



ID: 418881
Cookbook: browseurl.jbs
Time: 20:32:34
Date: 20/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report https://risefundraiser.com/campaign/help-india-fight-covid-19-donate-for-oxygen 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
AV Detection: 5
Phishing: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 12
Public 12
General Information 12
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 14
ASN 14
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
Static File Info 47
No static file info 47
Network Behavior 47
Network Port Distribution 47
TCP Packets 47
UDP Packets 49
DNS Queries 50
DNS Answers 51
HTTPS Packets 52
Code Manipulations 58
Statistics 58
Behavior 58
System Behavior 58

Copyright Joe Security LLC 2021

Analysis Process: iexplore.exe PID: 4852 Parent PID: 792 58
General 58
File Activities 59
Registry Activities 59
Analysis Process: iexplore.exe PID: 5172 Parent PID: 4852 59
General 59
File Activities 59
Registry Activities 59
Disassembly 59

Copyright Joe Security LLC 2021

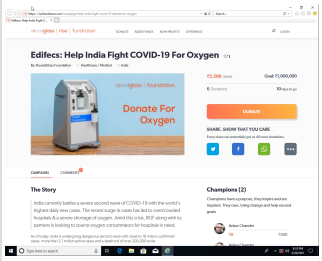
Analysis Report https://risefundraiser.com/campaign/he…

Overview

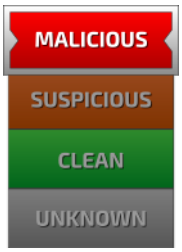
General Information

Sample URL:	http://https://risefundraiser.com/campaign/help-india-fight-covid-19-donate-for-oxygen
Analysis ID:	418881
Infos:	

Most interesting Screenshot:



Detection

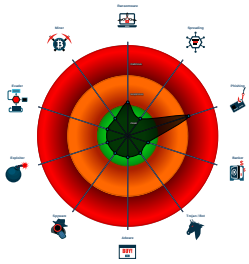


Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Phishing site detected (based on log…
- Invalid T&C link found

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 4852 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5172 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4852 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

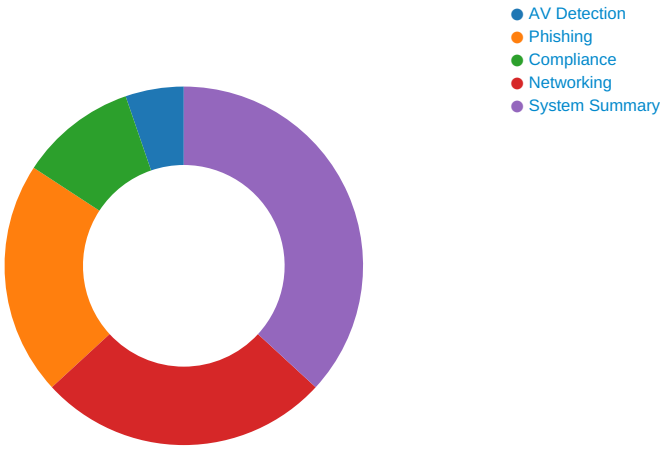
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Copyright Joe Security LLC 2021



Click to jump to signature section

AV Detection:



Antivirus detection for URL or domain

Phishing:

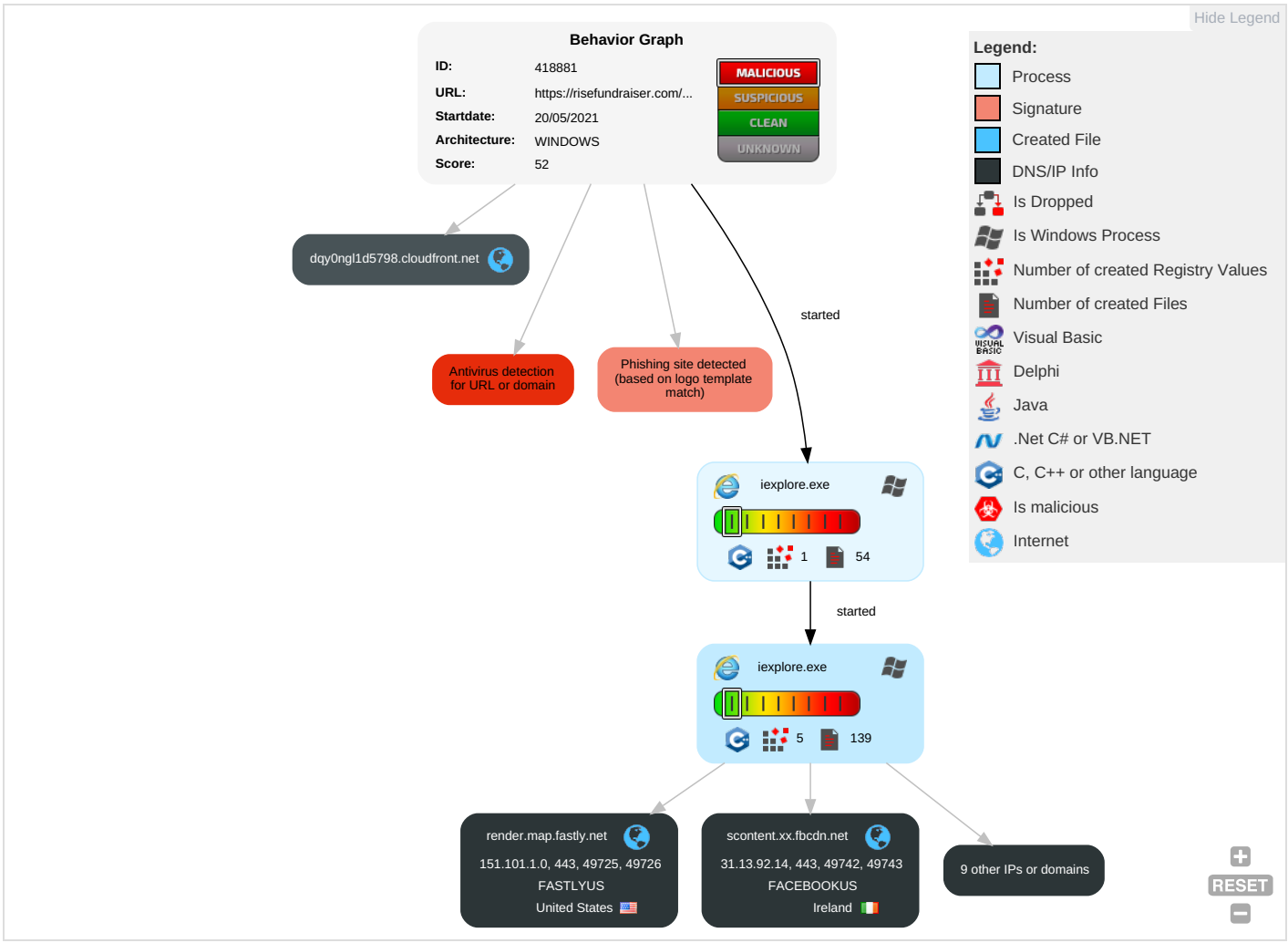


Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

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

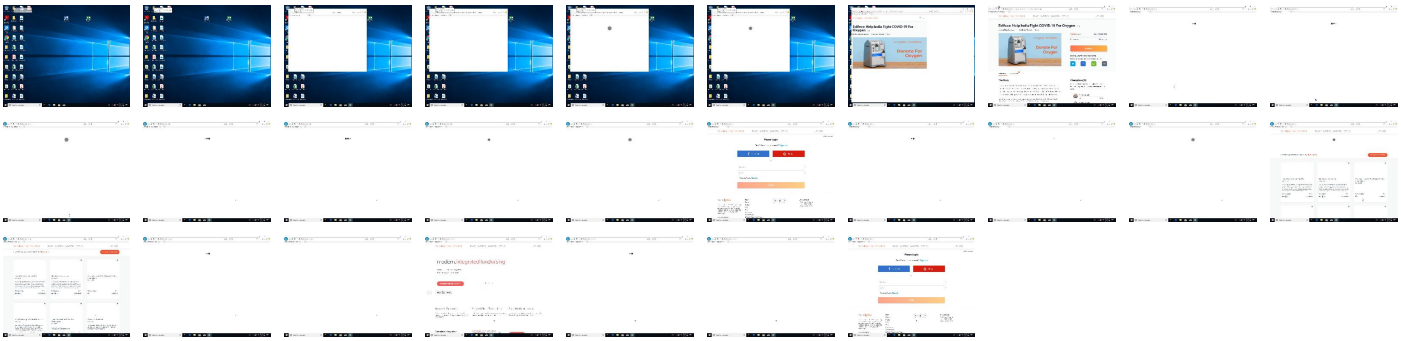
Behavior Graph

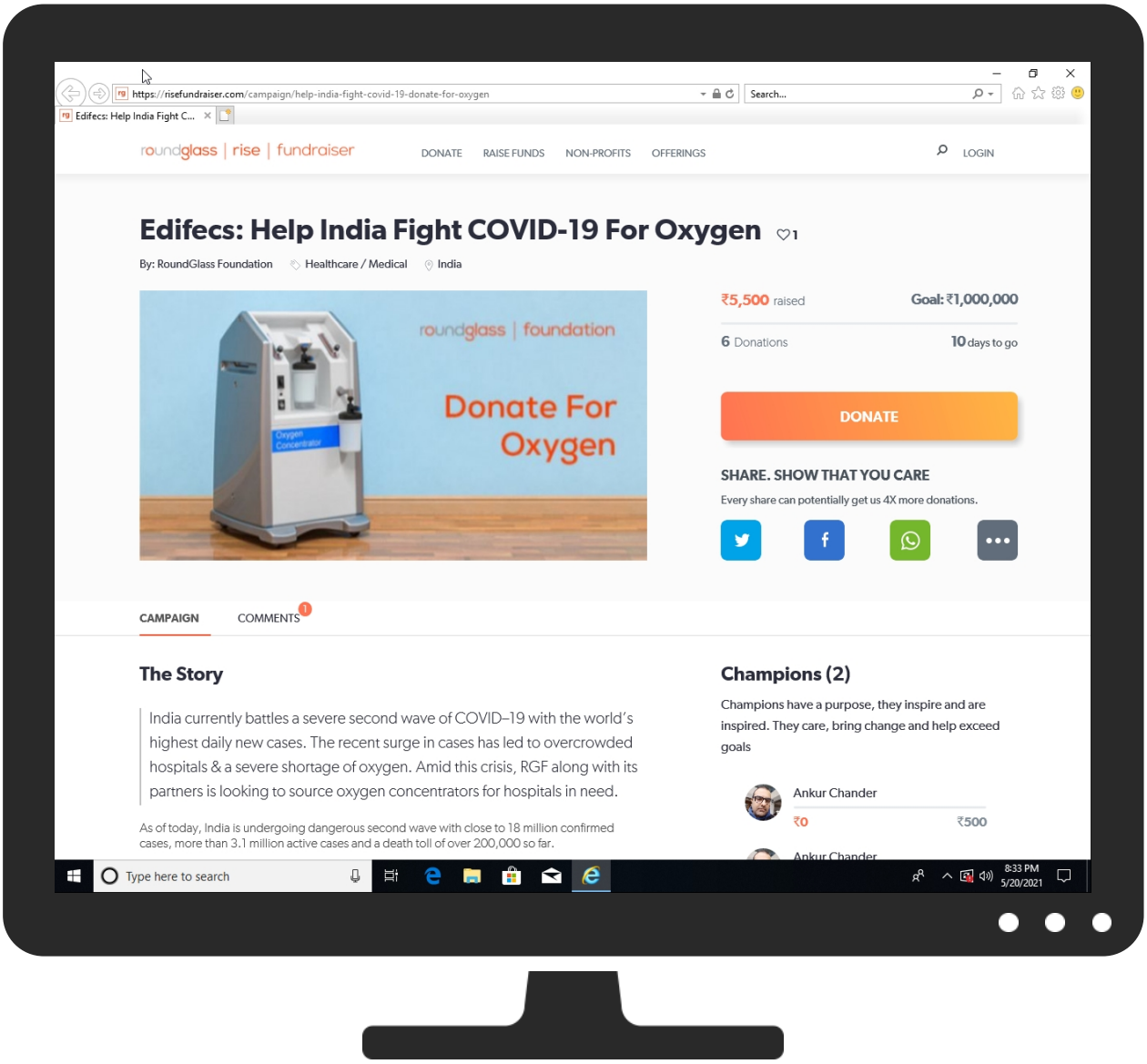


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://risefundraiser.com/campaign/help-india-fight-covid-19-donate-for-oxygen	1%	Virustotal		Browse
http://https://risefundraiser.com/campaign/help-india-fight-covid-19-donate-for-oxygen	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://https://risefundr.com/loginRoot	0%	Avira URL Cloud	safe	
http://https://risefundr.com/reaten/support-a-year-of-tuition-for-a-child-in-indiaRoot	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://https://risefundraiser.com/loginationhttps://dqy0ngl1d5798.cloudfront.net/assets/images/icon/favicon	0%	Avira URL Cloud	safe	
http://https://risefundraiser.com/campaign/help-india-fight-covid-19-donate-for-oxygenZEdifecs:	0%	Avira URL Cloud	safe	
http://https://risefundraiser.com/reaten/support-a-year-of-tuition-for-a-child-in-indiaTL0	0%	Avira URL Cloud	safe	
http://https://risefundraiser.com/"	0%	Avira URL Cloud	safe	
http://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://https://risefundraiser.com/loginon	0%	Avira URL Cloud	safe	
http://https://risefundr.com/createn/support-a-year-of-tuition-for-a-child-in-indiaRoot	0%	Avira URL Cloud	safe	
http://https://risefundr.com/orgsRoot	0%	Avira URL Cloud	safe	
http://https://fengyuanchen.github.io/cropperjs	0%	Avira URL Cloud	safe	
http://https://risefundraiser.com/otificationX	0%	Avira URL Cloud	safe	
http://https://risefundraiser.com/createn/support-a-year-of-tuition-for-a-child-in-india	0%	Avira URL Cloud	safe	
http://https://risefundraiser.com/campaign/help-india-fight-covid-19-donate-for-oxygen.com/campaign/help-in	0%	Avira URL Cloud	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://installw.com/ajax/libs/jquery/3.0.1/jquery.min.js	100%	Avira URL Cloud	malware	
http://https://risefundr.com/offeringsRoot	0%	Avira URL Cloud	safe	
http://https://risefundraiser.com/loginn/support-a-year-of-tuition-for-a-child-in-india.com/	0%	Avira URL Cloud	safe	
http://https://risefundraiser.com/campaign/support-a-year-of-tuition-for-a-child-in-indiaTL0	0%	Avira URL Cloud	safe	
http://https://risefundraiser.com/offeringsV	0%	Avira URL Cloud	safe	
http://daneden.me/animate	0%	URL Reputation	safe	
http://daneden.me/animate	0%	URL Reputation	safe	
http://daneden.me/animate	0%	URL Reputation	safe	
http://https://risttps://risefundraiser.com/offerings	0%	Avira URL Cloud	safe	
http://https://risefundr.com/campaign/support-a-year-of-tuition-for-a-child-in-indiaRoot	0%	Avira URL Cloud	safe	
http://https://risefundr.com/notificationRoot	0%	Avira URL Cloud	safe	
http://fontawesome.iohttp://fontawesome.iohttp://fontawesome.io/license/http://fontawesome.io/licens	0%	Avira URL Cloud	safe	
http://https://risefundraiser.com/campaign/support-a-year-of-tuition-for-a-child-in-india	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
risefundraiser.com	54.201.10.107	true	false	• 0%, Virustotal, Browse	unknown
scontent.xx.fbcdn.net	31.13.92.14	true	false		high
js.hsforms.net	104.17.183.73	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
dqy0ngl1d5798.cloudfront.net	13.224.89.44	true	false		high
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high
render.map.fastly.net	151.101.1.0	true	false		unknown
s3-us-west-2.amazonaws.com	52.218.221.248	true	false		high
cdn.quilljs.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://risefundraiser.com/orgs	true		unknown
http://https://risefundraiser.com/offerings	true		unknown
http://https://risefundraiser.com/campaign/help-india-fight-covid-19-donate-for-oxygen	true		unknown
http://https://risefundraiser.com/login	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontawesome.io	fontawesome-webfont[1].eot.4.dr, font-awesome.min[1].css.4.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/OwlCarousel2/2.1.6/assets/owl.carousel.min.css	help-india-fight-covid-19-donate-for-oxygen[1].htm.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_2_0.ttf	style-layout[1].css.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/images/icon/favicon.ico?v=2-931	~DF693C7156C5077509.TMP.2.dr	false		high
http://https://risefundr.com/loginRoot	{4AAB30E6-B9E5-11EB-90E5-ECF4BB2D2496}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.quilljs.com/1.2.2/quill.snow.css	help-india-fight-covid-19-donate-for-oxygen[1].htm.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_4_0.eot?#iefix	style-layout[1].css.4.dr	false		high
http://chartjs.org/	Chart.bundle.min[1].js.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_0_0.eot?#iefix	style-layout[1].css.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/1.9.7_P9_patch2/main.94919de6defa08284319.js	help-india-fight-covid-19-donate-for-oxygen[1].htm.4.dr	false		high
http://https://risefundr.com/reaten/support-a-year-of-tuition-for-a-child-in-indiaRoot	{4AAB30E6-B9E5-11EB-90E5-ECF4BB2D2496}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://risefundraiser.com/loginationhttps://dqy0ngl1d5798.cloudfront.net/assets/images/icon/favicon	~DF693C7156C5077509.TMP.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css	help-india-fight-covid-19-donate-for-oxygen[1].htm.4.dr	false		high
http://https://risefundraiser.com/campaign/help-india-fight-covid-19-donate-for-oxygenZEdifecs:	{4AAB30E6-B9E5-11EB-90E5-ECF4BB2D2496}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://dqy0ngl1d5798.cloudfront.net/assets/images/icon/favicon.ico?v=2	help-india-fight-covid-19-donate-for-oxygen[1].htm.4.dr, ~DF693C7156C5077509.TMP.2.dr	false		high
http://https://connect.facebook.net/en_US/fbevents.js	help-india-fight-covid-19-donate-for-oxygen[1].htm.4.dr	false		high
http://https://risefundraiser.com/reaten/support-a-year-of-tuition-for-a-child-in-indiaTL0	~DF693C7156C5077509.TMP.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://risefundraiser.com/"	risefundraiser[1].xml.4.dr	false	• Avira URL Cloud: safe	unknown
http://getbootstrap.com)	bootstrap.min[1].css.4.dr	false	• Avira URL Cloud: safe	low
http://https://dqy0ngl1d5798.cloudfront.net/1.9.7_P9_patch2/scripts.d004d92bf73ccd662204.js	help-india-fight-covid-19-donate-for-oxygen[1].htm.4.dr	false		high
http://https://github.com/krux/postscribe/blob/master/LICENSE.	gtm[1].js.4.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/Swiper/4.5.0/css/swiper.min.css	help-india-fight-covid-19-donate-for-oxygen[1].htm.4.dr	false		high
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_2_0.eot	style-layout[1].css.4.dr	false		high
http://https://risefundraiser.com/loginon	~DF693C7156C5077509.TMP.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://risefundr.com/createn/support-a-year-of-tuition-for-a-child-in-indiaRoot	{4AAB30E6-B9E5-11EB-90E5-ECF4BB2D2496}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://risefundr.com/orgsRoot	{4AAB30E6-B9E5-11EB-90E5-ECF4BB2D2496}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://fengyuanchen.github.io/cropperjs	styles.a19aec6bac6aa86c5932[1].css.4.dr	false	• Avira URL Cloud: safe	unknown
http://round.glass/rise/"	risefundraiser[1].xml.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_4_0.ttf	style-layout[1].css.4.dr	false		high
http://https://risefundraiser.com/campaign/help-india-fight-covid-19-donate-for-oxygen	{4AAB30E6-B9E5-11EB-90E5-ECF4BB2D2496}.dat.2.dr	false		unknown
http://https://risefundraiser.com/otificationX	~DF693C7156C5077509.TMP.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://dqy0ngl1d5798.cloudfront.net/1.9.7_P9_patch2/polyfills.661b9383b7c93a39b0f5.js	help-india-fight-covid-19-donate-for-oxygen[1].htm.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_5_0.eot	style-layout[1].css.4.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://risefundraiser.com/createn/support-a-year-of-tuition-for-a-child-in-india	~DF693C7156C5077509.TMP.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_5_0.eot?#iefix	style-layout[1].css.4.dr	false		high
http://www.idangero.us/swiper/	swiper.min[1].js.4.dr	false		high
http://https://risefundraiser.com/campaign/help-india-fight-covid-19-donate-for-oxygen.com/campaign/help-in	{4AAB30E6-B9E5-11EB-90E5-ECF4BB2D2496}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_3_0.eot?#iefix	style-layout[1].css.4.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/systemjs/0.19.39/system.src.js	help-india-fight-covid-19-donate-for-oxygen[1].htm.4.dr	false		high
http://https://cct.google/taggy/agent.js	gtm[1].js.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_1_0.eot?#iefix	style-layout[1].css.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/images/microsite/hero.jpg	style-layout[1].css.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_4_0.eot	style-layout[1].css.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/images/microsite/storybg.png)	style-layout[1].css.4.dr	false		high
http://https://s3-us-west-2.amazonaws.com/rg-fundraiser/assets/images/calculator-v1.js	help-india-fight-covid-19-donate-for-oxygen[1].htm.4.dr	false		high
http://https://www.google.%/ads/ga-audiences	analytics[1].js.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://installw.com/ajax/libs/jquery/3.0.1/jquery.min.js	calculator-v1[1].js.4.dr	true	• Avira URL Cloud: malware	unknown
http://https://quilljs.com/	quill.snow[1].css.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_5_0.ttf	style-layout[1].css.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/images/icon/favicon.ico?v=2~	imagestore.dat.4.dr	false		high
http://https://risefundr.com/offeringsRoot	{4AAB30E6-B9E5-11EB-90E5-ECF4BB2D2496}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap.min[1].css.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/images/icon/favicon.ico?v=2z	~DF693C7156C5077509.TMP.2.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/themes/style-layout.css	help-india-fight-covid-19-donate-for-oxygen[1].htm.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_7_0.eot?#iefix	style-layout[1].css.4.dr	false		high
http://https://risefundraiser.com/loginn/support-a-year-of-tuition-for-a-child-in-india.com/	~DF693C7156C5077509.TMP.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://dqy0ngl1d5798.cloudfront.net/assets/images/icon/favicon.ico?v=2n	~DF693C7156C5077509.TMP.2.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_5_0.woff	style-layout[1].css.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_6_0.woff	style-layout[1].css.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/images/icon/favicon.ico?v=2j	~DF693C7156C5077509.TMP.2.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_7_0.woff	style-layout[1].css.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_3_0.woff	style-layout[1].css.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_4_0.woff	style-layout[1].css.4.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_0_0.eot	style-layout[1].css.4.dr	false		high
http://https://github.com/chartjs/Chart.js/blob/master/LICENSE.md	Chart.bundle.min[1].js.4.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/Swiper/4.5.0/js/swiper.min.js	help-india-fight-covid-19-donate-for-oxygen[1].htm.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/1.9.7_P9_patch2/vendor.7b1b41a937a083fd16b0.js	help-india-fight-covid-19-donate-for-oxygen[1].htm.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_0_0.woff	style-layout[1].css.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_6_0.eot	style-layout[1].css.4.dr	false		high
http://https://risefundraiser.com/campaign/support-a-year-of-tuition-for-a-child-in-indiaTL0	~DF693C7156C5077509.TMP.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://risefundraiser.com/offeringsV	~DF693C7156C5077509.TMP.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_1_0.woff	style-layout[1].css.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_2_0.woff	style-layout[1].css.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_2_0.eot?#iefix	style-layout[1].css.4.dr	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js	help-india-fight-covid-19-donate-for-oxygen[1].htm.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_3_0.eot	style-layout[1].css.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_3_0.ttf	style-layout[1].css.4.dr	false		high
http://daneden.me/animate	animate.min[1].css.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://risttps://risefundraiser.com/offerings	{4AAB30E6-B9E5-11EB-90E5-ECF4BB2D2496}.dat.2.dr	false	• Avira URL Cloud: safe	low
http://https://github.com/OwlCarousel2/OwlCarousel2/blob/master/LICENSE)	owl.carousel.min[1].css.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/images/microsite/icon/fundraiser-Ico.png	style-layout[1].css.4.dr	false		high
http://https://risefundr.com/campaign/support-a-year-of-tuition-for-a-child-in-indiaRoot	{4AAB30E6-B9E5-11EB-90E5-ECF4BB2D2496}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_6_0.ttf	style-layout[1].css.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_0_0.ttf	style-layout[1].css.4.dr	false		high
http://https://risefundr.com/notificationRoot	{4AAB30E6-B9E5-11EB-90E5-ECF4BB2D2496}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://dqy0ngl1d5798.cloudfront.net/assets/images/microsite/icon/promote-Ico.png	style-layout[1].css.4.dr	false		high
http://fontawesome.iohttp://fontawesome.iohttp://fontawesome.io/license/http://fontawesome.io/licens	fontawesome-webfont[1].eot.4.dr	false	• Avira URL Cloud: safe	unknown
http://https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css	help-india-fight-covid-19-donate-for-oxygen[1].htm.4.dr	false		high
http://https://risefundraiser.com/orgs	{4AAB30E6-B9E5-11EB-90E5-ECF4BB2D2496}.dat.2.dr, ~DF693C7156C5077509.TMP.2.dr	false		unknown
http://https://risefundraiser.com/offerings	{4AAB30E6-B9E5-11EB-90E5-ECF4BB2D2496}.dat.2.dr, ~DF693C7156C5077509.TMP.2.dr	false		unknown
http://https://risefundraiser.com/campaign/support-a-year-of-tuition-for-a-child-in-india	~DF693C7156C5077509.TMP.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.quilljs.com/1.2.2/quill.bubble.css	help-india-fight-covid-19-donate-for-oxygen[1].htm.4.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_1_0.eot	style-layout[1].css.4.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/Chart.js/2.6.0/Chart.bundle.min.js	help-india-fight-covid-19-donate-for-oxygen[1].htm.4.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/images/logo.png"	risefundraiser[1].xml.4.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.17.183.73	js.hsforms.net	United States		13335	CLOUDFLARENETUS	false
104.18.10.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
52.218.221.248	s3-us-west-2.amazonaws.com	United States		16509	AMAZON-02US	false
31.13.92.14	scontent.xx.fbcdn.net	Ireland		32934	FACEBOOKUS	false
54.201.10.107	risefundraiser.com	United States		16509	AMAZON-02US	false
151.101.1.0	render.map.fastly.net	United States		54113	FASTLYUS	false
13.224.89.44	dqy0ngl1d5798.cloudfront.net	United States		16509	AMAZON-02US	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	418881
Start date:	20.05.2021
Start time:	20:32:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 38s
Hypervisor based Inspection enabled:	false

Copyright Joe Security LLC 2021

Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://risefundraiser.com/campaign/help-india-fight-covid-19-donate-for-oxygen
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal52.phis.win@3/98@9/8
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://risefundraiser.com/explore • Browsing link: https://risefundraiser.com/create • Browsing link: https://risefundraiser.com/orgs • Browsing link: https://risefundraiser.com/offerings • Browsing link: https://risefundraiser.com/notification
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 92.122.145.220, 13.88.21.125, 168.61.161.212, 88.221.62.148, 13.64.90.137, 172.217.16.106, 172.217.16.104, 142.250.184.206, 52.147.198.201, 104.43.139.144, 40.88.32.150, 20.82.210.154, 152.199.19.161, 205.185.216.10, 205.185.216.42, 92.122.213.194, 92.122.213.247, 52.155.217.156 • Excluded domains from analysis (whitelisted): store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, www.googletagmanager.com, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, www.google-analytics.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, www-google-analytics.l.google.com, ajax.googleapis.com, ie9comview.vo.msecnd.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, www-googletagmanager.l.google.com, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, cds.d2s7q6s2.hwcdn.net, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.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\DOMStore\EQAWN5DV\risefundraiser[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	766297
Entropy (8bit):	5.70853418194783
Encrypted:	false
SSDEEP:	12288:GU5iIDQSzB0xE9zd0U5iIDQSzB0xE9zdTU5iIDQSzB0xE9zdfU5iIDQSzB0xE9zD:GU5iIDQSzB0xE9zd0U5iIDQSzB0xE9z5
MD5:	BE6A33D12003F20D00769863D2E34F74
SHA1:	A2E17C7E2C9DEB4B06C8AC556B01F652C4CEBFA4
SHA-256:	7C5D4A3403F405633C257C3E99EEA5F2F4CF782664FF4E5D8F1B2A841AEFA3F4
SHA-512:	4B2F5A32C912FD5B93C196466D4C7B45441B23E8B3AD10C30B206DCCE27E039C67B0D65C2035C138F5508AF64233E8A5133BB20CBB957CE094818DEA706BD5
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="window.location.pathname" value="/campaign/help-india-fight-covid-19-donate-for-oxygen" ltime="279726640" htime="30887410" /></root><root><item name="window.location.pathname" value="/campaign/help-india-fight-covid-19-donate-for-oxygen" ltime="279726640" htime="30887410" /><item name="localStorage" value="1" ltime="280666640" htime="30887410" /></root><root><item name="window.location.pathname" value="/campaign/help-india-fight-covid-19-donate-for-oxygen" ltime="279726640" htime="30887410" /></root><root><item name="window.location.pathname" value="/campaign/help-india-fight-covid-19-donate-for-oxygen" ltime="279726640" htime="30887410" /><item name="taxonomyMeta" value="{"chapter":{"singular":"team","plural":"teams"},"champion":{"singular":"champion","plural":"champions"},"leadChampion":{"singular":"team leader","plural&

