I.^....}S.i.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\KFOlCnqEu92Fr1MmYUtfBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20392, version 1.1
Category:	downloaded
Size (bytes):	20392
Entropy (8bit):	7.969803364230641
Encrypted:	false
SSDEEP:	384:Ld21eNqGoVwVsb0PULg3ZaTn09dltEGKMmZvBxvSJ66JQ3GoT4G54:LY1eNqGM8jULg3Z609taBx6J6fT54
MD5:	BB1E4DC6333675D11ADA2E857E7F95D7
SHA1:	3E2625FE48669F4AD48823E8C18E6FB14B74C5A0
SHA-256:	E8586F9DB7C0503A984C944AD2F1F783BF6051AEA2A066BC21FDEDC8FE7FA68A
SHA-512:	7EBCB4E20E323880245FD9900D58FC54086132711A695825134A8F34D9C63A48610454C9F10210CBB1926A65D1FEBEA96176F865910E1A6A9487FF9BDD83D87B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v20/KFOlCnqEu92Fr1MmYUtfBBc-.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\KFOlCnqEu92Fr1MmYUtfBBc-[1].woff	
Preview:	wOFF.....O.....GDEF.....G...d....GPOS.....~..GSUB.....'.....r.OS/2.....O...`v...cmap...X.....W.cvt ...P...Z...Z...=fpgm.....3.....#.gasp..... ....glyf.....;...k@...hdmx..H....l....%(. head..I....6...6...Rhhea..l@.....$.]..hmtx..I`...y.....=.loca..K.....Mc1.maxp..M.... ... .(..name..M.....\|..9.post..N..... .m.dprep..N.....8. ..Cx...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R...A.J.x....dK...{....?..F?.\|.~.m...ms.{.Z..;.....U.]7s.....\.=D.=.7...>....x...D..O\|.U:...\|o..3.x.j.r"B...../.)x$.'"j.... .1LGmaGxQxG....~..:'.A..hd.z,.k..KO.....^.}H|#z_.O.....R..A...9..A..!.(./..."..:.Iq1.r..s..r.7r.7s..q.wr....nz..]....2..d4c..c....d....T.1...d....\....,c9k.g..Yv.#O."%..... ...t"uM..%..... j.#^.....}\c.q.i...<jy.D...C.01.2.r.....V..z.W.7b..L.S.41]..kUs.X/6..b.....(..(...K..{.^..'.....`#./..B.....N+p.m`...].IQ....Drg.M..Kx.^.S.*.....h ..$.k.'Hy.I.ze..4z.-T.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Robby-Blanchard- -Commission-Hero-280x150[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 119 x 150, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	5990
Entropy (8bit):	7.947407277681517
Encrypted:	false
SSDEEP:	96:QvGtm9iyOU6FGHomqx7NshRb4CO1Qkzqcr0fNtdu5PKzqy8kaN2iwzo3I/cwAlrP:sGEihQq7CBKQQAfNTu5S1h4uoYylVvuA
MD5:	B77AA56BBAA5B353126118C3A7B367BE
SHA1:	4857AB87A8E5EAFB2CC43CC4C83346C05D474A2A
SHA-256:	B024BB0D30A3F3C3AA040CDE08354BF026BC1E152120D251FA7573ECA0A8FAEE
SHA-512:	BB7471EE3A4F982C2A0CDF8EE90D193BF171EF6C97061B7A25ADE589C5ACE7F764B07C8920D5135CFE00C04CC4963FA48A7B3929AF1DD9232246484AA7BFF05
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...w.....PLTELiq.....@@@.....vvw.....~.....zxz.....feg.....GFGcbc..... .....4"..""!-!..%:***!-?,,-3, <*.224<2"E0./9I78;@8)=<>J<&@?@T="CBCXB'OE2GGHDLWgF#MLJbJ*ZM5QPQhN.aQ5UTUsO&P\`WVW_WEYWYhY;]\sY7e ]Q}{3`ac.X%kaHvaAgfhmg[.c5wjLlll.iB.g4popzp\.pPtsisrs.m7.sK.n?vuvyxx~yl.wH.{]|{|.wCz.v.}U.~..z?..n.....a..U....|7..N.....C..g.....v..].....U.....n.....a.....]..i..c.....x.....e..q..v.. ...l....d..x....l.....a.s..~.....x.....~.....h.....X.....H7.....AtRNS..... %'+168=>GH OPW\]blnvw.....~v].....IDATx..[...Wu...=...}..eIFFX.c#..*....@B.B..T.T.*.D..$.RI.....J ....ll.,Y+..Z...o.c.=.}.9..{fgvgvg..%..iv

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Robby-Blanchard- -Commission-Hero[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 593 x 750, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	79450
Entropy (8bit):	7.9686014232203854
Encrypted:	false
SSDEEP:	1536:IU7j/XPUCJYUuluWzrg/GhsZ8OqdL/x7IZ3nm3Y4+N3R8RjhRAPllZy:IM/PUCJCIWzrg/jlqd1I43voh8RvANlE
MD5:	9BDAE345BBD30F7BAC5B0279343A7055
SHA1:	AA837275C560E9BD7A9E4CF6CEF999580C58CA33
SHA-256:	9579F9DBD6F4A60331A7B927C491F1B6EC00A0E706B25F8CAF6176202473D351
SHA-512:	9F075239100CA0EFD24033BAC53312FF422CA73ABA7113FADD757B563A507249DB79D482E49D9932240C070FC59FDF34395E92AC0EEF81754899495C95E113C1
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...Q.....>.L....PLTELiq.....999.....<:<.....lll...:9:.....FFF.....WVWBAB.....?>?.....qoq..... .RQS...yxx...utu\{\...|{|.....KIJlkl...878.....)>.$:.g9bab....f0.m2.....Xefj.f>..4!.A..^....^..111ENZ...$...7.....f..1....$""Val.M..f.}R.....d..w=.v....+**:).'6I.....~bB.}F... .y.....".....B5..wM.....S..%...i..fWB%...o@3>NcL*PWb..k....W.mdS7..^..e70.Vl6..q.x..o..~..@GR.zq.mQe[R.oGm[?..Q8.B3'..y.q\QI...I?+{nL...\FTf}qcqbN..r.....yU..J....O rg].y4.`%..NvS,.\|f..M....r..`.....}.\|.....t3....h....o.....V5EZ.C..9..\|..(._...K...uh6.....\|.n+.^...d14@..\|..T.....SL(..]..G.....afB.....b..W.y=.9.m...rnT...$tRNS.....$/4;CJUZaioy|..... .....G..+..2.IDATx...h.g..C(.P...&!.t.....,.;V@..a#X..g..i..E8.K..ij...^.#7..:.:v..q...8.....`....y.w~H3.)N.._.....y.yg.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Unbenannt[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 120x120, segment length 16, progressive, precision 8, 1035x664, frames 3
Category:	downloaded
Size (bytes):	60919
Entropy (8bit):	7.939031644304479
Encrypted:	false
SSDEEP:	1536:BA4CQQtY8gKTQQkh1N6mFMu87W2Uf1NSP9g:BA4828gbPPLOW2UtQlg
MD5:	8BC627DF8412161B13FFFA0E9323BEA0
SHA1:	289ADF4D8D81B4317CFD8F7BD1E97CCC53A5DBED
SHA-256:	B47ABB247EFCD370914976832170EC922A28DDE656B7C7DBC87E61CE78C4804D
SHA-512:	8B72E3F1E90548DC9CF4AA22FB459F93887FBDBDA1312E01C253EF7C39113FA7CF3ED8CB81F6D567B42617AAD52023472809236B82C90D2F590F789858398F7D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2020/09/Unbenannt.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Unbenannt[1].jpg	
Preview:	......JFIF.....x.x.....'!..%..."."%()+,+. /3/*2'*+*.....*...**********.....".....".....p7..E.....3e.....5.r:..r...m+Uw%..g.....`.....?.....K.<+N.WVk..4.D->{.^.....>.....V.K..3.....h.....Zr..u.w..i.B...6.....7...rd..`....OwK...K0.s.k...../....<....._c.....v?@.p.....|}.z.....y.l.....y..~..ky.b.....4...-(.=..t]B.z.....js;t.eOcn....{.'.P..`....`...s./....\...=.....Eb....".{?@=.s..$..Kv/B~.[.Cg..[Q.3...=..J..].ho.w.....&<.%..X....DK}..._#.....efz..+.....]..jkb...L..,U..:>F<.Jf9....6.F.....Ly..0u.....*...M!zx.....??<...`j3..Z.(...@. ."..B..+{.....y.z....1<c....^s.d....OY...#.&j.....U_5~y...2r&.7.o.Ws.....z.....kGkSk.....~.....4..|..J..?._.!.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\VideoAppSuite[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 525 x 341, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	32854
Entropy (8bit):	7.953144349515157
Encrypted:	false
SSDEEP:	768:O3vNRGBODY2eXOkOYzM3V6+4AlTaAAUfsunaYuNCXzn/ydcn:O3vNRGUDXeXBOOM3V74AlMUfs86OWo
MD5:	2A8593CDEDFE59C72D1C58D6E7C0C83B
SHA1:	A25D5348C52967F4DFD2C2254FEA207D67ABF801
SHA-256:	A8D8AA3EDC3FE7A7AC553BB317E99ED4BAE0CC97A77DA985FD7DF07622783EB7
SHA-512:	6D213BA192185A9293413E1698A9689D5364EC49DB45F989B77F8A0F292354062AD2F0009AA8DA67EF0C986C1FA2DB0F2263DB4658C5F9BC51F18644336117AE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2019/07/VideoAppSuite.png
Preview:	.PNG.....IHDR.....U.....[.,.....PLTELiqskv....w.....xn.....xwy.....vwv.....z{yK.....hhi...~.|t5.....=:?{~z.....}.zv5.....|.yr1.....}'%'.K.\=m6.K.....s).k!.p..n%.i...80y1.....=.c..._WabbK..~7._..Z..~4..A..J..XR.>.w,.h'..C.UVU.....<...LC.....V.....v...Q....\\\...T.....`!....~>.....v4.....j,.@..q)..C.`..rssY..u8.yzy yB.y.....e..j$..>4.W.....?6O...dWj'..L.M.u....UM.8.b'.^$z...b!.....T!ns*.{0.U.xlllK.iC.lggg._...vo....MMN..w..3(.....Q>m?..W..o..+!99:.....%..JCEFF.o.....n:..d..=.x..,$.:\|.*....t..97.K..R`.a\.I..D..yu...Fs...4.....1..2..V.8].5..... .....]....7tRNS....)469ELLNYabcdlxz~.....d.l...}IIDATx...O\....^E.....z"U9RS.Wj..&'....1.2..:CB .<.....@!..{.....:%/-Ry....a.....0.....z.{.....Yk....)3.....S.....I{.....y.g~..s.=.....g...}.....w.....${....Nd.=...~..K.j.K/..o.{..=...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Webp.net-resizeimage-8-1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 472 x 469, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	46645
Entropy (8bit):	7.987429092534171
Encrypted:	false
SSDEEP:	768:DguqpMUKnyLYMxeBpnTsihooWx6OJe33/Zo5OXnQkxzwNaOldwMgEB/q:cuqpvKnLBpTs96OE/jvwbFq
MD5:	CCEEE076B69FED960A472DB748141C83
SHA1:	B7F2968896BC97C253FCF3684E29269CED68F4E9
SHA-256:	C1CACC57FCC003EF4A017C042252769C79413B893693E42DA09B2D20C6C43703
SHA-512:	EF4F2EE0EBC8398A59154B1AF411CDF0D70B54639AFE90063C4CF249BD7C9381422DAB238540AAE86766CFBDDECABEFF79009470AE3B9F58A037693166A23FA8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2020/09/Webp.net-resizeimage-8-1.png
Preview:	.PNG.....IHDR.....e..u....PLTE.....h.....S.....T.....b..... ...'*.)-2$(-.....$ #(,04.....Q#%*....._037.'"..#...26:.....-25..mmm.%)...59>--..]..a.....U.....#####}}066.....9>BWO-. ...(((.....e..d..M.....[?BG..bJ@..._GEEOSV..DIM..W.....111.....KNP.....]`aA@@.....nrs.....{UZ[.....uwvfii.....544....t.....PG$.....u.....{...cdc....s..d....^.....DNT.....g.....`G@Oab:99..k9KN...u.....uQLU:5.y.ZT...Wjl...~..~mc.t.liaVQ.um...$".bV7AVZ:)...}.....xt.a]E14..P...auwj`A.gd)9?.....s^\m...~tPKJ.....-.....1..n-.....P`.GWm.....|o@=.....}x_..thQj...-=...~_"$BQt..[r..0.P%...l.v\.j<.zQ.QO.\|6.a\9q.A....IDATx..}yTSY.oN...\.. +...W7...<..AH aIY...Z...a.!$`.e.+A!.(.N....p`.Z.J]....]E.J.%....wE.a...?..I... ...|p...o.g.....7I....I..4....I`'(M.;Ai...J..NP.g....4 ...N.ya.qC...i..Hk.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\YTSupremacy-280x150[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 280 x 123, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	9533
Entropy (8bit):	7.950664649552398
Encrypted:	false
SSDEEP:	192:dYWtCNrBsqZGqEeGRSuzZfxbf8Z5htIrqXV5t:SWtmtGqE/pbfIPtIOXPt
MD5:	137765B751CEE7BB13759FC558784655
SHA1:	9D3BB98A2D60ACF9FB23D87BF24F77EA886A5639
SHA-256:	9AC6E7A8F8D0514DE98F4DFD3093CF9F6D6BBC6C25EC276B24B9865F8E10621E
SHA-512:	90762ECCC79CF39B446EDC869C5D12770458B4D6A1BA2A2C548CB9B7EEBAFE8EC12342D2A94EB8CF557DC07B946021B5A583B5FC66DC012FD740F411989A23C9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2019/07/YTSupremacy-280x150.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\YTSupremacy-280x150[1].png	
Preview:	.PNG.....IHDR.....{.....Go.....PLTELiq.....}..Um.{..h}.g|.Kd.cx.:U.Yp.Ri.B\.1O.Le.C^.(G.@[..@.=X.5Q.2N./K.&D.'F.'F..:.%D..<..4..?..1..;..8..3..1../.....,.*..(..... .....!.....&.....-..6.....=.....D.....L.....R..-.. Z..'"""a..$$$k..&''s..B.$)))z.....+,,7'*U.%,//...o."....21222043354655945=35..''@24K-3E04O,3I/4888T+2e#0[(2a&1m!0t./..- {....,;;;...,..+..*..)...,..)..(..)..(..'?>>..(..$..'..%Y4;..'..'.-DDD.'9o5?JJJ..6_CHOOOv?HSSS.&?WVV.>JkRW\[[.,E___sW\baa.FT.3Neee{_c.CWhhh.[b.=Ukkk.VbIIlmnn.Pb. G^rrruuu.Viyyy.Pf~}}.px....[o.ev....ey....dy.....n.....}.....}..... .....~....tRNS.....!(0<=GIRZ^ghsx|.....&[..!.IDATx..y.\.}..9w...[.....IHb.Y.&K&N..b....2..L*..R..J9..1U....g...q.....%8...d.... .}y..{...,...~...d.dY..}...s>...s.8...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Youtube-Affiliate-Hack[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, 960x540, frames 3
Category:	downloaded
Size (bytes):	33414
Entropy (8bit):	7.913699781145412
Encrypted:	false
SSDEEP:	768:8c16BpdXT7dI20PKyJrhHsx471vZ5fyGehv4W:8fdDhhk/Jt+CUvL
MD5:	C7A172E40F891F318A4BBCA13F63368A
SHA1:	4FBF98E027A7991D110358D27C3B7CB927627AF6
SHA-256:	6DE1D50FFFA085B3523FBF4B2F387D0E639ED10DFC921F48E96F718F5880AA44
SHA-512:	43BB778F5826220204B993AF118DF8634E461EA08B6DE8B7F2562EE9C4FB5491F6153F78B06BEB8A200969E862B5A2C77C889FD876C7139D5FAA2946575A78A1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2019/07/Youtube-Affiliate-Hack.jpg
Preview:	......JFIF..... $.' ",#..(7),01444.'9=82<.342.....2!.!2222222222222222222222222222222222222222222222222222.....",..... .....q.....c.2..1..1. .9.\..C.'.N".&1.8.....,A*..VG....{...t.YJ.9.....dk..1.q<U4..o....i5.h.r....[.r.....j..'...C.D.*..a...i`....Vg.[l7.[.WH.!?.....~..&E..Z....V.m..;.l.> a.alx.P...V...#...0h6..[.N..9[.....O....i.X...;.G-.....fa.....t+S.E..(.-q...oV..i...,r.&Z.!MubT..7....v:....~..]tf.|+u.. .+a.@....~U...G0o+[.@.....l.M,....".u..6...l.s.w..\4...V..V..3-Z.$J.2I..... f.)r..X..V.....n.:...l4h.S.....q.m..7... L.....+W..+..jaH..E:...=[1\.....?}.U....;L.D...)....r....e 8.....w.MZ&....juH...h.<..smT..m..7...t.....w.bxc.0._n..F.....zn.ak....*.....e.w...2.J.z...= `...?i.....Y.K[.!.1..T.....*:.U.M..`.V....X.....F.....Z.R/.QN.ak.V.W=7y...P.,.m.ek..2.-..W=.O...g..&.....u.1..T.....Z.cV....m..7... L.....5.S.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\admin-ajax[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	30913
Entropy (8bit):	5.07585598384244
Encrypted:	false
SSDEEP:	384:hArSu4z8qfe4zfN/3P2ycLvj4/kFXxeCWHDkBc8MmuF8JEQ5oEx6GQ+G:hA5Tqf3pVcLvkkzBJpuF7QC
MD5:	B495588F067FBBE6F3DB606F7D75F8D0
SHA1:	FBC837AD43370F2291E70EBE3206D5C7AE41FAD3
SHA-256:	CDBB5CCA83B7ED073A9FA0A2860D9FF698CE324A60DADD77B92C004F6E89BB59
SHA-512:	294F47728950B458D1AE43F48F3F59B2BE2BBC1CE09E95F0445DF06CE88432AB2912F81E84874619547867F10F7B6CB191AD84A9B61F83778BFF47D8E8AE0BBB
Malicious:	false
Reputation:	low
Preview:	@import url('https://fonts.googleapis.com/css?family=Roboto:100,100i,300,300i,400,400i,500,500i,700,700i,900,900i');@import url('https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css');@import url('https://code.ionicframework.com/ionicons/2.0.1/css/ionicons.min.css');.theme__sm-6 .mw-elements-wrapper__link{color:white;}[data-toggle~="collapse"]{cursor:pointer;}.bt{box-shadow:0 0 0 1px #000 inset;}.list-none ul,.list-none li{margin:0;padding:0;list-style:none;}.fntWN{font-weight:normal;}.fntB{font-weight:500;}.fntBB{font-weight:bold;}.txtUp{text-transform:uppercase;}.txtDecorNoneAlways{text-decoration:none;}.txtDecorNoneAlways:hover,.txtDecorNoneAlways:active{text-decoration:none;}.bgOk{background:#4ebb74;color:#fff;}.clear:after{content:" ";display:block;clear:both;}.mw-content--editor{overflow:hidden;}.mw-content--editor img{max-width:100%;height:auto;}.mw-content--editor iframe{max-width:100%;margin:10px 0;}.mw-content--editor .alignleft{float:left;margin:5px