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{4AAB30E4-B9E5-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.851451777237491

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{4AAB30E4-B9E5-11EB-90E5-ECF4BB2D2496}.dat	
Encrypted:	false
SSDEEP:	96:rBZVZK2SWlltlUAflPKW1MeuTZoRU+fXKLlX:rBZVZK2SWlltlXflPxMz+1fXMX
MD5:	E0B5BCF94882ED510BA0D464F797661A
SHA1:	C5C5BA93BB978FC8D21C57BD1FDD302D31A973EB
SHA-256:	D8E5067449B06806DB30F7D8863F3B09F7B4AB844CA1F208FA584E2637418C6A
SHA-512:	96325DDAE1E5BC1F658E581B4F97425E872394FA0C14F1D7E0D7AFB592CF79A11A33B37DFFAE130BC11A082511161D92ABDD8BA9E7282DD7B82D4EA18EFE7F36
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\{4AAB30E6-B9E5-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	162814
Entropy (8bit):	2.458334968497267
Encrypted:	false
SSDEEP:	384:rBlX3iAla2/A1JfryJf7WoFHMuWxYFuFH16I+XF3TiLIHR5hTbK9Tr+zQ/KiF61/:YJ+JcXCXdTHFT8TmQiTrt1/
MD5:	80EC5B62CCF50E71D692F2121C6DFFBD
SHA1:	109AC0A12DFBEC50EC53AB306B5056FE33C4CC51
SHA-256:	4FD9B4AE0F0867E6AFDC3E59355DCB885F4ADB68A4F0C6627C1B42C093D7F3B0
SHA-512:	80CDE571DF515AEE332B6F12D698C939824D30FAA753EC29E8A11C9D25DD226BF4D59CFE05A2843F56925856FC67EADADBFD97EB9F65FCDF6BAB33383546195
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\{54D6F9D2-B9E5-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5664259580629745
Encrypted:	false
SSDEEP:	48:IwtGcprEGwpaKG4pQ/GrapbSf7GQpKxG7HpRmTGIpG:rzZ8Qq6DBSf1AgTSA
MD5:	9EB9322B48144D0E6DF2A2DE646682F7
SHA1:	127E7FB0F2E40AFF1E524F20FF5D62DFAF90D02C
SHA-256:	5650B1D290F2662C92F07A8FC1B2FE96B2C5EDE6F5C017329CF4845267A7B6F2
SHA-512:	609933FF70088304269AE8629C45C89A1A0D6376CD026A14E86D1BCC89EF1E08CB21A88E1902A259F3804963938AE317482A8748C1EF0F2268407C2A1546F042
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\wlm7n14\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1330
Entropy (8bit):	3.786144307937114
Encrypted:	false
SSDEEP:	12:u7HOU3zaX6plkdAoLREno28noBbCMwo0+HnoNVnoBMoLFinokoqboVt5cgoAoA1W:8HjzaXcklyCD+4V1GvZW
MD5:	29CAD5B3B0339933E3C96F14018FB752
SHA1:	947842CC1DB72244FB0AB6C82CC94C9A18B1CD20
SHA-256:	BD11AEFAB4A5B6269093545C71B4B9803293D4ADB37F9BAF79A9D0A6F2E28A1F
SHA-512:	132AB5BA35FC1E7E285541AEDCCF37789A92496C67B0C0C4A847290C981D5443C5AB6F8110C777AA0EC221F9EA016F2C5B5D1160CBCCB6D3D512A2DE2DC0FA5

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\wlm7n14\imagestore.dat	
Malicious:	false
Reputation:	low
Preview:	G.h.t.t.p.s.:./.d.q.y.0.n.g.l.1.d.5.7.9.8...c.l.o.u.d.f.r.o.n.t...n.e.t./.a.s.s.e.t.s./.i.m.a.g.e.s./.i.c.o.n./.f.a.v.i.c.o.n...i.c.o.?.v.=.2.~..... .h.....(..... ....#...#..... 'N..'N..'N..'N..'N..'N..'N..'N..'N..'N..'N..'N..'N..)K..(M..(M..(M..(M..(M..(M..(M..(M..(M..)K..'N..'N..'N.&N..'N.....'N..(M..'N..'N.&N..'N.....'N..' N..'N..'N..'N..'N..'N..(M..'N..'N.&N..'N.....&N..'N..'N.3'N..'N..'N.'N.Q'N..'N..(M..'N..'N.&N..'N..'N..'N.$'N..'N..'N.0'N.{'N.Y'N..'N..'N.('N..(M..'N..'N.&N..'N..'N.%'N..'N.U'N..'N..'N.' N..'N..'N..'N.H'N..(M..'N..'N.&N..'N..'N.)'N..'N.]'N..'N..'N..'N.b'N..'N..'N.I'N..(M..'N..'N.&N..'N..'N.)'N..'N.k'N..'N..'N..'N..'N.A'N..'N.J'N..(M..'N..'N.&N..'N..'N.)'N..'N..'N.k'N..'N..'N.R'N..'N..' N..I'N..(M..'N..'N.&N..'N..'N. 'N..'N..'N..'N..='N..'N..'N..'N..:'N..(M..'N..'N..'N.&N..'N..'N..'N..'N..'N..'N..'N..'N..'N..'N..'N..'N..(M..'N..'N..'N.&N..'N..'N.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\0.5dfdaa7dfd5376b677fc[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):	17679
Entropy (8bit):	5.14165843260012
Encrypted:	false
SSDEEP:	192:lZ1jIo6WZSd6KF4Ie3LtdtAG062BPmjb95t5hfICPvAI5oh/a:lMo6OFE4/l062BPMRN45o9a
MD5:	70263DB7C4A020915B912D676257F4C7
SHA1:	7960A1890B37481524188FE0BC5EC5BEE88D867A
SHA-256:	3337B28ED58DCF883AE4F25887DE585B3E4070A143F0451DC34D1A03A3611A95
SHA-512:	F6F2F29A502F1893AFC60EB176CD56A9D1CE5084FBE14A02BC6689FB26FE395E97538CC66D4FF50745B001ADC03A51F3EE569ACF982D0E647C1BF1551A9A6E6E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://risefundraiser.com/0.5dfdaa7dfd5376b677fc.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[0],{"8e6m":function(t,n,e){"use strict";e.r(n),e.d(n,"CarouselComponent",function(){return c}),e.d(n,"CarouselModule",function(){return a}),e.d(n,"SlideComponent",function(){return u}),e.d(n,"CarouselConfig",function(){return r});var i=e("CcnG"),o=e("rpEJ"),r=function(){this.interval=5e3,this.noPause=!1,this.noWrap=!1,this.showIndicators=!0},s=function(){var t={UNKNOWN:0,NEXT:1,PREV:2};return t[t.UNKNOWN]="UNKNOWN",t[t.NEXT]="NEXT",t[t.PREV]="PREV",t}(),c=function(){function t(t,n){this.ngZone=n,this.activeSlideChange=new i.EventEmitter(!1),this._slides=new o[!1],this.destroyed=!1,Object.assign(this,t)}return Object.defineProperty(t.prototype,"activeSlide",{get:function(){return this._currentActiveSlide},set:function(t){this._slides.length&&t!==this._currentActiveSlide&&this._select(t)},enumerable:!0,configurable:!0}),Object.defineProperty(t.prototype,"interval",{get:function(){return this._interval},set:function(t){this._interval=t,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\1.5cf16574643d5c9fb418[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):	70769
Entropy (8bit):	5.184361894353211
Encrypted:	false
SSDEEP:	768:BtDXMsEdIB0DG5RLP2w/MY/P+wYqpodNXqH86xyVcp8C+s3M3Jpu3yfCJ+lQ8nk9:BVI7GhJ8OLYyL/5tm9VsShHJOR/jZS3q
MD5:	DC1AB1848707F8E095AEFB39A8E4750C
SHA1:	9AFCFB18F7B0698D8695CAB0BF6427A8C0B7C484
SHA-256:	DC9449A8A415DD94F061F9022A021503672ADE942640407E22F2510F162DDC57
SHA-512:	231C4848C63AF94D4F74DF9F00A5A8BD993FBCB2A9725AD0B56666EA5359F98104154CC8E158A6FF147E1BBB6D6AFCB8A1F503F746732B561813D6E03AB0C7E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://risefundraiser.com/1.5cf16574643d5c9fb418.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[1],{F6Qp:function(l,n,e){"use strict";e.d(n,"a",function(){return i});var t=e("IoZi"),u=e("4ALx"),i=function(){return function(l){this.sponsors=[],this.page=0,this.status="loading",this.isRequesting=!0,l==t.d.createSponsor?(this.createSponsor=!0,this.title=t.f.Tags.HEADER_TAG("Sponsors")+t.f.Tags.PARAGRAPH_TAG("Use this section to recognize organizations or individuals who have made significant contribution of support to your cause. Upload their logos and they will appear on the campaign pages as sponsors.")):(this.createSponsor=!1,this.title=t.f.Tags.HEADER_TAG("Sponsors")),this.sponsors.splice(0,0,new u.a)}}()},"L+Rj":function(l,n,e){"use strict";e.d(n,"a",function(){return a});var t=e("CcnG"),u=e("gIcY"),i=(e("vEwd"),e("rac4")),o=e("zGuP"),e("IoZi")),s=e("hApR"),r=(e("sDE+"),e("Jq6N")),a=function(){function l(l,n){var e=this;this.fb=l,this.missionService=n,this.onEventUpdate=new t.EventEmitter,this.startSettings=new i.a(o.d.EVENT

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\19.7daa68dd33aae7e5e751[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):	16512
Entropy (8bit):	5.49158064857455
Encrypted:	false
SSDEEP:	384:A7XzU+7sUru4fHEcp7P+LFIX+LAgZCi3CprWJmR5/cxXYUJhz9lA0ql:AHU+7sEZfHN7P+LFa+LjCQCprWJmT/cS
MD5:	966FA0601455C35A11EFDB4C146FD68C
SHA1:	F4A65D518ED65537EF7CCA6F576B54980B8F617C
SHA-256:	E8016EC2AF237FE1192265447E4965B234CC42C7B1BCD92E8342732095C5AF23
SHA-512:	88DD38F1D776CF2AA6E7A31D6910BDA9825D63436916281A2C6CAFE72839FB3432BE389A9B04876C25E28124DFE6574276A596A63151ABC6FD5EADE2A6B1859

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\19.7daa68dd33aae7e5e751[1].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://risefundraiser.com/19.7daa68dd33aae7e5e751.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[19],{"O+Es":function(e,n,t){"use strict";t.r(n);var l=t("CcnG"),o=function(){},i=t("pMnS"),a=t("3jF4"),r=t("1kLp"),s=t("ZYCi"),u=t("Ip0R"),d=t("bWc+"),c=t("HPAU"),p=t("sDE+"),g=t("/NYq"),m=t("m+5+"),f=t("dU8u"),h=t("EC1T"),y=t("IoZi"),v=t("eSc6"),O=t("ngAm"),C=t("yGML"),S=function(){function e(e,n,t,l,o,i){var a=this;this.router=e,this.route=n,this.missionService=t,this.userService=l,this.campaignService=o,this.seoService=i,this.enableAddOrganization=!0,this.orderByFilter="asc",this.sortByFilter="relevance",this.currentIndex=0,this.page=1,this.loadedFrom=-1,this.popupBySorting=new h.a(y.d.NPO_LIST_SORTING),this.popupByOrder=new h.a(y.d.NPO_LIST_ORDER),this.size=9,this.currentSortTypeIndex=y.d.SORT_BY_NPO_NAME,this.offset=0,this.isRelevance=!0,this.disableBtn=!1,this.missionService.announceMissionToShowHideLoader({requestType:y.d.showLoader}),this.route.queryParams.subscribe(function(e){a.page=parseInt(e.page||"1",0),a.page>1&&-1===a.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\2020-01-23_22-57-36[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, 200x200, frames 3
Category:	downloaded
Size (bytes):	8992
Entropy (8bit):	7.952617077694567
Encrypted:	false
SSDEEP:	192:4VuGf0aP5Fs0wLN6f1cFb0I8YXnA7tmW40ntaUE0:4MG0o5FFwLNW8G7wWNnD
MD5:	508492BEA54F640A5730FB7668E39005
SHA1:	568614B96B6D1A1A0A0F6DA49EF2A3838B137C30
SHA-256:	1BE88288625A7D7E4D97DA195A123F7407A70251F5CD9BAF1A8E38DE60C6EE6A
SHA-512:	CFA49C34DDA8ABB65EDE83A14420813FF678CC1503A71E7FE417E675F1D4B6868D19E46813CE0C0FE51A97F6CC45E9D6D3E8113B0DB795F561EA4053628BB9 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/media/17142/2020-01-23_22-57-36.jpg
Preview:	......JFIF.....C.....%...#... , #&')*)..-0-(0%()(...C.....(...((((((

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\2126210880948599[1].js	
SHA-256:	CD23C1588831E8E86CC4565585F2CCD769F38184C2A9DCEF5C6D8537F314021A
SHA-512:	661F13C40BC1BA634B16061E4F9EC0BA3D5D907F725F369B8510AA5FE0AB4F28DD173036100E081D3962BA7EAF16E040E588F3F8803B51359C7511E29FA362C2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://connect.facebook.net/signals/config/2126210880948599?v=2.9.39&r=stable
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\2126210880948599[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	260087
Entropy (8bit):	5.469219756242312
Encrypted:	false
SSDEEP:	6144:Rk1HgCSntDV/HaK3V/Ha8NEPjQHguH3HpQrwzzmy:dNESh
MD5:	AE4DA01D599640A4F84724E8CB5C890E
SHA1:	12FD721F9A99A063BFE2419CDFFBF48A95DED5B1
SHA-256:	8D4A8EF94E0F6FED90678AC8974450340DDAAE87E74003A774EF518C1A109C4D
SHA-512:	8AE3F7781E73A40D7F96743FBBD546EA952A1096E576F8BB26F1E11CF0C00ED3555639AD5FA3F41A7F07E200BCA6B1D0B5C0493B134131FCF677237F85400115
Malicious:	false
Reputation:	low
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\22.ffb009f27d517354a7bf[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):	5921
Entropy (8bit):	5.553976080662558
Encrypted:	false
SSDEEP:	48:lD58eBgVbIaCamVpU8hu4F01E2Av9AXxatwyw1vWjFYrpM1qDIw/1c/cLkjJ2HOQ:1awu8rv9egRw1vWjFYrO8OL/9q9og
MD5:	A9963E007E9D8BDA1DED3FD7B87A8C9C
SHA1:	2E08A3B913F2FAFBCE4A69AFBC833B81B85155F7
SHA-256:	F262C7DEEF76FDE080C7350AABEDA4FBB6E3AF3D34ED01189863DD5B42CAAE63
SHA-512:	56871B498EA5374EDEB8E4AAA52E237D9BFEF1E60D303BACF1964571BA9F89520394106E7939937EE5183E701BF8786D0D212D7AC0FC34F2E2353F894ADB24C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://risefundraiser.com/22.ffb009f27d517354a7bf.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[22],{"2pkJ":function(a,t,p){"use strict";p.r(t),p.d(t,"CampaignAdminModuleNgFactory",function(){return Ma});var e=p("CcnG"),o=p("mMh9"),d=p("pMnS"),m=p("hzjW"),n=p("wueL"),i=p("Xg1U"),c=p("atuK"),r=p("iutN"),s=p("ES0t"),h=p("z5nN"),l=p("SfUx"),u=p("54hb"),A=p("rEId") ,R=p("brvc"),g=p("yOyS"),f=p("EgHg"),b=p("IzQX"),C=p("47zY"),T=p("whYo"),y=p("rz5k"),E=p("HzBr"),w=p("2zfs"),L=p("B5F5"),N=p("/7p0"),_=p("dpgl"),G=p("OwLd"),M=p ("WdOE"),P=p("pk3G"),H=p("SxC3"),I=p("Ip0R"),D=p("gIcY"),x=p("p4DR"),z=p("9bPP"),k=p("dXze"),v=p("eajB"),O=p("NJnL"),S=p("lqqz"),F=p("ARl4"),j=p("xtZt"),U=p("fH IT"),W=p("OZfm"),X=p("DQlY"),Y=p("YAQW"),Z=p("rhjU"),Q=p("ETNk"),q=p("yEXN"),B=p("KKpL"),J=p("t/Na"),K=p("m+5+"),V=p("ZYCi"),$=p("sDE+"),aa=p("IyfZ"), ta=p("sWsQ"),pa=p("AiR7"),ea=p("+xv6"),oa=p("ctsa"),da=p("A+LG"),ma=p("kO4o"),na=p("Xpkg"),ia=p("mHTr"),ca=p("Wual"),ra=p("wT8T"),sa=p("yD1i"),ha=p("9 EwZ"),la=p("AS82"),ua=p("t1w2"),Aa=p("LeXK"),Ra=p("6Q8y"),ga

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\5.4b476a3f79802388bd4a[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):	298460
Entropy (8bit):	5.275642956187841
Encrypted:	false
SSDEEP:	6144:jMjqOBp75vfx6W7/TdsI90F2zcxRM+n88iLKaW6ddel7IssRy+:jM3p/TsF2zc7M+ncKaW6d/
MD5:	8A4123418A60168AE555AD20DD879091

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\5.4b476a3f79802388bd4a[1].js	
SHA1:	08D039A314232F8328407EC25C6529D1B6515D6E
SHA-256:	B12190456495212ACD9DC0032705EA04DD853AAF00FF7CBDD343BFCBAB924359
SHA-512:	D526D8DEDA0699817374485D53F8AF33463CD6121F2251615BD08F22FA70CD4AB371F0889B584EACF69F10AD834ABBF8DE3BC707AEA6073018E2D188B7738F4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://risefundraiser.com/5.4b476a3f79802388bd4a.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[5],{"/Jor":function(n,l,e){"use strict";e.d(l,"a",function(){return y});var t=e("hApR"),u=e("9dFV"),i=e("U7CQ"),a=e("gpD0"),o=e("cabi"),r=e("zGuP"),s=e("F6Qp"),d=e("E7mM"),c=e("sdBo"),p=e("q5CE"),g=(e("eSc6"),e("m+5+")),m=(e("/NYq"),e("sDE+"),e("Q2Sq"),e("0CYw"),e("yGML")),f=(e("EO9k"),e("IoZi")),v=e("4ALx"),h=e("QtBy"),C=e("PSfJ"),y=(e("GwH4"),function(){function n(n,l,e,t,u,i,a,o,r,s){var d=this;this.route=n,this.router=l,this._userService=e,this.uxService=t,this._restApiService=u,this.missionService=i,this._mediaServer=a,this._formDataServer=o,this._location=r,this.dialogService=s,this.loading=!1,this.params={},this.taxonomy=m.b.getInstance().getTaxonomy()||!1,this.missionService.announceMissionToShowHideLoader({requestType:f.d.showLoader}),n.params.subscribe(function(n){d.params.id=n.id}),n.data.subscribe(function(n){d.params.type=n.type})}return n.prototype.canDeactivate=function(){return!0},n.prototype.ngOnInit=function(){this.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\Concentrator[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 320 x 450, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	181357
Entropy (8bit):	7.96801869311152
Encrypted:	false
SSDEEP:	3072:cGE2Jgn2ZDn9bGTeG+sJNRuwmIWiYMvDa0WViIAApcV1d1ydYCTeJnT/GVeqPjaU:i2S2ZT9bGTeGrNRuhMvDajVkdV9yuCTZ
MD5:	1B3DB60867FD9FE7A2A62D73EDFAEF18
SHA1:	AB1A73C090CF01D2A377DF4E190901EC83C0445B
SHA-256:	FE7426B19D6CB6DA9B052F9C2B7BEF43CD045566ADC1D9867200325A48BB818A
SHA-512:	EA42F1883D30CD5D37AA269B2830BF3ADCC89BFD48D9DE6CF54A9B2F526F338A0F574C1FE9CAE0876BC2CF423EEE7F50C5F4867C4F34A4EF77F02AEB7D83ECA8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/media/17536/Concentrator.png
Preview:	.PNG.....IHDR...@.....y.. .IDATx...s.iv...l.....ekk.n.^.k_..z.c_...{..ZT E.A.%u.rd.9.... ....s..T.L.n}.....+.T....[.:<o.....<'=.....+.....%..Q..{.;.[h..+...}..Y.....u.....}.....u.....o..=.}...?.....>...../D.g.{...v..S....^/.~...t]....}.Lz.....|R.....>.{..s..aL.}..}.c...k.....}]...>..z.....>./..3../.9?.....c},.....>.....kf.o.X.....$...R.....^.[.....G.kf.o.X.....\|. ...O_.{.{=..c..>/.{]..~~{=._.~}.2._...._o.....u~.~.....}"oz....u....q.....t..~)....l..v...}.}....C_g..n.....:.....w.@.....&....9{..n.}~..t.....}....&...^.{O.mo{..}..Z..-...KwM{..^.}..^.....}.....bo..D..q.....f.....O...wq.O....O.....?..._..C.lmm..e.mml....%.jk..d..... ...Cu].n..6>?....Z.....u].n....w...?..._....On.....$.x.7..ym..\}.....|...^.....{..4.s.(.....%.....m.:&U6.....}.}.t...Z.....3N.....,)....[....F\.....X...rk..^..<..^.....l...7.}].

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\calculator-v1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	11439
Entropy (8bit):	5.472845089548253
Encrypted:	false
SSDEEP:	192:Av7QiXi3ixF3lVzZiRiliGTbhAoovljYKA0ZzjUXQVoe39ZrWn6WjAxG+Dz1Gi6p:ziXi3ix1iZiRiliGhAr2K9Z3BVnKjAxS
MD5:	DD572A0354C02D76DA5DAEC1888CCFB8
SHA1:	5D380341EF58A8FFCE2599A472C864EB329C86F6
SHA-256:	D8106146E4CE35A796DA1B004F66E9DBA13D8B28E0608CB2C93D1AF3AFB4F4BA
SHA-512:	72C3449B6C8D763C5A971487D6F09D765FA1952351990ECFB2C8EF5A7CADA9C069B34612156E55AC0B3BEFC46F650F5C6EA15B0F3C70D77625D1D808DA62A25C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s3-us-west-2.amazonaws.com/rg-fundraiser/assets/images/calculator-v1.js
Preview:	function roundNumber(num, dec) {.. var result = String(Math.round(num * Math.pow(10, dec)) / Math.pow(10, dec));.. if (result.indexOf('.') < 0) { result += '.'; }.. while (result.length - result.indexOf('.') <= dec) { result += '0'; }.. return result;.. }.. .. function showBackForm() {.. document.getElementById("co2form").style.display = "";.. document.getElementById("divChart").style.display = "none";.. document.getElementById("restartButton").style.display = "none";.. }.. .. function resetForm() {.. document.forms[0].reset();.. }.. .. function calculateCarbonFootPrint() {.. var fam = document.getElementById('fam').value;.. fam = isNaN(fam) ? 0 : fam;.. .. var elec_cons = document.getElementById('elec_cons').value;.. elec_cons = isNaN(elec_cons) ? 0 : elec_cons;.. .. var lpg = document.getElementById('lpg').value;.. lpg = isNaN(lpg) ? 0 : lpg;.. .. var dist_taxi = document.getElementById('dist_taxi').value;.. dist_taxi = isNaN(dist_taxi)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\champions[1].htm	
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):	906
Entropy (8bit):	4.994297952788001
Encrypted:	false
SSDEEP:	24:Yt5E4YTyukluYANN7kTxX/RwQxKpukluYANN7kTxX/RwqZ:YtKTyuYEN7OX/PKpuYEN7OX/LZ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\champions[1].htm	
MD5:	5681981C98EC2F7DEB713C75594537F7
SHA1:	73E7CC7A7A44E760FB28C08DC33C3C607F5E2808
SHA-256:	9CD99917C79945C0C29EBA7E12AA9DFCB984BA1D4821CBABD93F38353CAB5073
SHA-512:	486C3FAC3235E9D343DE2D739737F2F1F2D4100FA521CEF1C5836F2A8CD3FE2206F97D98520C06485B5936AC7E2ACC84065156AA069DB2C18BA00A82C93485F
Malicious:	false
Reputation:	low
Preview:	{"status":true,"data":{"count":2,"donations":0,"entities":[{"id":"ankur-chander-1","champId":39589,"namespaceId":"2626","donors":0,"donations":null,"goalAmount":500,"status":"Accepted","user":{"id":37624,"email":"ankur.chander@edifecs.com","name":"Ankur Chander","avatar":"https:\/\/dqy0ngl1d5798.cloudfront.net\/media\/17142\/2020-01-23_22-57-36.jpg"},"isDefaultChapter":true,"unitInfo":{"unitName":null,"totalUnit":null,"pricePerUnit":null,"unitCount":0}},{"id":"ankur-chander-1","champId":39590,"namespaceId":"2626","donors":0,"donations":null,"goalAmount":500,"status":"Accepted","user":{"id":37624,"email":"ankur.chander@edifecs.com","name":"Ankur Chander","avatar":"https:\/\/dqy0ngl1d5798.cloudfront.net\/media\/17142\/2020-01-23_22-57-36.jpg"},"isDefaultChapter":true,"unitInfo":{"unitName":null,"totalUnit":null,"pricePerUnit":null,"unitCount":0}}],"pageSize":20,"pageNumber":1},"errorCode":10000}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\explore[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	9071
Entropy (8bit):	4.94862352509096
Encrypted:	false
SSDEEP:	192:LyAEQmFHFlHWjmRjLd0gpKQKdFr0y0Fo0l2P3OOv84aTmdZAckyFrJqyJhSgOIte:LxEQallHrBjSSFHJT4ZjGrxN8bfM
MD5:	2A5CEF0817081FC6AD1909B62ACD9919
SHA1:	B005FD522AD71CCADCBFE240599389ACA8BECDCA
SHA-256:	B6F1F3701DC121B979E593EBD27D71CDDD16BDECFB3FEDD70C7ADB5F2D0BA3F3
SHA-512:	B26C4C7F146FC8CC2BDD1BFBB1FA5085BE540A9299B592375BE1D5E60D75807E0768FD76BA41FEF1B1A0B74EE88582833C63EF6852C4A48C952504C453EB9EF3
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html lang="en">..<head>. <meta http-equiv="Content-type" content="text/html; charset=utf-8" />. <meta http-equiv="X-UA-Compatible" content="ie=edge">. <meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate">. <meta http-equiv="Pragma" content="no-cache">. <meta http-equiv="Expires" content="0">. <meta name="fragment" content="!" />. <meta name="viewport" content="width=device-width, initial-scale=1.0, minimum-scale=1.0, maximum-scale=1.0, user-scalable=no">.. <link href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" rel="stylesheet">. <link href="https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css" rel="stylesheet" />. <link href="https://cdnjs.cloudflare.com/ajax/libs/OwlCarousel2/2.1.6/assets/owl.carousel.min.css" rel="stylesheet" />. <link href="https://cdn.quilljs.com/1.2.2/quill.snow.css" rel="stylesheet">. <link href="https://cdn.quilljs.com/1.2.2/quill.bub

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\fb-pixel-events[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	1736
Entropy (8bit):	4.6218144099516705
Encrypted:	false
SSDEEP:	24:NI9pzjoSwD6M4eAi93zioUmBL5b553ZM4i6:NkpoSsiisoUmBLpjD
MD5:	13495DCB6FC91AD79E80FA3153CAFFBE
SHA1:	1B154CD723D77AD0D1823C01F0DA82453CE1AE3D
SHA-256:	EE5D1522A909E9749A263422880B8A9D6E0711ADCEE6036AA9460E207CF70FD7
SHA-512:	BB397F04AF02E51AF2CA0420D8DC4C636BF4A64B695FF5D76659A807F05C87840C9E6C084CDBB521E6E7F5323389B20D52BB1226BE9AB9ED654BD2B9130A180C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://risefundraiser.com/assets/js/fb-pixel-events.js
Preview:	.// $('[fbPixel]').click(function (e) {.// console.log(e);.// let attributes = e.attributes ? e.attributes : null;.// if (attributes && attributes.pixelAction) {.// fbq('track', attributes.pixelAction, {.// content_name: attributes.pixelContentName || null,.// content_category: attributes.pixelContentCategory || null,.// content_ids: attributes.pixelContentIds ? [attributes.pixelContentIds] : [],//comma seprated string.// content_type: attributes.pixelContentType || null,.// value: attributes.pixelContentValue || null,.// currency: attributes.pixelContentCurrency || null,.// });.// }.// }).window.onclick = function (e) {. // console.log(e.target);. let attributes = e.target.attributes ? e.target.attributes : null;. if (attributes && attributes.fbPixel && attributes.name && attributes.name.value) {. fbq('track', attributes.name.value, {. content_name: attributes.pixelContentName && attributes.pixelContentName.value ? attri