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\background_gradient[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 1x800, frames 3
Category:	dropped
Size (bytes):	906
Entropy (8bit):	5.019973044227213
Encrypted:	false
SSDEEP:	12:V/XPYhiPRd8j7+9LoIrobtHTdbKs/XPYhiPRd8j7+9LoIrobtHTdbKi:dkiPoj7+XrobPbNkiPoj7+XrobPbX
MD5:	65B40239A269922CC6DB52BB57B142CB
SHA1:	C2B0F017A39CADE113A2F3E1E12C229E72A6E134
SHA-256:	13C0147E89DEF62D785AB0C6F772C7A01298DECC8F756DE5A7E7897C6FB84672
SHA-512:	122C07B70BC963D5DCC438E45DE0B31F0D4A3A9D1E3D8C91176A80247CD3FBD13E3C6F3D3F13EC2327CDCE4A8C78D113BA95DC76B3FC80D1ADB3931F57DF5A8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\background_gradient[1]	
Preview:	.....JFIF.....d.d.....Ducky.....P.....Adobe.d..... ..... W..... .....Qa.....?.....%.....x.....s...Z.....j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.....p.....A.....BP..qD.(.....ntH.@.....h?.....JFIF .....d.d.....Ducky.....P.....Adobe.d..... ..... W..... .....Qa.....?.....%.....x.....s...Z.....j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.....p.....A.....BP..qD.(.....ntH.@.....h?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\bullet[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKIv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.;j.;l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\common[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	668
Entropy (8bit):	4.830230763847461
Encrypted:	false
SSDEEP:	12:zmjNwRiI/0asfZVMtnXfK4FXJ+jyZR8y3t3EXuZX0e3KJRD:IaQfjMdTZYyP8yx8kke6JR
MD5:	70C32E124E81A8F574A02BB870BC869A
SHA1:	28EEE1F95A68FD71E6D031469DE9A7D3115DA6E5
SHA-256:	8C34BA09C45B461460ECDF4603AA5192CA3E32A4D4985E12AE9A8607378566AC
SHA-512:	F4EB1EC50A9C5077CED4E88A55F5D4E76358C0F8D863B2794B03302D1B267BE372D1FD7BEA45A2D9F54C72ABAF726E5C9616AF6A096A722523E10037897902F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/plugins/wp-product-review/assets/css/common.css?ver=3.7.11
Preview:	.affiliate-button {..clear: both;..width: 100%;..margin-bottom: 20px;.}...affiliate-button2 {..float: left;..clear: none !important;..width: 50% !important;..margin-bottom: 20px;.} ...affiliate-button a {..display: table;..margin: 20px auto 0;..padding: 10px 35px;..border: none;..border-radius: 5px;..text-decoration: none !important;.}...affiliate-button a:ho ver span {..text-decoration: none;..;.}...affiliate-button a span {..margin-left: -10px;..padding-left: 20px;..font-size: 14px;..font-weight: normal;..font-style: italic;..text-dec oration: none;..text-transform: uppercase;.}....wppr-template .wppr-dashicons {..height: 47px;..width: 47px;..font-size: 47px;.}

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):	2156
Entropy (8bit):	5.180499084569838
Encrypted:	false
SSDEEP:	48:UY3QS7N1Y3QWNrY3QLNbBY3QgNnY3QCNiY3QMN+OS7N2OWNsOLNtCOgNCOCNfOMW:UYgS7N1YgWNrYgLNlYggNnYgCNiYgMNE
MD5:	AF74D74E24EF776EACA7A6813BD318B5
SHA1:	C92907BD79BBE8AC71A8BC20B6D2CBDEFF7E1620
SHA-256:	76EA784F35F6BE7794F1F5069719F6FC0441F00691AA97540418582A81B4F936
SHA-512:	7679130214ABEF91978D522260787554A29A7273B9642F24A26376FA3CFAD2EF21BA541B81756E2E7E95885EFC51BF2E99461D2B52EFAA891674999F8EC22C0A
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Roboto';. font-style: italic;. font-weight: 100;. src: url(https://fonts.gstatic.com/s/roboto/v20/KFOiCnqEu92Fr1Mu51QrEzAdKQ.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: italic;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/roboto/v20/KFOjCnqEu92Fr1Mu51TjASc6CsI.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: italic;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/roboto/v20/KFOkCnqEu92Fr1Mu51xIIzQ.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: italic;. font-weight: 500;. src: url(https://fonts.gstatic.com/s/roboto/v20/KFOjCnqEu92Fr1Mu51S 7ACc6CsI.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: italic;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/roboto/v20/KFOjCnq Eu92Fr1Mu51TzBic6CsI.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: italic;. font-weight: 900;. src: url(http