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\fbevents[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	187548
Entropy (8bit):	5.392602416896564
Encrypted:	false
SSDEEP:	1536:sM+OWt6w6aic9MeipKKqQqcThe7Kdv0a9sIOC1jaMu5Qm2B+QNSMngUSZYSlIUiR:sOQMj1SVBYDGKqOQMj1SVBYDGKx

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\fbevents[1].js	
MD5:	D67E6D12EB6608E9D939B0E3EB70F7E5
SHA1:	AF4A18DD4EA23B6DF3B0092618A64A3733C2AE55
SHA-256:	8A407F25943E3E96B80C488FD36FF80000A45C9D85BAFA80E5C05890874E6695
SHA-512:	6B871EEFE532476E7FA735211C049F2CB33B684A765F5FE06F1107B0937940FCEB8FC8A71177141BDA7D6319643244B09C033F132FDF8E68D5CD4B7C39869D74
Malicious:	false
Reputation:	low
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\fbevents[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	93774
Entropy (8bit):	5.392602416896564
Encrypted:	false
SSDEEP:	1536:sM+OWt6w6aic9MeipKKqQqcThe7Kdv0a9sIOC1jaMu5Qm2B+QNSMngUSZYSlIUiX:sOQMj1SVBYDGKx
MD5:	077B8B6E85C9EDF74D372D155180E6D3
SHA1:	4A24BE343819AD355807ADB01579366A1E64B8B9
SHA-256:	A517525B8A7D39BCAF1CF5F9695C5BE8FCE7A6B920A3924C1A4F70E8EA748C05
SHA-512:	DB714A2EAF14E6727086795FE151F3729DA32BFA0B87AB74289B7DF9E0808E1FEBCA38D2622EF47B7AA263479BDB66857011E2302DD1AFC9E814EF6B74642DF 9
Malicious:	false
Reputation:	low
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\freshdesk[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	9081
Entropy (8bit):	5.202740687003741
Encrypted:	false
SSDEEP:	96:d4GR00j0m9us7Xc7yq7pp3O6hf8+yumyds97CzlukfZU11ysr+Ut44SAImcrtsnP:dR0e0mns7ya4+y6M1y3UthahpdS
MD5:	CFF3B62B96E2A16C4F6227CE13BD4F51
SHA1:	C80CABBC76CD2E54F36D4C3F3CFEF153939CC5C2
SHA-256:	D41D43E89387B0A0783307E1721DA4EF1957313D4CD030E0BCAEA8A0C2F4456B
SHA-512:	0CFF58B9F5D71804D0F648F4F01307FE68A57FC0E2B13172F0A052C48568FA69A651ADDF203B63EC0B41CAFA6CB0307AC05DB4B7635065E68D55F95C7A4A7C2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://risefundraiser.com/assets/freshdesk.js
Preview:	/**. * Created by saurabh on 16/05/17.. */.!function(){function e(e){try{return e()}catch(t){window.console&&window.console.log&&window.console.log.apply&&windo w.console.log("Freshdesk Error: ",t)}}function t(e){return e&&!L.test(e)?B.location.protocol+"//"+e:e}function i(e){var t=B.createElement("link");t.setAttribute("rel","st ylesheet"),t.setAttribute("type","text/css"),t.setAttribute("href",e),"undefined"!=typeof t&&B.getElementsByTagName("head")[0].appendChild(t)}function o(e){var t=B.create Element("script");t.setAttribute("type","text/javascript"),t.setAttribute("src",e),"undefined"!=typeof t&&B.getElementsByTagName("head")[0].appendChild(t)}function n(e,t,i) {e&&e.addEventListener?e.addEventListener(t,i,!1):e&&e.attachEvent&&e.attachEvent("on"+t,i)}function r(e){var i;for(i in e)C.hasOwnProperty(i)&&("url"===i||"assetUrl"== =i?C[i]=t(e[i]):C[i]=e[i])}function a(e){var t=e.src,i=window.navigator&&window.navigator.appVersion.split("MSIE"),o=parseFloat(i[1]);return o>=5.5&&7>o&&B.body

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\glyphicons-halflings-regular[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), GLYPHICONS Halflings family
Category:	downloaded
Size (bytes):	20127
Entropy (8bit):	7.955177976966453
Encrypted:	false
SSDEEP:	384:KMymENGOF7p8jngOxqVQhBWQE+eudXKQ++2fMfTF2/89NbbeGymiGCQ0YL:7ylqVxqVQ7WYe6KQf2fMfuCHeHWCNYL

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\glyphicons-halflings-regular[1].eot	
MD5:	F4769F9BDB7466BE65088239C12046D1
SHA1:	86B6F62B7853E67D3E635F6512A5A5EFC58EA3C3
SHA-256:	13634DA87D9E23F8C3ED9108CE1724D183A39AD072E73E1B3D8CBF646D2D0407
SHA-512:	EFC910C96B9F5C58EA11A84577CF60AE995503B1EE670BB7E7D4A413B7403769920F82600B581F1BD4EE03D71C76C15255F0972ED66AD969487B5A4043F472C4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/fonts/glyphicons-halflings-regular.eot?
Preview:	.N..AM.....LP.....'.,.....(.G.L.Y.P.H.I.C.O.N.S. .H.a.l.f.l.i.n.g.s.....R.e.g.u.l.a.r...x.V.e.r.s.i.o.n. .1...0.0.9.;.P.S. .0.0.1...0.0.9.;.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...8.G.L.Y.P.H.I.C.O.N.S. .H.a.l.f.l.i.n.g.s. .R.e.g.u.l.a.r.....BSGP.....M..M..F.....(u..<.0D.B/X..N....CC.^...rmR2 sk..PJ"5+.gl.W*i.W./E...4#..U.~.f....UD.....J.1./!../...s..7...k.....(...h.N..8o..d$yq..1...9..@.-..HG.....S".Fj...6C3..&.....W51.....B..a..QaR.U/..{*.....=.@d..h$..1.T.nc+c..A.....Z..@ Q.c.a....l..2>.K....m.' ....C.HM.fB.X.,.Y....p.e....U....*..z..m...i..O1nE.....hx!aC.XT..V.....R....%...|I.H...P.5".b.N....=...r./_.R...._..%..uz....5.2....P.).....F.7S..q.F.{n.i.a ....@D..s.;...}9..?.....R{.Tk.;...U\N.Z..Q-.^.s..7.f.0....S3A..._n..`W.7P..p.....i..!.g./._p....Z.-=..~WZ#/.4 KF.`. ...z...0..|.D.....&d.I.....;.M.{'.om..m..I...!w.i9|H:.....{..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\help-india-fight-covid-19-donate-for-oxygen[1].htm	
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):	9933
Entropy (8bit):	5.233640574972931
Encrypted:	false
SSDEEP:	192:InFxXtSPDmAhkj6FxX8SJcfZimFZso1AjuApFpgth49tpzn8:ALXUmapLX8uZmZ1A3C
MD5:	9089539730FFA50D23244CD2B466D9B2
SHA1:	62CD5F1C2BDE857C9436754B0E702E7195DF9A56
SHA-256:	C81981F08D7ACDE582ADBB9EC41D21807C658EF21DEFF2A56E8F72D06F6D2236
SHA-512:	91421B72C29830AF55539673947A53735C63325C6BB6CC8974C2916DF2C44FC9461D3EEF95472D1BF6DD4E4BB5E899F4975A515597DBD7481F943C08B6FBEB0A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://risefundraiser.com/fundraising-api/public/api/1.0/campaign/help-india-fight-covid-19-donate-for-oxygen
Preview:	{"status":true,"data":{"gatewayInfo":{"INR":{"gatewayType":"System","id":4,"gatewayName":"Razorpay","merchantLiveKey":"XvraiCi7XGJBu8pPSeZWrGlt","merc hantLiveSecret":null,"merchantTestKey":null,"merchantTestSecret":null,"signatureLive":null,"signatureTest":null,"isApplePayEnabled":null,"defaultCurrency":"INR" ,"GatewayMode":"Production","currencies":null,"gatewayLoginUrl":null,"loginRequestMethod":null,"gatewayLoginParameters":null,"plans":[{"id":"plan_CYYnactp0rWYix ","amount":"100","currency":"INR"},{"id":"plan_CYYoEw8QeAt1tN","amount":"200","currency":"INR"},{"id":"plan_CYYoYQzYHszI0t","amount":"500","currency":"INR"},{"i d":"plan_CYYoo9k9DCRFKz","amount":"1000","currency":"INR"},{"id":"plan_CYYp2WIZDuWXCD","amount":"2500","currency":"INR"}],"donationLevels":[500,1000,2 500,5000],"namespace":"System"}},"likes":"1","causeInvolvment":null,"organization":{"id":"roundglass-foundation","orgType":"Profitable","selfPaymentGateway":0," name":"RoundGlass Foundation","creationDate":"2018-06-03 09:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\mobile-brandlogo[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	72983
Entropy (8bit):	4.51309914730978
Encrypted:	false
SSDEEP:	768:EkD3TQyEGaqQ3Cw5GvFisqPqJUhWlQSvh5T:E1FcUjY
MD5:	7489C8DB6CF91158E37B6B22F0727958
SHA1:	422D4085CA80D199908FFE97E636DE31D667C451
SHA-256:	122886B71B3B906F61231B8932A20AA733AB0F1DA775C2AFEDD6B63F535BEB98
SHA-512:	E0F1E5945B1F08C3EC69B4DC6230832CDA071B7402A8E0E7DFDA825B50833388A2F39489E5549DFBB505368B3820B7ADD40F402C0697B33FD50B2A2CDE12C1D D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s3-us-west-2.amazonaws.com/rg-fundraiser/assets/images/mobile-brandlogo.svg
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="152pt" height="22pt" viewBox="0 0 152 22" version="1.1">.<g id="surface1">.<path style=" stroke:none;fill-rule:nonzero;fill:rgb(73.333333%,74.117647%,74.901961%);fill-opacity:1;" d="M 29.730469 14.695312 C 28.160156 14.695312 27.101562 13.609375 27.101562 11.988281 C 27.101562 10.371094 28.164062 9.277344 29.742188 9.277344 C 30.503906 9.2 77344 31.148438 9.542969 31.589844 10.027344 L 31.589844 7.808594 C 31.59375 7.539062 31.8125 7.320312 32.082031 7.320312 L 32.425781 7.320312 L 32.42 5781 14.617188 L 31.589844 14.617188 L 31.589844 13.910156 C 31.105469 14.417969 30.433594 14.703125 29.730469 14.695312 Z M 29.761719 10.109375 C 28. 417969 10.109375 27.9375 11.078125 27.9375 11.988281 C 27.9375 13.125 28.652344 13.859375 29.761719 13.859375 C 30.832031 13.859375 31.582031 13.085938 31.582031 11.980469 C 31.582031 10.894531 30.820312 10.109375 29.761719 10.109

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\quill.snow[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	23302
Entropy (8bit):	4.8909285158547835
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\quill.snow[1].css	
SSDEEP:	384:OXa6h8sJ1vcYCW+3P3/YgJhgosEJRJByKnRWI7FFrFhFrFJMSFWprGymGibPz7Ql:OXZh8NYCW+3P3/YgJhgosEJRJByKnRWZ
MD5:	455913274305F030C2944F8DE75A0996
SHA1:	12165B0AABA2E1E44311B6160CF54313598508AE
SHA-256:	C99A5C5600B39A3FC8A4B2A47BD9B8C6276F399284C1F32D893852979C5197DA
SHA-512:	D7747CD19AD3DB2C93FC5A617B7D861FCA77AE7E59E993380A8981ACC4A8DA5E33E19868197C8CCCA8F7D3A939E1FE96530CF1989EB3CD3D3F32781F91699F7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.quilljs.com/1.2.2/quill.snow.css
Preview:	/*!. * Quill Editor v1.2.2. * https://quilljs.com/. * Copyright (c) 2014, Jason Chen. * Copyright (c) 2013, salesforce.com. */..ql-container {. box-sizing: border-box;. font-family: Helvetica, Arial, sans-serif;. font-size: 13px;. height: 100%;. margin: 0px;. position: relative;.}..ql-container.ql-disabled .ql-tooltip {. visibility: hidden;.}..ql-container.ql-disabled .ql-editor ul[data-checked] > li::before {. pointer-events: none;.}..ql-clipboard {. left: -100000px;. height: 1px;. overflow-y: hidden;. position: absolute;. top: 50%;.}..ql-clipboard p {. margin: 0;. padding: 0;.}..ql-editor {. box-sizing: border-box;. cursor: text;. line-height: 1.42;. height: 100%;. outline: none;. overflow-y: auto;. padding: 12px 15px;. tab-size: 4;. -moz-tab-size: 4;. text-align: left;. white-space: pre-wrap;. word-wrap: break-word;.}..ql-editor p,..ql-editor ol,..ql-editor ul,..ql-editor pre,..ql-editor blockquote,..ql-editor h1,..ql-editor h2,..ql-editor h3,..ql-editor h

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\runtime.c7dadc7bcd65c1e7f27b[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):	2427
Entropy (8bit):	5.416928874788694
Encrypted:	false
SSDEEP:	48:EnpxZ6Sqw7urxbssl4bzdOJP3CUPFpf+ujk3X6u81:EnpxXt76l4bJOJSUtpfK3X6Z
MD5:	4D70C2741203113B3B393B9DED9D8873
SHA1:	17D1E0A391D5890AB738CF54B412BB9CA4CB96A6
SHA-256:	B1A4BDDE12FDD220324934B565CDA709A039F6E204CFED16124E00D30345BFF1
SHA-512:	2147ACF14EE528918B49C93A6D54FAD9231AED28EC8A8235387D3A22DB9A669D814F6B8995CE51C36E53B268F6E0BFC03166646C11E561D6306E73E23E267743
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://risefundraiser.com/runtime.c7dadc7bcd65c1e7f27b.js
Preview:	!function(e){function r(r){for(var a,o,f=r[0],d=r[1],u=r[2],b=0,l=[];b<f.length;b++)n[o=f[b]]&&l.push(n[o][0]),n[o]=0;for(a in d)Object.prototype.hasOwnProperty.call(d,a)&&(e[a]=d[a]);for(i&&i(r);l.length;)l.shift()();return c.push.apply(c,u||[]),t()}function t(){for(var e,r=0;r<c.length;r++){for(var t=c[r],a=!0,f=1;f<t.length;f++)0!==n[t[f]]&&(a=!1);a&&(c.splice(r--,1),e=o(o.s=t[0]))}return e}var a={},n={24:0},c=[];function o(r){if(a[r])return a[r].exports;var t=a[r]={i:r,l:!1,exports:{}};return e[r].call(t.exports,t,t.exports,o),t.l=!0,t.exports}o.e=function(e){var r=[],t=n[e];if(0!==t)if(t)r.push(t[2]);else{var a=new Promise(function(r,a){t=n[e]=[r,a]});r.push(t[2]=a);var c=document.getElementsByTagName("head")[0],f=document.createElement("script");f.charset="utf-8",f.timeout=120,o.nc&&f.setAttribute("nonce",o.nc),f.src=function(e){return o.p+""+({}[e]||e)+"."+{0:"5dfdaa7dfd5376b677fc",1:"5cf16574643d5c9fb418",2:"4b9b9b512c2d18bea2fa",3:"1e9a7dfc99a3185c2eb4",4:"14b0baaac4d1bc468f07

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\search-icon[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 14 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	448
Entropy (8bit):	5.689172818708485
Encrypted:	false
SSDEEP:	6:6v/lhPEmNT7xWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWC:6v/7sml7rQxOmp9ZZ/3VHdlAXVHT1
MD5:	D5771DF738B58A49F97A7E81FC57950F
SHA1:	4127BF2E7D5704BF750D6C55C82DF54DD21A6712
SHA-256:	3EB6E5F60B14BE86B9C5778047CC617BDFBE7D9DF5B40AA0BE17E642885DF0A6
SHA-512:	E8CFCA24489BA4AF6B16FB0E2387C64F44E46BD68D8747FD9A875231170D70ABAFE89439024E4D1BD12151FBA97BE6E9B187CACA2B7C3015FE171A14F5782F63
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/assets/images/search-icon.png
Preview:	.PNG.....IHDR.....F....PLTESZ^...SZ^SZ^SZ^

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\unite[1].jpg	
MD5:	DA278FF50AB1BCBABA3F4837841E1D72
SHA1:	E6798E6764AC059A64636B132E523E14D7F82DD0
SHA-256:	FC1E2BA78A3DB54DAD1D17006ABACBFB12B99BCC209E6F6737684F03D3470465
SHA-512:	37379411B2743046DCB7F5D42FBBA758268F89E18DD6C7D296AD2C4DCD5A210411EA638D2F798C2E0B48E9C8133203CA690D2D5EC4A1AE5A5275FBEC7847E05
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/media/17553/conversions/unite.jpg
Preview:	......JFIF.....`.`.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... .....W.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..N..F.._V|["nx.h3..W.....8..PFs@._.(...@.... b.(.....J.7.../.@.....Y...z.p`G..''...1..:.^...@.PG.....=....#e9.@..Z@!.RX..22..G...Rs@.f..F.@...= h).@.c.=...@..j.6.Z.Z.....[..f..@._..9NFh.I.j....0.....h.h..H4..9.I.....x..<.. 9.AH...@.. ....-...".h.O .!.".D..P.....#....@.....;4.....D.7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\2.4b9b9b512c2d18bea2fa[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):	115132
Entropy (8bit):	5.305624636425158
Encrypted:	false
SSDEEP:	768:N2g73hvi2XaBo7FE/jVqJC9EtEJ/YjXhlJovY5c4SFboED8JHICiA51IEfF5+Rbt:vwZoM/iXhlwYINoEw7LjICybjnPB
MD5:	017187A9DE9A04C22B9B4E95220FBB08
SHA1:	08BD4D11B431CAFB66B4870D20C1623F868D2496
SHA-256:	F7ABCB2A2CFD0A4B0505C16F61B243ED013986C3C2675CD82651631A29539964
SHA-512:	756B5CBEB43BDAA444D005AB64C77B2879D15B179F6AE761F4E07AC853BEE6A02837A7F30D8219FC8F06F4D1D347089F7ACFCE368A2B4389ACA6538397208E4F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://risefundraiser.com/2.4b9b9b512c2d18bea2fa.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[2],{"0tKZ":function(n,l,e){"use strict";e.d(l,"a",function(){return t}),e("OgS7");var t=function(){}},"8/JR":function(n,l,e){"use strict";var t=e("8T9/"),i=e("Ibf7");n.exports=function(n,l){var e=l||{},u={};return void 0===n&&(n={}),n.on=function(l,e){return u[l]?u[l].push(e):u[l]=[e],n},n.once=function(l,e){return e._once=!0,n.on(l,e),n},n.off=function(l,e){var t=arguments.length;if(1===t)delete u[l];else if(0===t)u={};else{var i=u[l];if(!i)return n;i.splice(i.indexOf(e),1)}return n},n.emit=function(){var l=t(arguments);return n.emitterSnapshot(l.shift()).apply(this,l)},n.emitterSnapshot=function(l){var o=(u[l]||[]).slice(0);return function(){var u=t(arguments),a=this||n;if("error"===l&&!1!==e.throws&&!o.length)throw 1===u.length?u[0]:u;return o.forEach(function(t){e.async?i(t,u,a):t.apply(a,u),t._once&&n.off(l,t)}),n}},n}},"8T9/":function(n,l){n.exports=function(n,l){return Array.prototype.slice.call(n,l)}},"96Ym":function(n,l,e){"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\313E30_0_0[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT)
Category:	downloaded
Size (bytes):	40264
Entropy (8bit):	7.9760423376025384
Encrypted:	false
SSDEEP:	768:490RwCN0iKz2/IZ/puYUGaXX7OUUaOv5mf8ir86ZnWF1GsaSlgW3Gj4:49nViKq/IpHaXX7OUUajnZ41GpSD
MD5:	423A531319FA7BB3AD352D18D5903C71
SHA1:	0E660CD60C23DA420647A195C0CD1827F85A714A
SHA-256:	95EEDB1B0291336A5F7A809F5BE68C78A6507E43ED8405A5D8757451B3EE0F65
SHA-512:	5F8621DD688005B20399C79A5A35270C8B9845B416D53A2DE9030656F436255B8F36D5EC0F33411DFBBC5FF5FDEEE3F3F2561A04E7F73015384EAADDF70C293D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_0_0.eot?
Preview:	H...(.....LP/...J..P..... .....&....V.e.r.s.i.o.n. .1...0.0.0.;.c.o.m...m.y.f.o.n.t.s...c.a.n.a.d.a.t.y.p.e...g.i.b.s.o.n...l.i.g.h.t.-.i.t.a.l.i.c...w.f.k.i.t.2. ..h.x.k.7.....&G.i.b.s.o.n.-.L.i.g.h.t.I.t.....BSGP.....@..@..E .....Y.D.N....x...>..KPJQ....I...SNgQ.25J..*.I. ..0.L..f.....dF.....;.[.....i.x.Y2b...../.V..p.P$&.....t-md.N)..$.w..7)M.p..!..ISR.....x.....d...v.iG...{}_..4>....d.@^e...1..s....|....l~..>}pJ.....]...*?. q..V.e..84.Bo.x7.....t.r~..~...PMq..Z_A....%.Kq{..{[...Bu.B...&.F..@.....;..''..L.|.h.& ...'..-Rj@.m.p.e..4 ..H@....<W..z&7...C.....j...|..C."...{r=.6...r(>....R...K`.F.2..^A.KJz.Sj@Cr..0'..~N.`fQF...m+..d.P....b)..s.....2h...G..m.0.F.T6l.s.e.'.G..pZ.n.(.....5cc8.f. x.....0.cVZ.<.....0r..g#rT.l..L.-....2...E..W.<`...).W.W..E..&.E=&....n'.[.O.n.*8..J.U.~ V.....e...Vl...l..D.....hoSx..&o...{z.8.Up*.....y..j3H