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Reputation:	low
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\fe-1024x632[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1023 x 632, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	135289
Entropy (8bit):	7.819010177028649
Encrypted:	false
SSDEEP:	3072:NVKiHgxkJbatkpZXJ13kQ+WMc3tPfxQHLcRt1riCDtrMI:NVoxkJGU5H3tTRxQHLcdiI4I
MD5:	628820E6FA6341D9E7284322E5C89FEF
SHA1:	D54A1FC08640205E924E007BBEFA5B8759724761
SHA-256:	B9E642D4AF294ACC40FDFCD25240486767065C527A92CA1ECE5CD450B060A39C
SHA-512:	BCE327D378908C556048D56C192C2BA0A5F8F0FAB54FDAE2976C6EE29C6FFDA4A9E26916AB1A89790BA4F67FDB1ED127B7D8286DF13483917DD7814B6271D0 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2019/02/fe-1024x632.png
Preview:	.PNG.....IHDR.....x.....PLTELiq.....kb.....]X\.....Xg.OIK.....MGD...{un.....PRsZL....._I....NLL.....G8#.....:.g/..Y.E....I.....&x# /o..c:O.....L.....L.....L.....#L....+M....[P....TP..L.OP.AN.2M.<M.]N..D..K.JN....cP..G.....PPQaR..J. X..R.WP.([..J.....O..L..N..O.(N..K..LLL.`.7N.EM....K....4X.^L .....O.....h}.6e...W..L.1C..D.t.....A.....CCB....<..F.....=.?B.CW..... ...RK.aq.WY..7.{.....@I..(()...Nw.X.....MB.....d.....;.o.....id.Ye.....~.....c.... ...8...vt.....A.~....Hd..Q.W|...../....tuuFr...5.]^`Uq...%X.iij..r:h.n....|....j^.555.+.p....F6..w.....Js.XF....6<].../a.Co.23.G@.31.2F.V`...;..`.....=tRNS.....(22?@LMZ_dflxz.... .....m.3.....IDATx..MO.G..6..4!4....%Q...~. .BI.".#...QD..{...B..F.....*a..*z.....T...!UO.....;;..o.yf..%...`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	24210
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	384:xPini/i+1Btvjy815ZVUwiki3ayimi5eqBG1fm304Pini/i+1Btvjy815ZVUwik5:8i6+1B1y815PUNZ3ab3fBK9i6+1B1y8d
MD5:	7B6C8BD51E49F7F56E2B21311D0EA59B
SHA1:	EDB0F7D21BCEC6C48DEDC14E9ED41383740BAE37
SHA-256:	620BD33A4E0358498D9429FE2DBA00F85A86D6059FA796B482E2A9F6B0794F2D
SHA-512:	DD1D524872EE165D230BE5B3872DEE108B806AB684AACFA955F07B7A87C1ACA63FA3B59210442E1E3C9A2D33409583E0AC3B1A6A0D4EB91BBEEF62D311FD1E C4
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.su bstring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var pound Index = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC134
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.../...0.....#.....IDATx^...pUU..{....KB.....!....F.....jp.Q.....Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{.....[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po.....X..;.=.P...../...+...9./..s.....9..|.....*.7v.`..V.....-^.$S[[[.....K..z.....3..3....5 ...0..''/n/.c...&.{.ht..?....A..I{.n.....|....t.....N}..%.v...:.E..i....`....a.k.mg.LX..fcFU.fO-..YEfd.}...~.''.. ....}l$....^.re..'^X..*}.?.^U.G..... .30...X.....f[.l0.P`..KC...[..[..6....~..i..Q.|;x..T .....s.5...n+.0..;...H#.2..#.M..m[^3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..l[..a... .N,,.h.....5...f*.y...}...BX{.G^...?.c.....s^..P.(..G...t.0.:.X.DCs.....]vf...py).....x..>-..Be.a...G...Y!...z...g.{....d.s.o.....%.x.....R.W.....Z.b,....!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a).:t..e.j.W.....C<.1.....c..l1w....]3%....tR;,..3..-.NW.5...t..H..h..D..b.....M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\instaglory-1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 233 x 78, 8-bit grayscale, non-interlaced
Category:	downloaded
Size (bytes):	1740
Entropy (8bit):	7.835575513524889
Encrypted:	false
SSDEEP:	24:a+QD6pq1k8M0GPVtzZOmtxT1+BHgixnM7Wc/y5c1+NjL7nWtrTgzWMVs9UUcAogK:N5Q+8M08VV4MjZ2nqf/y1LWgW39vBhM
MD5:	75F3486DD2FB8E78A8F14BEBC3627E4D
SHA1:	BD2576D12E2426F9377824C09820D0C5E1EEABFE
SHA-256:	65D699479EA068128501285F8954E9A833EF778D2AD0E931A75CC8B407D1E05B
SHA-512:	164060A2BF6AC90D7BEF7972A3D5A4CEA820DA4E4244DFAF32DBA3423AE9AC4C3D9532931B87FF52BED516D78484FFFA16795B3CD09A15180790C5B44BBC79BC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-content/uploads/2019/03/instaglory-1.png
Preview:	.PNG.....IHDR.....N.....Eni....IDATx...k.....y ..A..*Y2..Y.,NB.....E:8.')tpp... tpqp.n.N..q.R.!.!.!..p^.Ib..j.:.x...jL.....Ri*M..4...T.JSi*...z.u5.s..Rw..E.jHJe...E.....P..h"C.(..-.K.;./.RG=..+..S..+Eo>A.v?.DGc.a.8.R.....L}jc.T.$C....}./..i&T.:..~\..3[!.i..I....tv..K.?.p.m._i.|'Z*.....j.B:.....Hk.....<.d~.L...L....0e...VC.9.....`..L.s....Y.{8?...e.e/;*...}...V..qY..B..... E;.F.3.E.....\h.5.a)GN..4Bw..m...e...u.K..E.o.r?..g.9&.0....|=..fX0.e^.e..-ya.D.cw8Q.3....F.h...a)T....m..^.v8.s.]...M)T.G.C.Dd%..G.^H...s.s...Y.U..Ljj...6'....x-5.$.e~..b0.nU.C. .].f...H.y.-../...-s....1...&.D.V.8Yo._=f...;.....'?#.i.........{.S...'.45.oJ..B...J.}.2.<. .Y.1..dH.d+\a..i.....d.E..~%w.2"1.cg8M..I.5"-...FS.\Z.x....I.).=.....ID.%....#.=.d.G.....-..K^.C.Z _6..H..0N..\j.v._.V.-.=....*.U.Amnv.Y....K8.....:.%.....L...#m..P.o.wA..".\....!.|.>.h.U.s.}.....Z..^.%.K.N.Y....`...I.....x...}.D.H.2..F.xkI..+s.....S:..B0k..XR...Y.R2...,9.}*.q