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\313E30_1_0[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT)
Category:	downloaded
Size (bytes):	34766
Entropy (8bit):	7.972652960678206
Encrypted:	false
SSDEEP:	768:ff0XeIMyf8lXwJnF1g/pJer8fwxyo04Oi:ff0vMyYaF2Cr8+S4t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\313E30_1_0[1].eot	
MD5:	4DDA6EB189D2EFA2074CA89FED5E043C
SHA1:	669A381B62C1E868E20265BE869A21C867A14706
SHA-256:	570F31FB731A0CB6F5FC324C4DF06893B34A47658086434558A0D21A368DEE5E
SHA-512:	5264165232E1AA3169674B02365D93D7239F03CFEE26BAF3D41E793F4D6B5A3973603D1DD5C45885573CEE9188DE420AFDA7F364576299FA854E81CA88C37727
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_1_0.eot?
Preview:	.....LP/...J..P..... .....fm.....&....V.e.r.s.i.o.n. .1...0.0.0.;.c.o.m...m.y.f.o.n.t.s...c.a.n.a.d.a.t.y.p.e...g.i.b.s.o.n...b.o.l.d.-.i.t.a.l.i.c...w.f.k.i.t.2...h .x.k.7...$..&G.i.b.s.o.n.-.B.o.l.d.I.t.a.l.i.c.....BSGP.....?..?..B.....Y.D.N....x...>..KPJQ....a:mM9.D8...G.P.Nhi$..am>.q(...9>..Z..L.B._~w.....[.Dn..w:...o +"...).ppR..... p..u.....:..u8:..1).igHl..{.qZ...../tS^.U."...5*z-c...G..O.....V."%..t.l.F.....U!.q...`.ksA..Z3. |.F....k..5.....P$..o..J....a..]..f.....$._..M~c.|.....1S.4..R^...Z..!z....&.?(.....%.,..L Jj.U....%.4..3.{M...W..AXg..e.)ud.EN.].a..o...z=.....8.,.....!{.....B..v..>v.....W .r..G(.,...bMzs..1.>s.>.....)O.A...T..|..VX.....(s.AI...|.....t.A*..Z....j.V..|.Ho.K.\K.U..@. .+lCAB.i4..dV...<..}...X.[ZF..&.%.@_R..`6..G..y...J..YGO.n...M.9..9.TxZn[.2.(..HZ.s.....o-"...gnP.#.....f.DxY.m.j.....:c....@..2,.>...m.....d.-.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\313E30_2_0[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT)
Category:	downloaded
Size (bytes):	37239
Entropy (8bit):	7.9763829706402145
Encrypted:	false
SSDEEP:	768:fcJ8+UHCNdsbLAgtjr5uWheiFlmPcpn34uDOaclAgfK2ERAEJfjDfc:fcJ4iNuA0EWRvm0pnouDxeAt2UNc
MD5:	6C34DEB8139898E1C02C5FD4DAA63D06
SHA1:	190D8BF28320C11CB24EEF9D6BF7D877ADDD18EF
SHA-256:	397BD2855C15F0D88512F26AE75CA95AA5D71AA008BE88EC47C6C32B0F6D49C4
SHA-512:	59F14DF6E600F1909DF5FEDBFD0EBE8FA74540CAF47BF9BA274CABA8FEE2F8ABDFF790D7C31CAC0678DC9099394FD829269BECF4E181B36C06916ED3036A3 72
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_2_0.eot?
Preview:	w...l.....LP/...J..P..... .....&....V.e.r.s.i.o.n. .1...0.0.0.;.c.o.m...m.y.f.o.n.t.s...c.a.n.a.d.a.t.y.p.e...g.i.b.s.o.n...s.e.m.i.-.b.o.l.d.-.i.t.a.l.i.c...w.f.k .i.t.2...h.x.k.7...$..&G.i.b.s.o.n.-.S.e.m.i.b.o.l.d.I.t.....BSGP.....@..@..CD.....Y.D.N....x...>..KPJQ....a:mM9.D8...6L.M'44...0..L..f.r..O.-.T&g(..l.....%.....M..2Z.[.J"... S.....'...5...,6.1.+....c]b...m7.....)....vH.EjA....Y.k....b:.....M....{.]Q_!.....4=....P.."Z+..y...4.,...$.....@cZ.....*...C.>;. .Q...P...<O..i....4U8SK .%.|.U._c..X(....`.#J....x7 ...=.!i.M.g..]/A...A....$.....U.....D.....0....]L. .Q...T....+.l.D..s...wb.....Dh..8c....H.K..W..g.....@lg8}...Y.B.7..O..b...O.e=4.S;...%.aQ[*0.....N..Bz.....'.g^...T..i&.K'..v"g|.. e.3U.`..OX@.KSJR.\QC4@8..X..a....V'.....'."......9.....$*....X..C.+9.2...h.Y.dP+..&xs.....Tj.(d....H..E.LBLlv.....:.2.~....m.....Q,.g.q.&..%...u.dUF...(y..G.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\313E30_3_0[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT)
Category:	downloaded
Size (bytes):	32026
Entropy (8bit):	7.970416945002761
Encrypted:	false
SSDEEP:	768:TshODAmb7UG+UjhDvSx1rWNqmp9wIbgrHoXy/jimcTDk1Cd:a4P+cL7p9LbKe/sCd
MD5:	3D8EABC4181E2E0DB2FAFC92983FA830
SHA1:	CBF5E62B66D3577C4D50920BB03D67FB1ADC7FE7
SHA-256:	A8AD2DA00D1D4F8C4DD79FD9BEB57BD40110F7A59DCB604C6C95FF32067D5B9E
SHA-512:	E649C3D5138D49D0D3DABFF1C5AA0BC83204397C782EE2495C467B9ADCB27C18C46A41CE99DB69363FA5468B279DBFBF864AB03AB0DD7CB281CDF07958EC9 00
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_3_0.eot?
Preview:	.}...|.....LP/...J..P..... .....&..x.V.e.r.s.i.o.n. .1...0.0.0.;.c.o.m...m.y.f.o.n.t.s...c.a.n.a.d.a.t.y.p.e...g.i.b.s.o.n...b.o.l.d...w.f.k.i.t.2...h.x.k.7.....&G. i.b.s.o.n.-.B.o.l.d.....BSGP.....<..<..=.....U.D.-..ith.`....GLFM....`.-...$8...,I#04.....&'R.p..z.K.B.....*...(.doh..:.....[L.`._H..J....0.d.l..(Q[.z.]|.).,.;.4.5..(.N/...Z.~e../.... x.f.C$;...Z.7.._A.m....P.Tk8../]...5.....&'.....Fi;.?..}.!(..[.T.&..Y..R...~+.K..F...w?g.#.kp.H>.....M*.....|....fj.E....d...~.....Q..L.>...c.R.m..b.)CI.l..%?.H.....$...F...v<..d.t...A....? 0..kz.-.....Y...%.C.T..~....W.,6C...B...@.=.....c....w3..>.%...Bn<.>..".^.D.3iM.....(.~.D.aS@v@#E..BzPz...X..*..2(.&...q.I....T..{.TO.t.V....R..h.+..18.h....F;.?...n1.\..h...-,.....\.@9 qT"...,3/...6.)i..+]...j%I..ei2.o..b3w.We.....L...e..".....>a..&.a...../...[..X..p...2/{;...d..O...C>.....b..vJk/. ...:...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\313E30_4_0[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT)
Category:	downloaded
Size (bytes):	37736
Entropy (8bit):	7.97299207458296
Encrypted:	false
SSDEEP:	768:lSOhpY66PNvZd4XBgHv+dyWzN1PcK2Z2GjqUMR+fb2gsPB4V/jLDB:YOhuNvZ++myWRZcLZhW+fKgf/jLDB
MD5:	3711ACF094B06C8BB46D4B9AD9FF006A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\313E30_4_0[1].eot	
SHA1:	05373A160BD17A3A9D714130FE0C754E8A69E925
SHA-256:	1C3871A9DD5E7B39413D66F8DFC7833C0420F1550CD0609C25523CC9097FBD47
SHA-512:	4D29AC2A5D5417B9AC42E213252D5F7443C2DA93629582420DE4BC391EB3B26B9841E29115EABAE254058D7FF35857C05F8E10731DFC1288CC154248D4590004
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_4_0.eot?
Preview:	h...R.....LP/...J..P..... .....a.....&..~.V.e.r.s.i.o.n. .1...0.0.0.;.c.o.m...m.y.f.o.n.t.s...c.a.n.a.d.a.t.y.p.e...g.i.b.s.o.n...r.e.g.u.l.a.r...w.f.k.i.t.2. ..h.x.k.7.....&G.i.b.s.o.n.-.R.e.g.u.l.a.r.....BSGP.....^.@5.@9.>.....U.D.-..ith.`....GLFM....`.-...$8...E.I#05.W.r....E~....zE8.....$.a+.[`.{V. ....z.D..7.....G...4{ &4Y... o.M.Lc.B.Z.z.....s.Y...w....z%.7..|g...@...Wn..F.C...~.0CU;`.7X.Z.\U.8..h^..A2..m.Sb...-.<k*.....,...`.....*B.0...K..)D.V.....Cx...5..._..v..:..|aR.U..h.T..!.C....x.Ze..Z..M...+..sd`.".(.d ..-.X..ib(..S.2.N.....PU2hXu...pJ.O2.RwTS.e.f..&.5A...G/..y.P..%2..T.Q+.....M.}..HWi.L...[\.H....-...i..rT,...Gh.<f.... .tb6.e...O.&..`....C.D/.SQh.\.h.:~.z...*.Ll.E...../.....0.%...# ..ny.,T.L..E... ....C.E.J.d.{.....j.6.3U..w...s.6..|V.-D.*...*.. ....|9..m....q.....V.3.1-'^..{l.u.mC`..e..S..q..\.@.....\.z.@..'.Z.....j...d.-'..00...T..q..^.O.&-.;.....,..... J...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\313E30_5_0[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT)
Category:	downloaded
Size (bytes):	35650
Entropy (8bit):	7.97643756100948
Encrypted:	false
SSDEEP:	768:TWkmj0O3aBsCCHdOTVpXztLhRoMpbMvgvDFdiNyy:ix3aZCHETVpXNhDR4gvDFkyy
MD5:	FF7F9E17F3E9DC0191B32D172D513CAB
SHA1:	9E27AB17F652CAAE8C32C16B24EB6D85C74D909E
SHA-256:	94E73FBEF5E43F2736B9956317D5BD8ACC71703332C8A3760FD7ACDCF217C355
SHA-512:	BC4B35BC26F967D508E230D737BA6D3FBF401B4584D2038563418CDC08055ACDC968CE1D019CE2E0D4D84A058EA40CE90503A720D06BC8319F1F4905182D136
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_5_0.eot?
Preview:	B...&.....LP/...J..P..... .....O.B.....&....V.e.r.s.i.o.n. .1...0.0.0.;.c.o.m...m.y.f.o.n.t.s...c.a.n.a.d.a.t.y.p.e...g.i.b.s.o.n...s.e.m.i.-.b.o.l.d...w.f.k.i. t.2...h.x.k.7... ..&G.i.b.s.o.n.-.S.e.m.i.B.o.l.d.....BSGP.....?{.?..>.....U.D.-..ith.`....GLFM....`.-...$8...4H.I#04.W.r....E`v..."..A.DxnMa.$.._.3kb.o...F.<.R(..`.}....+x ...^....@6.P`.....3k.M.....K.4:4..o>..I....~w.-.@....uj..d.|C....~...e...7h.]0..dq.*.1.. .....*.~.d.....^..Z3I.....1.HX..../.....f.#.N.##...y..|..?Eq.....qSm8..v\mSj.U.)._.z-...y.b.x'l4h.4..... f..d_.A*.S.=.q...b.).O.=S@.D...H+.....n.L.e.j<.Ne@.^..HB..d*....bi.q...."1[.>...E.....QE.....7.....n..X[.@v&$S.....T....wNG....`<..sR..m+...T.G.a..?...1b=>2 .+%.E..d..I. ..eu.."J.Tg:Qh4<&;....VI.?E...(.....EM..j}.v....-...Ck..z.o..m..K....n.r.....d..DoA..`....V...?..4<)..n/..-m.s....y..vh....."+.....ctDpY...ujV.A..-.(..E.N...(*.....,.....l.^..@.F:.'kz.h.:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\313E30_6_0[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT)
Category:	downloaded
Size (bytes):	39520
Entropy (8bit):	7.976877911687657
Encrypted:	false
SSDEEP:	768:Pm0e62hlOMgcGMYZnUp8jU8SCaj/qMYJIlk7jg0uulYB9LryHMPkmC:N2hlOMVBYZyoU8i/qVX40uy09fS
MD5:	8D20465818A4456D9BA479747C164786
SHA1:	C3E172AD9DFA94BF53042900699DAC679900D997
SHA-256:	CE69C1FB10432714DBF98010612CD151773961955047D6C35F3B57629F60071D
SHA-512:	5021868D9886DDE7B3ECD1624E62279C3F8034EFBE3E63D068E023D77185990BDAF0B09DAB04B5F4256B99A512699DF46A375A7B72EB5618CA2300117EA8066E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_6_0.eot?
Preview:	`...N.....LP/...J..P..... .....&..|.V.e.r.s.i.o.n. .1...0.0.0.;.c.o.m...m.y.f.o.n.t.s...c.a.n.a.d.a.t.y.p.e...g.i.b.s.o.n...i.t.a.l.i.c...w.f.k.i.t.2...h.x.k.7.... ..&G.i.b.s.o.n.-.I.t.a.l.i.c.....BSGP.....@..@..DB.....Y.D.N....x...>..KPJQ...l.SM..3... ....scJ.%L.../*.....$.....-.K..$7.G.s..j.B.L3.....H-.....k.Z.d..u.)D....>:.a).&.!.;.h F.!.+.....,_.^.....$..GZ.0q. .4..<M...X>2D V...dI..=..j.]...e.Q...a...u...;.S!.....$.0t..J...McZ...`../....O..r...D.),-a...R. .x.....TT.)i{@....2.p.R...."i.L*_....5....n..G9.YJ.N..*{..A.... .R.@...m...O `..'U.."d...N.2.Z..R...] ..u.:..t O.....`B...T...Mx."md..nn.e.;..{~....k.M[>`:.a..)O.GI..p.49@.$F..Zj%B....dQw...~..M.....T.+.4....1.um<....Q..V...M*..kK1t-.>mT.... f.W".YAQ.uK...#...GnF'.Y.....X..#k6#.p.....A.w.b"Rs...43.Y.v..a.].....*}../u$.>...d....)ZB..._.o..O.I..p;8dzJ.%....m2.xg..).X.....R.j.I4..r]Jw.....D..0G[.=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\313E30_7_0[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT)
Category:	downloaded
Size (bytes):	36418
Entropy (8bit):	7.97458158803009
Encrypted:	false
SSDEEP:	768:KVuEhI88wS+KruiNUDGQ0uoapZ161d3hQGGEjCZK4Xtq4kmGKOTaXa:i0oiKDG/uooT6bOGG7TPkzKSca
MD5:	90F042EA002D0DA7AB730EF4A591184C
SHA1:	379A4E0E9195A0EA97FA78F4FF93778BD4EF49CF
SHA-256:	8652FBF147490DD5A7E47AFDF8B84E829563B2767C10FDD9E2C006C5A8DC83C8
SHA-512:	5F471AE1101312F90E4B482AEEC0C47FA7711D38210C626119B2519BC331D4F93F4C20492D9360EA5496E3ECF35F2E08B81E230A4DF63EC61B2F6AF8939859DF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\313E30_7_0[1].eot	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_7_0.eot?
Preview:	B...4.....LP/...J..P..... .....2.....&..z.V.e.r.s.i.o.n. .1...0.0.0.;.c.o.m...m.y.f.o.n.t.s...c.a.n.a.d.a.t.y.p.e...g.i.b.s.o.n...l.i.g.h.t...w.f.k.i.t.2...h.x.k.7.....&.i.b.s.o.n.-.L.i.g.h.t.....BSGP.....~.=..=..>.....U.D.-..ith.`....GLFM....`.-...$8....H.F`j.....&'R.p..|..I..3.[....Z.K|.....:.....:.[S.`.....6:...+T.P.g.V.#CD.D:f...,M).t_Y/2.j....;..K...).....62..>R(4....M.e.:m.Q...>...9xr...1m..u+@..#4../.m>..L+...'(.{...h.E|(e...q.Tm.S~c.~...n...X8...^.q[.....HzH..m}...Q.A..8..G6..R*[{6K.^..dq.LQK....E..$..R.OJ5?..V}3...$...B...=.M.2.J9.../..W`V.....F.c9P.!5...A..#.L6.QwX. ...EQ....y&.G.E.\.b....$....F..+.i%C..B\.)\N!.`.....,...lQ.9....V{.o..;.@..Y..... 89...WIwAX.v.E3.e..&.....;'..#.>ad..l]...~..-....Kg.o._.,...&.&..-:3.wmH.p.....DL.f.?.....+#..4.=...A....h8.]....#.....p..w..c5O.|m.|.,.K...2._..n....ZO..`h....#..t0..$A.:4X...P...l02.G.o.[.Jm..../.x..2..Z..*

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\bootstrap.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	121200
Entropy (8bit):	5.0982146191887106
Encrypted:	false
SSDEEP:	768:Vy3Gxw/Vc/QWlJxtQOIuiHlq5mzI4X8OAduFKbv2ctg2Bd8JP7ecQVvH1FS:nw/a1fIuiHlq5mN8lDbNmPbh
MD5:	EC3BB52A00E176A7181D454DFFAEA219
SHA1:	6527D8BF3E1E9368BAB8C7B60F56BC01FA3AFD68
SHA-256:	F75E846CC83BD11432F4B1E21A45F31BC85283D11D372F7B19ACCD1BF6A2635C
SHA-512:	E8C5DAF01EAE68ED7C1E277A6E544C7AD108A0FA877FB531D6D9F2210769B7DA88E4E002C7B0BE3B72154EBF7CBF01A795C8342CE2DAD368BD6351E956195F8B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css
Preview:	/*!. * Bootstrap v3.3.7 (http://getbootstrap.com). * Copyright 2011-2016 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). *//*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */html{font-family:sans-serif;-webkit-text-size-adjust:100%;-ms-text-size-adjust:100%}body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background-color:transparent}a:active,a:hover{outline:0}abbr[title]{border-bottom:1px dotted}b,strong{font-weight:700}dfn{font-style:italic}h1{margin:.67em 0;font-size:2em}mark{color:#000;background:#ff0}small{font-size:80%}sub,sup{position:relative;font-size:75%;line-height:0;vertical-align:baseline}sup{top:-.5em}sub{bottom:-.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:1em 40px}hr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\bootstrap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	37045
Entropy (8bit):	5.174934618594778
Encrypted:	false
SSDEEP:	768:o2rGy27UwlNqMl95qNmCFejhqs8snmi+CSFXfbx8Gf3Zq7Q:Jg73zhq0GvbJ3ZKQ
MD5:	5869C96CC8F19086AEE625D670D741F9
SHA1:	430A443D74830FE9BE26EFCA431F448C1B3740F9
SHA-256:	53964478A7C634E8DAD34ECC303DD8048D00DCE4993906DE1BACF67F663486EF
SHA-512:	8B3B64A1BB2F9E329F02D4CD7479065630184EBAED942EE61A9FF9E1CE34C28C0EECB854458977815CF3704A8697FA8A5D096D2761F032B74B70D51DA3E37F4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v3.3.7 (http://getbootstrap.com). * Copyright 2011-2016 Twitter, Inc.. * Licensed under the MIT license. */.if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires jQuery");+function(a){"use strict";var b=a.fn.jquery.split(" ")[0].split(".");if(b[0]<2&&b[1]<9||1==b[0]&&9==b[1]&&b[2]<1||b[0]>3)throw new Error("Bootstrap's JavaScript requires jQuery version 1.9.1 or higher, but lower than version 4")}(jQuery),+function(a){"use strict";function b(){var a=document.creat eElement("bootstrap"),b={WebkitTransition:"webkitTransitionEnd",MozTransition:"transitionend",OTransition:"oTransitionEnd otransitionend",transition:"transitionend"};for(var c in b)if(void 0!==a.style[c])return{end:b[c]};return!1}a.fn.emulateTransitionEnd=function(b){var c=!1,d=this;a(this).one("bsTransitionEnd",function(){c=!0});var e=fu nction(){c||a(d).trigger(a.support.transition.end)};return setTimeout(e,b),this},a(function(){a.support.transition=b(),a.support.transition&&(a.event.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\branded_fundraising[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 986 x 720, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	7809
Entropy (8bit):	7.9504714392476545
Encrypted:	false
SSDEEP:	96:pxaswhRgwJrhhXLBorM+ZwUHl3kFcvg+etKEIy0D1R+zqsyhVhtUkGg8EavBL7x/:fc7JCmtKEA+zqsyhTCkGkavBHPaZgr
MD5:	B6C5FA85DA2C07F93DBE8BC42E522D4C
SHA1:	93E716A4F19734B7D68F6EF5EBA7E8E71D8DF516
SHA-256:	3E72DC3224ADF9D68FC081A8E5B9E6417655048ADFB2AC172399D69441311CCC
SHA-512:	8C8BC7B9058831DC09257A034DB701D020722973CEBE34BFD0E2C6CE8AEB06868883F1C5C020A201340E113E9E062458716D57A9AF493092F8308B12C7EE0A45

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\branded_fundraising[1].png	
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....o.....sRGB.....@.IDATx..K.-I...y^y.q.>.....hQ-. .....3{~.}....jv... `..B.....l."@@..Z.@. H.3.L....^...<.L.~.s.s.V....F..p777377ws..8....._..l~.'...G.....b .i6l6[....d2...\.O.y.P...&.tV0..zx....b>L..n.{...$..<..AI.48..9....t2..-...}.f.pt<K.d.f.)8..\.$<.....F...C..i.....p@Rn.h.....]..!.{....).+d.....V.a.....l...Y....[2n...a..&..r>.C.Z~.....n;.'?.. .N..B.....M.,...o..|.....aX...#...b....|2..c.~...0...R\....\...T.j.....9U.\"seK.....;.\.....x .?JTaqD...8ep.....f.<..a6..g.l.5...C.j3|.....v.....p.d9..g.....Z.4..B.....S~.b$.x.6..B..Xy.. m...%.=.h=...m...=.',...&..W....6u.....fXo.....~...=.N..E.....~n.W.....|.r8\.....~.....^.[..1%.nX.7..JU.....r...._....ct.f...~.....;...O..?.4..|.....?.^<{.....~3..?.....O ..P.....p....W..7..~...O?..z.....u8.^~.5e..p}}.....O>.IX....{ww.v}q..a$..k{.Om.b...W..:T...pq8...iC3.C...../..D{..NN..'G....tu.....l>..f..y.}:[.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\font-awesome.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	31000
Entropy (8bit):	4.746143404849733
Encrypted:	false
SSDEEP:	384:wHu5yWeTUKW+KlkJ5de2UYDyVfwYUas2l8yQ/8dwmaU8G:wwlr+Klk3Yi+fwYUf2l8yQ/e9vf
MD5:	269550530CC127B6AA5A35925A7DE6CE
SHA1:	512C7D79033E3028A9BE61B540CF1A6870C896F8
SHA-256:	799AEB25CC0373FDEE0E1B1DB7AD6C2F6A0E058DFADAA3379689F583213190BD
SHA-512:	49F4E24E55FA924FAA8AD7DEBE5FFB2E26D439E25696DF6B6F20E7F766B50EA58EC3DBD61B6305A1ACACD2C80E6E659ACCEE4140F885B9C9E71008E9001FB F4B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css
Preview:	/*!. * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome. * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License). */@font-face{font-family:'FontAwesome';src:url('../fonts/fontawesome-webfont.eot?v=4.7.0');src:url('../fonts/fontawesome-webfont.eot?#iefix&v=4.7.0') format('embedded-opentype'),url('../fonts/fontawesome-webfont.woff2?v=4.7.0') format('woff2'),url('../fonts/fontawesome-webfont.woff?v=4.7.0') format('woff'),url('../fonts/fontawesome-web font.ttf?v=4.7.0') format('truetype'),url('../fonts/fontawesome-webfont.svg?v=4.7.0#fontawesomeregular') format('svg');font-weight:normal;font-style:normal}.fa{display:inline-block;font:normal normal normal 14px/1 FontAwesome;font-size:inherit;text-rendering:auto;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}.fa-lg{ font-size:1.33333333em;line-height:.75em;vertical-align:-15%}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-fw{width:1.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\gtm[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	126327
Entropy (8bit):	5.505079917608965
Encrypted:	false
SSDEEP:	1536:EDRnpXBMY2t4FP0M+HRCfVF9pUnG/wZjd/bWB41E9DKPEI31IqB1XBgj4+Tl:EtnpXBMY2UP06fVn/EdSBc+Tl
MD5:	CFD133DB5D20ECB5F3C193DD53371887
SHA1:	E10CD14FCC13C31A78D484A03C4420C5BEAB5A14
SHA-256:	49A4F7295AAB8734001583DD503E6904F059E977267179C4C48FB78B1CDEA2B7
SHA-512:	5F4AB42BABDB6A79F43435A7693646B36DF91784FE171A3404D5A298A1CD2179F71D5D8AF6967FE4F0C4B6FD0210932367DED03A6C971EE52381CA58B240ED3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.googletagmanager.com/gtm.js?id=GTM-K54ZJZ4
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(){..var data = {."resource": {. "version":"14",. . "macros":[{. "function":"__v",. "vtp_name":"gtm.elemen tId",. "vtp_dataLayerVersion":1. },{. "function":"__e". },{. "function":"__u",. "vtp_component":"URL". },{. "function":"__aev",. "vtp_varType":"TEXT". },{. "function":"__gas",. "vtp_cookieDomain":"auto",. "vtp_doubleClick":false,. "vtp_setTrackerName":false,. "vtp_useDebugVersion":false,. "vtp_use HashAutoLink":false,. "vtp_decorateFormsAutoLink":false,. "vtp_enableLinkId":false,. "vtp_enableEcommerce":false,. "vtp_trackingId":"UA-84651813-3",. "vtp_enableUaRlsa":false,. "vtp_enableUseInternalVersion":false. },{. "function":"__u",. "vtp_component":"PATH". },{. "function":"__v",. "vtp_na me":"gtm.elementUrl",. "vtp_dataLayerVersion":1. },{. "function":"__u",. "vtp_comp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\help-india-fight-covid-19-donate-for-oxygen[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	84
Entropy (8bit):	4.363819698065086
Encrypted:	false
SSDEEP:	3:YWR4b5LCE02Rgq9LPALI7AX6Mn:YWyb5LHxWq9LPIIEXD
MD5:	C4CBFE5BDC03042E1247747430A6AC87
SHA1:	C8DEFD12416E3F28EF6CC22CC25E970804710706
SHA-256:	1A34D9AD2C22D54E57B66F10972A34AFCDF769F80D49AA10C202EA1D615CC7B2
SHA-512:	EA3C40D5710749E1014A7492BF7C64D4D322EAB6E3BA4A378CCEA050ACDC02C138E5A4F16E0946FC06E3C165E242F17A9D1F765C3D6BB77B3C7850901AF977 7
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\help-india-fight-covid-19-donate-for-oxygen[1].json	
Reputation:	low
IE Cache URL:	http://https://risefundraiser.com/fundraising-api/public/api/1.0/chapter/campaign/help-india-fight-covid-19-donate-for-oxygen?order=desc&sortBy=donation_amount&offSet=0&size=20&isManager=false
Preview:	{"status":true,"data":null,"id":200,"errorCode":10000,"message":"No Chapter exist."}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\icon-sprite[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 70 x 1800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	20031
Entropy (8bit):	7.834817063767024
Encrypted:	false
SSDEEP:	384:bSTTIiC7L234aCSySR1WZUnt/X3tm4kEty+CaMvGKOSk0+1lAs2ZL:mFCVaChetv9m4kP9wSv+1liL
MD5:	DBC207D114CDB2D6A45298C1496762FD
SHA1:	5A94DCE9715A32C316E6B61FFF12541A4361EC52
SHA-256:	ED608E7B73C8D11DE411E62F7DB311ABFA25B9252D93174229F2FB6DA35AED0B
SHA-512:	60A53E385CF1C000F69C8FC0F4822E352E0D5DEEC141B6D3BAF12C98B054C74A590BB7E66E285659BE412CC71221983C5B12ADADE44237C4C0DA7CA4320E952
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/assets/images/icon-sprite.png
Preview:	.PNG.....IHDR...F..... .IDATx.....D..W..(..QQ.S.!.h....S..hb.4F....F.n.1b#6,.cG.....+ E:.V...}....fg.e.g...~.....<{.9...r.....=..p.p..0M..fi7.>..y....mF).-..f..|c.}.....R..Y.5c.*./...CV...VI.1Z.G+e....D.#...`J..}.{....t..e..c.H.1.....yJ..Z.+..,Y...*.....MXC~.3.i.....s...]..O..|.... 7.....}.....}..H..9...Qm..]..(..9f|c.....}.i`z..9.?....&..{Q...3C.M...?Z{.....9.H=7.1k}....Q....%..<0....)ZK...G6E...znfc....)...fx.%V...=7.1.J/.4n.....R~..znfc6^..ws..._c..&..S.Mm..o.E-...hMQ...&.....g..X..y..g.W{..Jr.../...}.....c./...M..9...Z...h.e.[P. ..q^M.2.s..s.w.:.~.....Z.....<..or...9z.e.kI....z.=`.. .7....1.N.....&.].%.I=...YU."..:}...2E..s.V.7....#;.p..?.5g.J..yj.z....3.....g_O..r.L.4O....61...).t.#..5..[..]6.TC.X.C.<5.U..%.....d.....zH.q.....1z..ayi.+=.N.1.....X.s.]....co.2.....}..Af.....i.M.....c..hy..p.d.c....h=.....x.'.$.B....K;...i.t.<.....WX.V.q.&6Z.....P..K.....Y5.9.f.b... .

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\loader[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3062
Entropy (8bit):	4.8897014177136535
Encrypted:	false
SSDEEP:	48:tYTWge+08gJ+H8gQ+f8g/+6K8gf++8gY+C8gp+j8gp+xK8gw+u8gL+u8gH+Y8g8O:dGqD+LN0EVL8VjY
MD5:	1BE6A381570D862ED6A40697AB62E59E
SHA1:	A24D97AF249A2865A35740AD462C83A798769A78
SHA-256:	118B16D8228652DB85B050E341407A0ABA2D4261A611663B700066E842E137E5
SHA-512:	FB78B74288B5C607633DF52FE286917FBD00096C2427B65EAB0AF9057D406BB03840967BFC31564F9FA0C01652BE38A17FAE4C45CF7DE4E60C01FE30D9F06AC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/assets/images/loader.svg
Preview:	<svg width='194px' height='194px' xmlns="http://www.w3.org/2000/svg" viewBox="0 0 100 100" preserveAspectRatio="xMidYMid" class="uil-default"><rect x="0" y="0" width="100" height="100" fill="none" class="bk"></rect><rect x='46.5' y='40' width='7' height='20' rx='5' ry='5' fill='#f65533' transform='rotate(0 50 50) translate(0 -30)'> <animate attributeName='opacity' from='1' to='0' dur='1s' begin='0s' repeatCount='indefinite'/></rect><rect x='46.5' y='40' width='7' height='20' rx='5' ry='5' fill='#f65533' transform='rotate(30 50 50) translate(0 -30)'> <animate attributeName='opacity' from='1' to='0' dur='1s' begin='0.08333333333333333s' repeatCount='indefinite'/></rect> <rect x='46.5' y='40' width='7' height='20' rx='5' ry='5' fill='#f65533' transform='rotate(60 50 50) translate(0 -30)'> <animate attributeName='opacity' from='1' to='0' dur='1s' begin='0.16666666666666666s' repeatCount='indefinite'/></rect><rect x='46.5' y='40' width='7' height='20' rx='5' ry='5' fill='#f65533' tran

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\main.94919de6defa08284319[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):	2635444
Entropy (8bit):	5.373019424777936
Encrypted:	false
SSDEEP:	49152:yIG1VVB4XBustAiw/na8eZ5oolxRMpFA+0oYv8pk5S5p02imEv8h5jvjIOa3rATR:E
MD5:	D588B9A4FDA0E8BF8551B0C1DACE7476
SHA1:	F02399F4BFE067DF6F32AF15FDD6AE7D556DDC63
SHA-256:	C970C9766ECC73F2B1EC364EFBDEA2C9B14A4B31D82BD7EB5F204D977863313A
SHA-512:	BBD6D65390E97CAAF32F60D7B387C08AFA1FB58E4AA265D1ACA8B2C1F2E149627E9E04B10903ADC4FAAF866D0B9974A67DD2D788F5846EC50133F6C352CEB249
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/1.9.7_P9_patch2/main.94919de6defa08284319.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\main.94919de6defa08284319[1].js	
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[28],{"+xv6":function(n,l,e){"use strict";e("KKpL"),e("sDE+");var t=e("IoZi"),o=(e("AiR7"),"228899524475948");e.d(l,"a",function(){return i});var i=function(){function n(n,l,e,t){this._ajaxService=n,this.router=l,this.missionService=e,this.likeDeslikeService=t,this.api=n.getApi("comment"),this.userId=localStorage.getItem("id")}return n.prototype.setUserId=function(n){n.userId=localStorage.getItem("id")},n.prototype.search=function(n,l){var e=this;return void 0===l&&(l=!0),localStorage.getItem("id")&&(n.filters||(n.filters=[]),n.filters.every(function(n){return"userId"!=n.field})?n.filters.push({field:"userId",value:localStorage.getItem("id")}):n.filters.find(function(n){return"userId"==n.field}).value=localStorage.getItem("id")),this._ajaxService.getApi("comments").page(n).toPromise().then(function(n){return n}).catch(function(n){if(l)return e.handleError(n)})},n.prototype.create=function(n){var l=this;return this.setUserId(n),this.ap

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\offerings[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	9071
Entropy (8bit):	4.94862352509096
Encrypted:	false
SSDEEP:	192:LyAEQmFHFlHWjmRjLd0gpKQKdFr0y0Fo0l2P3OOv84aTmdZAckyFrJqyJhSgOIte:LxEQallHrBjSSFHJT4ZjGrxN8bfM
MD5:	2A5CEF0817081FC6AD1909B62ACD9919
SHA1:	B005FD522AD71CCADCBFE240599389ACA8BECDCA
SHA-256:	B6F1F3701DC121B979E593EBD27D71CDDD16BDECFB3FEDD70C7ADB5F2D0BA3F3
SHA-512:	B26C4C7F146FC8CC2BDD1BFBB1FA5085BE540A9299B592375BE1D5E60D75807E0768FD76BA41FEF1B1A0B74EE88582833C63EF6852C4A48C952504C453EB9E3
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html lang="en">..<head>. <meta http-equiv="Content-type" content="text/html; charset=utf-8" />. <meta http-equiv="X-UA-Compatible" content="ie=edge">. <meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate">. <meta http-equiv="Pragma" content="no-cache">. <meta http-equiv="Expires" content="0">. <meta name="fragment" content="!" />. <meta name="viewport" content="width=device-width, initial-scale=1.0, minimum-scale=1.0, maximum-scale=1.0, user-scalable=no">.. <link href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" rel="stylesheet">. <link href="https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css" rel="stylesheet" />. <link href="https://cdnjs.cloudflare.com/ajax/libs/OwlCarousel2/2.1.6/assets/owl.carousel.min.css" rel="stylesheet" />. <link href="https://cdn.quilljs.com/1.2.2/quill.snow.css" rel="stylesheet">. <link href="https://cdn.quilljs.com/1.2.2/quill.bub