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\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):	10056
Entropy (8bit):	5.308628526814024
Encrypted:	false
SSDEEP:	192:kZrk/GNyd31svs7wkX8KzJcqSDdAcHX4YE5NLR:srhNyNO0kkMKzFSDdAcIYwLR
MD5:	7121994EEC5320FBE6586463BF9651C2
SHA1:	90532AFF6D4121954254CDF04994D834F7EC169B
SHA-256:	48EB8B500AE6A38617B5738D2B3FAEC481922A7782246E31D2755C034A45CD5D
SHA-512:	B74A2F03C64E883B9A34DE43690429327DFB4AA230A7A6AFCA8150A16E3D84E98461245FF264C26368D9904562CC34FE219F71F951D364FA5C68C039B76776CD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-includes/js/jquery/jquery-migrate.min.js?v=1.500.1
Preview:	/*! jQuery Migrate v1.4.1 | (c) jQuery Foundation and other contributors | jquery.org/license */."undefined"==typeof jQuery.migrateMute&&(jQuery.migrateMute=!0),function(a,b,c){function d(c){var d=b.console;f[c]||(f[c]=!0,a.migrateWarnings.push(c),d&&d.warn&&!a.migrateMute&&(d.warn("JQMIGRATE: "+c),a.migrateTrace&&d.trace&&d.tra ce()))}function e(b,c,e,f){if(Object.defineProperty)try{return void Object.defineProperty(b,c,{configurable:!0,enumerable:!0,get:function(){return d(f),e},set:function(a) {d(f),e=a}})}catch(g){}a._definePropertyBroken=!0,b[c]=e}a.migrateVersion="1.4.1";var f={};a.migrateWarnings=[],b.console&&b.console.log&&b.console.log("JQMIGRATE: Migrate is installed"+(a.migrateMute?"":" with logging active")+", version "+a.migrateVersion),a.migrateTrace===c&&(a.migrateTrace=!0),a.migrateReset=function(){f={}, a.migrateWarnings.length=0},"BackCompat"===document.compatMode&&d("jQuery is not compatible with Quirks Mode");var g=a("<input/>",{size:1}).attr("size")&&a.attr Fn,h=a.att

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\jquery[1].js	
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	96874
Entropy (8bit):	5.3722595540197595
Encrypted:	false
SSDEEP:	1536:HYE1fGBiByJsbfXXeRJ/shgWCeLLccJdZVHk04ssx+/mvaSIFSet43tpXJIGVypf:fsAg0psxTva/FSeKy2bDD5a98HrU
MD5:	DC5BA5044FCCC0297BE7B262CE669A7C
SHA1:	F137FF98AE379E35B0702967D3B6866A0A40E3BE
SHA-256:	CF34E1B87BBFD9D9B185DEC994924A496E279D8DC9387AD8D35BC0110134C4D3
SHA-512:	BAB5EB2C4ACC0CB1C65E8DEDBD6B422480FC20076D6C1B12879CBF1E5B352969E1553A0E878401C2F2B9507B64B02E8ABD4C6D1AB7E3D2C06272A491EE7128A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/wp-includes/js/jquery/jquery.js?v=1.500.1
Preview:	/*! jQuery v1.12.4 | (c) jQuery Foundation | jquery.org/license | WordPress 2019-05-16 */.!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="1.12.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?a<0?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return this.pushStack(n.map(this,fu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\navcancl[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5426
Entropy (8bit):	4.1712007174415895
Encrypted:	false
SSDEEP:	48:upU0GVeLVGBXvrp4n/1a5TI7Ve/G79K+pU0GVeLVGBXvrp4n/1a5TI7Ve/G79KX:uSpNEaKVaC9jSpNEaKVaC9i
MD5:	88BEA10874964E8AE41B14BAABF876CD
SHA1:	AF5BB819916D8DBE26FBC43C1E24CC72ECDC2DA7
SHA-256:	6ADC5890B85D784B3BB634AFC33698845052EE8DB8C14509B9F98F184A32F975
SHA-512:	9B99C25F19258F3E7009A237B22AB70013D2841C63123DDF17ED314AADFD73AC26BADA90AD4B8F5B8CF91FF17FFD2D0AF9DFB061BF5CC9781E89AABEDF17AF7
Malicious:	false
Reputation:	low
Preview:	.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html>.... <head>.. <link rel="stylesheet" type="text/css" href="res://ieframe.dll/ErrorPageTemplate.css" />.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />.... <title>Navigation Canceled</title>.... <script src="res://ieframe.dll/errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="res://ieframe.dll/httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:navCancelInit(); ">.... <table width="730" cellpadding="0" cellspacing="0" border="0">.... Error title -->.. <tr>.. <td id="infoIconAlign" width="60" align="left" valign="top" rowspan="2">.. <img src="res://ieframe.dll/info_48.png" id="infoIcon" alt="Info icon">..

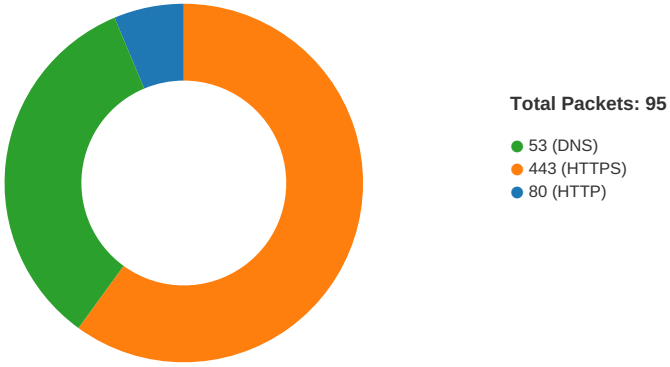
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\online-marketing[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	38272
Entropy (8bit):	5.25377998331116
Encrypted:	false
SSDEEP:	768:QP41eJKhbtprociR8dQl0uYTPtv4Fnxf6:QqMKhbtprXiRbl0uYTPtv4Fnxf6
MD5:	F112BE16470360695CF9093300EEDFAF
SHA1:	813A36B908A36F5F3558F56A0F1A19A10193B96C
SHA-256:	86E9EEC719812B50EBA916A3AC3570D464D8DB4B7FA3B4AAA7D74E95EEBE4746
SHA-512:	D58F10F6712D1A05A74AC984DF3E19A6196519F340546051E2B1EC006880DDF8C6C90AA2682F07716E7968DA5CE186CC04E31FC07DFD53C074780AA226E62F5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bonusbomber.com/category/online-marketing/
Preview:	<!DOCTYPE html>.<html lang="en-US">.<head>... [if lt IE 9]>..<script src="https://bonusbomber.com/wp-content/themes/rise/js/html5/dist/html5shiv.js"></script>..<script src="//css3-mediaqueries-js.googlecode.com/svn/trunk/css3-mediaqueries.js"></script>..<![endif]-->.. [if IE 8]>..<link rel="stylesheet" type="text/css" href="https://bonusbomber.com/wp-content/themes/rise/css/ie8.css"/>..<![endif]-->.. [if IE 7]>..<link rel="stylesheet" type="text/css" href="https://bonusbomber.com/wp-content/themes/rise/css/ie7.css"/>..<![endif]-->..<meta name="viewport" content="width=device-width, initial-scale=1.0"/>..<meta charset="UTF-8">.....<title>Online Marketing Archives - Bonusbomber</title>.. This site is optimized with the Yoast SEO plugin v11.3 - https://yoast.com/wordpress/plugins/seo/ -->.<link rel="canonical" href="https://bonusbomber.com/category/online-marketing/" />.<meta property="og:locale" content="en_US" />.<meta property="og:type" content="object" />.<meta property

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 14:06:17.401072979 CET	49695	80	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:17.401480913 CET	49696	80	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:17.434829950 CET	80	49695	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:17.434878111 CET	80	49696	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:17.434954882 CET	49695	80	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:17.434998035 CET	49696	80	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:17.437320948 CET	49695	80	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:17.472938061 CET	80	49695	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:17.473043919 CET	49695	80	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:17.484916925 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:17.518507957 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:17.518613100 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:17.523344040 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:17.557105064 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:17.557183027 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:17.557224035 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:17.557251930 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:17.557252884 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:17.557310104 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:17.557343960 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:17.558499098 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:17.558676004 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:17.646507025 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:17.652955055 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:17.653095007 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:17.680427074 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:17.680567026 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:17.686552048 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:17.686794043 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:17.687047005 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:17.720437050 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:19.169801950 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:19.169857979 CET	443	49697	185.61.152.57	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 14:06:19.169888020 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:19.169917107 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:19.169949055 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:19.169986963 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:19.170023918 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:19.170059919 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:19.170162916 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.170200109 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.170206070 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.500189066 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.509582043 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.510094881 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.510536909 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.511143923 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.511615992 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.512064934 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.512558937 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.573770046 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.576453924 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.583323956 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.587711096 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.593656063 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.597470999 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:19.597580910 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:19.597711086 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.600960970 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.602739096 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:19.602873087 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:19.602879047 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.602909088 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:19.602935076 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.602962017 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.603025913 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:19.603060961 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:19.603085041 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.603116035 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.603600979 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:19.603643894 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:19.603668928 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.603713989 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.604401112 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.604753971 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:19.604794979 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:19.604835033 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.604835987 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:19.604861975 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.604902983 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.609792948 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:19.619020939 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.619446993 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.619853973 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.620254993 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.620657921 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.621181965 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:19.624768019 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.625202894 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.626817942 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.627274036 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.627732992 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.628165960 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.628709078 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.629703999 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.630713940 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.631386995 CET	443	49697	185.61.152.57	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 14:06:19.631767035 CET	49697	443	192.168.2.3	185.61.152.57
Nov 29, 2020 14:06:19.636466980 CET	443	49697	185.61.152.57	192.168.2.3
Nov 29, 2020 14:06:19.636518955 CET	443	49697	185.61.152.57	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 14:06:11.442995071 CET	58643	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:11.478718996 CET	53	58643	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:12.280688047 CET	60985	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:12.308068037 CET	53	60985	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:13.242124081 CET	50200	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:13.269231081 CET	53	50200	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:16.288793087 CET	51281	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:16.326062918 CET	53	51281	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:16.599666119 CET	49199	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:16.635253906 CET	53	49199	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:17.349495888 CET	50620	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:17.389456034 CET	53	50620	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:17.933233023 CET	64938	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:17.968884945 CET	53	64938	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:19.011799097 CET	60152	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:19.047379971 CET	53	60152	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:20.459703922 CET	57544	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:20.503016949 CET	53	57544	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:20.513528109 CET	55984	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:20.516072989 CET	64185	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:20.543030024 CET	53	64185	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:20.548960924 CET	53	55984	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:21.231307983 CET	65110	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:21.269311905 CET	53	65110	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:21.926892996 CET	58361	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:21.962507010 CET	53	58361	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:23.158782959 CET	63492	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:23.185925007 CET	53	63492	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:24.007231951 CET	60831	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:24.051187038 CET	53	60831	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:25.258229971 CET	60100	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:25.293940067 CET	53	60100	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:26.364876986 CET	53195	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:26.400456905 CET	53	53195	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:44.078737974 CET	50141	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:44.117202997 CET	53	50141	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:46.310726881 CET	53023	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:46.338027000 CET	53	53023	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:46.996299028 CET	49563	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:47.000735044 CET	51352	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:47.027822971 CET	53	51352	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:47.035345078 CET	53	49563	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:47.329221964 CET	53023	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:47.356385946 CET	53	53023	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:48.115509987 CET	51352	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:48.142795086 CET	53	51352	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:48.342591047 CET	53023	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:48.369820118 CET	53	53023	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:49.118534088 CET	51352	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:49.145629883 CET	53	51352	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:50.359232903 CET	53023	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:50.386317015 CET	53	53023	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:50.416734934 CET	59349	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:50.452321053 CET	53	59349	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:50.642577887 CET	57084	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:50.679866076 CET	53	57084	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:51.139619112 CET	51352	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 14:06:51.166718960 CET	53	51352	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:54.373300076 CET	53023	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:54.402476072 CET	53	53023	8.8.8.8	192.168.2.3
Nov 29, 2020 14:06:55.138983965 CET	51352	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:06:55.166321039 CET	53	51352	8.8.8.8	192.168.2.3
Nov 29, 2020 14:07:00.980304956 CET	58823	53	192.168.2.3	8.8.8.8
Nov 29, 2020 14:07:01.019586086 CET	53	58823	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 29, 2020 14:06:17.349495888 CET	192.168.2.3	8.8.8.8	0x3dab	Standard query (0)	bonusbombe r.com	A (IP address)	IN (0x0001)
Nov 29, 2020 14:06:20.513528109 CET	192.168.2.3	8.8.8.8	0xcac3	Standard query (0)	code.ionic framework.com	A (IP address)	IN (0x0001)
Nov 29, 2020 14:06:20.516072989 CET	192.168.2.3	8.8.8.8	0x3655	Standard query (0)	cdnjs.clou dflare.com	A (IP address)	IN (0x0001)
Nov 29, 2020 14:06:44.078737974 CET	192.168.2.3	8.8.8.8	0xbf3	Standard query (0)	bonusbombe r.com	A (IP address)	IN (0x0001)
Nov 29, 2020 14:06:50.416734934 CET	192.168.2.3	8.8.8.8	0x9fc6	Standard query (0)	www.facebo ok.com	A (IP address)	IN (0x0001)
Nov 29, 2020 14:06:50.642577887 CET	192.168.2.3	8.8.8.8	0xf095	Standard query (0)	m.facebook.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 29, 2020 14:06:17.389456034 CET	8.8.8.8	192.168.2.3	0x3dab	No error (0)	bonusbombe r.com		185.61.152.57	A (IP address)	IN (0x0001)
Nov 29, 2020 14:06:20.543030024 CET	8.8.8.8	192.168.2.3	0x3655	No error (0)	cdnjs.clou dflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Nov 29, 2020 14:06:20.543030024 CET	8.8.8.8	192.168.2.3	0x3655	No error (0)	cdnjs.clou dflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Nov 29, 2020 14:06:20.548960924 CET	8.8.8.8	192.168.2.3	0xcac3	No error (0)	code.ionic framework.com		104.26.6.173	A (IP address)	IN (0x0001)
Nov 29, 2020 14:06:20.548960924 CET	8.8.8.8	192.168.2.3	0xcac3	No error (0)	code.ionic framework.com		104.26.7.173	A (IP address)	IN (0x0001)
Nov 29, 2020 14:06:20.548960924 CET	8.8.8.8	192.168.2.3	0xcac3	No error (0)	code.ionic framework.com		172.67.69.29	A (IP address)	IN (0x0001)
Nov 29, 2020 14:06:44.117202997 CET	8.8.8.8	192.168.2.3	0xbf3	No error (0)	bonusbombe r.com		185.61.152.57	A (IP address)	IN (0x0001)
Nov 29, 2020 14:06:50.452321053 CET	8.8.8.8	192.168.2.3	0x9fc6	No error (0)	www.facebo ok.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Nov 29, 2020 14:06:50.452321053 CET	8.8.8.8	192.168.2.3	0x9fc6	No error (0)	star-mini. c10r.faceb ook.com		185.60.216.35	A (IP address)	IN (0x0001)
Nov 29, 2020 14:06:50.679866076 CET	8.8.8.8	192.168.2.3	0xf095	No error (0)	m.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Nov 29, 2020 14:06:50.679866076 CET	8.8.8.8	192.168.2.3	0xf095	No error (0)	star-mini. c10r.faceb ook.com		185.60.216.35	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- bonusbomber.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49695	185.61.152.57	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 29, 2020 14:06:17.437320948 CET	60	OUT	GET / HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: bonusbomber.com Connection: Keep-Alive
Nov 29, 2020 14:06:17.472938061 CET	61	IN	HTTP/1.1 301 Moved Permanently date: Sun, 29 Nov 2020 13:06:17 GMT server: Apache location: https://bonusbomber.com/ content-length: 232 content-type: text/html; charset=iso-8859-1 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff strict-transport-security: max-age=31536000; includeSubDomains; preload; referrer-policy: no-referrer-when-downgrade Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 62 6f 6e 75 73 62 6f 6d 62 65 72 2e 63 6f 6d 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	185.61.152.57	80	192.168.2.3	49696	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 29, 2020 14:06:33.470174074 CET	1609	IN	HTTP/1.1 408 Request Time-out content-length: 110 cache-control: no-cache content-type: text/html connection: close Data Raw: 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 3c 68 31 3e 34 30 38 20 52 65 71 75 65 73 74 20 54 69 6d 65 2d 6f 75 74 3c 2f 68 31 3e 0a 59 6f 75 72 20 62 72 6f 77 73 65 72 20 64 69 64 6e 27 74 20 73 65 6e 64 20 61 20 63 6f 6d 70 6c 65 74 65 20 72 65 71 75 65 73 74 20 69 6e 20 74 69 6d 65 2e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <html><body> 408 Request Time-out Your browser didn't send a complete request in time.</body></html>