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\styles.a19aec6bac6aa86c5932[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	69723
Entropy (8bit):	5.185648108263596
Encrypted:	false
SSDEEP:	768:w1ybSgYG5fIVvx2H6B/k/GmZmoa8oXM7hpQp:cyb2G5IVp2/iXMFU
MD5:	F753655555A8CCF2D9F3D2F2DD14CBEE
SHA1:	1307C82DA95EE428D6AA5456A9D5B8C36DD3B804
SHA-256:	FA6D0F89AA5233FCA7459485DB8CC8AD2D3ED702EA5C653376A350ADA4624FEB
SHA-512:	F26A9CE232CA9E7C5486F880B9EC516B35859A7E6901D3FA096388078F3123E1B93600883FBD932E7FAE9410C87961BE073897F0738928C77EB6A03878DA1B2B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://risefundraiser.com/styles.a19aec6bac6aa86c5932.css
Preview:	/*!. * Cropper.js v1.4.1. * https://fengyuanchen.github.io/cropperjs. *. * Copyright 2015-present Chen Fengyuan. * Released under the MIT license. *. * Date: 2018-07-15T09:54:43.167Z. */.cropper-container{direction:ltr;font-size:0;line-height:0;position:relative;touch-action:none;-webkit-user-select:none;-moz-user-select:none;-ms-user-select:none;user-select:none}.cropper-container img{display:block;height:100%;image-orientation:0deg;max-height:none!important;max-width:none!important;min-height:0!important;min-width:0!important;width:100%}.cropper-canvas,.cropper-crop-box,.cropper-drag-box,.cropper-modal,.cropper-wrap-box{bottom:0;left:0;position:absolute;right:0;top:0}.cropper-canvas,.cropper-wrap-box{overflow:hidden}.cropper-drag-box{background-color:#fff;opacity:0}.cropper-modal{background-color:#000;opacity:.5}.cropper-view-box{display:block;height:100%;outline:#39f solid 1px;overflow:hidden;width:100%}.cropper-dashed{border:0 dashed #eee;display:block;opacity:.5;position:absolute}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\14.2ec136e8a48c6b3f9416[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):	4299
Entropy (8bit):	5.414203703723618
Encrypted:	false
SSDEEP:	48:lD58SOLNqJrY4nDa9G08Y0nfGJtKwVzKc6R8aBabLD1wmYT7D0+l/Gqv3/wAgPAS:QN6DB2tKA4abvNYw+l/GlRoohdJ8DSN
MD5:	3E92E103CFCA77F19512F7F3A3B4E983
SHA1:	31ECF4F9339AB809C5B9AF4B6542F9E5C5C7537A
SHA-256:	A2D6C3F2746CC05938B09983DA239FD913ADA43EF378484B7D294717ECA19FF9
SHA-512:	669F18BBC7D58CE33B102C9E672CE6533A82317D7A7AFF113B97DF0924FFC663EF98BDCEBD37ED8829BBB88F667881A8FC683E0D93D58A396648D0999E7819E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\14.2ec136e8a48c6b3f9416[1].js	
IE Cache URL:	http://https://risefundraiser.com/14.2ec136e8a48c6b3f9416.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[14],{edbG:function(a,d,p){"use strict";p.r(d),p.d(d,"CreateCampaignModuleNgFactory",function(){return fa});var m=p("CcnG"),o=p("o0FY"),e=p("pMnS"),c=p("Xg1U"),n=p("atuK"),t=p("iutN"),r=p("ES0t"),i=p("z5nN"),C=p("SfUx"),R=p("54hb"),l=p("rEId"),b=p("brvc"),u=p("yOyS"),A=p("EgHg"),f=p("IzQX"),s=p("vLZ9"),N=p("1ntt"),L=p("WCjn"),E=p("Ip0R"),g=p("gIcY"),h=p("p4DR"),v=p("9bPP"),y=p("dXze"),M=p("eajB"),w=p("NJnL"),I=p("lqqz"),D=p("ARl4"),F=p("xtZt"),_=p("fHIT"),T=p("OZfm"),O=p("DQlY"),S=p("YAQW"),P=p("rhjU"),Z=p("ETNk"),k=p("yEXN"),U=p("KKpL"),z=p("t/Na"),H=p("m+5+"),Q=p("ZYCi"),j=p("sDE+"),G=p("IyfZ"),K=p("sWsQ"),X=p("AiR7"),Y=p("+xv6"),x=p("ctsa"),J=p("A+LG"),W=p("kO4o"),q=p("l5Q0"),B=p("nf2m"),V=p("wT8T"),$=p("yD1i"),aa=p("9EwZ"),da=p("AS82"),pa=p("t1w2"),ma=p("LeXK"),oa=p("6Q8y"),ea=p("WH67"),ca=p("uOf+"),na=p("dU8u"),ta=p("iAsR"),ra=p("PCNd"),ia=p("gsdd"),Ca=p("0tKZ"),Ra=p("n4xA"),la=p("FcNq"),ba=p("5M9k"),ua=p("/Jor"),Aa=p("S/oi"),fa=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\2126210880948599[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	260087
Entropy (8bit):	5.469219756242312
Encrypted:	false
SSDEEP:	6144:Rk1HgCSntDV/HaK3V/Ha8NEPjQHguH3HpQrwzzmy:dNESh
MD5:	AE4DA01D599640A4F84724E8CB5C890E
SHA1:	12FD721F9A99A063BFE2419CDFFBF48A95DED5B1
SHA-256:	8D4A8EF94E0F6FED90678AC8974450340DDAAE87E74003A774EF518C1A109C4D
SHA-512:	8AE3F7781E73A40D7F96743FBBD546EA952A1096E576F8BB26F1E11CF0C00ED3555639AD5FA3F41A7F07E200BCA6B1D0B5C0493B134131FCF677237F85400115
Malicious:	false
Reputation:	low
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\7.e3eae7715a1007e2167a[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):	1184156
Entropy (8bit):	5.2861856260380495
Encrypted:	false
SSDEEP:	24576:9PfC5Dp/S5O/T5htcPgOQy5vYQV5fnJRpdRi+xgSdww8L/d5Z/Q5brN2HL/x5p/P:9PfC5Dp/S5O/T5htcPgOQy5vYQV5fnJS
MD5:	7B4A071FDED67BA056AB3EA2DD656F28
SHA1:	776C8ED313535BF0224485B060598508C2617D7F
SHA-256:	D975085BF84CEE9D6FCF995615E578F114278EFA8D3ADC47F6E74F43D10B1EBA
SHA-512:	EC3BF0445B46E8DA33EC922A92B2D0F54C6B088D1A225140E12799223C91B19CBF0E09B408F4D16530833D7B6414CB22D75F298402C494607D6184AA92E37F6D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://risefundraiser.com/7.e3eae7715a1007e2167a.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[7],{"/7p0":function(n,l,e){"use strict";var t=e("CcnG"),u=e("Ip0R"),a=e("0Ef4"),i=e("DvhZ"),o=e("6dFk"),c=e("DxRy"),r=e("tO/L"),s=e("ZYCi"),d=e("8j1u"),p=e("4ikF"),m=e("hokr"),g=e("ZfHp"),f=e("sDE+"),h=e("/NYq"),v=e("LNqW"),C=e("mZsc"),I=e("3hWu"),b=e("2hNF"),x=e("sbQS"),D=e("m+5+");e.d(l,"b",function(){return w}),e.d(l,"c",function(){return K}),e.d(l,"a",function(){return Z});var w=t["\u0275crt"]({encapsulation:0,styles:[[".unity-view-all[_ngcontent-%COMP%]{font-family:Gibson-SemiBold,arial,sans-serif;font-size:13px;letter-spacing:0;text-align:center;color:#475059;text-transform:uppercase}.unity-count[_ngcontent-%COMP%]{font-size:16px;font-family:Gibson-Light,arial,sans-serif;line-height:30px;letter-spacing:2px;text-align:left;color:#2b2d3c}.unity-h1[_ngcontent-%COMP%]{font-family:Gibson-SemiBold,arial,sans-serif;font-size:36px;line-height:.97;letter-spacing:0;text-align:left;color:#2b2d3c;text-transform:capitalize}.unite-h2[_ngcont

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\RG-FoundationYoutubeProfile[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, 200x200, frames 3
Category:	downloaded
Size (bytes):	4185
Entropy (8bit):	7.749989778896806
Encrypted:	false
SSDEEP:	96:xW9NIMYevAODnWUuQDgQp7wkEf9tz5xWRRqXKt+585R2m:e3Z4sWUTDgQBwhV1XKx1
MD5:	513E3901D2C8FEA9F3F113A02AF3A1DB
SHA1:	10E907BE368B69B925DCA74D929A82E6138E94A1
SHA-256:	D12413B19C3157EFBFEFBFD3CB05EBE8EECF4DFEC83C5E92A5D0691F59FF994E
SHA-512:	4A52CDC46D920FABFCB3921E0E29036BEFCB28DD81D27CE9BDC249A9101237C4F174113DAAFD05DE3D85866A1AF2A4248E640FF09F48F28797522AC1D461EE7
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\RG-FoundationYoutubeProfile[1].jpg	
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/media/17437/RG-FoundationYoutubeProfile.jpg
Preview:	......JFIF.....C.....%...#... , #&')*)..-0-(0%()(...C.....(...((((((

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\create[1].htm	
Reputation:	low
Preview:	<!DOCTYPE html>.<html lang="en">..<head>. <meta http-equiv="Content-type" content="text/html; charset=utf-8" />. <meta http-equiv="X-UA-Compatible" content="ie=edge">. <meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate">. <meta http-equiv="Pragma" content="no-cache">. <meta http-equiv="Expires" content="0">. <meta name="fragment" content="!" />. <meta name="viewport" content="width=device-width, initial-scale=1.0, minimum-scale=1.0, maximum-scale=1.0, user-scalable=no">.. <link href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" rel="stylesheet">. <link href="https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css" rel="stylesheet" />. <link href="https://cdnjs.cloudflare.com/ajax/libs/OwlCarousel2/2.1.6/assets/owl.carousel.min.css" rel="stylesheet" />. <link href="https://cdn.quilljs.com/1.2.2/quill.snow.css" rel="stylesheet">. <link href="https://cdn.quilljs.com/1.2.2/quill.bub

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\fontawesome-webfont[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), FontAwesome family
Category:	downloaded
Size (bytes):	165742
Entropy (8bit):	6.705073372195656
Encrypted:	false
SSDEEP:	3072:qbhEnD+IzsU9z9QJ6/P3Xe2iEiEPGFCMW1JVJG6wVTDsk6BmG6S1yKshojskO+b2:qenD+IzsU9z9QJ6/PO2FiEP2C/DVJG6I
MD5:	674F50D287A8C48DC19BA404D20FE713
SHA1:	D980C2CE873DC43AF460D4D572D441304499F400
SHA-256:	7BFCAB6DB99D5CFBF1705CA0536DDC78585432CC5FA41BBD7AD0F009033B2979
SHA-512:	C160D3D77E67EFF986043461693B2A831E1175F579490D7F0B411005EA81BD4F5850FF534F6721B727C002973F3F9027EA960FAC4317D37DB1D4CB53EC9D343A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/fonts/fontawesome-webfont.eot?
Preview:	n.....LP.....Yx.....F.o.n.t.A.w.e.s.o.m.e.....R.e.g.u.l.a.r...$.V.e.r.s.i.o.n. .4...7...0. .2.0.1.6.....F.o.n.t.A.w.e.s.o.m.e.....PFFTMk.G.....GDEF.....p... OS/2.2z@...X...`cmap..:.....gasp.....h....glyf...M.....L.head...-.....6hhea.....$hmtxEy.....loca...\.....maxp.,.....8... name....gh....post.....k....u.....xY_.<.....3.2.....3.2.....'.....@.....i.....3.....3...s.....pyrs.@. ....p.....U.....].....y...n.....2.....@.....z.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\help-india-fight-covid-19-donate-for-oxygen[1].htm	
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):	748
Entropy (8bit):	5.022483032586562
Encrypted:	false
SSDEEP:	12:YWyb5EGGi6BOVMNPBFRLZJp7GMxPWPD3RLZJp7GM4tPD3RLZJp7GMpdpVfkCKBY8:Yt5E9pLVKIqBLVKtBLVKCkCKSF4
MD5:	4462F1E77507365714C59D8661420218
SHA1:	9410BBCE02D966274428C8CF49CF8E3F0EDBBCBC
SHA-256:	4192117ED03F25BDCDC9B8684ABECAB6690CC6502515B54390F26137D154F393
SHA-512:	B81B17C9D0B5F7312066464C9769F0E0C69F2F47F7F588CBF1DA9869F13F4DA111B27537E1A884AEC4C2F34E4ACFD04FBB5A8B5FDAEDE815D58B514246EFEE8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://risefundraiser.com/fundraising-api/public/api/1.0/template/campaign/help-india-fight-covid-19-donate-for-oxygen
Preview:	{"status":true,"data":{"id":1,"name":"unite","displayName":"Unite","tabs":{"campaign":{"embed":"EMBED NOW","campaign":"CAMPAIGN","updates":"UPDATES","documents":"DOCUMENTS","faq":"FAQ","sponsors":"SPONSORS","events":"EVENTS","story":"STORY"},"chapter":{"campaign":"WHY THIS","updates":"UPDATES","documents":"DOCUMENTS","faq":"FAQ","sponsors":"SPONSORS","events":"EVENTS","story":"STORY"},"champion":{"campaign":"WHY THIS","updates":"UPDATES","documents":"DOCUMENTS","faq":"FAQ","sponsors":"SPONSORS","events":"EVENTS","story":"STORY"}},"summary":"New Campaign Template","thumbnail":"https:\/\/dqy0ngl1d5798.cloudfront.net\/assets\/images\/campaign\/unite\/unite.jpg","preview":"","path":null,"type":"fundraising","version":"1.0"},"errorCode":10000}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\help-india-fight-covid-19-donate-for-oxygen[2].htm	
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):	3090
Entropy (8bit):	5.0683789310705585
Encrypted:	false
SSDEEP:	48:YtCxOABCOsTTHG7hsDOA5COs1ZsDOAuCOsN3zSOAyCOsJokTlp5sSOA1+COs6PPA:IUVto99m360/Td12tuPUzrk
MD5:	7AA9341861D9D44D56551FEEB7366257
SHA1:	C43B293106C61D88658E72119105D45BAA1A0803
SHA-256:	E2C198778D5D68F11B07BCF16F598A967B41EFC34839679728654F9FB4896792
SHA-512:	9FA11408907EFD5B687752F92AE0078B483D313B7B58F30C4B70430F3E8B2693CC2BE1328A0F8522313E5FF104213D580640B1D8A7EB829B6954DE473F6AFB68
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\help-india-fight-covid-19-donate-for-oxygen[2].htm	
Preview:	{"status":true,"data":{"count":6,"entities":[{"id":354866,"donations":"2000.00","anonymous":false,"hideName":false,"hideAmount":false,"comment":null,"donationDate":"2021-05-20 07:01:50","currency":"INR","orgId":null,"OrgName":null,"giftId":null,"giftName":null,"campaignId":1749,"campaignName":"Edifecs: Help India Fight COVID-19 For Oxygen","chapterId":2626,"chapterName":"__default","championId":0,"championName":null,"firstName":"Ankur","lastName":"Chander","user":{"id":37624,"name":"Ankur Chander","email":"ankur.chander@edifecs.com","avatar":"https:\/\/dqy0ngl1d5798.cloudfront.net\/media\/17142\/2020-01-23_22-57-36.jpg"}},{"id":354867,"donations":"1000.00","anonymous":false,"hideName":false,"hideAmount":false,"comment":null,"donationDate":"2021-05-20 08:55:16","currency":"INR","orgId":null,"OrgName":null,"giftId":null,"giftName":null,"campaignId":1749,"campaignName":"Edifecs: Help India Fight COVID-19 For Oxygen","chapterId":2626,"chapterName":"__default","championId":null,"championNam

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	85659
Entropy (8bit):	5.366267621178451
Encrypted:	false
SSDEEP:	1536:MYE1JVoiB9JqZdXXe2pD3PgoIiulrUndZ6a4tfOi79xfWBZ+Bjda4w9W3qG9a986:n4J+OlfOM9xrCW6G9a98Hr2
MD5:	33CABFA15C1060AAA3D207C653AFB1EE
SHA1:	E3DBB65F2B541D842B50D37304B0102A2D5F2387
SHA-256:	6B6DE0D4DB7876D1183A3EDB47EBD3BBBF93F153F5DE1BA66450493486281O9A
SHA-512:	48568D6F7C42D3C93F59FE8244CD49F8EFEFBF8616CAB3C149DCB4A3ED67A8ACDFFAE2EB2019DA7A8F1A62800039DDF59CC347C17F33C15C1331B6C226303 2A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/jquery/2.2.3/jquery.min.js
Preview:	/*! jQuery v2.2.3 | (c) jQuery Foundation | jquery.org/license */!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="2.2.3",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?0>a?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,function(b,c){return a.call

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\leftArrow[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 128 x 87, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1257
Entropy (8bit):	5.982497977529783
Encrypted:	false
SSDEEP:	12:6v/7gy3gH22kfXhl/72KV5YUbLerMh7zxkMiJOWK6+RBbtDit83KsNOhttgDDale:qgH4xl/RLXViMiJ/atZkcKsNQSDCl
MD5:	3E17B647B666C1CC32D5A9129DF3EBC1
SHA1:	1051DBEC03BB54D05DE1E28A963D8565DFE56A5A
SHA-256:	B65110C1AD2C6331645F12186DECF9F3E9717ADB6266FB60C8CA81B250DA8FFB
SHA-512:	4F69C2588167336B90AF84957B41AD16B7A6EB07E71BDCC8DA3D30D97264CF47E8559F2238856693809C155DF34A1F22ECD6D16B56082F8C2CDA771D905E735
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/assets/images/leftArrow.png
Preview:	.PNG.....IHDR.....W.....n....PLTE..... .....mp....tRNS..... !#%&'()*,-/02578;>ADGHIKNOQRSUVY]abceimquvz}~.....mIDATh...R.a...MB/...AB@....&..&]. ..#..4%.d.....~..p.3.....$.r.....s8..g..e<..R.3.Y~....$....W..}.pq.0%.....'..v-~...wD...%.].....G?....[L....zL.G.o....c....]..W....._...'../.....R...s.....D.~...w.....~...1.~?.....X...!._.....{.....g.....3.n#.....e.....K....?.....;.!.w..#..W.S..U....3r..N...{a.;.....B.o....H.u.K.,..d....Q..)8...x.A|RE)h.G.i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 320 x 29, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	7017
Entropy (8bit):	7.938025060960611
Encrypted:	false
SSDEEP:	96:gkndil8HPNG8ApJgRG0TBsD4Lp8mwBoUkHpYgDicUVPVd734VEyD2tp0YjW/uILY:Pndil8vWpy049CB6OgdMD4VFD2lWu9
MD5:	37757573A86E0D9806E2026E5AD0ED98
SHA1:	F7F1401D4A1A1C59B9273D0D2CD99DEB8E12D700
SHA-256:	E233C0A97EB72959AB358ED12E6AD2AC1C844714DF3C65BC2A453F0FDEB516CE
SHA-512:	26C569182D3AAB26912CFFE89BDDACB6FBABB658D428F3FE7758754486B606823BBC1D1761E4B42319C133287DE9067B3A5325D3081BD064610FB145215BA4A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/assets/images/logo.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\logo[1].png	
Preview:	.PNG.....IHDR...@.....7....gAMA.....a.... cHRM..z&.....u0...`..:....p..Q<....bKGD.....pHYs...#...#.x.?v....tIME.....,R?.....XIDATx..y.]U.....K.&...Kd....D.".1.. .G..."...3..6.Q.aT@tP.E.D.....b...8l.I.....Y:..w._U..N...n.....w.Y....SU.6.....M.....G..B..P.J.....Y...$S.LNg...L.29..N...1.M....-.i..IsKk..i\.H..(.....Z.....c.'|r:..kMh.....-.. V\>.Mp\+C).6O....<..F`.!.\....X.w....7+8...~3.c...b..V...E.<.8=./.r..g.....Do.|...C9g..~o.....H.....&cT.....<f..M.by..K..&...G...7....i.....F(.5.7....?....5....tDx...f.h...]E.{./.....%.... .....A.....\.&.....{....k[...A...<.|.. p...F./O..dG..`...`.....'.T.....b...._...<.h.....lfM...l...6..!/k.!.k0p]S..}...X.l..e..".r}.t.x^y....G...o.....f..&.|..;..<u.....0.i.Nl.....}'..)....W..K.N.L.S.L.x."`h(.."... ..[.....0p..I.M..V!.....z.0(.4T.....(Dm....s..y...}7.....n....C.Q./....0v.....y.2.."Y...z.T.g9.....|/.....U%."Y..*R-?....n...u.....PH....E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\no-user[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 200 x 200, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	7627
Entropy (8bit):	7.96123786545665
Encrypted:	false
SSDEEP:	192:nPbEMDuTO2meovHkc+tZLII+CBlkjVSDS6htOzPlZ+Jzz60OM5:ndDoXPovR+PLII+AlqASXjn+40OE
MD5:	EE262C61148B2CFAF2D98E2116260913
SHA1:	BF866FE9AD1188D2EC88019E157D199EEA4CBC29
SHA-256:	2295CD1857C674138B50309846EA160191F9CC958CCE71E862F0B471A400D3F8
SHA-512:	2AB8A0CEB9E0B32D794DBD27B0FFD93717768927F8137363B6A9EECDE6F7373AEE8C5DBF38EA0BA55B94C6913DA908C1CE9AA6A2EE35D311717810B55D004E 68
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/assets/images/no-user.png
Preview:	.PNG.....IHDR.....":9.....IDATx^..!.. ..A....o 9..E..Q..;.....BX.....a!,...BX ,..9.....I..v..gZ.s..;..8.k.....r.H.Hm..[Nl.../.....uo..|. 7H|o.o..J.lq_f.z...,.G.DRT.3.GT...$f..>...*2.... 8.....c.}.p....S&...f8f.....c..0..@H?. .O.i>#K..QY5"...A..|..~...h.EF&. ~p..i.$.dj..!B.iP.eb...Q~.....Q.h*UU.....y..2B8...oUU-.&..o.^fYbM.....8..!.|.s....p....v!J...t;.^?....4..r%.rff vzz*...w..V+.9.9.ih.[a..|.....&...#..*WW.e.E..."`R.s.sv"666...xYp.q.1..&....i..jM....3./^..n.....e...Cl.o.....{.+..d.1.....A...C.{ooo}}.....C2...P...0.v.&....[].5Z.....%.8TZ.G.A. .1#.qB&...,Wr.n..B[!...f.....u][.3.Q. .....W .....k./0.4....].r../..g....DZiM.\..2..DbYia....VWW_.z...!.#...G./.D...j.HJ.$.m....]]^^FE2..=.J.a.$V5....1.0.V"Py.. ..@.M.`..T.;...b..~7.'n!,... Wkk....7n.~....." .X"H.ew.8@w.t,.....?.|.R.'..84L.4...@.i.{.3..x.j.K.hcc.e..YN..P.VV...T...+H..!a#.....mm.....~F.{.I.:...G.6....[a...n.._.v..-,0...B.I...z..Xg..XD).....R.?_[[...s.U8.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\notification[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	9071
Entropy (8bit):	4.94862352509096
Encrypted:	false
SSDEEP:	192:LyAEQmFHFlHWjmRjLd0gpKQKdFr0y0Fo0l2P3OOv84aTmdZAckyFrJqyJhSgOIte:LxEQallHrBjSSFHJT4ZjGrxN8bfM
MD5:	2A5CEF0817081FC6AD1909B62ACD9919
SHA1:	B005FD522AD71CCADCBFE240599389ACA8BECDCA
SHA-256:	B6F1F3701DC121B979E593EBD27D71CDDD16BDECFB3FEDD70C7ADB5F2D0BA3F3
SHA-512:	B26C4C7F146FC8CC2BDD1BFBB1FA5085BE540A9299B592375BE1D5E60D75807E0768FD76BA41FEF1B1A0B74EE88582833C63EF6852C4A48C952504C453EB9EF 3
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html lang="en">..<head>. <meta http-equiv="Content-type" content="text/html; charset=utf-8" />. <meta http-equiv="X-UA-Compatible" conten t="ie=edge">. <meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate">. <meta http-equiv="Pragma" content="no-cache">. <meta http-equiv="Expires" content="0">. <meta name="fragment" content="!" />. <meta name="viewport" content="width=device-width, initial-scale=1.0, minimum-scale=1.0, maximum-scale=1.0, user-scalable=no">.. <link href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" rel="stylesheet">. <link href="https ://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css" rel="stylesheet" />. <link href="https://cdnjs.cloudflare.com/ajax/libs/OwlCarousel2/ 2.1.6/assets/owl.carousel.min.css" rel="stylesheet" />. <link href="https://cdn.quilljs.com/1.2.2/quill.snow.css" rel="stylesheet">. <link href="https://cdn.quilljs.com/1.2.2 /quill.bub

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\orgs[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	9071
Entropy (8bit):	4.94862352509096
Encrypted:	false
SSDEEP:	192:LyAEQmFHFlHWjmRjLd0gpKQKdFr0y0Fo0l2P3OOv84aTmdZAckyFrJqyJhSgOIte:LxEQallHrBjSSFHJT4ZjGrxN8bfM
MD5:	2A5CEF0817081FC6AD1909B62ACD9919
SHA1:	B005FD522AD71CCADCBFE240599389ACA8BECDCA
SHA-256:	B6F1F3701DC121B979E593EBD27D71CDDD16BDECFB3FEDD70C7ADB5F2D0BA3F3
SHA-512:	B26C4C7F146FC8CC2BDD1BFBB1FA5085BE540A9299B592375BE1D5E60D75807E0768FD76BA41FEF1B1A0B74EE88582833C63EF6852C4A48C952504C453EB9EF 3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\orgs[1].htm	
Preview:	<!DOCTYPE html>.<html lang="en">..<head>. <meta http-equiv="Content-type" content="text/html; charset=utf-8" />. <meta http-equiv="X-UA-Compatible" content="ie=edge">. <meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate">. <meta http-equiv="Pragma" content="no-cache">. <meta http-equiv="Expires" content="0">. <meta name="fragment" content="!" />. <meta name="viewport" content="width=device-width, initial-scale=1.0, minimum-scale=1.0, maximum-scale=1.0, user-scalable=no">.. <link href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" rel="stylesheet">. <link href="https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css" rel="stylesheet" />. <link href="https://cdnjs.cloudflare.com/ajax/libs/OwlCarousel2/2.1.6/assets/owl.carousel.min.css" rel="stylesheet" />. <link href="https://cdn.quilljs.com/1.2.2/quill.snow.css" rel="stylesheet">. <link href="https://cdn.quilljs.com/1.2.2/quill.bub

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\owl.carousel.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2763
Entropy (8bit):	4.887850519060259
Encrypted:	false
SSDEEP:	48:u1F8GL+IJWmQq+opeju+zY/+wl+weizFsAvqeQXoHHy3Vc9oRvfdflHbiutTYj1K:1Xw6ei1DEn7pxaIJICNMM
MD5:	61847D9B7353713B59DA014C409CFE6E
SHA1:	7AF97410BEF0C5CF04044AE95256714E4DDD9E29
SHA-256:	3B794F3708960B080C92F863E8936343433D11BCAB48CC68A834E970A394C47E
SHA-512:	CD979A386048369678D2C7F4BD25C31EEAC2E1EB8C212BCAFAA13185D7683EB36E89B7FA686F5899CAE63DB94569AA1AB3C32D6CD8D7E583897EDE433A84D3F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/OwlCarousel2/2.1.6/assets/owl.carousel.min.css
Preview:	/**. * Owl Carousel v2.1.6. * Copyright 2013-2016 David Deutsch. * Licensed under MIT (https://github.com/OwlCarousel2/OwlCarousel2/blob/master/LICENSE). */..owl-carousel,.owl-carousel .owl-item{-webkit-tap-highlight-color:transparent;position:relative}.owl-carousel{display:none;width:100%;z-index:1}.owl-carousel .owl-stage{position:relative;-ms-touch-action:pan-Y}.owl-carousel .owl-stage:after{content:".";display:block;clear:both;visibility:hidden;line-height:0;height:0}.owl-carousel .owl-stage-outer{position:relative;overflow:hidden;-webkit-transform:translate3d(0,0,0)}.owl-carousel .owl-item{min-height:1px;float:left;-webkit-backface-visibility:hidden;-webkit-touch-callout:none}.owl-carousel .owl-item img{display:block;width:100%;-webkit-transform-style:preserve-3d}.owl-carousel .owl-dots.disabled,.owl-carousel .owl-nav.disabled{display:none}.owl-carousel .owl-dot,.owl-carousel .owl-nav .owl-next,.owl-carousel .owl-nav .owl-prev{cursor:pointer;cursor:hand;-webkit-user-select:none;-k

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\quill.bubble[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	23796
Entropy (8bit):	4.868625793155267
Encrypted:	false
SSDEEP:	384:OXa6h8sJ1vOUrxTg2QKtDMObtfFKM6gb1md9x+OdFrF4FrFJOhFW88csUk4j/q:OXZh8PUrxTg2QKtDMObtfFKM6gb1md98
MD5:	BF72827F7B8BA905583BB96B3CBCECFA
SHA1:	CC207D56A87886E74E83256F9C59DD053A6749BA
SHA-256:	588FC4B888D104066129BB5DB7A43B9A3518A80A79FF12055EFBCDE6FE212B56
SHA-512:	5904E92F9D446ACE15AD200818FB1B132A01E5487C48BEF5ACEDF9C869652736B1BAF3F42D007ADF424160A239752C547432CFE14607D155D9F040A238F56A70
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.quilljs.com/1.2.2/quill.bubble.css
Preview:	/*!. * Quill Editor v1.2.2. * https://quilljs.com/. * Copyright (c) 2014, Jason Chen. * Copyright (c) 2013, salesforce.com. */..ql-container {. box-sizing: border-box;. font-family: Helvetica, Arial, sans-serif;. font-size: 13px;. height: 100%;. margin: 0px;. position: relative;.}..ql-container.ql-disabled .ql-tooltip {. visibility: hidden;.}..ql-container.ql-disabled .ql-editor ul[data-checked] > li::before {. pointer-events: none;.}..ql-clipboard {. left: -100000px;. height: 1px;. overflow-y: hidden;. position: absolute;. top: 50%;.}..ql-clipboard p {. margin: 0;. padding: 0;.}..ql-editor {. box-sizing: border-box;. cursor: text;. line-height: 1.42;. height: 100%;. outline: none;. overflow-y: auto;. padding: 12px 15px;. tab-size: 4;. -moz-tab-size: 4;. text-align: left;. white-space: pre-wrap;. word-wrap: break-word;.}..ql-editor p,..ql-editor ol,..ql-editor ul,..ql-editor pre,..ql-editor blockquote,..ql-editor h1,..ql-editor h2,..ql-editor h3,..ql-editor h

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\scripts.d004d92bf73ccd662204[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):	77938
Entropy (8bit):	5.16658993245112
Encrypted:	false
SSDEEP:	1536:Tn0HMF9UzZvtpVfg7gtlcd+xY+JrZ2i8btJ:T+zZ1rvc+JrZ2p
MD5:	20E3AD8573552DC6216513076660AE02
SHA1:	A6986325320D54162B1164D3F0A39ABBC6619FA3
SHA-256:	7FC07124DFC5B6E5C0F8E420286BACEBD05317632F569FC89EB887FA4D2A20D5
SHA-512:	CE082B5C45181B112482C3F341DDAF4AE0896EDE7E1E67F29DECA0B7F500254934AB8E42E0AB24D556DD3FB9EE696FC3265AA97C7FC77DCAADF81261C447BF4
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\scripts.d004d92bf73ccd662204[1].js	
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/1.9.7_P9_patch2/scripts.d004d92bf73ccd662204.js
Preview:	!function(t,e,i,s){function n(e,i){this.settings=null,this.options=t.extend({},n.Defaults,i),this.$element=t(e),this._handlers={},this._plugins={},this._supress={},this._current=null,this._speed=null,this._coordinates=[],this._breakpoint=null,this._width=null,this._items=[],this._clones=[],this._mergers=[],this._widths=[],this._invalidated={},this._pipe=[],this._drag={time:null,target:null,pointer:null,stage:{start:null,current:null},direction:null},this._states={current:{},tags:{initializing:["busy"],animating:["busy"],dragging:["interacting"]}},t.each(["onResize","onThrottledResize"],t.proxy(function(e,i){this._handlers[i]=t.proxy(this[i],this)},this)),t.each(n.Plugins,t.proxy(function(t,e){this._plugins[t.charAt(0).toLowerCase()+t.slice(1)]=new e(this)},this)),t.each(n.Workers,t.proxy(function(e,i){this._pipe.push({filter:i.filter,run:t.proxy(i.run,this)})},this)),this.setup(),this.initialize()}n.Defaults={items:3,loop:!1,center:!1,rewind:!1,mouseDrag:!0,touchDrag:!0,pullDrag:!0,fre

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\tenant[1].htm	
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):	25841
Entropy (8bit):	5.981757434662876
Encrypted:	false
SSDEEP:	768:lJPKIuTDlh1nuQqatYt7olp5lVch2QZeX+c6nJ:DvqaW7olp5lVepZW+c6nJ
MD5:	C2336E16B9A28A26B02A159709285AEE
SHA1:	42BCB6B3FEABB9DA0E9A3D494B2FAFC15998CF00
SHA-256:	7F846B5EFA0FE287C4D6CDFD887F9EEC4742381181AF689CF16155C97D15C852
SHA-512:	E2C2A13F8803B9548942B71DC615F287A6EA75BCD9F8ADF3A2000471E2B875CA6FC22699090414AE6F5F9F899E1088EBBE7CE60BBC7CE41203FBB1850D5DA40B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://risefundraiser.com/fundraising-api/public/api/1.0/tenant?id=https://risefundraiser.com/
Preview:	{"status":true,"data":{"id":1,"creationDate":"2017-01-17 09:49:39","name":"default","url":"https:\/\/risefundraiser.com\/","brandingProperties":{"header":{"logo":"https:\/\/dqy0ngl1d5798.cloudfront.net\/assets\/images\/logo.png","logo_mobile":"","title":"RoundGlass Rise | Fundraiser","description":"Social enterprise platform empowering mission-driven organizations to grow and scale. Rise tools help Non-profits fundraise, improve efficiency, grow their supporter base and engage with the community ","keywords":"Online fundraising, Free online fundraising, Risefundraiser, Roundglass, Fundraising campaigns","links":{"forNonProfit":true,"pricing":true,"campaigns":true,"newCampaign":true,"organization":true,"newOrganization":false},"useNavigationLinks":"custom","logoRedirectUrl":""},"colorClass":"jamTheme","colorCode":"","footer":{"logo":"https:\/\/dqy0ngl1d5798.cloudfront.net\/assets\/images\/rg-logo.png","company_name":"RoundGlass Rise | Fundraiser","company_description":"Social enterprise

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\v2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	578850
Entropy (8bit):	5.90527580429016
Encrypted:	false
SSDEEP:	6144:OA1FlLyIvG0FRyJkdG9+r90fuR8rV/0Ty/Jodl6q0+T6jxcbs6:ZRU0XCkdG9g0fuR8rV/0MR+T/
MD5:	F01130E2D2ED0B752B178AE3428286FA
SHA1:	B076703BB26B62AAAE800B470C1841ADE1B24B91
SHA-256:	C93BEA6EB2C5CD796052D336D8F42741459817D0D02BA2C279B0A88691AE8190
SHA-512:	EE6C2032F16A1B24BCAEAA464BD7A946E2901CB223E88AAA9C45FD17DB351A0C4A72898607BC73410DC58D672A9040B10E9642CB225239EFACC79FFB8904DC60
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://js.hsforms.net/forms/v2.js
Preview:	window.hubspot=window.hubspot||{};window.hubspot.formsnext=window.hubspot.formsnext||{};window.hubspot.formsnext.version="FormsNext-static";void 0===window.hbspt&&(window.hbspt={});void 0===window.hbspt.forms&&(window.hbspt.forms={});void 0===window.hbspt.forms.deps&&(window.hbspt.forms.deps={});window.__hsRoot={globals:["reqwest","React","ReactDOM","I18n","Pikaday","Promise","require","requirejs","define","exports","module","bootstrap"],saveGlobal:function(e){void 0===window.hspreserve&&(window.hspreserve={});if(void 0!==window[e]){window.hspreserve[e]=window[e];window[e]=void 0}},restoreGlobal:function(e){window.hbspt.forms.deps[e]=window[e];window[e]=window.hspreserve[e]}};!function(){for(var e=0;e<window.__hsRoot.globals.length;e++)window.__hsRoot.saveGlobal(window.__hsRoot.globals[e])}();!function(){window.hbspt.forms.deps.React?this.React=window.hbspt.forms.deps.React:function(e){if("object"==typeof exports&&"undefined"!=typeof module)module.exports=e();else if("function"==typeof

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\vendor.7b1b41a937a083fd16b0[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):	1899004
Entropy (8bit):	5.4539955915716805
Encrypted:	false
SSDEEP:	24576:wEa3TSZWkcSO2dp7pl6niUWPQbLXxAhVuhX3uPW6HpOOK/aOqAFpGpGXQWy/GN7T:wEfuiUxu0qbGXOq7MfIF0vRcR
MD5:	C86E5AC192DD7863E71E6900DD48626E
SHA1:	9FB46A182EC58A16DEC1540EC49F18E88A86B0D3
SHA-256:	5AC5AACFB3040CEE52DF80CED8CBD3E0F6ACC34CA7025120FC641FC0CC79AF23

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\vendor.7b1b41a937a083fd16b0[1].js	
SHA-512:	A889939321296825FD7101EAB396E9CEE39C06C072B997C4C40064DE1D03ABEC81E597280CD43F24EE4DD536292206A8DAD69FC2B45AC642F61A9BBDDDA3ED DB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/1.9.7_P9_patch2/vendor.7b1b41a937a083fd16b0.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[25],{"+W7E":function(e,t,n){"use strict";var r=n("Q1FS"),i=n("mbIT"),o=n("pshJ"),a=n("q3Kh");t.fromEventPat tern=function e(t,n,s){return s?e(t,n).pipe(a.map(function(e){return i.isArray(e)?s.apply(void 0,e):s(e)})):new r.Observable(function(e){var r,i=function(){for(var t=[],n =0;n<arguments.length;n++)t[n]=arguments[n];return e.next(1===t.length?t[0]:t)};try{r=t(i)}catch(t){return void e.error(t)}if(o.isFunction(n))return function(){return n(i,r)}}}},"+Zhm":function(e,t,n){"use strict";var r=this&&this.__extends||function(){var e=function(t,n){return(e=Object.setPrototypeOf||{__proto__:[]}instanceof Array&&function(e,t) {e.__proto__=t}||function(e,t){for(var n in t)t.hasOwnProperty(n)&&(e[n]=t[n])})(t,n)};return function(t,n){function r(){this.constructor=t}e(t,n),t.prototype=null===n?Object.crea te(n):(r.prototype=n.prototype,new r)}}(),i=n("ds6q"),o=n("xHZb"),a=n("zB/H"),s=n("AFwO"),u=n("Mxlh"),l=n("FiyT");t.ReplaySubject=function(e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\verified[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 192 x 188, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	24667
Entropy (8bit):	7.962442179749081
Encrypted:	false
SSDEEP:	768:4/oe+OToeDgu5gfRKnqKMchsFbogG2oTN:ZekQgfRKn3xhsi52oTN
MD5:	857DF0AA759363E37FD9FA439513F2BD
SHA1:	FCDB2F20D9BDB6AE6F0962F83C13DE93ADBA8DAF
SHA-256:	DD81B41BFD3B51F117F403713469039311C3803F95ECE56673434EAB76542B89
SHA-512:	1DDEB0AD1E144CC784655322AD869D994C777C4D8C2BFB9DD296DF5E7779870F0153CB69F86236F938CF7A4EA78C97BC9D62875863664C09E2B7CF12670C8A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/assets/images/unite/verified.png
Preview:	.PNG.....IHDR.....<.....sRGB.....@.IDATx.....U..wf{I6m.CB.....v.c.\.aA...AQA./."EA.. *..E...."H...Z..BBz..3....yN.;;;..$.d.....9..9.9.y.*.f.Q ..J.,.JeKIWN.....".%8....y. W..../.W..$..f@.%..J.....}.@.(..=...Qf..Rrs.2.l..\l.....s.....[ZZ...F.3.G\1f(3.....z9..~....#.8..x..~i>y.d..m..fyb....L`$+....(..] a.....|...W..z....~....T .G..m~."..IF.g.2.....Pz.]+eo... ..z.>k.....@...6..S...10...#.....L.d.....c..W...?...?.....F..4_.jUM&3.{.t.Sp.5..uuuf..13.....f.../..rU..O.81..w.;.a.....m/....W.M..[....jj..TUU\;u\.}....fa.."f..K.fQ.`.W....e&.Q. ..2..A.b.w.').Qs..1.....e.Z...k..".=..*+...q#.>1vl.....).3..c3.O2..e3F.....OJ[d..z.Q...={.....+W.L#.....Huvv.V.....y..|\}:...PN.8.*R....p.....6n.....A.g\5Z.dI....1..v.....;6..P.4..%? ...I./U%..#.....G.X...I...]....=o...o..tW<:...o_....<..8OS.J=8ft.1..S.UUUY.....3..I...c....B.[..Yv.vH....1`.`l..:..t}..._.vm.UG*P..KJ.7UT4,_..S...._.?{...|.C..E.Is..n.p...w

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\2126210880948599[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	520174
Entropy (8bit):	5.469219756242312
Encrypted:	false
SSDEEP:	6144:Rk1HgCSntDV/HaK3V/Ha8NEPjQHguH3HpQrwzzmak1HgCSntDV/HaK3V/Ha8NEPC:dNESXNESh
MD5:	808520535955CC1E341511FF493C6704
SHA1:	0176C6F76E6EC2F308C4C561460FD5BC8ACD711F
SHA-256:	CD23C1588831E8E86CC4565585F2CCD769F38184C2A9DCEF5C6D8537F314021A
SHA-512:	661F13C40BC1BA634B16061E4F9EC0BA3D5D907F725F369B8510AA5FE0AB4F28DD173036100E081D3962BA7EAF16E040E588F3F8803B51359C7511E29FA362C2
Malicious:	false
Reputation:	low
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\Accepted[1].htm	
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):	19422
Entropy (8bit):	5.1843123997041145
Encrypted:	false
SSDEEP:	384:j1V/42msNhzfFN02La7f3ovx3jF2LF2LGc2Ly2L5:j1uKoVf3SWivO
MD5:	288E6EE8E808BD945E9A136FA7D8A308
SHA1:	91C4D08B6C6A4AC425CEE367B3ACD6C318093885
SHA-256:	5E51D0F93AB174017FD8F52F4846434180DC6DDC65F934C13AD0C7BE8B7907EC

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\Accepted[1].htm	
SHA-512:	41242BA0E9F8F06E02A78B9DD85B8BFB8EF812AFFAC5F32D3A33A77C09D016E82DCD69D7CFFB0A9A428A43C48F643369BEB48AB53481F509E1B8D4F6B36202E 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://risefundraiser.com/fundraising-api/public/api/1.0/paginated/nonprofits/Accepted?order=asc&sortBy=relevance&offSet=0&size=9
Preview:	{"status":true,"data":{"count":194,"entities":[{"id":"roundglass-foundation-usa","isLiked":null,"likes":0,"isSubscribed":false,"isSubscriberPending":false,"likeCount":0," orgType":"Non-Profit","selfPaymentGateway":false,"name":"RoundGlass Foundation USA","creationDate":"2020-04-07 07:09:19","slug":"roundglass-foundation-usa","abo ut":"<p>RoundGlass Foundation USA's relief fund donates money directly to the Community Foundation most active in the area impacted by the disaster. Community f oundations are uniquely position to act as effective managers of relief and recovery funding because they have strong connections with organizations, agencies, and outside groups that work in the area, and can assure that the money will be spent on the area of greatest need.<\/p><p>This Disaster Relief Fund uses the no-fee RiseF undraiser platform to ensure that the maximum amount of your donation will go to the people who need it most. Whenever possible, we find sponsors to defray the credit card fees to

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\Chart.bundle.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	201572
Entropy (8bit):	5.39163533494191
Encrypted:	false
SSDEEP:	1536:fXA4wIAGvktJH1QfemJPfsdld2LtXeJ/xqn3qJCuwM7c+M03o1KAyDjt2gyvbocG:fBrvsGZa3d4lqXHzVaL16fFGamKRhtZ
MD5:	658DCA7101C0E348DA6A8898F04A383F
SHA1:	37F92D10CDF56F5C78AFD05ABDB72F93EE8D2686
SHA-256:	54D6D7F4D8D03515BE064D361BF44EE968932AE867716238132ECB9126C4FB9B
SHA-512:	91DA46598E704BAC9372A2B1A3A735E3EE2793DF615854F04395ED4B210B271570A561F6DCC37CD224D5CE4320D63BF71596DD28F6C558BAFDF00034DFFCCFI 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/Chart.js/2.6.0/Chart.bundle.min.js
Preview:	/*!. * Chart.js. * http://chartjs.org/. * Version: 2.6.0. *. * Copyright 2017 Nick Downie. * Released under the MIT license. * https://github.com/chartjs/Chart.js/blob/ma ster/LICENSE.md. */.!function(t){if("object"==typeof exports&&"undefined"!=typeof module)module.exports=t();else if("function"==typeof define&&define.amd)define([],t);els e{var e;e="undefined"!=typeof window?window:"undefined"!=typeof global?global:"undefined"!=typeof self?self:this,e.Chart=t()}}(function(){var t;return function t(e,n,i){f unction a(o,s){if(!n[o]){if(!e[o]){var l="function"==typeof require&&require;if(!s&&l)return l(o,!0);if(r)return r(o,!0);var u=new Error("Cannot find module '"+o+"'");throw u.code= "MODULE_NOT_FOUND",u}var d=n[o]={exports:{}};e[o][0].call(d.exports,function(t){var n=e[o][1][t];return a(n?n:t)},d,d.exports,t,e,n,i)}return n[o].exports}for(var r="func tion"==typeof require&&require,o=0;o<i.length;o++)a(i[o]);return a}({1:[function(t,e,n){function i(t){if(t){var e=/^#([a-fA-F0-9]{3})$/,n=/^

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\analytics[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	49153
Entropy (8bit):	5.520906949461031
Encrypted:	false
SSDEEP:	768:/yR3fYFBLbfs5sP5XqY3TyPnHpl1WY3SoavFVv6PU+CgYUD0lgEw0stZM:/y9gZfl5h3UHpaY3SoRCw0sk
MD5:	6DF1787C4BE82D1BB24F8BFFA10C7738
SHA1:	3634E839429E462E49C5F42B75FBFB4BA318AF6D
SHA-256:	2CB09C7B3E19BFC41743CA3624EF81C3258D56525647FEAC76AA757E0292627A
SHA-512:	CB3CE2BCEB61F390298C21E470423CCEB6DD93E648A7DD0467195B11FEF30BF7A086DFF47C4494E2533498D1448C1A22AAB1414C14FD73278F1C92E0F7BC3F 4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google-analytics.com/analytics.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var n=this||self,p=function(a,b){a=a.split(".");var c=n;a[0]in c||"undefin ed"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===b?c=c[d]&&c[d]!==Object.prototype[d]?c[d]:c[d]={}:c[d]=b};var q= {},r=function(){q.TAGGING=q.TAGGING||[];q.TAGGING[1]=!0};var t=function(a,b){for(var c in b)b.hasOwnProperty(c)&&(a[c]=b[c])},v=function(a){for(var b in a)if(a. hasOwnProperty(b))return!0;return!1};var x=/^(?:(?:https?|mailto|ftp):|[^:/?#]*(?:[/?#]|$))/i;var y=window,z=document,A=function(a,b){z.addEventListener?z.addEventListene r(a,b,!1):z.attachEvent&&z.attachEvent("on"+a,b)};var B=/:[0-9]+$/,C=function(a,b,c){a=a.split("&");for(var d=0;d<a.length;d++){var e=a[d].split("=");if(decodeURIComponen t(e[0]).replace(/\+/g," ")===b)return b=e.slice(1).join("="),c?b:decodeURIComponent(b).replace(/\+/g," ")}},F=function(a,b){b&&(b=String(b).toLowerCase());if("p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\animate.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	52789
Entropy (8bit):	5.115740062849333
Encrypted:	false
SSDEEP:	768:KkZcIOlVjl2eIWInPywe1aAvkqDX3oyq5BrieD0OTbsysV:KkZ8Pywe1aAvkqDX3oyq5BrieD0OTq
MD5:	178B651958CEFF556CBC5F355E08BBF1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\animate.min[1].css	
SHA1:	97AFA151569F046B2E01F27C1871646E9CD87CAF
SHA-256:	8FE3FA119255ADB5E0C12479331F9E092E85BCFF56AB6ECC0510BFA2056B898D
SHA-512:	4F251A31B62B28565F41FA7EF67406384B7EBC6BB89CACCB93429A5779C589F2F72BC9FB9736FC0DAC93CCB38AD29372CF1189CC6452C3BF1EF31A89854449D D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/animate.css/3.5.2/animate.min.css
Preview:	@charset "UTF-8";../*!. * animate.css -http://daneden.me/animate. * Version - 3.5.1. * Licensed under the MIT license - http://opensource.org/licenses/MIT. *. * Copyright (c) 2016 Daniel Eden. */...animated{-webkit-animation-duration:1s;animation-duration:1s;-webkit-animation-fill-mode:both;animation-fill-mode:both}.animated.infinite{-webkit-animation-iteration-count:infinite;animation-iteration-count:infinite}.animated.hinge{-webkit-animation-duration:2s;animation-duration:2s}.animated.bounceIn,.animated.bounceOut,.animated.flipOutX,.animated.flipOutY{-webkit-animation-duration:.75s;animation-duration:.75s}@-webkit-keyframes bounce{0%,20%,53%,80%,to{-webkit-animation-timing-function:cubic-bezier(.215,.61,.355,1);animation-timing-function:cubic-bezier(.215,.61,.355,1);-webkit-transform:translateZ(0);transform:translateZ(0)}40%,43%{-webkit-transform:translate3d(0,-30px,0);transform:translate3d(0,-30px,0)}40%,43%,70%{-webkit-animation-timing-function:cubic-bezier(.755,.05,.855,.06);anima

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\campaign[1].htm	
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):	3456
Entropy (8bit):	4.500824822475747
Encrypted:	false
SSDEEP:	96:Iz8HlkoIcBMLQqPGNTXNUe80ql7M8+4sDAUNc0A2I1W+Oswgp:Iz8HlhBMLQqPGNTXie80ql7M8+4zUNct
MD5:	A2B7AE388BCF1BBB364A345F31013BC6
SHA1:	05D88AB7FD6996E815EA555F8EA33689591138F5
SHA-256:	80E7851E13A7E1A92B6C2790EB09220683D13A587C55C3BD1555D18F0B4CBF14
SHA-512:	CC586B68608AC8A5417BCDF10537465884F6E3E95880C537B4D456FE2206229DCDDEC7AFCCFCBD6836A8B72283ED3955BFCD77E2FBFACA14AB0533CB2B719 CD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://risefundraiser.com/fundraising-api/public/api/1.0/categories/campaign
Preview:	{"status":true,"data":{"count":0,"entities":[{"id":1,"name":"Competition","slug":"competition","namespace":"Campaign","status":"Active","parent":null},{"id":2,"name":"Education","slug":"education","namespace":"Campaign","status":"Active","parent":null},{"id":3,"name":"Healthcare \/ Medical","slug":"healthcare-medical","namespace":"Campaign","status":"Active","parent":null},{"id":4,"name":"Women empowerment","slug":"women-empowerment","namespace":"Campaign","status":"Active","parent":null},{"id":5,"name":"Elderly","slug":"elderly","namespace":"campaign","status":"Active","parent":null},{"id":7,"name":"Food & Hunger","slug":"food-hunger","namespace":"Campaign","status":"Active","parent":null},{"id":8,"name":"Children and Youth","slug":"children-and-youth","namespace":"Campaign","status":"Active","parent":null},{"id":9,"name":"Human rights","slug":"human-rights","namespace":"Campaign","status":"Active","parent":null},{"id":10,"name":"Refugee Relief","slug":"refugee-relief","namespace":"Ca

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\category[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 90 x 90, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	3736
Entropy (8bit):	7.926712173718147
Encrypted:	false
SSDEEP:	96:KAP1TmAJmzKiuSZQ8PF3AomBNTC9nlWEyOsDTF:KFLNuSZQOiD2nUEb6F
MD5:	D213CD5B7BEBEF7AF9FFCEBDEA489487
SHA1:	7CBE56B1A448AAAF458FB551929A44FED4C935ED
SHA-256:	07B6BC8A7FAE66A8884F04B3AA0BC85AAAD5DFEEC06A77FE66EBB7BF134E61EF
SHA-512:	01413879D1DF0318F314F5667911ED68CC74BA43F6113E3E15B2468CFB10940FF617C74B1BF344EFB24A7608EA9EA018AF3294E933B0075BBC17DD65A33670E4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/assets/images/unite/category.png
Preview:	.PNG.....IHDR...Z...Z.....8.A.....sRGB.....RIDATx..YP....{f.].B..k...$K .al...Qr.+...TR._...y.....U)W\.<.]N..|....@B...v@2..B .l\....|.....1+mW-....;.....\.....w.8+47.br8&,3l.j...~1d...b.H. Y..Y%.`....X..d.$J,(..O4.....U..\....q~.....n+.....,.!d..DQ....U.....PH\o.E&.DQ.u..e+.UA.<xP<.q..1.Z.X..$.z.%Z_.....'>.H..L.[.t[.3._h.-...'z..G.....t:.0.g.9m6..b1;,f..D....4....D..$.gg....n\8~.L..+Wo...ECP...]...l.5A.....;Gp^..TZ..Q...YP@....nu..%p..f69MF..D.DQ$.x ...c...;.7n....O.?.Y.?.{..4...#...#.p_~.'....Z,e.....?}..o{...g..w.<^'1....o~..?..*..xb....3.MrL....`f.3..i....Y./...)6pm.....`p..O>.....!{`k.~.q.I...~...U...;.p.d&X2.eX..h.....HYG...g4..?..[..|.Z../.f..vL.. ..l...q.;.P.a.5U..y..i>`.Z..._..E?3....O>.*.ned....YfG.q.`0)d.@....1.....4.}{.I.,.,.....C.]5..2.:~..8.4.8~..e%N..(...Tp..=MY.;.44>..k_..d.....d4..K..cX's.....<#.....`.s>.0.@.%.....J6....bf.*...b...9EfC.Pe].l..+....D.F.....\....P..JK.\1.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 16x16, 32 bits/pixel
Category:	downloaded
Size (bytes):	1150
Entropy (8bit):	3.4922727621866048
Encrypted:	false
SSDEEP:	12:mAoLREno28noBbCMwo0+HnoNVnoBMoLFinokoqboVt5cgoAoA1sl4:SyCD+4V1GvZ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\favicon[1].ico	
MD5:	C94E81065888B62BF227B3B3CDE05293
SHA1:	02B94517E6A1CEEAB8587A190A3CBBB62790A3E9
SHA-256:	C88E9605361E7AA6DAF9C8A53B63C9E3FFA6800D0F8F486D0AD410E85932F160
SHA-512:	8903E7359C3873EA7CDD24D34E9628788DD6A294527C72A187AF08EC657C5D3E7D29131F0B4E82F0EA4A31E08F6C963F1A184D1A655161AC5656443F22B0A11F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/assets/images/icon/favicon.ico?v=2
Preview:	..... .h.....(..... ....#...#.....'N..'N..'N..'N..'N..'N..'N..'N..'N..'N..'N..'N..'N..'N..)K..(M..(M..(M..(M..(M..(M..(M..(M..(M..)K..'N..'N..'N.&N..'N.....'N..(M..'N..'N.&N..'N.....'N..'N..'N..'N..'N..'N..(M..'N..'N.&N..'N.....&N..'N..'N.3'N..'N..'N.Q'N..'N..(M..'N..'N.&N..'N..'N..'N.$'N..'N..'N.0'N.{'N.Y'N..'N.('N..(M..'N..'N.&N..'N..'N.%'N..'N.U'N..'N..'N..'N..'N..'N.H'N..(M..'N..'N.&N..'N..'N.)'N..'N.]'N..'N..'N..'N.b'N..'N..'N.I'N..(M..'N..'N.&N..'N..'N.)'N..'N.k'N..'N..'N..'N.A'N..'N.J'N..(M..'N..'N.&N..'N..'N.)'N..'N..'N.k'N..'N..'N.R'N..'N..'N.I'N..(M..'N..'N.&N..'N..'N. 'N..'N..'N..'N.='N..'N..'N..'N..'N..(M..'N..'N.&N..'N..'N..'N..'N..'N..'N..'N..'N..'N..'N..'N..'N..(M..'N..'N.&N..'N.....'N..(M..'N..'N..'N..%N..&N..&N..&N..&N..&N..&N..&N..&N

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\fbevents[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	187548
Entropy (8bit):	5.392602416896564
Encrypted:	false
SSDEEP:	1536:sM+OWt6w6aic9MeipKKqQqcThe7Kdv0a9sIOC1jaMu5Qm2B+QNSMngUSZYSlIUiR:sOQMj1SVBYDGKqOQMj1SVBYDGKx
MD5:	D67E6D12EB6608E9D939B0E3EB70F7E5
SHA1:	AF4A18DD4EA23B6DF3B0092618A64A3733C2AE55
SHA-256:	8A407F25943E3E96B80C488FD36FF80000A45C9D85BAFA80E5C05890874E6695
SHA-512:	6B871EEFE532476E7FA735211C049F2CB33B684A765F5FE06F1107B0937940FCEB8FC8A71177141BDA7D6319643244B09C033F132FDF8E68D5CD4B7C39869D74
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://connect.facebook.net/en_US/fbevents.js
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\fbevents[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	93774
Entropy (8bit):	5.392602416896564
Encrypted:	false
SSDEEP:	1536:sM+OWt6w6aic9MeipKKqQqcThe7Kdv0a9sIOC1jaMu5Qm2B+QNSMngUSZYSlIUiX:sOQMj1SVBYDGKx
MD5:	077B8B6E85C9EDF74D372D155180E6D3
SHA1:	4A24BE343819AD355807ADB01579366A1E64B8B9
SHA-256:	A517525B8A7D39BCAF1CF5F9695C5BE8FCE7A6B920A3924C1A4F70E8EA748C05
SHA-512:	DB714A2EAF14E6727086795FE151F3729DA32BFA0B87AB74289B7DF9E0808E1FEBCA38D2622EF47B7AA263479BDB66857011E2302DD1AFC9E814EF6B74642DF9
Malicious:	false
Reputation:	low
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\help-india-fight-covid-19-donate-for-oxygen[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	9071
Entropy (8bit):	4.94862352509096
Encrypted:	false
SSDEEP:	192:LyAEQmFHFlHWjmRjLd0gpKQKdFr0y0Fo0l2P3OOv84aTmdZAckyFrJqyJhSgOIte:LxEQallHrBjSSFHJT4ZjGrxN8bfM

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\help-india-fight-covid-19-donate-for-oxygen[1].htm	
MD5:	2A5CEF0817081FC6AD1909B62ACD9919
SHA1:	B005FD522AD71CCADCBFE240599389ACA8BECDCA
SHA-256:	B6F1F3701DC121B979E593EBD27D71CDDD16BDECFB3FEDD70C7ADB5F2D0BA3F3
SHA-512:	B26C4C7F146FC8CC2BDD1BFBB1FA5085BE540A9299B592375BE1D5E60D75807E0768FD76BA41FEF1B1A0B74EE88582833C63EF6852C4A48C952504C453EB9E 3
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html lang="en">..<head>. <meta http-equiv="Content-type" content="text/html; charset=utf-8" />. <meta http-equiv="X-UA-Compatible" conten t="ie=edge">. <meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate">. <meta http-equiv="Pragma" content="no-cache">. <meta http- equiv="Expires" content="0">. <meta name="fragment" content="!" />. <meta name="viewport" content="width=device-width, initial-scale=1.0, minimum-scale=1.0, maximum-scale=1.0, user-scalable=no">.. <link href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" rel="stylesheet">. <link href="https ://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css" rel="stylesheet" />. <link href="https://cdnjs.cloudflare.com/ajax/libs/OwlCarousel2/ 2.1.6/assets/owl.carousel.min.css" rel="stylesheet" />. <link href="https://cdn.quilljs.com/1.2.2/quill.snow.css" rel="stylesheet">. <link href="https://cdn.quilljs.com/1.2.2 /quill.bub

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\help-india-fight-covid-19-donate-for-oxygen[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	84
Entropy (8bit):	4.363819698065086
Encrypted:	false
SSDEEP:	3:YWR4b5LCE02Rgq9LPALI7AX6Mn:YWyb5LHxWq9LPIIEXD
MD5:	C4CBFE5BDC03042E1247747430A6AC87
SHA1:	C8DEFD12416E3F28EF6CC22CC25E970804710706
SHA-256:	1A34D9AD2C22D54E57B66F10972A34AFCDF769F80D49AA10C202EA1D615CC7B2
SHA-512:	EA3C40D5710749E1014A7492BF7C64D4D322EAB6E3BA4A378CCEA050ACDC02C138E5A4F16E0946FC06E3C165E242F17A9D1F765C3D6BB77B3C7850901AF977 7
Malicious:	false
Reputation:	low
Preview:	{"status":true,"data":null,"id":200,"errorCode":10000,"message":"No Chapter exist."}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\help-india-fight-covid-19-donate-for-oxygen[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	62
Entropy (8bit):	4.039211536948157
Encrypted:	false
SSDEEP:	3:YWR4b5L5RERDZLCE0/9an:YWyb5L5iRVLH29a
MD5:	1D9CBC9183CC4856FDE20A4975B21934
SHA1:	8BA065FFB062AD0DEEB8CDFCEA073C6AF22057E9
SHA-256:	13E377274C138BC7DD7FD92337470C8501CC358B2A8A930CF3D04A71D37DBA50
SHA-512:	C1142D0FC21BF70B1822F4D2D2F700CC72778525BA0F07C3922C3F67BFC5413AD3F24F804DD9E60AE517F01D5ABB4747E5FFA6A107F75DA9C6215946BF4A38E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://risefundraiser.com/fundraising-api/public/api/1.0/tip/campaign/help-india-fight-covid-19-donate-for-oxygen
Preview:	{"status":true,"tipStatus":true,"data":null,"errorCode":10000}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\help-india-fight-covid-19-donate-for-oxygen[3].htm	
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):	3090
Entropy (8bit):	5.0683789310705585
Encrypted:	false
SSDEEP:	48:YtCxOABCOsTTHG7hsDOA5COs1ZsDOAuCOsN3zSOAyCOsJokTlp5sSOA1+COs6PPA:IUVto99m360/Td12tuPUzrk
MD5:	7AA9341861D9D44D56551FEEB7366257
SHA1:	C43B293106C61D88658E72119105D45BAA1A0803
SHA-256:	E2C198778D5D68F11B07BCF16F598A967B41EFC34839679728654F9FB4896792
SHA-512:	9FA11408907EFD5B687752F92AE0078B483D313B7B58F30C4B70430F3E8B2693CC2BE1328A0F8522313E5FF104213D580640B1D8A7EB829B6954DE473F6AFB68
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://risefundraiser.com/fundraising-api/public/api/1.0/donation/campaign/help-india-fight-covid-19-donate-for-oxygen? order=desc&sortBy=donation_amount&offSet=0&size=25

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\help-india-fight-covid-19-donate-for-oxygen[3].htm	
Preview:	{"status":true,"data":{"count":6,"entities":[{"id":354866,"donations":"2000.00","anonymous":false,"hideName":false,"hideAmount":false,"comment":null,"donationDate":"2021-05-20 07:01:50","currency":"INR","orgId":null,"OrgName":null,"giftId":null,"giftName":null,"campaignId":1749,"campaignName":"Edifecs: Help India Fight COVID-19 For Oxygen","chapterId":2626,"chapterName":"__default","championId":0,"championName":null,"firstName":"Ankur","lastName":"Chander","user":{"id":37624,"name":"Ankur Chander","email":"ankur.chander@edifecs.com","avatar":"https:\/\/dqy0ngl1d5798.cloudfront.net\/media\/17142\/2020-01-23_22-57-36.jpg"}},{"id":354867,"donations":"1000.00","anonymous":false,"hideName":false,"hideAmount":false,"comment":null,"donationDate":"2021-05-20 08:55:16","currency":"INR","orgId":null,"OrgName":null,"giftId":null,"giftName":null,"campaignId":1749,"campaignName":"Edifecs: Help India Fight COVID-19 For Oxygen","chapterId":2626,"chapterName":"__default","championId":null,"championNam

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\jointeam[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 92 x 92, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	2599
Entropy (8bit):	7.907526082742143
Encrypted:	false
SSDEEP:	48:+ZGqCmHpzUxd50zsirbP+l6Z1UCPs7bKrBzUL2XgOF6fuQoCrCGz/1:+Z3ms+lEUC+KrBo2gu6vrCGz/1
MD5:	741D4857CCE301D72EBE085A6886B56F
SHA1:	11836A0AFDCE67AEBF26BB066716D954555F13A3
SHA-256:	B8D01AE7996702EF28157FF4F93A623031308EF130D86BB94B67676638561548
SHA-512:	4ADFD1A268CE03A8FBF4380C393B0C2AA07D53E3C09A29F1044479033C14C132692A1F2489FFC411DBD928541349D457C1FC4D936D7E5CA42BA988204890C83
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/assets/images/icon/jointeam.png
Preview:	.PNG.....IHDR...\...\.....X....sRGB.....IDATx..w..U..y....."v....b.yJb.$.....c.&.....bo1.... A.,..#..`...}d.....93.o._.e..s.i;{..w_.>.Qj.:J..p....*...pC8.....s.....x].....ep*... ...?<..^..u..`...g.,`l..ho89O.....cc..z.d.8.I.,.d..^QP_...?|...[....O.e$.>..)P.".[..m..I.._/...6.w.fq....y8..Irg.H.kt..3.....zpc..<.....y....=Z.b.....*/.f.P...G..0..Cv{..J...GT.;t.K.0}V.g..a..c..>z.>.^...r]...I.....|.W....}).@.....u,...0.Or..T.$v)..W..[f....?>.....6.HlJ .....N).oKm.. .[.|."...zp1tAq.*.w.....7...y.4...bw>.wx...H....u...D.t@.W<>``..p.u..K..g\..]B.v.O..V]....c.^f...^...8.\.7.$;.#..i..._|.>...W.oai.i.ncZ.r.....i.u.}E].4r.1....h)....6t.....+#.>.....v...7Gw..n.....W.\...z.a!.&.....[_.o.....0.z@..|..a.[K.Y:EdU.-..h5Q.uf...c.=...hf<..N.B...i....s.l..S.m..w....e. B.=..h3....}..]..9.....i.#...hX.&..ZF..e0.$;.,.8~.&;L.p.w..7....j}.....8....M.I._@.+.....0..~.).....:c..1...8....T.v._..!..3..l6...h..7.. T...#...W.y...'.X..U..L..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\location[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 66 x 90, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	5592
Entropy (8bit):	7.948777804949589
Encrypted:	false
SSDEEP:	96:KnowyRaGlSyXZAIwPWpxHt1a8/cRdwlSmNX0vD/5jljwhoycTU2AzKxJvhUccrnf:Kn9WAyX/wPq1aTRuzvDB3he4xzWDVag8
MD5:	86583862DCE94A02753B1C1A367168AE
SHA1:	B23B9FCF8F4EF2C4F63A3A6A644CCF9F14BE0ABF
SHA-256:	F6DC49880D1400795E5F3F5951749DFCB11828462953A5A9EB07022D8A85B337
SHA-512:	5EDDFCAF66698C14632DA38DCFBD84D661568203E23C817773B7F36DC4575C38E5AFD86E3B0390986BB523A2B9F479946C188C9875EF343C7674E2CEB924F49
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/assets/images/unite/location.png
Preview:	.PNG.....IHDR...B...Z.....sRGB.....IDATx..\.SUW...{y).FEQ.E|G....M.F..$.t..$U3I...|...35..j....:...3....I..c..... .....s..Y.....s.u...`..k.....B..?Q.'..B.m..I/....t..3..e.b.f.....)..i....!.....!:|.....Q\..?...p...q..zMo..M3..a.Z.Iks....]..^...7?....`.=..=&...^ye.....6.....x..-=.=V.h.'.. ....-k.M.}.d.]..,c..s.IONJ\..&{.O.a.....4.L..7..uvvv.....WZ.....o..1..E....>h.g,z...2u....a.....e.[.3.~....y.H.Cw..=_y....|E.....h.o..S.w.^.Y.6?!B....p.Q.0.\..?....M.w"'.q.O4...Sw....~WR..E..0.....;..n.Q."{.sl.?.D,.....KJ....8.x<b.3.....8]L.F'...^o`..|~...D_....hq..C.....J{z.n.?Q.....P.|..VR~.X.*s.....4;.....bcc.....y)bAj.$.1:.S.....C.nk.....Tg.l.U..O_.....=....].D.].bc..~..<..p...w...?&N...eXp..."ci.....F.M..r[...p.....c.....3E...I.J.o..J..o..bI@.....AB||..6sF..i.X. Um{..H..5g.3....^.../.y....Y.<....V.C.Z.H].dU...k.9.q#&DN.K)C..O[R.oZl...w.;&..p.V...D.....Q..O.](H..c..C"8.3c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\mobile-brandlogo[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	72983
Entropy (8bit):	4.51309914730978
Encrypted:	false
SSDEEP:	768:EkD3TQyEGaqQ3Cw5GvFisqPqJUhWlQSvh5T:E1FcUjY
MD5:	7489C8DB6CF91158E37B6B22F0727958
SHA1:	422D4085CA80D199908FFE97E636DE31D667C451
SHA-256:	122886B71B3B906F61231B8932A20AA733AB0F1DA775C2AFEDD6B63F535BEB98
SHA-512:	E0F1E5945B1F08C3EC69B4DC6230832CDA071B7402A8E0E7DFDA825B50833388A2F39489E5549DFBB505368B3820B7ADD40F402C0697B33FD50B2A2CDE12C1D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/assets/images/mobile-brandlogo.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\mobile-brandlogo[1].svg	
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="152pt" height="22pt" viewBox="0 0 152 22" version="1.1">.<g id="surface1">.<path style=" stroke:none;fill-rule:nonzero;fill:rgb(73.333333%,74.117647%,74.901961%);fill-opacity:1;" d="M 29.730469 14.695312 C 28.160156 14.695312 27.101562 13.609375 27.101562 11.988281 C 27.101562 10.371094 28.164062 9.277344 29.742188 9.277344 C 30.503906 9.277344 31.148438 9.542969 31.589844 10.027344 L 31.589844 7.808594 C 31.59375 7.539062 31.8125 7.320312 32.082031 7.320312 L 32.425781 7.320312 L 32.425781 14.617188 L 31.589844 14.617188 L 31.589844 13.910156 C 31.105469 14.417969 30.433594 14.703125 29.730469 14.695312 Z M 29.761719 10.109375 C 28.417969 10.109375 27.9375 11.078125 27.9375 11.988281 C 27.9375 13.125 28.652344 13.859375 29.761719 13.859375 C 30.832031 13.859375 31.582031 13.085938 31.582031 11.980469 C 31.582031 10.894531 30.820312 10.109375 29.761719 10.109

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\polyfills.661b9383b7c93a39b0f5[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):	188221
Entropy (8bit):	5.403768175072065
Encrypted:	false
SSDEEP:	1536:OXoDmTwaN6kooH62YDDCDIAEtxW44+LCfUPk99lu83SN1wr2G9GUyqbKBgPgRIYk:O4qp6koop0cDUPOcbwPqpgPgKYk
MD5:	64EE510D298F7A9D5D903C09DFD5DD2E
SHA1:	6AC796273F014314F7B9192CB522EA54E43BB6A6
SHA-256:	1511EE988EA9B78FFED8A19D8CAF41323B5113D4B4604A59D290D3D69EF8FF8F
SHA-512:	4A0473DD722092B8338631CF44F042E2B0ECECFD9A99AA3B2DE617856E8EECDDF8A4D59B1EE7E9B5FFB8DFD97E99386473313C1FA1690E69AB6A0ECF411F33A4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/1.9.7_P9_patch2/polyfills.661b9383b7c93a39b0f5.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[27],{"+auO":function(t,e,n){var r=n("XKFU"),i=n("lvtm");r(r.S,"Math",{cbrt:function(t){return i(t=+t)*Math.pow(Math.abs(t),1/3)}})},"+oPb":function(t,e,n){"use strict";n("OGtf")("blink",function(t){return function(){return t(this,"blink","","")}})},"+rLv":function(t,e,n){var r=n("dyZX").document;t.exports=r&&r.documentElement},"/KAi":function(t,e,n){var r=n("XKFU"),i=n("dyZX").isFinite;r(r.S,"Number",{isFinite:function(t){return"number"==typeof t&&i(t)}})},"/SS/":function(t,e,n){var r=n("XKFU");r(r.S,"Object",{setPrototypeOf:n("i5dc").set})},"/e88":function(t,e){t.exports="\t\n\v\f\r \xa0\u1680\u180e\u2000\u2001\u2002\u2003\u2004\u2005\u2006\u2007\u2008\u2009\u200a\u202f\u205f\u3000\u2028\u2029\ufeff"},"0/R4":function(t,e){t.exports=function(t){return"object"==typeof t?null!==t:"function"==typeof t}},"0E+W":function(t,e,n){n("elZq")("Array")},"0LDn":function(t,e,n){"use strict";n("OGtf")("italics",function(t){return function(){return

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\rg-logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 132 x 29, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	7526
Entropy (8bit):	7.923667111512587
Encrypted:	false
SSDEEP:	192:bNK6RFD/g1EBwR4jdlQS9vj5P7mbjRR6rQM/aiMOLayKsI:M6FDoEBYmNSNEXRlMinKsb
MD5:	5BB12C7EBA967DF8194BF92F9475D567
SHA1:	653730CEDE43F53A37C3B84B4B85E78F90AAA0BD
SHA-256:	AD4E18AC6E1292031A527498496F3FD4F4F7E3132C30552947E302BA6C4BD7FD
SHA-512:	7795ED91CF274A8E9C0379FB982299EB49E83C2BC2C7F9E0B98EF070BB24865F9061D7D137AFBE61E12E1F9DCB3EF8B6397D901789270E1EE73D8BDC5AEE17F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/assets/images/rg-logo.png
Preview:	.PNG.....IHDR.....k-.,....gAMA.....a.... cHRM..z&.....u0...`.:....p..Q<....bKGD.....tIME.....$2..@....EIDATh..{i.]U.....>..s....Bz....B...(....b....(.B..*.g....RK!.....D.!. ....Ms.s.....~.s..jYV..Q5.c..Ys.5..9.\....e.....8..\<.g~..w.5....}...6...f KWH.9...O..:....=..K..=.?....].p.U.O.p6.@..Q.A.t.....\|.[..}..%.y.i3~....m.....N.....B... .y.^..$....?Q4g..e.sh.....r..]....]......408.I8.-o.7..r.X.....C...Z..*....f .....o...~."Zs.....M. ...Y...o..l4dkW.oy.a.v.!..R....C....E4s.ol.f.[...ED1....:.....[.D...J..j..]..$.$..~._.3u..c0.5..<`.UI.`.h`.....b.u... 3c.....,...\.u.\..:.....3....S...z.....,.P_.....L.X(.t.5...|..wahp...1.2..[....)r.4f$g.j...,.....po.....E.@.)....b!...Ry.P.....E..V../.....qdK;j+V`.j.t.\..L!#..EB...z.M<...v.....;.be.^...".SS...`..>.y.....s<.s..+..sB.@..M>3..n|..Q../..U!.....d.9..i..... I|....L..i...8/....D..S.NC...^...~.)}..[iFI`...../..]..>....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\rightArrow[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 128 x 87, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1254
Entropy (8bit):	6.008603077517121
Encrypted:	false
SSDEEP:	24:qgH4xl/RLr6Myrsgr/R6tJ8Zt3dt3MMP5:qgYT5LNwLr/RYuZt3dtDP5
MD5:	C2894FAB6ABF5DE744D3B84AEDABFF0E
SHA1:	D0D8563F97EDCB212B55FEC732C4D06892DDA43B
SHA-256:	25A17D9101C3458A597C9B5C0927FAA40887DD07447460E7A1DC2E759D457C1C
SHA-512:	7C469750962E73D39906F48C6E3C2AF8E5B539B1A82C6CBAEB709539F2A6CE5B08C121FE3444B3DA7C997E9CC1A7DD855B739A11A9B82DDE5E50DF77E3F6B8E3
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\rightArrow[1].png	
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/assets/images/rightArrow.png
Preview:	.PNG.....IHDR.....W.....n....PLTE.....mp....tRNS..... !#%&'()*,-/02578;>ADGHIKNOQRSUVY]abceimquvz}~.....jIDATh...gS.Q.....Q.`.1... JU..(]J...Qz....$...jH..[..g..|..o&..=..i.....g..N^..4.L.. ..1.sYC...=...#..c..#....p3.." ..6...T.....H.f.E...#E`..3..|....A.....A....-...U....A.2....A."..d. }.._*C..`>.!H.B....$~.`9.!..C...!..B.3.!..!.(...@.UL.|.`...h. ..,M].....:""8+....D..,..a.....7" -..d o4C...R.....*(...x[A.....;..9.. .#.....V.....8..._.....k_...3..X.s.~.9..cA.....~.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\style-layout[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	18151
Entropy (8bit):	5.106769082143242
Encrypted:	false
SSDEEP:	384:GnovDpreafq9lL3Z5Cad9FFFhBEvD5HA+rvLr+YmwA18civCmH:h/qPL3Z5Cad9F7Er5H5rjZsKcivCmH
MD5:	4358F223535895B968CE0B87F7A745DA
SHA1:	CC2760B005F14AD70A87CA1B8A616298C11E6118
SHA-256:	ACB1CA8F2038623F6E718DEEEDDD458BBDA9B6DFF25718AA4B5F3DFCE08CD3A5
SHA-512:	194F33882F562B466D3AE730031BB0657AA86FDC833CB3944809E24C320F86482F46A627E1A8593B973F3D56A7C4DF7F4040F86D89CE97FEE3FDC6C6B7E92559
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/assets/themes/style-layout.css
Preview:	/********** new temp **********/..@font-face {. font-family: 'Gibson';. src: url('https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_0_0.eot');. src: url('https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_0_0.eot?#iefix') format('embedded-opentype'), url('https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_0_0.woff') format('woff'), url('https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_0_0.ttf') format('truetype');. font-weight: 300;. font-style: italic;.}..@font-face {. font-family: 'Gibson';. src: url('https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_1_0.eot');. src: url('https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_1_0.eot?#iefix') format('embedded-opentype'), url('https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_1_0.woff') format('woff'), url('https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_1_0.ttf') format('truetype');. font-weight: 700;. font-style: italic;.}..@font-face

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\swiper.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	19778
Entropy (8bit):	5.144035443519331
Encrypted:	false
SSDEEP:	192:cpaNf/lSSyJWCh8zfi5o/mXDN3eBxwdJ5c:cpa1/lS0Cifi5o/mXOGJ5c
MD5:	9097E7972B059ECAE0F5BB78A0186F71
SHA1:	87312E89335AEE051F552BA29644AE9B1F8CC0C1
SHA-256:	5F07D43571A20235B2506061C9729D91179D32B8B3C75123AA8FCD45E60D7541
SHA-512:	34AD5AF9FC158079D6939EE5882715778FC29BD99E4A6618635DF462A4377C4383EE0C37190DFA509F8265655FA4CFC2B44D3C624A488383011B3C0D1B63F749
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/Swiper/4.5.0/css/swiper.min.css
Preview:	/**. * Swiper 4.5.0. * Most modern mobile touch slider and framework with hardware accelerated transitions. * http://www.idangero.us/swiper/. *. * Copyright 2014-2019 Vladimir Kharlampidi. *. * Released under the MIT License. *. * Released on: February 22, 2019. */..swiper-container{margin:0 auto;position:relative;overflow:hidden;list-style:none;padding:0;z-index:1}.swiper-container-no-flexbox .swiper-slide{float:left}.swiper-container-vertical>.swiper-wrapper{-webkit-box-orient:vertical;-webkit-box-direction:normal;-webkit-flex-direction:column;-ms-flex-direction:column;flex-direction:column}.swiper-wrapper{position:relative;width:100%;height:100%;z-index:1;display:-webkit-box;display:-webkit-flex;display:-ms-flexbox;display:flex;-webkit-transition-property:-webkit-transform;transition-property:-webkit-transform;-o-transition-property:transform;transition-property:transform;transition-property:transform,-webkit-transform;-webkit-box-sizing:content-box;box-sizing:content-box}.swiper-co

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\swiper.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	127934
Entropy (8bit):	5.234616936050802
Encrypted:	false
SSDEEP:	1536:+apNOiO5/c9XrYK8SnTLANcelWyVAyvK05Du1u+GlpuXvH7WcWUmcPqMjCE8EtO7:N9XrTrANcwQll+GqfH7WcWUmcPquXbq
MD5:	53FC0155C6C3CB55F34B749325EBB370
SHA1:	A0738B4767A38B90E17792041D648ED621DAB2AE
SHA-256:	B9C90C601BC81AD71ED8BE557FF9B095DE5AAE947926E84011E2728CF65250A6
SHA-512:	13D7B31F6F6DBAD80617D644160E3720AFF5074AD1AE2426E681C21B91F2AC91C022706764F3A0A11727B229D667EFD07154626AD7695EB741650873A5BCFB47
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\swiper.min[1].js	
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/Swiper/4.5.0/js/swiper.min.js
Preview:	/**. * Swiper 4.5.0. * Most modern mobile touch slider and framework with hardware accelerated transitions. * http://www.idangero.us/swiper/. *. * Copyright 2014-2019 Vladimir Kharlampidi. *. * Released under the MIT License. *. * Released on: February 22, 2019. */!function(e,t){"object"==typeof exports&&"undefined"!=typeof module?module.exports=t():"function"==typeof define&&define.amd?define(t):(e=e||self).Swiper=t()}(this,function(){"use strict";var f="undefined"==typeof document?{body:{},addEventListener:function(){},removeEventListener:function(){},activeElement:{blur:function(){},nodeName:""},querySelector:function(){return null},querySelectorAll:function(){return[]},getElementById:function(){return null},createEvent:function(){return{initEvent:function(){}}},createElement:function(){return{children:[],childNodes:[],style:{},setAttribute:function(){},getElementsByTagName:function(){return[]}}},location:{hash:""}}:document,J="undefined"==typeof window?{document:f,navigator:{userA

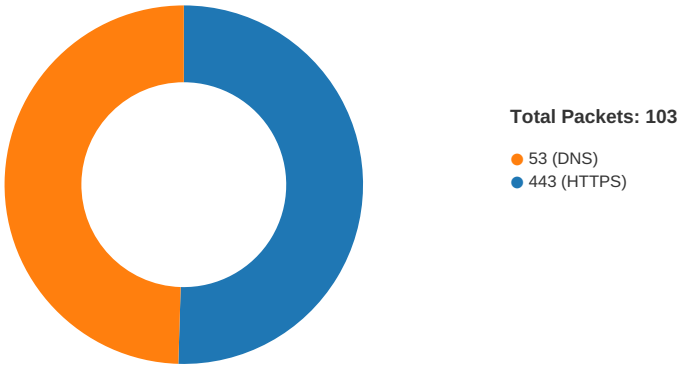
C:\Users\user\AppData\Local\Temp\~DF693C7156C5077509.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	160849
Entropy (8bit):	1.2921037566423867
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+357yZW51JfxJfUJlgXr9E4+f1oI9hv/92wv6TRgbegI0cu09ohFIC:LJZJMdXzdZODEX
MD5:	3781F620177B56E5689DFF15EAE19863
SHA1:	D02C5D1691E1B0AAD0C3BB273CF8D020223FF029
SHA-256:	670381422849C92B59998816F8EB591AF03B89783789FB86CEAD66C30CA0BA3D
SHA-512:	AAA5626F6C835294182A3E98C3D3EC8B73A52D4DF051D72CC65B408F0AFBB807F48142A8423155BDE5A1B59B0D174DCD55C6104FB2FA494DE81BB5D7B41A783
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 20, 2021 20:33:24.289479971 CEST	49717	443	192.168.2.6	54.201.10.107
May 20, 2021 20:33:24.290530920 CEST	49718	443	192.168.2.6	54.201.10.107
May 20, 2021 20:33:24.505614042 CEST	443	49718	54.201.10.107	192.168.2.6
May 20, 2021 20:33:24.505799055 CEST	49718	443	192.168.2.6	54.201.10.107
May 20, 2021 20:33:24.506141901 CEST	443	49717	54.201.10.107	192.168.2.6
May 20, 2021 20:33:24.506315947 CEST	49717	443	192.168.2.6	54.201.10.107
May 20, 2021 20:33:24.515738010 CEST	49718	443	192.168.2.6	54.201.10.107
May 20, 2021 20:33:24.515885115 CEST	49717	443	192.168.2.6	54.201.10.107
May 20, 2021 20:33:24.732523918 CEST	443	49718	54.201.10.107	192.168.2.6
May 20, 2021 20:33:24.733644962 CEST	443	49717	54.201.10.107	192.168.2.6
May 20, 2021 20:33:24.734524965 CEST	443	49718	54.201.10.107	192.168.2.6
May 20, 2021 20:33:24.734539986 CEST	443	49718	54.201.10.107	192.168.2.6
May 20, 2021 20:33:24.734551907 CEST	443	49718	54.201.10.107	192.168.2.6
May 20, 2021 20:33:24.734565020 CEST	443	49718	54.201.10.107	192.168.2.6
May 20, 2021 20:33:24.734683037 CEST	443	49717	54.201.10.107	192.168.2.6
May 20, 2021 20:33:24.734723091 CEST	49718	443	192.168.2.6	54.201.10.107
May 20, 2021 20:33:24.734736919 CEST	443	49717	54.201.10.107	192.168.2.6
May 20, 2021 20:33:24.734750986 CEST	443	49717	54.201.10.107	192.168.2.6
May 20, 2021 20:33:24.734761953 CEST	443	49717	54.201.10.107	192.168.2.6
May 20, 2021 20:33:24.734805107 CEST	49717	443	192.168.2.6	54.201.10.107
May 20, 2021 20:33:24.734855890 CEST	49717	443	192.168.2.6	54.201.10.107
May 20, 2021 20:33:24.777869940 CEST	49717	443	192.168.2.6	54.201.10.107
May 20, 2021 20:33:24.778072119 CEST	49718	443	192.168.2.6	54.201.10.107
May 20, 2021 20:33:24.784621000 CEST	49717	443	192.168.2.6	54.201.10.107
May 20, 2021 20:33:24.784822941 CEST	49718	443	192.168.2.6	54.201.10.107
May 20, 2021 20:33:24.784919977 CEST	49717	443	192.168.2.6	54.201.10.107
May 20, 2021 20:33:24.993355036 CEST	443	49718	54.201.10.107	192.168.2.6
May 20, 2021 20:33:24.993371010 CEST	443	49718	54.201.10.107	192.168.2.6
May 20, 2021 20:33:24.993618011 CEST	49718	443	192.168.2.6	54.201.10.107
May 20, 2021 20:33:24.994256020 CEST	443	49717	54.201.10.107	192.168.2.6

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 20, 2021 20:33:24.994267941 CEST	443	49717	54.201.10.107	192.168.2.6
May 20, 2021 20:33:24.994287968 CEST	49718	443	192.168.2.6	54.201.10.107
May 20, 2021 20:33:24.994366884 CEST	49717	443	192.168.2.6	54.201.10.107
May 20, 2021 20:33:24.994908094 CEST	49717	443	192.168.2.6	54.201.10.107
May 20, 2021 20:33:24.999845028 CEST	443	49718	54.201.10.107	192.168.2.6
May 20, 2021 20:33:25.000721931 CEST	443	49717	54.201.10.107	192.168.2.6
May 20, 2021 20:33:25.000978947 CEST	49717	443	192.168.2.6	54.201.10.107
May 20, 2021 20:33:25.001187086 CEST	49718	443	192.168.2.6	54.201.10.107
May 20, 2021 20:33:25.003213882 CEST	443	49717	54.201.10.107	192.168.2.6
May 20, 2021 20:33:25.003232002 CEST	443	49717	54.201.10.107	192.168.2.6
May 20, 2021 20:33:25.003242016 CEST	443	49717	54.201.10.107	192.168.2.6
May 20, 2021 20:33:25.003349066 CEST	49717	443	192.168.2.6	54.201.10.107
May 20, 2021 20:33:25.228801012 CEST	49719	443	192.168.2.6	104.16.19.94
May 20, 2021 20:33:25.230938911 CEST	49720	443	192.168.2.6	104.16.19.94
May 20, 2021 20:33:25.232325077 CEST	49721	443	192.168.2.6	104.16.19.94
May 20, 2021 20:33:25.233833075 CEST	49722	443	192.168.2.6	104.16.19.94
May 20, 2021 20:33:25.235845089 CEST	49723	443	192.168.2.6	104.18.10.207
May 20, 2021 20:33:25.243969917 CEST	49724	443	192.168.2.6	104.18.10.207
May 20, 2021 20:33:25.251127005 CEST	443	49718	54.201.10.107	192.168.2.6
May 20, 2021 20:33:25.252279043 CEST	443	49717	54.201.10.107	192.168.2.6
May 20, 2021 20:33:25.266254902 CEST	443	49719	104.16.19.94	192.168.2.6
May 20, 2021 20:33:25.266897917 CEST	49719	443	192.168.2.6	104.16.19.94
May 20, 2021 20:33:25.267930031 CEST	443	49720	104.16.19.94	192.168.2.6
May 20, 2021 20:33:25.268948078 CEST	49720	443	192.168.2.6	104.16.19.94
May 20, 2021 20:33:25.269767046 CEST	443	49721	104.16.19.94	192.168.2.6
May 20, 2021 20:33:25.270062923 CEST	49721	443	192.168.2.6	104.16.19.94
May 20, 2021 20:33:25.271431923 CEST	443	49722	104.16.19.94	192.168.2.6
May 20, 2021 20:33:25.273237944 CEST	443	49723	104.18.10.207	192.168.2.6
May 20, 2021 20:33:25.273410082 CEST	49722	443	192.168.2.6	104.16.19.94
May 20, 2021 20:33:25.275152922 CEST	49723	443	192.168.2.6	104.18.10.207
May 20, 2021 20:33:25.281395912 CEST	443	49724	104.18.10.207	192.168.2.6
May 20, 2021 20:33:25.283211946 CEST	49724	443	192.168.2.6	104.18.10.207
May 20, 2021 20:33:25.290493965 CEST	49724	443	192.168.2.6	104.18.10.207
May 20, 2021 20:33:25.291610956 CEST	49719	443	192.168.2.6	104.16.19.94
May 20, 2021 20:33:25.291687965 CEST	49722	443	192.168.2.6	104.16.19.94
May 20, 2021 20:33:25.292423010 CEST	49721	443	192.168.2.6	104.16.19.94
May 20, 2021 20:33:25.293926954 CEST	49725	443	192.168.2.6	151.101.1.0
May 20, 2021 20:33:25.295042038 CEST	49726	443	192.168.2.6	151.101.1.0
May 20, 2021 20:33:25.296636105 CEST	49717	443	192.168.2.6	54.201.10.107
May 20, 2021 20:33:25.302067995 CEST	49723	443	192.168.2.6	104.18.10.207
May 20, 2021 20:33:25.302105904 CEST	49720	443	192.168.2.6	104.16.19.94
May 20, 2021 20:33:25.326488972 CEST	443	49724	104.18.10.207	192.168.2.6
May 20, 2021 20:33:25.326982021 CEST	443	49724	104.18.10.207	192.168.2.6
May 20, 2021 20:33:25.327013969 CEST	443	49724	104.18.10.207	192.168.2.6
May 20, 2021 20:33:25.327094078 CEST	49724	443	192.168.2.6	104.18.10.207
May 20, 2021 20:33:25.327470064 CEST	443	49719	104.16.19.94	192.168.2.6
May 20, 2021 20:33:25.327579021 CEST	443	49722	104.16.19.94	192.168.2.6
May 20, 2021 20:33:25.327663898 CEST	49717	443	192.168.2.6	54.201.10.107
May 20, 2021 20:33:25.328176975 CEST	443	49722	104.16.19.94	192.168.2.6
May 20, 2021 20:33:25.328202963 CEST	443	49722	104.16.19.94	192.168.2.6
May 20, 2021 20:33:25.328248024 CEST	443	49719	104.16.19.94	192.168.2.6
May 20, 2021 20:33:25.328290939 CEST	443	49719	104.16.19.94	192.168.2.6
May 20, 2021 20:33:25.328315973 CEST	49722	443	192.168.2.6	104.16.19.94
May 20, 2021 20:33:25.328320026 CEST	443	49721	104.16.19.94	192.168.2.6
May 20, 2021 20:33:25.328366041 CEST	49719	443	192.168.2.6	104.16.19.94
May 20, 2021 20:33:25.328382969 CEST	49719	443	192.168.2.6	104.16.19.94
May 20, 2021 20:33:25.328959942 CEST	443	49721	104.16.19.94	192.168.2.6
May 20, 2021 20:33:25.329030991 CEST	443	49721	104.16.19.94	192.168.2.6
May 20, 2021 20:33:25.329497099 CEST	49721	443	192.168.2.6	104.16.19.94
May 20, 2021 20:33:25.333739042 CEST	49717	443	192.168.2.6	54.201.10.107
May 20, 2021 20:33:25.337909937 CEST	49724	443	192.168.2.6	104.18.10.207
May 20, 2021 20:33:25.338016033 CEST	443	49725	151.101.1.0	192.168.2.6
May 20, 2021 20:33:25.338057995 CEST	443	49723	104.18.10.207	192.168.2.6
May 20, 2021 20:33:25.338084936 CEST	443	49720	104.16.19.94	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 20, 2021 20:33:25.338118076 CEST	49725	443	192.168.2.6	151.101.1.0
May 20, 2021 20:33:25.338679075 CEST	443	49720	104.16.19.94	192.168.2.6
May 20, 2021 20:33:25.338713884 CEST	443	49720	104.16.19.94	192.168.2.6
May 20, 2021 20:33:25.338746071 CEST	443	49723	104.18.10.207	192.168.2.6
May 20, 2021 20:33:25.338783979 CEST	443	49723	104.18.10.207	192.168.2.6
May 20, 2021 20:33:25.338824987 CEST	49720	443	192.168.2.6	104.16.19.94

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 20, 2021 20:33:15.785666943 CEST	64267	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:15.835445881 CEST	53	64267	8.8.8.8	192.168.2.6
May 20, 2021 20:33:16.252178907 CEST	49448	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:16.311460018 CEST	53	49448	8.8.8.8	192.168.2.6
May 20, 2021 20:33:16.639385939 CEST	60342	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:16.689093113 CEST	53	60342	8.8.8.8	192.168.2.6
May 20, 2021 20:33:17.447165966 CEST	61346	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:17.496974945 CEST	53	61346	8.8.8.8	192.168.2.6
May 20, 2021 20:33:18.260689974 CEST	51774	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:18.318340063 CEST	53	51774	8.8.8.8	192.168.2.6
May 20, 2021 20:33:19.784753084 CEST	56023	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:19.834321022 CEST	53	56023	8.8.8.8	192.168.2.6
May 20, 2021 20:33:20.731211901 CEST	58384	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:20.780738115 CEST	53	58384	8.8.8.8	192.168.2.6
May 20, 2021 20:33:21.534374952 CEST	60261	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:21.595055103 CEST	53	60261	8.8.8.8	192.168.2.6
May 20, 2021 20:33:22.548973083 CEST	56061	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:22.601119041 CEST	53	56061	8.8.8.8	192.168.2.6
May 20, 2021 20:33:22.859419107 CEST	58336	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:22.917462111 CEST	53	58336	8.8.8.8	192.168.2.6
May 20, 2021 20:33:23.653045893 CEST	53781	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:23.702333927 CEST	53	53781	8.8.8.8	192.168.2.6
May 20, 2021 20:33:24.213021040 CEST	54064	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:24.275921106 CEST	53	54064	8.8.8.8	192.168.2.6
May 20, 2021 20:33:25.126697063 CEST	52811	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:25.136356115 CEST	55299	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:25.186114073 CEST	53	52811	8.8.8.8	192.168.2.6
May 20, 2021 20:33:25.197213888 CEST	53	55299	8.8.8.8	192.168.2.6
May 20, 2021 20:33:25.201272011 CEST	63745	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:25.267302036 CEST	53	63745	8.8.8.8	192.168.2.6
May 20, 2021 20:33:25.316229105 CEST	50055	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:25.352056026 CEST	61374	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:25.371620893 CEST	53	50055	8.8.8.8	192.168.2.6
May 20, 2021 20:33:25.420568943 CEST	53	61374	8.8.8.8	192.168.2.6
May 20, 2021 20:33:25.595091105 CEST	50339	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:25.597119093 CEST	63307	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:25.651551008 CEST	53	50339	8.8.8.8	192.168.2.6
May 20, 2021 20:33:25.657690048 CEST	53	63307	8.8.8.8	192.168.2.6
May 20, 2021 20:33:26.310112953 CEST	49694	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:26.367773056 CEST	53	49694	8.8.8.8	192.168.2.6
May 20, 2021 20:33:26.448317051 CEST	54982	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:26.510432005 CEST	53	54982	8.8.8.8	192.168.2.6
May 20, 2021 20:33:27.428695917 CEST	50010	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:27.477917910 CEST	53	50010	8.8.8.8	192.168.2.6
May 20, 2021 20:33:27.864514112 CEST	63718	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:27.913770914 CEST	53	63718	8.8.8.8	192.168.2.6
May 20, 2021 20:33:28.805614948 CEST	62116	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:28.857937098 CEST	53	62116	8.8.8.8	192.168.2.6
May 20, 2021 20:33:29.663779020 CEST	63816	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:29.713175058 CEST	53	63816	8.8.8.8	192.168.2.6
May 20, 2021 20:33:33.697658062 CEST	55014	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:33.748429060 CEST	53	55014	8.8.8.8	192.168.2.6
May 20, 2021 20:33:34.621942997 CEST	62208	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:34.673990965 CEST	53	62208	8.8.8.8	192.168.2.6

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 20, 2021 20:33:35.585597038 CEST	57574	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:35.636725903 CEST	53	57574	8.8.8.8	192.168.2.6
May 20, 2021 20:33:42.813472986 CEST	51818	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:42.909379959 CEST	53	51818	8.8.8.8	192.168.2.6
May 20, 2021 20:33:43.359509945 CEST	56628	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:43.408919096 CEST	53	56628	8.8.8.8	192.168.2.6
May 20, 2021 20:33:44.299730062 CEST	60778	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:44.352195024 CEST	53	60778	8.8.8.8	192.168.2.6
May 20, 2021 20:33:52.747010946 CEST	53799	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:52.817214012 CEST	53	53799	8.8.8.8	192.168.2.6
May 20, 2021 20:33:52.869556904 CEST	54683	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:52.921714067 CEST	53	54683	8.8.8.8	192.168.2.6
May 20, 2021 20:33:53.595197916 CEST	59329	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:53.647566080 CEST	53	59329	8.8.8.8	192.168.2.6
May 20, 2021 20:33:53.883318901 CEST	54683	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:53.935749054 CEST	53	54683	8.8.8.8	192.168.2.6
May 20, 2021 20:33:54.598361969 CEST	59329	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:54.659588099 CEST	53	59329	8.8.8.8	192.168.2.6
May 20, 2021 20:33:54.923022032 CEST	54683	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:54.985090017 CEST	53	54683	8.8.8.8	192.168.2.6
May 20, 2021 20:33:55.601974964 CEST	59329	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:55.663007975 CEST	53	59329	8.8.8.8	192.168.2.6
May 20, 2021 20:33:56.918234110 CEST	54683	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:56.979239941 CEST	53	54683	8.8.8.8	192.168.2.6
May 20, 2021 20:33:57.603595018 CEST	59329	53	192.168.2.6	8.8.8.8
May 20, 2021 20:33:57.656527042 CEST	53	59329	8.8.8.8	192.168.2.6
May 20, 2021 20:34:00.919734955 CEST	54683	53	192.168.2.6	8.8.8.8
May 20, 2021 20:34:00.971977949 CEST	53	54683	8.8.8.8	192.168.2.6
May 20, 2021 20:34:01.620306015 CEST	59329	53	192.168.2.6	8.8.8.8
May 20, 2021 20:34:01.673149109 CEST	53	59329	8.8.8.8	192.168.2.6
May 20, 2021 20:34:10.993407965 CEST	64021	53	192.168.2.6	8.8.8.8
May 20, 2021 20:34:11.051218987 CEST	53	64021	8.8.8.8	192.168.2.6
May 20, 2021 20:34:55.929481983 CEST	56129	53	192.168.2.6	8.8.8.8
May 20, 2021 20:34:55.982822895 CEST	53	56129	8.8.8.8	192.168.2.6
May 20, 2021 20:35:00.497904062 CEST	58177	53	192.168.2.6	8.8.8.8
May 20, 2021 20:35:00.633569956 CEST	53	58177	8.8.8.8	192.168.2.6
May 20, 2021 20:35:01.634673119 CEST	50700	53	192.168.2.6	8.8.8.8
May 20, 2021 20:35:01.696074963 CEST	53	50700	8.8.8.8	192.168.2.6
May 20, 2021 20:35:02.465272903 CEST	54069	53	192.168.2.6	8.8.8.8
May 20, 2021 20:35:02.518758059 CEST	53	54069	8.8.8.8	192.168.2.6
May 20, 2021 20:35:03.598453045 CEST	61178	53	192.168.2.6	8.8.8.8
May 20, 2021 20:35:03.661030054 CEST	53	61178	8.8.8.8	192.168.2.6
May 20, 2021 20:35:04.418832064 CEST	57017	53	192.168.2.6	8.8.8.8
May 20, 2021 20:35:04.469075918 CEST	53	57017	8.8.8.8	192.168.2.6
May 20, 2021 20:35:04.935997963 CEST	56327	53	192.168.2.6	8.8.8.8
May 20, 2021 20:35:04.993995905 CEST	53	56327	8.8.8.8	192.168.2.6
May 20, 2021 20:35:05.785017014 CEST	50243	53	192.168.2.6	8.8.8.8
May 20, 2021 20:35:05.845499992 CEST	53	50243	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 20, 2021 20:33:24.213021040 CEST	192.168.2.6	8.8.8.8	0x165e	Standard query (0)	risefundraiser.com	A (IP address)	IN (0x0001)
May 20, 2021 20:33:25.126697063 CEST	192.168.2.6	8.8.8.8	0x8f83	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
May 20, 2021 20:33:25.136356115 CEST	192.168.2.6	8.8.8.8	0x99e9	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
May 20, 2021 20:33:25.201272011 CEST	192.168.2.6	8.8.8.8	0xd616	Standard query (0)	cdn.quilljs.com	A (IP address)	IN (0x0001)
May 20, 2021 20:33:25.316229105 CEST	192.168.2.6	8.8.8.8	0xb0cd	Standard query (0)	dqy0ngl1d5798.cloudfront.net	A (IP address)	IN (0x0001)
May 20, 2021 20:33:25.595091105 CEST	192.168.2.6	8.8.8.8	0x61bf	Standard query (0)	js.hsforms.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 20, 2021 20:33:25.597119093 CEST	192.168.2.6	8.8.8.8	0x52c3	Standard query (0)	s3-us-west-2.amazonaws.com	A (IP address)	IN (0x0001)
May 20, 2021 20:33:26.448317051 CEST	192.168.2.6	8.8.8.8	0x88ed	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
May 20, 2021 20:33:42.813472986 CEST	192.168.2.6	8.8.8.8	0xf86b	Standard query (0)	dqy0ngl1d5798.cloudfront.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 20, 2021 20:33:24.275921106 CEST	8.8.8.8	192.168.2.6	0x165e	No error (0)	risefundraiser.com		54.201.10.107	A (IP address)	IN (0x0001)
May 20, 2021 20:33:24.275921106 CEST	8.8.8.8	192.168.2.6	0x165e	No error (0)	risefundraiser.com		54.186.33.74	A (IP address)	IN (0x0001)
May 20, 2021 20:33:25.186114073 CEST	8.8.8.8	192.168.2.6	0x8f83	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
May 20, 2021 20:33:25.186114073 CEST	8.8.8.8	192.168.2.6	0x8f83	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
May 20, 2021 20:33:25.197213888 CEST	8.8.8.8	192.168.2.6	0x99e9	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
May 20, 2021 20:33:25.197213888 CEST	8.8.8.8	192.168.2.6	0x99e9	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
May 20, 2021 20:33:25.267302036 CEST	8.8.8.8	192.168.2.6	0xd616	No error (0)	cdn.quilljs.com	cdn-quilljs-com-7quy.onrender.com		CNAME (Canonical name)	IN (0x0001)
May 20, 2021 20:33:25.267302036 CEST	8.8.8.8	192.168.2.6	0xd616	No error (0)	cdn-quilljs-com-7quy.onrender.com	render.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 20, 2021 20:33:25.267302036 CEST	8.8.8.8	192.168.2.6	0xd616	No error (0)	render.map.fastly.net		151.101.1.0	A (IP address)	IN (0x0001)
May 20, 2021 20:33:25.267302036 CEST	8.8.8.8	192.168.2.6	0xd616	No error (0)	render.map.fastly.net		151.101.65.0	A (IP address)	IN (0x0001)
May 20, 2021 20:33:25.267302036 CEST	8.8.8.8	192.168.2.6	0xd616	No error (0)	render.map.fastly.net		151.101.129.0	A (IP address)	IN (0x0001)
May 20, 2021 20:33:25.267302036 CEST	8.8.8.8	192.168.2.6	0xd616	No error (0)	render.map.fastly.net		151.101.193.0	A (IP address)	IN (0x0001)
May 20, 2021 20:33:25.371620893 CEST	8.8.8.8	192.168.2.6	0xb0cd	No error (0)	dqy0ngl1d5798.cloudfront.net		13.224.89.44	A (IP address)	IN (0x0001)
May 20, 2021 20:33:25.371620893 CEST	8.8.8.8	192.168.2.6	0xb0cd	No error (0)	dqy0ngl1d5798.cloudfront.net		13.224.89.190	A (IP address)	IN (0x0001)
May 20, 2021 20:33:25.371620893 CEST	8.8.8.8	192.168.2.6	0xb0cd	No error (0)	dqy0ngl1d5798.cloudfront.net		13.224.89.71	A (IP address)	IN (0x0001)
May 20, 2021 20:33:25.371620893 CEST	8.8.8.8	192.168.2.6	0xb0cd	No error (0)	dqy0ngl1d5798.cloudfront.net		13.224.89.17	A (IP address)	IN (0x0001)
May 20, 2021 20:33:25.651551008 CEST	8.8.8.8	192.168.2.6	0x61bf	No error (0)	js.hsforms.net		104.17.183.73	A (IP address)	IN (0x0001)
May 20, 2021 20:33:25.651551008 CEST	8.8.8.8	192.168.2.6	0x61bf	No error (0)	js.hsforms.net		104.17.186.73	A (IP address)	IN (0x0001)
May 20, 2021 20:33:25.651551008 CEST	8.8.8.8	192.168.2.6	0x61bf	No error (0)	js.hsforms.net		104.17.185.73	A (IP address)	IN (0x0001)
May 20, 2021 20:33:25.651551008 CEST	8.8.8.8	192.168.2.6	0x61bf	No error (0)	js.hsforms.net		104.17.184.73	A (IP address)	IN (0x0001)
May 20, 2021 20:33:25.651551008 CEST	8.8.8.8	192.168.2.6	0x61bf	No error (0)	js.hsforms.net		104.17.182.73	A (IP address)	IN (0x0001)
May 20, 2021 20:33:25.657690048 CEST	8.8.8.8	192.168.2.6	0x52c3	No error (0)	s3-us-west-2.amazonaws.com		52.218.221.248	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 20, 2021 20:33:26.510432005 CEST	8.8.8.8	192.168.2.6	0x88ed	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
May 20, 2021 20:33:26.510432005 CEST	8.8.8.8	192.168.2.6	0x88ed	No error (0)	scontent.xx.fbcdn.net		31.13.92.14	A (IP address)	IN (0x0001)
May 20, 2021 20:33:42.909379959 CEST	8.8.8.8	192.168.2.6	0xf86b	No error (0)	dqy0ngl1d5798.cloudfront.net		13.224.89.71	A (IP address)	IN (0x0001)
May 20, 2021 20:33:42.909379959 CEST	8.8.8.8	192.168.2.6	0xf86b	No error (0)	dqy0ngl1d5798.cloudfront.net		13.224.89.44	A (IP address)	IN (0x0001)
May 20, 2021 20:33:42.909379959 CEST	8.8.8.8	192.168.2.6	0xf86b	No error (0)	dqy0ngl1d5798.cloudfront.net		13.224.89.17	A (IP address)	IN (0x0001)
May 20, 2021 20:33:42.909379959 CEST	8.8.8.8	192.168.2.6	0xf86b	No error (0)	dqy0ngl1d5798.cloudfront.net		13.224.89.190	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 20, 2021 20:33:24.734565020 CEST	54.201.10.107	443	192.168.2.6	49718	CN=risefundraiser.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Jan 20 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Fri Feb 18 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 20, 2021 20:33:24.734761953 CEST	54.201.10.107	443	192.168.2.6	49717	CN=risefundraiser.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Jan 20 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Fri Feb 18 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 20, 2021 20:33:25.327013969 CEST	104.18.10.207	443	192.168.2.6	49724	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Mar 01 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Tue Mar 01 00:59:59 CET 2022 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		
May 20, 2021 20:33:25.328202963 CEST	104.16.19.94	443	192.168.2.6	49722	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		
May 20, 2021 20:33:25.328290939 CEST	104.16.19.94	443	192.168.2.6	49719	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		
May 20, 2021 20:33:25.329030991 CEST	104.16.19.94	443	192.168.2.6	49721	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 20, 2021 20:33:25.338713884 CEST	104.16.19.94	443	192.168.2.6	49720	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		
May 20, 2021 20:33:25.338783979 CEST	104.18.10.207	443	192.168.2.6	49723	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Mar 01 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Tue Mar 01 00:59:59 CET 2022 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		
May 20, 2021 20:33:25.401293993 CEST	151.101.1.0	443	192.168.2.6	49725	CN=cdn.quilljs.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu May 06 22:45:41 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Wed Aug 04 22:45:41 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
May 20, 2021 20:33:25.413702965 CEST	151.101.1.0	443	192.168.2.6	49726	CN=cdn.quilljs.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu May 06 22:45:41 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Wed Aug 04 22:45:41 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 20, 2021 20:33:25.582401037 CEST	104.16.19.94	443	192.168.2.6	49727	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020	Thu Oct 21 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
May 20, 2021 20:33:25.697061062 CEST	13.224.89.44	443	192.168.2.6	49731	CN=*.cloudfront.net CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Feb 22 01:00:00 CET 2021 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Tue Feb 22 00:59:59 CET 2022 Tue Aug 01 14:00:00 CEST 2028 Sun Nov 06 00:59:59 CET 2022	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 Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
May 20, 2021 20:33:25.702574968 CEST	13.224.89.44	443	192.168.2.6	49732	CN=*.cloudfront.net CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Feb 22 01:00:00 CET 2021 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Tue Feb 22 00:59:59 CET 2022 Tue Aug 01 14:00:00 CEST 2028 Sun Nov 06 00:59:59 CET 2022	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 Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 20, 2021 20:33:25.724039078 CEST	13.224.89.44	443	192.168.2.6	49735	CN=*.cloudfront.net CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Feb 22 01:00:00 CET 2021 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Tue Feb 22 00:59:59 CET 2022 Tue Aug 01 14:00:00 CEST 2028 Sun Nov 06 00:59:59 CET 2022	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 Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
May 20, 2021 20:33:25.729434013 CEST	13.224.89.44	443	192.168.2.6	49734	CN=*.cloudfront.net CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Feb 22 01:00:00 CET 2021 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Tue Feb 22 00:59:59 CET 2022 Tue Aug 01 14:00:00 CEST 2028 Sun Nov 06 00:59:59 CET 2022	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 Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
May 20, 2021 20:33:25.739680052 CEST	13.224.89.44	443	192.168.2.6	49733	CN=*.cloudfront.net CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Feb 22 01:00:00 CET 2021 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Tue Feb 22 00:59:59 CET 2022 Tue Aug 01 14:00:00 CEST 2028 Sun Nov 06 00:59:59 CET 2022	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 Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
May 20, 2021 20:33:25.827510118 CEST	104.17.183.73	443	192.168.2.6	49736	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sun Aug 16 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Mon Aug 16 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		
May 20, 2021 20:33:25.851089001 CEST	104.17.183.73	443	192.168.2.6	49737	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sun Aug 16 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Mon Aug 16 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		
May 20, 2021 20:33:26.499476910 CEST	52.218.221.248	443	192.168.2.6	49739	CN=*.s3-us-west-2.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jul 30 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Wed Aug 04 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
May 20, 2021 20:33:26.500135899 CEST	52.218.221.248	443	192.168.2.6	49738	CN=*.s3-us-west-2.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jul 30 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Wed Aug 04 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	3faf2df7ab96c36419c31725cb1fa7d6
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
May 20, 2021 20:33:27.045907021 CEST	31.13.92.14	443	192.168.2.6	49742	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Apr 06 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Sun Jul 04 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 20, 2021 20:33:27.069473028 CEST	31.13.92.14	443	192.168.2.6	49743	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Apr 06 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Sun Jul 04 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 4852 Parent PID: 792

General

Start time:	20:33:22
Start date:	20/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff721e20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Copyright Joe Security LLC 2021

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

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

Analysis Process: iexplore.exe PID: 5172 Parent PID: 4852

General

Start time:	20:33:22
Start date:	20/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4852 CREDAT:17410 /prefetch:2
Imagebase:	0xe60000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly

Copyright Joe Security LLC 2021