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 29, 2020 14:06:17.558499098 CET	185.61.152.57	443	192.168.2.3	49697	CN=bonusbomber.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	Sun Jul 26 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Tue Jul 27 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 29, 2020 14:06:20.579756975 CET	104.16.19.94	443	192.168.2.3	49702	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 29, 2020 14:06:20.586416960 CET	104.16.19.94	443	192.168.2.3	49703	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 29, 2020 14:06:20.942712069 CET	104.26.6.173	443	192.168.2.3	49704	CN=ionicframework.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Jul 01 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Jul 01 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 29, 2020 14:06:20.944322109 CET	104.26.6.173	443	192.168.2.3	49705	CN=ionicframework.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Jul 01 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Jul 01 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 29, 2020 14:06:44.204452991 CET	185.61.152.57	443	192.168.2.3	49717	CN=bonusbomber.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	Sun Jul 26 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Tue Jul 27 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Nov 29, 2020 14:06:50.487941027 CET	185.60.216.35	443	192.168.2.3	49721	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 02 01:00:00 CET 2020 Tue Oct 22 14:00:00 CEST 2013	Sun Jan 31 00:59:59 CET 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Nov 29, 2020 14:06:50.489005089 CET	185.60.216.35	443	192.168.2.3	49722	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 02 01:00:00 CET 2020 Tue Oct 22 14:00:00 CEST 2013	Sun Jan 31 00:59:59 CET 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Nov 29, 2020 14:06:50.815443039 CET	185.60.216.35	443	192.168.2.3	49723	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 02 01:00:00 CET 2020 Tue Oct 22 14:00:00 CEST 2013	Sun Jan 31 00:59:59 CET 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Nov 29, 2020 14:06:50.815658092 CET	185.60.216.35	443	192.168.2.3	49724	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 02 01:00:00 CET 2020 Tue Oct 22 14:00:00 CEST 2013	Sun Jan 31 00:59:59 CET 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Code Manipulations

Statistics

Behavior

● iexplore.exe
● iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6024 Parent PID: 792

General

Start time:	14:06:15
Start date:	29/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff72e790000
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: 6068 Parent PID: 6024

General

Start time:	14:06:16
Start date:	29/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6024 CREDAT:17410 /prefetch:2
Imagebase:	0x12d0000
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	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly