ID: 418883
Cookbook: browseurl.jbs
Time: 20:36:16
Date: 20/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

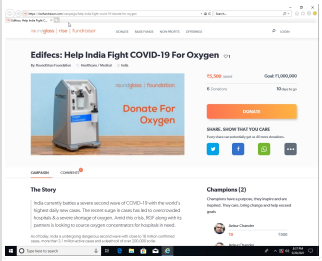
Analysis Report https://risefundraiser.com/campaign/he…

Overview

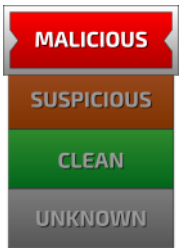
General Information

Sample URL:	http://https://risefundraiser.com/campaign/help-india-fight-covid-19-donate-for-oxygen
Analysis ID:	418883
Infos:	

Most interesting Screenshot:



Detection

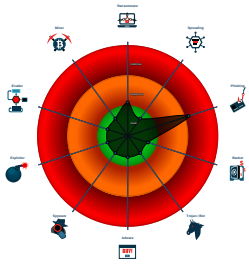


Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 2480 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 1496 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2480 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

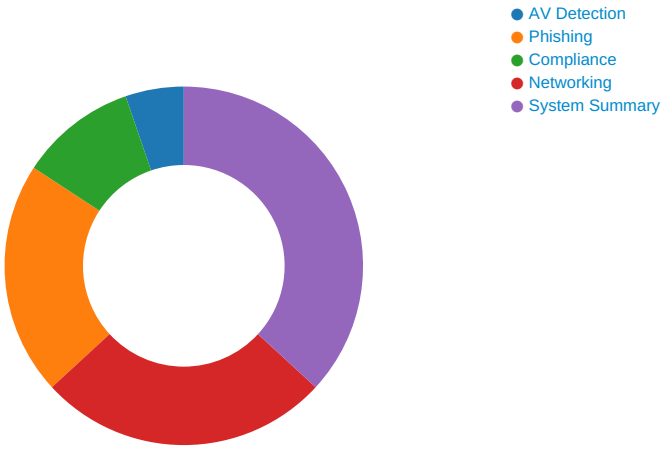
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

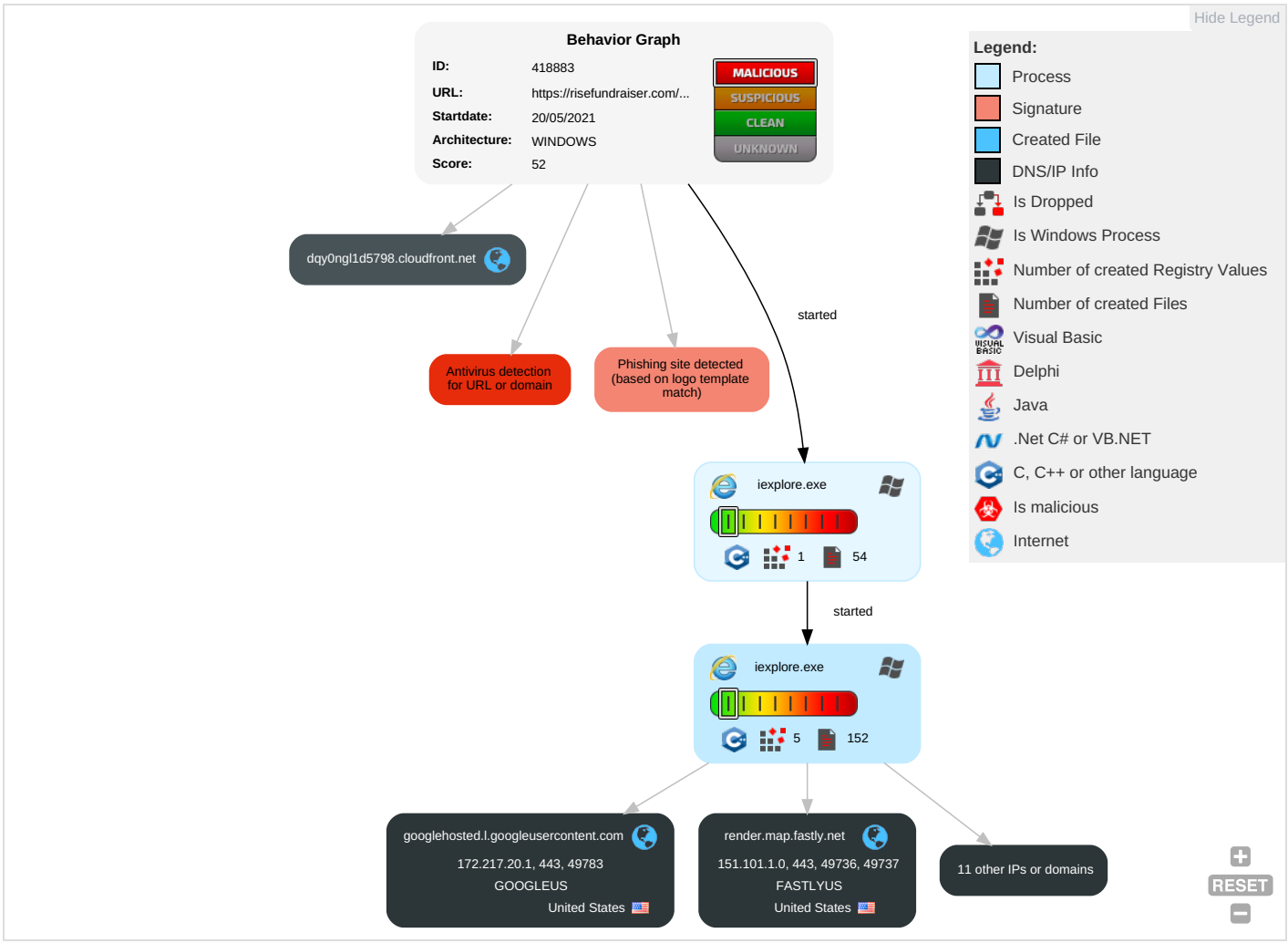
Phishing:

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

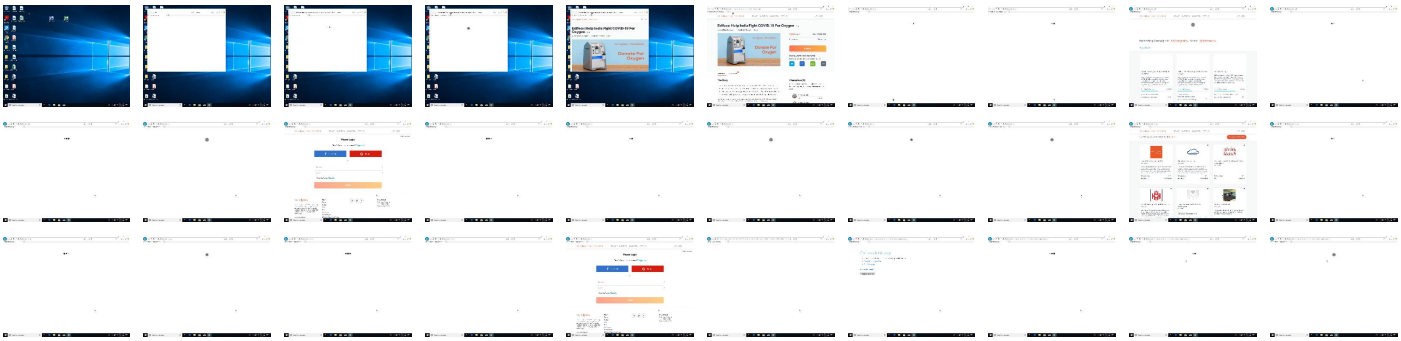
Behavior Graph

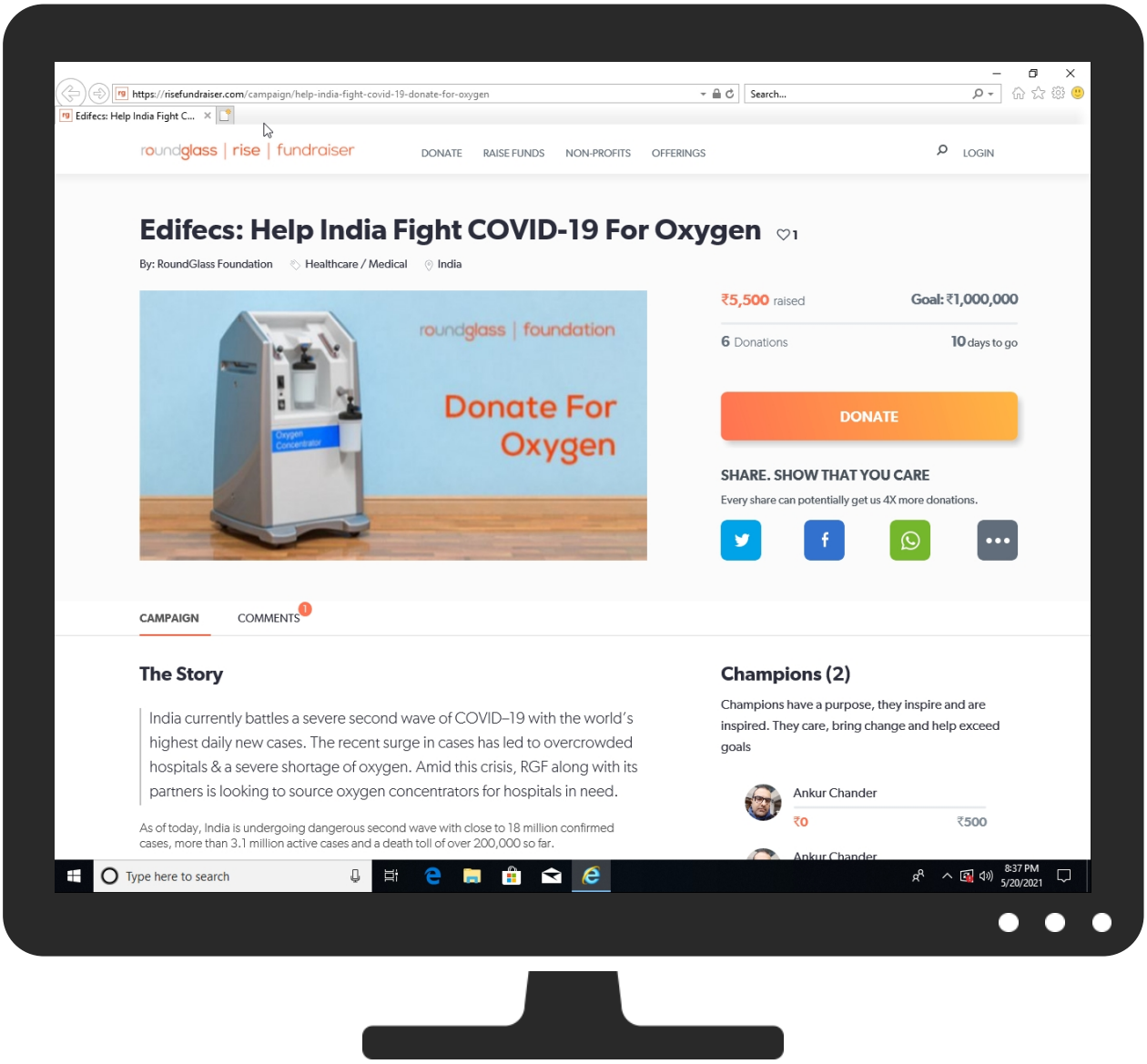


Screenshots

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
render.map.fastly.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://risefundraiser.com/orgs$	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://risefundr.com/loginRoot	0%	Avira URL Cloud	safe	
http://https://risefundraiser.com/create	0%	Avira URL Cloud	safe	
http://https://risefundraiser.com/reatehelp-india-fight-covid-19-donate-for-oxygeniser.com/	0%	Avira URL Cloud	safe	
http://https://risefundraiser.com/loginationhttps://dqy0ngl1d5798.cloudfront.net/assets/images/icon/favicon	0%	Avira URL Cloud	safe	
http://https://risefundr.com/reatehelp-india-fight-covid-19-donate-for-oxygenRoot	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/"	0%	Avira URL Cloud	safe	
http://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://https://risefundr.com/campaign/help-india-fight-ctegrated	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/loginhelp-india-fight-covid-19-donate-for-oxygen	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://risefundr.com/createhelp-india-fight-covid-19-donate-for-oxygenRoot	0%	Avira URL Cloud	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/offeringsj	0%	Avira URL Cloud	safe	
http://https://risefundraiser.com/createhelp-india-fight-covid-19-donate-for-oxygen	0%	Avira URL Cloud	safe	
http://https://risefundraiser.com/loginhelp-india-fight-covid-19-donate-for-oxygenb	0%	Avira URL Cloud	safe	
http://https://risefundraiser.com/campaign/help-india-fight-covid-19-donate-for-oxygen#campaigna-fight-covi	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://api.whatsapp.c	0%	Avira URL Cloud	safe	
http://https://risefundraiser.com/createhelp-india-fight-covid-19-donate-for-oxygend	0%	Avira URL Cloud	safe	
http://https://risefundr.com/notificationRoot	0%	Avira URL Cloud	safe	
http://https://risefundraiser.com/otification	0%	Avira URL Cloud	safe	
http://https://risefundraiser.Root	0%	Avira URL Cloud	safe	
http://fontawesome.iohttp://fontawesome.iohttp://fontawesome.io/license/http://fontawesome.io/licens	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	104.17.182.73	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
dqy0ngl1d5798.cloudfront.net	13.224.89.71	true	false		high
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high
render.map.fastly.net	151.101.1.0	true	false	• 0%, Virustotal, Browse	unknown
googlehosted.l.googleusercontent.com	172.217.20.1	true	false		high
s3-us-west-2.amazonaws.com	52.218.236.192	true	false		high
cdn.quilljs.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
lh3.googleusercontent.com	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

Name	Malicious	Antivirus Detection	Reputation
http://https://risefundraiser.com/campaign/help-india-fight-covid-19-donate-for-oxygen	true		unknown
http://https://risefundraiser.com/login	true		unknown
http://https://risefundraiser.com/campaign/help-india-fight-covid-19-donate-for-oxygen#campaign	true		unknown
http://https://api.whatsapp.com/send?text=https%3A%2F%2Frisefundraiser.com%2Fcampaign%2Fhelp-india-fight-covid-19-donate-for-oxygen%3Futm_source%3Dwhatsapp%26utm_medium%3Dsocial	false		high

URLs from Memory and Binaries

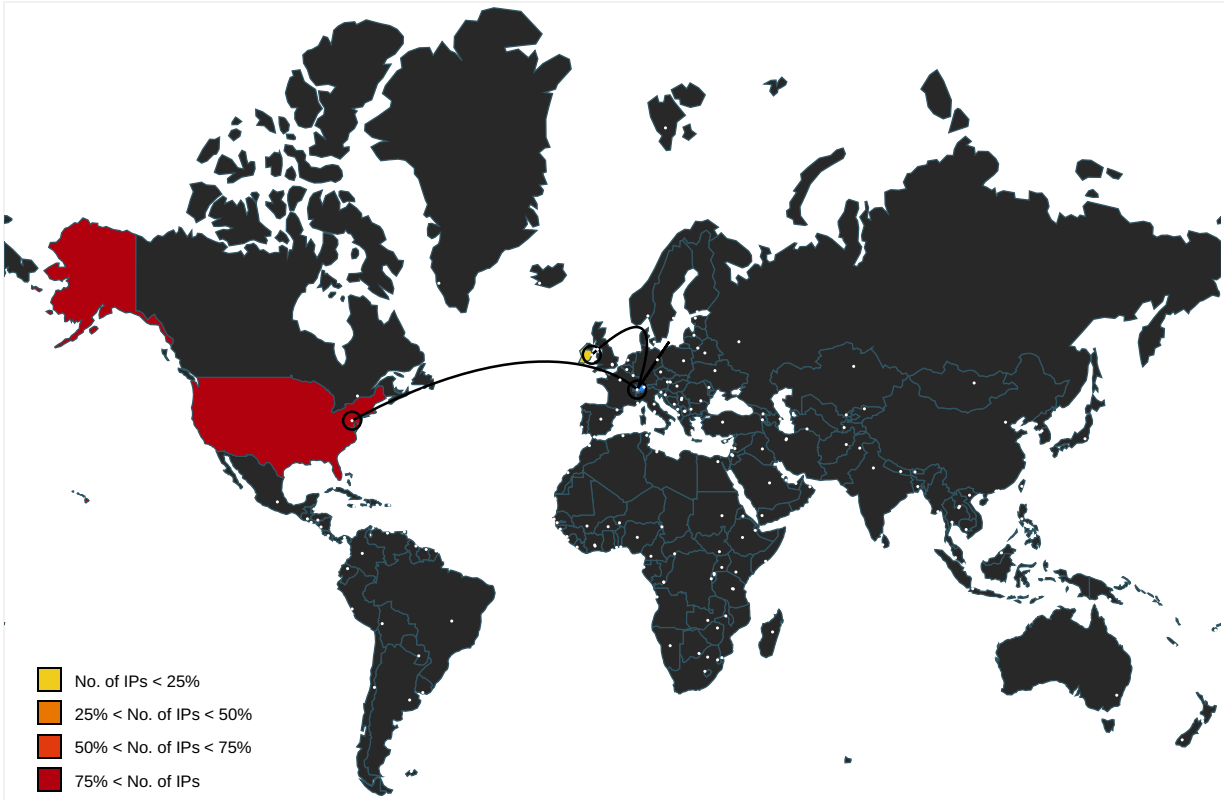
Name	Source	Malicious	Antivirus Detection	Reputation
http://fontawesome.io	fontawesome-webfont[1].eot.3.dr, font-awesome.min[1].css.3.dr	false		high
http://https://risefundraiser.com/orgs$	~DF6F133FC75023CC50.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/OwlCarousel2/2.1.6/assets/owl.carousel.min.css	create[1].htm.3.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_2_0.ttf	style-layout[1].css.3.dr	false		high
http://https://risefundr.com/loginRoot	{622DD189-B99A-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.quilljs.com/1.2.2/quill.snow.css	create[1].htm.3.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_4_0.eot?#iefix	style-layout[1].css.3.dr	false		high
http://https://risefundraiser.com/create	{622DD189-B99A-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://chartjs.org/	Chart.bundle.min[1].js.3.dr	false		high
http://https://risefundraiser.com/reatehelp-india-fight-covid-19-donate-for-oxygeniser.com/	~DF6F133FC75023CC50.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_0_0.eot?#iefix	style-layout[1].css.3.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/1.9.7_P9_patch2/main.94919de6defa08284319.js	create[1].htm.3.dr	false		high
http://https://risefundraiser.com/loginationhttps://dqy0ngl1d5798.cloudfront.net/assets/images/icon/favicon	~DF6F133FC75023CC50.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://risefundr.com/reatehelp-india-fight-covid-19-donate-for-oxygenRoot	{622DD189-B99A-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css	create[1].htm.3.dr	false		high
http://https://risefundraiser.com/campaign/help-india-fight-covid-19-donate-for-oxygenZEdifecs:	{622DD189-B99A-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://dqy0ngl1d5798.cloudfront.net/assets/images/icon/favicon.ico?v=2	create[1].htm.3.dr, ~DF6F133FC75023CC50.TMP.1.dr	false		high
http://https://connect.facebook.net/en_US/fbevents.js	create[1].htm.3.dr	false		high
http://https://risefundraiser.com/"	risefundraiser[1].xml.3.dr	false	• Avira URL Cloud: safe	unknown
http://getbootstrap.com)	bootstrap.min[1].css.3.dr	false	• Avira URL Cloud: safe	low
http://https://dqy0ngl1d5798.cloudfront.net/1.9.7_P9_patch2/scripts.d004d92bf73ccd662204.js	create[1].htm.3.dr	false		high
http://https://github.com/krux/postscribe/blob/master/LICENSE.	gtm[1].js.3.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/Swiper/4.5.0/css/swiper.min.css	create[1].htm.3.dr	false		high
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.3.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_2_0.eot	style-layout[1].css.3.dr	false		high
http://https://risefundr.com/campaign/help-india-fight-ctegrated	{622DD189-B99A-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://risefundr.com/orgsRoot	{622DD189-B99A-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://fengyuanchen.github.io/cropperjs	styles.a19aec6bac6aa86c5932[1].css2.3.dr	false	• Avira URL Cloud: safe	unknown
http://round.glass/rise/"	risefundraiser[1].xml.3.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_4_0.ttf	style-layout[1].css.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://risefundraiser.com/campaign/help-india-fight-covid-19-donate-for-oxygen#campaign	{622DD189-B99A-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false		unknown
http://https://risefundraiser.com/campaign/help-india-fight-covid-19-donate-for-oxygen	{622DD189-B99A-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false		unknown
http://https://risefundraiser.com/loginhelp-india-fight-covid-19-donate-for-oxygen	~DF6F133FC75023CC50.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://dqy0ngl1d5798.cloudfront.net/1.9.7_P9_patch2/polyfills.661b9383b7c93a39b0f5.js	create[1].htm.3.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_5_0.eot	style-layout[1].css.3.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_5_0.eot?#iefix	style-layout[1].css.3.dr	false		high
http://www.idangero.us/swiper/	swiper.min[1].css.3.dr	false		high
http://https://risefundraiser.com/campaign/help-india-fight-covid-19-donate-for-oxygen.com/campaign/help-in	{622DD189-B99A-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_3_0.eot?#iefix	style-layout[1].css.3.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/systemjs/0.19.39/system.src.js	create[1].htm.3.dr	false		high
http://https://cct.google/taggy/agent.js	gtm[1].js.3.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.3.dr	false		high
http://https://risefundr.com/createhelp-india-fight-covid-19-donate-for-oxygenRoot	{622DD189-B99A-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://dqy0ngl1d5798.cloudfront.net/assets/images/microsite/hero.jpg	style-layout[1].css.3.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_4_0.eot	style-layout[1].css.3.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/images/microsite/storybg.png)	style-layout[1].css.3.dr	false		high
http://https://s3-us-west-2.amazonaws.com/rg-fundraiser/assets/images/calculator-v1.js	create[1].htm.3.dr	false		high
http://https://www.google.%/ads/ga-audiences	analytics[1].js.3.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.3.dr	true	• Avira URL Cloud: malware	unknown
http://https://quilljs.com/	quill.bubble[1].css.3.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_5_0.ttf	style-layout[1].css.3.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/images/icon/favicon.ico?v=2~	imagestore.dat.3.dr	false		high
http://https://risefundr.com/offeringsRoot	{622DD189-B99A-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap.min[1].css.3.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/themes/style-layout.css	create[1].htm.3.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_7_0.eot?#iefix	style-layout[1].css.3.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_5_0.woff	style-layout[1].css.3.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_6_0.woff	style-layout[1].css.3.dr	false		high
http://https://risefundraiser.com/offeringsj	~DF6F133FC75023CC50.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_7_0.woff	style-layout[1].css.3.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_3_0.woff	style-layout[1].css.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_4_0.woff	style-layout[1].css.3.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_0_0.eot	style-layout[1].css.3.dr	false		high
http://https://risefundraiser.com/createhelp-india-fight-covid-19-donate-for-oxygen	~DF6F133FC75023CC50.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/chartjs/Chart.js/blob/master/LICENSE.md	Chart.bundle.min[1].js.3.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/Swiper/4.5.0/js/swiper.min.js	create[1].htm.3.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/1.9.7_P9_patch2/vendor.7b1b41a937a083fd16b0.js	create[1].htm.3.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_0_0.woff	style-layout[1].css.3.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_6_0.eot	style-layout[1].css.3.dr	false		high
http://https://risefundraiser.com/loginhelp-india-fight-covid-19-donate-for-oxygenb	~DF6F133FC75023CC50.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://api.whatsapp.com/send?text=https%3A%2F%2Frisefundraiser.com%2Fcampaign%2Fhelp-india-fight-co	{622DD189-B99A-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_1_0.woff	style-layout[1].css.3.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_2_0.woff	style-layout[1].css.3.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_2_0.eot?#iefix	style-layout[1].css.3.dr	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js	create[1].htm.3.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_3_0.eot	style-layout[1].css.3.dr	false		high
http://https://risefundraiser.com/campaign/help-india-fight-covid-19-donate-for-oxygen#campaigna-fight-covi	~DF6F133FC75023CC50.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_3_0.ttf	style-layout[1].css.3.dr	false		high
http://daneden.me/animate	animate.min[1].css.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/OwlCarousel2/OwlCarousel2/blob/master/LICENSE)	owl.carousel.min[1].css.3.dr	false		high
http://https://api.whatsapp.c	{622DD189-B99A-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://dqy0ngl1d5798.cloudfront.net/assets/images/microsite/icon/fundraiser-Ico.png	style-layout[1].css.3.dr	false		high
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_6_0.ttf	style-layout[1].css.3.dr	false		high
http://https://risefundraiser.com/createhelp-india-fight-covid-19-donate-for-oxygend	~DF6F133FC75023CC50.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://dqy0ngl1d5798.cloudfront.net/assets/fonts/313E30_0_0.ttf	style-layout[1].css.3.dr	false		high
http://https://risefundr.com/notificationRoot	{622DD189-B99A-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://risefundraiser.com/otification	~DF6F133FC75023CC50.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://risefundraiser.Root	{622DD189-B99A-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://dqy0ngl1d5798.cloudfront.net/assets/images/microsite/icon/promote-Ico.png	style-layout[1].css.3.dr	false		high
http://fontawesome.iohttp://fontawesome.iohttp://fontawesome.io/license/http://fontawesome.io/licens	fontawesome-webfont[1].eot.3.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css	create[1].htm.3.dr	false		high
http://https://risefundraiser.com/orgs	{622DD189-B99A-11EB-90EB-ECF4BBEA1588}.dat.1.dr, ~DF6F133FC75023CC50.TMP.1.dr	false		unknown
http://https://risefundraiser.com/offerings	~DF6F133FC75023CC50.TMP.1.dr	false		unknown
http://https://cdn.quilljs.com/1.2.2/quill.bubble.css	create[1].htm.3.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.17.182.73	js.hsforms.net	United States		13335	CLOUDFLARENETUS	false
104.18.10.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
31.13.92.14	scontent.xx.fbcdn.net	Ireland		32934	FACEBOOKUS	false
52.218.236.192	s3-us-west-2.amazonaws.com	United States		16509	AMAZON-02US	false
13.224.89.71	dqy0ngl1d5798.cloudfront.net	United States		16509	AMAZON-02US	false
172.217.20.1	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	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
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	418883
Start date:	20.05.2021
Start time:	20:36:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 51s

Hypervisor based Inspection enabled:	false
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:	12
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@3/115@10/9
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 • Browsing link: https://api.whatsapp.com/send?text=https%3A%2F%2Frisefundraiser.com%2Fcampaign%2Fhelp-india-fight-covid-19-donate-for-oxygen%3Futm_source%3Dwhatsapp%26utm_medium%3Dsocial • Browsing link: https://risefundraiser.com/campaign/help-india-fight-covid-19-donate-for-oxygen#campaign
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.64.90.137, 92.122.145.220, 104.43.193.48, 13.88.21.125, 168.61.161.212, 88.221.62.148, 172.217.16.106, 172.217.16.104, 142.250.186.110, 52.147.198.201, 20.82.210.154, 152.199.19.161, 92.122.213.247, 92.122.213.194 • 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, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, go.microsoft.com, www.googletagmanager.com, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, www.google-analytics.com, skypedataprdcolwus17.cloudapp.net, www-google-analytics.l.google.com, ajax.googleapis.com, ie9comview.vo.msecnd.net, www-googletagmanager.l.google.com, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\E5F0NRSV\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:	dropped
Size (bytes):	838988
Entropy (8bit):	5.708891291986737
Encrypted:	false
SSDEEP:	24576:lU5iIDQSzB0xE9zdrU5iIDQSzB0xE9zdVU5iIDQSzB0xE9zd3U5iIDQSzB0xE9zd:lU5iIDQSzB0xE9zdrU5iIDQSzB0xE9zB
MD5:	8648A0A85D421BBAC0AD0108124F59C7
SHA1:	6D9059B0DD6E30C87B8A89DF53D247C88D7D6221
SHA-256:	88006176DF720C29F89F21390F9FFAAEB0136775B405A8EB5469B631A5B578A8
SHA-512:	D6AFB4F91B581F86E761A1363D9EFDFC93D3531C4F9FF9C32A43B1780C70BCC30F891579A631EBCA875669FDA0BEBFF0E7E46F709F1FEA85236BF37B5B833A24
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="window.location.pathname" value="/campaign/help-india-fight-covid-19-donate-for-oxygen" ltime="665883840" htime="30887335" /></root><root><item name="window.location.pathname" value="/campaign/help-india-fight-covid-19-donate-for-oxygen" ltime="665883840" htime="30887335" /><item name="localStorage" value="1" ltime="666823840" htime="30887335" /></root><root><item name="window.location.pathname" value="/campaign/help-india-fight-covid-19-donate-for-oxygen" ltime="665883840" htime="30887335" /></root><root><item name="window.location.pathname" value="/campaign/help-india-fight-covid-19-donate-for-oxygen" ltime="665883840" htime="30887335" /><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.{622DD187-B99A-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8541718340173605

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{622DD187-B99A-11EB-90EB-ECF4BBEA1588}.dat	
Encrypted:	false
SSDEEP:	192:r+Z1ZB2YWitYifFj9zML1BpvD1sfdjAjX:rK7wvaFMzNoC
MD5:	03F28B8D33F124CD82503434F5377938
SHA1:	875D024D9031109A47C69134F4D23220B3FAC39F
SHA-256:	01C2E13734C39908D3A6AE2942A04D38D643CEF2B062B571FDFACA10E0BA4B99
SHA-512:	D514BE6CED30755E85A98E45B19EA5171129C715A25F63855F1A009A7560BDA793E91848E8FC6374233F8F470791EBBA4C22EFA5673777F06786E93FF5B47D80
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\{622DD189-B99A-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	198238
Entropy (8bit):	2.5567369069229486
Encrypted:	false
SSDEEP:	384:riy4oAsc1CUt8Jfc/JfZ2Pqem4Djewgg4UVmw/VO9O8cCs701Pe2FUQaVgJGY1YV:DJeJXQp3SjkSjCztpf7VtFtQt/W
MD5:	4AC80084EEDD72E6C9739F63A6F1B08A
SHA1:	B276C101CF8B95BDAEE49F3F4166D2CF1B21F85D
SHA-256:	9705F11D65A8C5B6BD4385F5D19AFA3268576C17F6B3A75A59851D6D194B8A09
SHA-512:	0F35D501A64A82D1FAEABF7C1457E10F6F90F039699F562B206F0D37DB0B302759F95AABFBE6364CC23EAD13EEBD0BD162A5E8A9158AB0F455A652039663B38
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\{69711AB1-B99A-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5650344976895896
Encrypted:	false
SSDEEP:	48:IwgGcprpGwpaEG4pQMGrapbS5GQpKRG7HpRfTGIpG:rEZDQ06KBSTAATdA
MD5:	8344D75B8095BCBE66A47DB00685F205
SHA1:	CA8B66995CFE3A4ECAC01C1E80D0811D78D392C9
SHA-256:	1160832E036EA8C33BE823EAAFD884F2C6F49150CF7A194EBDB0E5A45D784F50
SHA-512:	7D0BB93106862092A26E93423313BBDC7BE5DD025243806D5E29E9277DA7FF69AC17356767C65FE844F48572141DD7B765FE8A29D9419EF455879C821BEF9410
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\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+HnoNVnoBMoLFinokoqboVt5cgoAoA1O:8HjzaXcklyCD+4V1GvZO
MD5:	24A94E19CB4AF83D9287422BD3C69317
SHA1:	C0E13E1C2A101B0455C3BB84F82EBADEF2745255
SHA-256:	8C07B91716A95827F8054DDD831A8C2A6B2AEAF80CD7ACC4C76D4754A7566F33
SHA-512:	22FDC0E06C2F5C1094F72AD4AC6594AA5156730A1AB1CA9B220F79F04DF9FE7C5456D7A7EEB5D4B62A550D1D9E861B611AE77A2D68A7A674B37FA65A2B9C60C
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
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..'N..)K..(M..(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.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..'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..(M..'N..'N.&N..'N.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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\2WF3MMUU\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\2WF3MMUU\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:	CB3CE2BCEB61F390298C21E470423CCEB6DD93E648A7DD0467195B11FEF30BF7A086DFF47C4494E2533498D1448C1A22AAB1414C14FD73278F1C92E0F7BC3F54
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\analytics[1].js	
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||"undefined"==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):|[^:/?#]*(?:[/?#]|$))/i;var y=window,z=document,A=function(a,b){z.addEventListener?z.addEventListener(a,b,!1):z.attachEvent&&z.attachEvent("on"+a,b)};var B=/:[0-9]+$/,C=function(a,b,c){a=a.split("&");for(var d=0;d<a.length;d++){var e=a[d].split("=");if(decodeURIComponent(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\2WF3MMUU\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:KkZcIOIVjl2eIWInPywe1aAvkqDX3oyq5BrieD0OTbsysV:KkZ8Pywe1aAvkqDX3oyq5BrieD0OTq
MD5:	178B651958CEFF556CBC5F355E08BBF1
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\2WF3MMUU\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:	E8C5DAF01EAE68ED7C1E277A6E544C7AD108A0FA877FB531D6D9F2210769B7DA88E4E002C7B0BE3B72154EBF7CBF01A795C8342CE2DAD368BD6351E956195F 8B
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\2WF3MMUU\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\campaign[1].htm	
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\2WF3MMUU\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...$K .al...Qr.+...TR._...y.....U)W\.<.]N..|....@B...v@2..B .I\....|.....1+mW-....;.....\.....w.8+47.br8&,3l.j...~1d...b.H. Y..Y%.`....X..d.$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.. ..I...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\2WF3MMUU\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";....//used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the website you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\font-awesome.min[1].css	
SHA-512:	49F4E24E55FA924FAA8AD7DEBE5FFB2E26D439E25696DF6B6F20E7F766B50EA58EC3DBD61B6305A1ACACD2C80E6E659ACCEE4140F885B9C9E71008E9001FBF4B
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-webfont.ttf?v=4.7.0') format('truetype'),url('../fonts/fontawesome-webfont.svg?v=4.7.0#fontawesomeregular') format('svg');font-weight:normal;font-style:normal}.fa{display:inline-block;font:normal normal normal 14px/1 FontAwesome;font-size:inherit;text-rendering:auto;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}.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\2WF3MMUU\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\2WF3MMUU\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):	5.504938494961797
Encrypted:	false
SSDEEP:	1536:EDRnpXBMY2t4FP0M+HRBfVF9pUnG/wZjd/bWB41E9DKPEI31IqB1XBgj4+Tl:EtnpXBMY2UP0pfVn/EdSBc+Tl
MD5:	FB03A97E6E876A1D9E4A65364DE9A0C7
SHA1:	4CE81401CDFF314C941024BE3F4DFDE0F7BF112F
SHA-256:	979425217C6C12165ADE9777989BBD0CE48E11A22E2BC45B550FF2AB66F7D08F
SHA-512:	165C3940DA887823606B446E6540189439FF52014F12D0695C9DBE5EA58CBC5109A564393C68BFC5486B5C2D800BB3E95A174C4B6CFDF93419B10ACD036C402E
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.elementId",. "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_useHashAutoLink":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_name":"gtm.elementUrl",. "vtp_dataLayerVersion":1. },{. "function":"__u",. "vtp_comp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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):	18142
Entropy (8bit):	4.94862352509096
Encrypted:	false
SSDEEP:	384:LxEQallHrBjSSFHJT4ZjGrxN8bfMxEQallHrBjSSFHJT4ZjGrxN8bfM:LxEQallHrBjfFpT4ZjkxN+ExEQallHrX
MD5:	930BEB337957CB670EA0A26E14F60641
SHA1:	82E9EDCFFFB9963BCAA5630B4E69EE31F3A022A0
SHA-256:	191023D73725AF7817E533FD81FC969E7218AEEFC55E4866B5B1BFFE7D5F07F0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\help-india-fight-covid-19-donate-for-oxygen[1].htm	
SHA-512:	76C95899A49630D4BDE42153E78B0A1BEDD992AFC46554504CB57D3F7F7472D1E6A6BA356079F3D3C7589D184D94028DC35573274EC8805BC7195505BCC552A
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\2WF3MMUU\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
Malicious:	false
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\2WF3MMUU\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:	downloaded
Size (bytes):	10681
Entropy (8bit):	5.248732891277713
Encrypted:	false
SSDEEP:	192:IYt5nFxXtSPDmAhkj6FxX8SJcfZimFZso1AjuApFpgth49tpzn8:9LXUmapLX8uZmZ1A3C
MD5:	1D73CB27C802DE1C89203C09A17F9E6C
SHA1:	7448E24A2D2CAE0A6A5D859171FCFDED3AE48239
SHA-256:	C5036FC0FBA17A3C421C1A8774B61338914D6B0C205F8459D29CE9FED63E15E9
SHA-512:	C2B30D70D5126D27A8C66E92A40CAB0F153E5C8C57E9466619F8CAE3607F043402C03186208E03FDB423C56E0F788EFAEE7F5742D5275C547A7E9356A11982FE
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":{"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}{"status":true,"data":{"gatewayInfo":{"INR":{"gatewayType":"System","id":4,"gatewayName":"Razorpay","merchantLiveKey":"XvraiCi7XGJBu8pPSeZWrGlt","merchantLiveSecret":null,"merchantTestKey":null,"merchantTestSecret":null,"signatureLive":null,"signatureT

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\help-india-fight-covid-19-donate-for-oxygen[3].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\help-india-fight-covid-19-donate-for-oxygen[3].htm	
Reputation:	low
Preview:	{"status":true,"tipStatus":true,"data":null,"errorCode":10000}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\help-india-fight-covid-19-donate-for-oxygen[4].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:	B81B17C9D0B5F7312066464C9769F0E0C69F2F47F7F588CBF1DA9869F13F4DA111B27537E1A884AEC4C2F34E4ACFD04FBB5A8B5FDAEDE815D58B514246EFEE 8
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","docu ments":"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\2WF3MMUU\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:	60A53E385CF1C000F69C8FC0F4822E352E0D5DEEC141B6D3BAF12C98B054C74A590BB7E66E285659BE412CC71221983C5B12ADADE44237C4C0DA7CA4320E95 2
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\2WF3MMUU\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:	26C569182D3AAB26912CFFE89BDDACB6FBABB658D428F3FE7758754486B606823BBC1D1761E4B42319C133287DE9067B3A5325D3081BD064610FB145215BA4A2
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\2WF3MMUU\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..l.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\2WF3MMUU\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://dqy0ngl1d5798.cloudfront.net/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 9.277344 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\2WF3MMUU\mobile-brandlogo[2].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 9.277344 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\2WF3MMUU\no-org[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 122 x 112, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	18123
Entropy (8bit):	3.243205595169036
Encrypted:	false
SSDEEP:	192:ASCk6zY3msAakSv5VZi0e5Qv4PyvQxKJcE:nB6zYWPakSv5VZiZaLv9cE
MD5:	F9984F14F3BA133B1498FE0E6B791DA2
SHA1:	BE38DCB9F30F900CFD866663C7FEB71CBD1D1703
SHA-256:	6E71FAC7555D79BF25BA3C919EB2A70BFE7CE92F1668737AA9F0DE1F8658DAD9
SHA-512:	D814EB6718C02958F0CA995EDD28B98080846C48958B6DA1356358E5BA15E158F59F9FD4501BAF67C0DE93A055FC8598312405F93C8F2AB30AF28F9FCDFF3163
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\no-org[1].png	
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/assets/images/no-org.png
Preview:	.PNG.....IHDR...z...p.....d.....pHYs.....9.iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?>.<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c111 79.158325, 2015/09/10-01:10:20 ">. <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">. <rdf:Description rdf:about="". xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/". xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#". xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#". xmlns:xmp="http://ns.adobe.com/xap/1.0/". xmlns:dc="http://purl.org/dc/elements/1.1/". xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/". xmlns:tiff="http://ns.adobe.com/tiff/1.0/". xmlns:exif="http://ns.adobe.com/exif/1.0/">. <xmpMM:OriginalDocumentID>xmp.did:FF6C3485085E11E6A7ED84C10F67A695</xmpMM:OriginalDocumentID>. <xmpMM:DocumentID>xmp.did:22416D54098311E68B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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:	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\2WF3MMUU\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\2WF3MMUU\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
SSDEEP:	384:OXa6h8sJ1vcYCW+3P3/YgJhgosEJRJByKnRWI7FFrFhFrFJMSFWprGymGibPz7Ql:OXZh8NYCW+3P3/YgJhgosEJRJByKnRWZ
MD5:	455913274305F030C2944F8DE75A0996
SHA1:	12165B0AABA2E1E44311B6160CF54313598508AE
SHA-256:	C99A5C5600B39A3FC8A4B2A47BD9B8C6276F399284C1F32D893852979C5197DA
SHA-512:	D7747CD19AD3DB2C93FC5A617B7D861FCA77AE7E59E993380A8981ACC4A8DA5E33E19868197C8CCCA8F7D3A939E1FE96530CF1989EB3CD3D3F32781F91699F7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\quill.snow[1].css

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\2WF3MMUU\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/lhPEmNT7xWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWC:6v/7sml7rQxOmp9ZZ/3VHdlAXVHT1
MD5:	D5771DF738B58A49F97A7E81FC57950F
SHA1:	4127BF2E7D5704BF750D6C55C82DF54DD21A6712
SHA-256:	3EB6E5F60B14BE86B9C5778047CC617BDFBE7D9DF5B40AA0BE17E642885DF0A6
SHA-512:	E8CFCA24489BA4AF6B16FB0E2387C64F44E46BD68D8747FD9A875231170D70ABAFE89439024E4D1BD12151FBA97BE6E9B187CACA2B7C3015FE171A14F5782F6 3
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^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^SZ^Z5.3...:tRNS.......... !$).689>RTWZbpx{.............................Bf ;.....IDAT..U....P.E.`.;.....\......\..9o.!'.8..&?...E,...@;.U-..l..#S.e@'i.\..PN.XU9++..2...^.fw..)..h..wo&....&.^.qu..G.GO........"5.`$....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\styles.a19aec6bac6aa86c5932[1].css

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
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
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\2WF3MMUU\theCenter2-350px[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=16, height=6144, manufacturer=Canon, model=Canon EOS 5D Mark II, orientation=upper-left, xresolution=2294, yresolution=2302, resolutionunit=2, software=Adobe Photoshop CC 2014 (Windows), datetime=2015:01:26 13:24:41, width=4096], baseline, precision 8, 350x400, frames 3
Category:	downloaded
Size (bytes):	199375
Entropy (8bit):	7.895687902636443
Encrypted:	false
SSDEEP:	3072:DkK056T7kio7o3rBgDEntCzPf8KE9ZwLMAR+8OEzMsev2UWGvz6MExsph:DkK056HoobnntOYZwLMY1ovFb6M2k
MD5:	1A7178933DC3BF18500C64C0A7D79E9A
SHA1:	5271FF428501C24DE6974FA436B688AFF9417E95
SHA-256:	AF3F9922E6DB913921379D60A91493099E2F2B041D798A9158A044850839031F
SHA-512:	A074514D5554024BFCF477285B40FB3D4DCA9A0D106B15AD4424E6EA1CDE7F2A76C62A6DB7F068CB5DD4821D64F23146836171270AE40897FAC88E08204660
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\theCenter2-350px[1].jpg	
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/media/10959/theCenter2-350px.jpg
Preview:	......Adobe.d.....2.Exif..MM.*.....(.....1....."....2.....(.;.....<.....-...P.i.....~.....&...F.....l..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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.s plice(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\9026IKNJ\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
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("lp0R"),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.enableAddOrgan ization=!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_SO RTING),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\9026IKNJ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\2020-01-23_22-57-36[1].jpg	
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...........(...((..........."...}........! 1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.................w... ....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..........?......a....:.y.Z]..D9.i.n.?. ..N.E..9...-..l.`....}s.../nJ.......a...*..Z......[.....=...~.}z......Q..n.=..'V.]...?......[..S..Mk....4.L..T.....*p...4.#/..rq[V..>..w.\.......=.H...=i...$d..R...a...r.'$.T...?5..JK...(m.7b.j..J.2.N .dsK...T.Uo2Z5.A......Ug9...K.X..._s.S.pH...VL0'4.e-P....M......M.......A o3..I..G...#....l.s.....%.j.I8.V..e....#g...3^

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\2126210880948599[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	780261
Entropy (8bit):	5.469219756242312
Encrypted:	false
SSDEEP:	6144:Rk1HgCSntDV/HaK3V/Ha8NEPjQHguH3HpQrwzzmak1HgCSntDV/HaK3V/Ha8NEPw:dNESXNESXNESh
MD5:	1A01B87AD9BFCFEF8085580509E16AC6
SHA1:	4A7DECF0126F8AF69B4762EC7CEE6F5767DA2AA7
SHA-256:	93538E2907F6D0F0E48C9A2886BCDCCFAB5077279F5CF6C755800176EEEB541D
SHA-512:	36AFA0962BFB12563C8C05444FC3E11C5F2814C6B2E2429E5761CC7820B57EAFE06C4BE0930D948C8CE5303A1D6FBC9AB45DD7D332D424FDE70372B56D4217D
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\9026IKNJ\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\9026IKNJ\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:lD58eBgVblaCamVpU8hu4F01E2Av9AXxatwyw1vWjFYrpM1qDIw/1c/cLkjJ2HOQ:1awu8rv9egRw1vWjFYrO8OL/9q9og
MD5:	A9963E007E9D8BDA1DED3FD7B87A8C9C
SHA1:	2E08A3B913F2FAFBCE4A69AFBC833B81B85155F7
SHA-256:	F262C7DEEF76FDE080C7350AABEDA4FBB6E3AF3D34ED01189863DD5B42CAAE63
SHA-512:	56871B498EA5374EDEB8E4AAA52E237D9BFEF1E60D303BACF1964571BA9F89520394106E7939937EE5183E701BF8786D0D212D7AC0FC34F2E2353F894ADB24C2
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\22.ffb009f27d517354a7bf[1].js	
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\9026IKNJ\GV[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):	6192
Entropy (8bit):	7.928433256605386
Encrypted:	false
SSDEEP:	192:NOnJb3r7NXkhpoiy6sV58EL9AO7e5IzpAIAc:NOnJbuhp7sz8ERAae5Zc
MD5:	380E05E08FDFE5A5363CF78157502BB1
SHA1:	C1D7F2B401855883C7B43A94DB0F41ED8B77C886
SHA-256:	B6F6686B11DCC853924923CCBD1F9B0916F848F8344C5CDB1744CFD2CC4FE0DE
SHA-512:	B0CAE6AEC6691C6F286E4BE0799A2D4845F0D81491C5304E072EBD05AA881DD5B7C197FC17AE40A6E55031A54B3A47A1AD6A6457E93424374C0BF70ED286C2 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/media/15987/GV.png
Preview:	......JFIF.............C....................................%...#... , #&')*)..-0-(0%()(...C...........(...((.........."......................................<.........................!.1 ."A.2Qaq..#B....$.Rb....Cr................................%.......................!1A.."#2Q.a...........?...!@..B..S^p.S.k. ......<&.y9.Pp.&.....i.t:Hw;9No..9.c)..&.v..?2.}...~Uf.<...+.B.9N....... .q......\|b.FF1.R.b.x$...r... ..d.O.x^...Sg^F.i....J.....HqB_D.N.".T9...o...(L...e!8......z...X....p..XP. p(%....3..d..c...(.1....E.TR.x..s....E..6...j.....++:!..e.o...w.....vX-.6..k..z[#H.`. I.8.c..y.0y..a]..C@.9..=.=..Jm..*0..8....!>$..o.43.......W.;D....H....A.w[.....D...[.=..........{*.....C.U.E.....Z.T......B...g!;.9.HJM.z.9.8+FV..5..JPr......K..X.<..A....Sr.....7...^.g....p q.]BoT.).n........I......F.{.z..VC).{.`*sSt..........]..U.J.fm...d......xmZ;.26d....=l4.&i.@..$.m.......*{.:.......w.7Fp.'.....geC.Z{)K.. .

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284 D
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #00 0000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\RG-FoundationYoutubeProfile[1].jpg</th></tr>
<tr><td>SHA-512:</td><td>4A52CDC46D920FABFCB3921E0E29036BEFCB28DD81D27CE9BDC249A9101237C4F174113DAAFD05DE3D85866A1AF2A4248E640FF09F48F28797522AC1D461EE7</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://dqy0ngl1d5798.cloudfront.net/media/17437/RG-FoundationYoutubeProfile.jpg</td></tr>
<tr><td>Preview:</td><td>......JFIF.............C....................................%...#... , #&')*)..-0-(0%()(...C...........(...((...........".......................................8....................
......!1AQ.."a..q25s...#B....6b..................................0.......................!.1Aa.Qq."2....#4R.r...............?..DE...a...D@...DD....D@...DD....D@...DD....D@...DD....D@...DD..
..D@...DD....D@...DD....D@...DD....D@...DD....D@...DD....D@...DD....D@...DD....D@...DD...w.N..@...DD....D@.]. .\n]..........=.".u8B3._...j..N..\.k!.j>..d.sF.F.^.el.O...n.
Z}...Q.......S\.}.~.]..S..z.-.,lq2..k.4.....@.Te...8K.*^a....D@...DD._.W.Y......_.W.Y.....^....<....eg..9.X........D.g.........k...}.Y....M.kZnY...%......:..$..+Q....................1....3.>~2.#|v"<.>
..D...#...W.Qd....M/E./#..:!...K.i....].-1.Y_...7T.......D..E.....A...8.p.u&>s..7.v..\Z.l.`.......s+.tl....Vf.$.6.XC......7.++.:.............81.6=...W..+8'g..I.....e..4;*..J-.../l....%.?.X./..J.</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\bootstrap.min[1].js</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>ASCII text, with very long lines</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>37045</td></tr>
<tr><td>Entropy (8bit):</td><td>5.174934618594778</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>768:o2rGy27UwlNqMl95qNmCFejhqs8snmi+CSFXfbx8Gf3Zq7Q:Jg73zhq0GvbJ3ZKQ</td></tr>
<tr><td>MD5:</td><td>5869C96CC8F19086AEE625D670D741F9</td></tr>
<tr><td>SHA1:</td><td>430A443D74830FE9BE26EFCA431F448C1B3740F9</td></tr>
<tr><td>SHA-256:</td><td>53964478A7C634E8DAD34ECC303DD8048D00DCE4993906DE1BACF67F663486EF</td></tr>
<tr><td>SHA-512:</td><td>8B3B64A1BB2F9E329F02D4CD7479065630184EBAED942EE61A9FF9E1CE34C28C0EECB854458977815CF3704A8697FA8A5D096D2761F032B74B70D51DA3E37F4</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js</td></tr>
<tr><td>Preview:</td><td>/*!. * 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.</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\campaigns[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	20111
Entropy (8bit):	5.219702401866339
Encrypted:	false
SSDEEP:	384:fGL5T/fwTmh0ym7lmnMoA8brieHDTRzaJQRrF:f45T/fwTmh0xRmMoA8bWwao
MD5:	FC718E4B02A1200AF8033BD30FE13D16
SHA1:	FC1081018C4CD2705882B7F667857E6FB51178F1
SHA-256:	E4B26102FE1F4C1AF342685DBD8C6932043810AB902B063117B382D0F743D9E6
SHA-512:	1383F314771DFA2DF93EAF86E0183F19DA53CF3356DB7005DD0BAB7E74EE19EC65284F828EB5F447B6E57371336F762FA39932E9D1C59A20AF0F373838AF8618
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://risefundraiser.com/fundraising-api/public/api/1.0/campaigns?order=desc&sortBy=featured&size=6
Preview:	{"status":true,"data":{"count":63,"entities":[{"orgName":"RoundGlass Foundation USA","isLiked":null,"likes":2,"organization":null,"taxonomyMeta":{"campaignElements":[{"ke y":"chapter","singular":"Team","plural":"Teams"},{"key":"champion","singular":"champion","plural":"champions"},{"key":"leadChampion","singular":"Team Leader","plural":"Te am Leaders"}]},"donationCurrency":"USD","pledgeCount":0,"isPledged":false,"customCategories":[{"id":430,"categoryName":"FEATURED"}],"tipConfig":null,"campaignMa nager":null,"campaignManagerImg":null,"campaignManagerEmail":null,"slides":[],"stats":[],"donationCustomFields":{"namespace":"Donation","groups":null},"id":"color-of-change-justiceforfloyd","causeId":null,"orgId":579,"teamSetting":{"isTeamAllowed":true,"isChampion":true,"isPersonalChamp":true,"isTeamImage":true},"name":"Color Of Change","summary":"Edifecs is supporting Color Of Change to combat injustice on our country. Color Of Change is the nation\u2019s largest online racial justice organizat

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\down[1]	
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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
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.'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.'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.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..'N..(M..'N.'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..(M..'N.'N.'N..%N..&N..&N..&N..&N..&N..&N..&N..&N

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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):	9995
Entropy (8bit):	5.2310751303620275
Encrypted:	false
SSDEEP:	192:InFxXtSPDmAhkj6FxX8SJcfZimFZso1AjuApFpgth49tpzn1o:ALXUmapLX8uZmZ1A38
MD5:	18109223E69FBE7321B036CEBC81D0ED
SHA1:	7DDB5D9E746E9884C562FD2DC348A04D3AE10E2F
SHA-256:	63098B6AFC6EDF946878339AE8966CBAFB87C201847DFAB973DC2BDB84304C1E
SHA-512:	6C8EE44A3BBCE9D8BD0A513DF6AB51AAEE960D85365003222026D7059198688C1A1C90022A2FE73078DF473041D5714E4CBE255FB937B291170157C4D1D901B
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,"data":{"gatewayInfo":{"INR":{"gatewayType":"System","id":4,"gatewayName":"Razorpay","merchantLiveKey":"XvraiCi7XGJBu8pPSeZWrGlt","merchantLiveSecret":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"},{"id":"plan_CYYoo9k9DCRFKz","amount":"1000","currency":"INR"},{"id":"plan_CYYp2WIZDuWXCD","amount":"2500","currency":"INR"}],"donationLevels":[500,1000,2500,5000],"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\9026IKNJ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\help-india-fight-covid-19-donate-for-oxygen[1].json	
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\9026IKNJ\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:	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
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\9026IKNJ\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\9026IKNJ\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\9026IKNJ\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\9026IKNJ\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\9026IKNJ\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:	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\9026IKNJ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\polyfills.661b9383b7c93a39b0f5[1].js	
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\9026IKNJ\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:	CE082B5C45181B112482C3F341DDAF4AE0896EDE7E1E67F29DECA0B7F500254934AB8E42E0AB24D556DD3FB9EE696FC3265AA97C7FC77DCAADF81261C447B3F4
Malicious:	false
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\9026IKNJ\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\9026IKNJ\styles.a19aec6bac6aa86c5932[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	139446
Entropy (8bit):	5.185648108263596
Encrypted:	false
SSDEEP:	768:w1ybSgYG5fIVvx2H6B/k/GmZmoa8oXM7hpQW1ybSgYG5fIVvx2H6B/k/GmZmoa8y:cyb2G5IVp2/iXMFtyb2G5IVp2/iXMFU
MD5:	474FEA01E60D3BDB011F756FE5F3DB55
SHA1:	6CCF3E80B0B9C4A01E995FF78170C7C57687FEF5
SHA-256:	85A1EF5D8C5694507F53BF36A6D48EEBF3A941A9424BD4EE3DE3C20A40BC9E1D
SHA-512:	075C4B8F0B69AE8B7749FA2BB9288464893E72A66F5513D830176E059CEF25E7434C7C586F4B58F87DD9429093746ED147BD6E32D1E1D98AB76719605401E3DF
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\styles.a19aec6bac6aa86c5932[1].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\9026IKNJ\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
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\Microsoft\Windows\INetCache\IE\9026IKNJ\unite[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 640x343, frames 3
Category:	downloaded
Size (bytes):	40732
Entropy (8bit):	7.966138653778096
Encrypted:	false
SSDEEP:	768:11aUwvDFeU8tpwvLIzqMsW3oK/lbEnSYmRZyNWu1VvqhfgH0:11Opeh2LZW4K/NvT7Q1Vv9U
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..".:..:.^...@.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\9026IKNJ\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
SHA-512:	A889939321296825FD7101EAB396E9CEE39C06C072B997C4C40064DE1D03ABEC81E597280CD43F24EE4DD536292206A8DAD69FC2B45AC642F61A9BBDDDA3EDDB
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\vendor.7b1b41a937a083fd16b0[1].js	
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.fromEventPattern=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.create(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\CS6IXJW6\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:lZ1jIo6WZSd6KF4Ie3LtdtAG062BPmjb95t5hflCPvAI5oh/a:lMo6OFE4/l062BPMRN45o9a
MD5:	70263DB7C4A020915B912D676257F4C7
SHA1:	7960A1890B37481524188FE0BC5EC5BEE88D867A
SHA-256:	3337B28ED58DCF883AE4F25887DE585B3E4070A143F0451DC34D1A03A3611A95
SHA-512:	F6F2F29A502F1893AFC60EB176CD56A9D1CE5084FBE14A02BC6689FB26FE395E97538CC66D4FF50745B001ADC03A51F3EE569ACF982D0E647C1BF1551A9A6EE
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\CS6IXJW6\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
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("lzQX"),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\CS6IXJW6\21.680500fdf3b5ae7c779f[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):	64416
Entropy (8bit):	5.394699404279847
Encrypted:	false
SSDEEP:	768:rN8AupoZYQDLOhSCm/XfhR8zkj/ZJsGUIF5GG:DSzQ/OhBm/X8wRhRT
MD5:	EE744D47A86ED7392F1431D9379725C8
SHA1:	D4A9F14E9FCC8D9922EA3A6B0359673249BC3843
SHA-256:	AB82A5653B0DB8345FC3C7503AFC98FDA2A917B2B4546AE51914E74F7F237A81
SHA-512:	7EC13463412C104D926FD5E64DEA724B181FC1BD6A508DEE23D26BF8E26706E1064B36D35123F6AB0AA4DE26BFD23F4F252DA2C19D83302CC0DAE4E696F31BF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\21.680500fdf3b5ae7c779f[1].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://risefundraiser.com/21.680500fdf3b5ae7c779f.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[21],{"a/6+":function(n,l,t){"use strict";t.r(l);var e=t("CcnG"),o=function(){},u=t("pMnS"),i=t("Ip0R"),a=t("cseH"),r=t("ebRn"),s=t("NhJc"),c=t("6rRr"),d=t("a/vR"),p=t("zZFE"),g=t("ZYCi"),m=t("HfCP"),f=t("HdYI"),h=t("1CEN"),C=t("ZYjt"),v=t("Xpkg"),b=t("Xtns"),x=t("7r2J"),y=t("zq+J"),P=t("T9q8"),M=t("OtJL"),_=t("ohT8"),O=t("LQ1l"),w=t("F1Ti"),k=t("Zf5U"),I=e["\u0275crt"]({encapsulation:0,styles:[["@-webkit-keyframes fade-in{from{opacity:0}to{opacity:1}}@keyframes fade-in{from{opacity:0}to{opacity:1}}.top-container[_ngcontent-%COMP%]{padding:26px 30px 45px 33px;text-align:center;position:relative}.stats-content[_ngcontent-%COMP%]{margin-bottom:25px}.p-d-i[_ngcontent-%COMP%]{font-family:Gibson-Light;font-size:15px;line-height:normal;letter-spacing:2.7px;color:#fff;margin-top:5px;text-transform:uppercase}.w-init[_ngcontent-%COMP%]{font-size:13px;line-height:normal;letter-spacing:.7px;color:#ffc400;margin-top:18px}.btn-g[_ngcontent-%COMP%]

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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\CS6IXJW6\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\CS6IXJW6\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\CS6IXJW6\Accepted[1].htm	
SHA-512:	41242BA0E9F8F06E02A78B9DD85B8BFB8EF812AFFAC5F32D3A33A77C09D016E82DCD69D7CFFB0A9A428A43C48F643369BEB48AB53481F509E1B8D4F6B36202E6
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","about":"<p>RoundGlass Foundation USA's relief fund donates money directly to the Community Foundation most active in the area impacted by the disaster. Community foundations 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 RiseFundraiser 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\CS6IXJW6\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:	91DA46598E704BAC9372A2B1A3A735E3EE2793DF615854F04395ED4B210B271570A561F6DCC37CD224D5CE4320D63BF71596DD28F6C558BAFDF00034DFFCCFE8
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/master/LICENSE.md. */.!function(t){if("object"==typeof exports&&"undefined"!=typeof module)module.exports=t();else if("function"==typeof define&&define.amd)define([],t);else{var e;e="undefined"!=typeof window?window:"undefined"!=typeof global?global:"undefined"!=typeof self?self:this,e.Chart=t()}}(function(){function t(e,n,i){function 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="function"==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\CS6IXJW6\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\CS6IXJW6\QuixoteCommunitiesLogo[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):	5180
Entropy (8bit):	7.8869788870364905
Encrypted:	false
SSDEEP:	96:lFctg6C0P+/RJYuJTGBIAwqOnFhhMXyqNqnX+X+YbbbbbbbbbbR:lF+g6QT9JlAwB7MXNqnX+X+Ybbbbbbbd
MD5:	02B0ABBE8B498B0E819C0DD670F58563

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\QuixoteCommunitiesLogo[1].jpg	
SHA1:	509A5D0CE9DABDB79137645319649C592A18B122
SHA-256:	67BC2EFAFE4295AB41707D9DC70913D2CB1BD2F89894C5313D48A9E4669F0F86
SHA-512:	EC23D1106D7E7ABC351F3F2596CE713E49C7AD31EC17443A4C462BB71253397F2DC018007AFC4DE58256722D7EB438D6566852E4E6FDE0E539683CDBA08651E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/media/15408/QuixoteCommunitiesLogo.png

Preview:

......JFIF.............C....................................%...#... , #&')*)..-0-(0%()(...C...........(...((..........."..T..........................!
.1AQa.."2Vqu....#7B.......Rbr....$56Us.34..CSet.................................$....................1A!...Qq."2a.............?.." "".'' "".'' "".'' "".'' "".'' "".'' ".JY..n.W...$.`. ....bp|n..t.......^.".*.z..<.E.
......^.".*.z..<.E. ......^.".*.z..<.E.V.>K5..k}...N........S...o>z.G..i......$...C...F5.....n....Oh..A&k......2..!~.n..w#.%[........2. "(......R..4....>.....jd.jG.E..{O.G...L.TV......)...Z+.......n
p.b...cccX.........D@DD.D@DD.D@DD.D@DD.].|.k/B....mc.Yz...=.J......bmht..2...`....4...[...4.._.?T..P....;u.M..7:.[.A..o".3OL....H...Z.?`2....w9...wk.;.%.S.vx....|.W.{.........DD.D@
DD.D@DD.D@DD.D@DD.].|.k/B....mc.Yz...=.J..V...<j{{..0......I.OFC.9..p..k..SE%.......w.:w.j../,..U....~q.=.o....*&S4.S...G....8?8mn..+.q......

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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:Av7QiXi3ixF3IVzZiRiliGTbhAoovljYKA0ZzjUXQVoe39ZrWn6WjAxG+Dz1Gi6p:ziXi3ix1iZiRiliGhAr2K9Z3BVnKjAxS
MD5:	DD572A0354C02D76DA5DAEC1888CCFB8
SHA1:	5D380341EF58A8FFCE2599A472C864EB329C86F6
SHA-256:	D8106146E4CE35A796DA1B004F66E9DBA13D8B28E0608CB2C93D1AF3AFB4F4BA
SHA-512:	72C3449B6C8D763C5A971487D6F09D765FA1952351990ECFB2C8EF5A7CADA9C069B34612156E55AC0B3BEFC46F650F5C6EA15B0F3C70D77625D1D808DA62A2! C
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\CS6IXJW6\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:	downloaded
Size (bytes):	1812
Entropy (8bit):	4.994297952788001
Encrypted:	false
SSDEEP:	48:YtKTyuYEN7OX/PKpuYEN7OX/LKKTyuYEN7OX/PKpuYEN7OX/LZ:ImYIEigYIE2mYIEigYIEF
MD5:	9B993DFDA3A96C079B9F06AF6AA1E011
SHA1:	0E8C864C232F1BE91BA39AA09324A16255226530
SHA-256:	FAB10F267B0BDC1AC8D7215DF27BEFC86334035DEAADF892EC9DC28349AF4944
SHA-512:	4A389D5927D3AC4D857777F289B2D74D15BE9CB66FDC20273BE22D002946E157F99D76A11322E023EB8F6225DE67B6418FF71E8B94D62B863A333F78CEE884F(
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/champions?order=desc&sortBy=donation_amount&offSet=0&size=10

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}{"status":true,"data":{"count":2,"donations":0,"entities":[{"id":"ankur-chander-1","champId":3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\champions[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):	906
Entropy (8bit):	4.994297952788001
Encrypted:	false
SSDEEP:	24:Yt5E4YTyukluYANN7kTxX/RwQxKpukluYANN7kTxX/RwqZ:YtKTyuYEN7OX/PKpuYEN7OX/LZ
MD5:	5681981C98EC2F7DEB713C75594537F7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\champions[2].htm	
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\CS6IXJW6\cloudbase[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 759 x 730, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	20522
Entropy (8bit):	7.798744208747665
Encrypted:	false
SSDEEP:	384:UqnnnnnnnnnnnnnnnnnnnnnStYqkBa9rSHj1c+7xYfm7saIy93ZnIAdGxFA7vR8O:UkDa9Oj1eW8yPIgi8ZcNhfI6E/sOh
MD5:	57AC25612BD9449C962B52F394D82BB6
SHA1:	07A2E37ED42CFBF063CC81DB8FA04D55F2D67DC8
SHA-256:	912B69EE2D6436E9D6EDAD69466E05049C4464B92393B28075473AC60861E5DF
SHA-512:	146C1403D8C699A4F8814C12B5F0E664EFA3D61EBE383D75590C8275A4E7CD72D3614572D14E5D55AB0D3895A26745C2DC9E75BB732F45FC9F37E70CF62CE06
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/media/11241/cloudbase.png
Preview:	.PNG.....IHDR.....:/.....sRGB.....gAMA.....a.....pHYs...%...%.IR$...O.IDATx^...[]U...6".JN[..!..tbh..F(^FK.{.Y.^.x{....GE.....y.....(...WJE.GAK.....\.6!I.&i.3&._..!d<.....uJk....w..[k.....z!....=.r....H9..@O.....'R.....).....D....z"....=.r....H9..@O.....'R.....).....D....z"....=.r....H9..@O.....'R.....).....D....z"....=.r....H9..@O.....'R.....).....D....z"....=.r....H9..@O.....'R.....).....D....z"....=.r....H9..@O.....'R.....).....D....z"....=.r....H9..@O.....'R.....).....D....z"....=.r....H9..@O.....'R.....).....D....z"....=.r....H9..@O.....'R.....).....D....z"....=.r....H9..@O.....'R.....).....D....z"....=.r....H9..@O.....'R.....).....D....z"....=.r....H9..@O.....'R.....).....D....z"....=.r....H9..@O

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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:	B26C4C7F146FC8CC2BDD1BFBB1FA5085BE540A9299B592375BE1D5E60D75807E0768FD76BA41FEF1B1A0B74EE88582833C63EF6852C4A48C952504C453EB9EB3
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\CS6IXJW6\fbevents[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	93774
Entropy (8bit):	5.392602416896564
Encrypted:	false
SSDEEP:	1536:sM+OWt6w6aic9MeipKKqQqcThe7Kdv0a9sIOC1jaMu5Qm2B+QNSMngUSZYSlIUiX:sOQMj1SVBYDGKx
MD5:	077B8B6E85C9EDF74D372D155180E6D3
SHA1:	4A24BE343819AD355807ADB01579366A1E64B8B9
SHA-256:	A517525B8A7D39BCAF1CF5F9695C5BE8FCE7A6B920A3924C1A4F70E8EA748C05

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\fbevents[1].js	
SHA-512:	DB714A2EAF14E6727086795FE151F3729DA32BFA0B87AB74289B7DF9E0808E1FEBCA38D2622EF47B7AA263479BDB66857011E2302DD1AFC9E814EF6B74642DF9
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\CS6IXJW6\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\CS6IXJW6\hammer[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=4], baseline, precision 8, 321x314, frames 3
Category:	downloaded
Size (bytes):	17987
Entropy (8bit):	6.36760952318392
Encrypted:	false
SSDEEP:	384:cEA6p+vuDssbvZJUFgTJ6WVXaDdhN5v3Rygd0cCTFuv0Wtu109d:cER++ssBJUFgTJ6WVXAt5vIaaQW09d
MD5:	E1654B657EC7DD6A262E5B23E7B26FAA
SHA1:	092BC58361329B174843A1CBB396A537DFACFA96
SHA-256:	EA04562ABE4B81CC3D7AB2F6E0A64E44527AEE8A1074068634E76471B079ADFD
SHA-512:	0CDD5340B1F4F33C026D01E15807FF0EF7FD477BCF6FDB8F19ED14FB6CBEB49F0974D50437F95B0B9E77D5991446603CFBC766CC83179C8DAB3819F3F244C8E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/media/11102/hammer.JPG
Preview:	......JFIF.....`.`.....Exif..MM.*.....;.....J.i.....X.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\healthandhope[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):	6468
Entropy (8bit):	7.896429631131336
Encrypted:	false
SSDEEP:	192:rVQMDhBaHKzQkRsssJYXlCRfjEGtlM84E:rl/QQVsJPEk
MD5:	ADA377310F923DC6C000B6F2AC2C1135
SHA1:	11B23513A91459BD6F532594681279B99A92360F
SHA-256:	FABBBBFA436C666AF8FC0195B62AD222D3D9E6FD75A2F8B293C30D38A1DAC329

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\healthandhope[1].jpg

SHA-512:	667FA3CC48A5F75C7DEBC73B035171D1310617CF5ED2BB6CCF5AA609AFB129B2A88F54890DBF8C047A9BF460AA46F898492EA5F5F04003BE90C085854228F6AB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/media/14244/healthandhope.PNG

Preview:

......JFIF............C....................................%...#... , #&')*)..-0-(0%()(...C..........(...((.........."...M...........................
!17A.6arstu....."3Qq..245.....RSUb..$B...#C..................................;.......................!..13Qq.5Aa..24r..."B.......#R.............?....X'.e..[..j..`.U.oR.n......@..@..@..@..O"...."X2
'Y.q....d.2...l..1......1p.\"_h.qL..-)<.fZm.H.......Q&p.k..#s-O...g..a..h.aq......lWX...(.wkk..Z.Y..2....".."..."...=D...4%Q.cG..........D.*.>.(... sTt.....z..p.E...".."..(.. .....L0...$.;3..
_@$./P...4....W...C.M?.vU....Q.].T.F......U...tG..<.T....e_|o.....OM.jw,[..u)Jb.3Q...Eq..m.jX)....h.*.3.Q.!v.@..fu.z.B.SO...W...F...Z..r.8.!.P..l.Vd...M?.vU....P.SO....}..Xk...>.
7...Y....4....W...FY.[y.:...KI).A.G...i....^.....G0.@.>.....EX..&..).*...=D...4..... .V..YF.,......X'.e..[..-.......|.H&fR...3b%.4.-6QX..} .]}k.Hp..A..i.91r.a..$.d..6."

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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:	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

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\CS6IXJW6\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:	EA3C40D5710749E1014A7492BF7C64D4D322EAB6E3BA4A378CCEA050ACDC02C138E5A4F16E0946FC06E3C165E242F17A9D1F765C3D6BB77B3C7850901AF9777
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\CS6IXJW6\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\CS6IXJW6\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\CS6IXJW6\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/5jIjwhoycTU2AzKxJvhUccrnf: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.oZI...w.;&..p.V...D.....Q..O.](H..c..C"8.3c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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+lJWmQq+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\CS6IXJW6\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/g1EBwR4jdIQS9vj5P7mbjRR6rQM/aiMOLayKsI:M6FDoEBYmNSNEXRlMinKsb
MD5:	5BB12C7EBA967DF8194BF92F9475D567
SHA1:	653730CEDE43F53A37C3B84B4B85E78F90AAA0BD
SHA-256:	AD4E18AC6E1292031A527498496F3FD4F4F7E3132C30552947E302BA6C4BD7FD
SHA-512:	7795ED91CF274A8E9C0379FB982299EB49E83C2BC2C7F9E0B98EF070BB24865F9061D7D137AFBE61E12E1F9DCB3EF8B6397D901789270E1EE73D8BDC5AEE17F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\rg-logo[1].png	
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\CS6IXJW6\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.getElementsByTa gName("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\CS6IXJW6\styles.a19aec6bac6aa86c5932[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	69723
Entropy (8bit):	5.185648108263596
Encrypted:	false
SSDEEP:	768:w1ybSgYG5flVvx2H6B/k/GmZmoa8oXM7hpQp:cyb2G5lVp2/iXMFU
MD5:	F753655555A8CCF2D9F3D2F2DD14CBEE
SHA1:	1307C82DA95EE428D6AA5456A9D5B8C36DD3B804
SHA-256:	FA6D0F89AA5233FCA7459485DB8CC8AD2D3ED702EA5C653376A350ADA4624FEB
SHA-512:	F26A9CE232CA9E7C5486F880B9EC516B35859A7E6901D3FA096388078F3123E1B93600883FBD932E7FAE9410C87961BE073897F0738928C77EB6A03878DA1B2B
Malicious:	false
Reputation:	low
Preview:	/*!. * Cropper.js v1.4.1. * https://fengyuanchen.github.io/cropperjs. *. * Copyright 2015-present Chen Fengyuan. * Released under the MIT license. *. * Date: 2018-07-15T0 9:54:43.167Z. */.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-sel ect: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:absol ute;right:0;top:0}.cropper-canvas,.cropper-wrap-box{overflow:hidden}.cropper-drag-box{background-color:#fff;opacity:0}.cropper-modal{background-color:#000;opaci ty:.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\CS6IXJW6\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\swiper.min[1].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\CS6IXJW6\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\CS6IXJW6\unnamed[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 96 x 96, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	797
Entropy (8bit):	7.160510329879692
Encrypted:	false
SSDEEP:	24:Q/BdHRmmmmmm3Jgmmmmm9b6cGELe1Zn8ceUm4lmmmmmmi:Q/Bdxmmmmmm3Kmmmmm9uqGDlmmmmmmi
MD5:	3FE7DAFC86ABF70ADD83ECA333BC53E9
SHA1:	75E668D9B4C1B3E8A2E67AB99C9FB5CFED5C20DC
SHA-256:	95EA2950394D84C4433D31F32D99D7C75388E1D0314094E58D55495E0A20656A
SHA-512:	3586FFD93E472391E1DA898A09958C8F54C8B5AE73096E59DCF12BCAED88FEE23E8B7EC35F17A13F3EA442C946EFE4EB5C0006C7F11D8372188718DC3161CFAF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/a/AATXAJwxW8QpWkJUGadt2HWiszXk98O-xYCsACeHbFus=s96-c
Preview:	.PNG.....IHDR...`...`.....m..o....sBIT.....O.....bKGD...6..B.....IDATx...k.a....r...Is&J..E(H)....._K.$NJ+...R]...;8.[...P.8..."....=K..I.Ii.s(.gh.I!y...}.s./o..!P.....<n/....` .....` .....` .....` .....` .....` .....` .....` .....` .....` .....` ....._...w..c.[:3...O..f.H..u.d..y{..n$....._..oV..2of....)..UZ...+..f.H.T...../...T...a..k.%5...c..> jW.wt..%=..W..J..p.U..G.o.Rz.9n;q.|.h....".a.+..o[.Y.j".y?K.-..BQ.F..3|.G..fRU'{....:...../....u.P.....[.6...zq%c..|..ij.H...H.....59.pcL.k\.$..{.e.o`..X....#-.&w..~.8..JZ..F....{7].#....'...A]..=..u.T...W..]||_.z6w..*..3....G..PU.XX.es3..'..^.=..3~....` .....` .....` .....` .....` .....` .....` ...?.Q.c.M.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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?

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\313E30_0_0[1].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....l...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...I..D.....hoSx..&o...{z.8.Up*.....y..j3H

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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
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..@. .+ICAB.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\OR0WKIO1\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\OR0WKIO1\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?

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\313E30_3_0[1].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...-,.....\.@9qT"...,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\OR0WKIO1\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
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\OR0WKIO1\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\OR0WKIO1\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?

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\313E30_6_0[1].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....I.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\OR0WKIO1\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
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..... .&G.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\OR0WKIO1\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
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.param s={},this.taxonomy=m.b.getInstance().getTaxonomy()||!1,this.missionService.announceMissionToShowHideLoader({requestType:f.d.showLoader}),n.params.subs cribe(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=functi on(){this.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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:	4A52CDC46D920FABFCB3921E0E29036BEFCB28DD81D27CE9BDC249A9101237C4F174113DAAFD05DE3D85866A1AF2A4248E640FF09F48F28797522AC1D461EE 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dqy0ngl1d5798.cloudfront.net/media/17438/RG-FoundationYoutubeProfile.jpg

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\RG-FoundationYoutubeProfile[1].jpg</th></tr>
<tr><td>Preview:</td><td>......JFIF.............C....................................%...#... , #&')*)..-0-(0%()(...C...........(...((...........".......................................8....................
......!1AQ.."a..q25s...#B....6b...................................0.......................!.1Aa.Qq."2....#4R.r...............?..DE...a...D@...DD....D@...DD....D@...DD....D@...DD....D@...DD..
..D@...DD....D@...DD....D@...DD....D@...DD....D@...DD....D@...DD....D@...DD....D@...DD...w.N..@...DD....D@.]. .\n]..........=.".u8B3._...j..N..\.k!.j>..d.sF.F.^.el.O...n.
Z}...Q.......S\.}.~.]..S..z.-.,lq2..k.4.....@.Te...8K.*^a....D@...DD._.W.Y......_.W.Y.....^....<....eg..9.X........D.g.........k...}.Y....M.kZnY...%......:..$..+Q....................1....3.>~2.#|v"<.>
..D...#...W.Qd....M/E./#..:!...K.i....].-1.Y_...7T.......D..E.....A...8.p.u&>s..7.v..\Z.l.`.......s+.tl....Vf.$.6.XC......7.++.:.............81.6=...W..+8'g..l.....e..4;*..J-.../l....%.?.X./..J.</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\TogetherLogoF[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 200x200, frames 3</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>3412</td></tr>
<tr><td>Entropy (8bit):</td><td>7.628972864764706</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>48:+iWmQo8s6oAFz8BVEa+Efpq0LjPmgalCF3De+5+MS:/BAp8NxbLjPpa+4MS</td></tr>
<tr><td>MD5:</td><td>24FFC51D9CFB323926C94791CE4DDBB6</td></tr>
<tr><td>SHA1:</td><td>8C5A325032BBAAA5ED0C0D1D6BEE062012334278</td></tr>
<tr><td>SHA-256:</td><td>9A364AB5511C8F248C673DDB55764E2F0FDD3A0090516B5E4098E80E0E09579F</td></tr>
<tr><td>SHA-512:</td><td>BC7331C76BF7F317C5320B5974980913231330548A38B0064FF83B293FC191314935CF056975557F69FC644A0099A021E3779C47F903D522392F590688BF6CB2</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://dqy0ngl1d5798.cloudfront.net/media/14716/TogetherLogoF.jpg</td></tr>
<tr><td>Preview:</td><td>......JFIF.............C....................................%...#... , #&')*)..-0-(0%()(...C...........(...((...........".......................................3..........................!..1
."A#2a.Qq..BR....................................../.......................!1...AQ."aq.......B...............?..D@...DD....D@...DD....D@...DD....D@...DD....D@...DD....D@...DD....D@...DD....D
@...DD....D@...DD....D@...DD....D@...DD....D@...DD....D@...DD....D@...E.kN.TR.!......Q,.i{j#.1.{..q.........uU.j....Ep...[YY..H.b..$4..y%......}../o..xK....f.....DD....D@...DD....D
@...DD.......Mh.T\+..R.|.dn...'...y'....Q..q...k-W.les....b...........;m.j+f...S.-mA4........h..H.q..y.Y]`.^&|.{].G#...r..p2C......9'.+.m...nI.......d......*^.%....7.o..".R}0.T.~..H.......v..6..v..n
.g....*7IY....5....oi....+.G..`.../......;.K...K$...Qp...MP...2....Fq..p1..CI.....D....'.]#[.T..h[.}....?Qz.t.3[...E[=,u3w.262....d..8.*e...........#....60x.G...#.</td></tr>
</table>

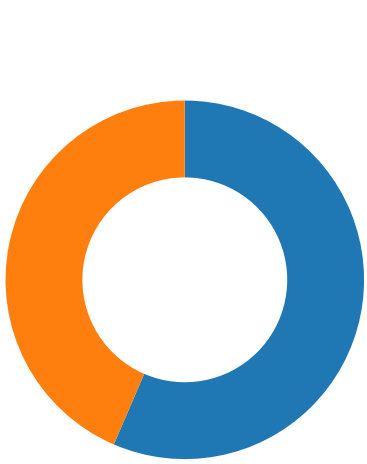
<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\create[1].htm</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>HTML document, ASCII text, with very long lines</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>9071</td></tr>
<tr><td>Entropy (8bit):</td><td>4.94862352509096</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>192:LyAEQmFHFlHWjmRjLd0gpKQKdFr0y0Fo0l2P3OOv84aTmdZAckyFrJqyJhSgOIte:LxEQallHrBjSSFHJT4ZjGrxN8bfM</td></tr>
<tr><td>MD5:</td><td>2A5CEF0817081FC6AD1909B62ACD9919</td></tr>
<tr><td>SHA1:</td><td>B005FD522AD71CCADCBFE240599389ACA8BECDCA</td></tr>
<tr><td>SHA-256:</td><td>B6F1F3701DC121B979E593EBD27D71CDDD16BDECFB3FEDD70C7ADB5F2D0BA3F3</td></tr>
<tr><td>SHA-512:</td><td>B26C4C7F146FC8CC2BDD1BFBB1FA5085BE540A9299B592375BE1D5E60D75807E0768FD76BA41FEF1B1A0B74EE88582833C63EF6852C4A48C952504C453EB9EF
3</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>Preview:</td><td><!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</td></tr>
</table>

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 20:37:11.059426069 CEST	49733	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.060559988 CEST	49734	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.278515100 CEST	443	49733	54.201.10.107	192.168.2.4
May 20, 2021 20:37:11.278604984 CEST	49733	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.280549049 CEST	443	49734	54.201.10.107	192.168.2.4
May 20, 2021 20:37:11.280653000 CEST	49734	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.283689976 CEST	49733	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.283746004 CEST	49734	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.500019073 CEST	443	49733	54.201.10.107	192.168.2.4
May 20, 2021 20:37:11.501032114 CEST	443	49734	54.201.10.107	192.168.2.4
May 20, 2021 20:37:11.501185894 CEST	443	49733	54.201.10.107	192.168.2.4
May 20, 2021 20:37:11.501210928 CEST	443	49733	54.201.10.107	192.168.2.4
May 20, 2021 20:37:11.501265049 CEST	49733	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.501286030 CEST	443	49733	54.201.10.107	192.168.2.4
May 20, 2021 20:37:11.501296997 CEST	49733	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.501306057 CEST	443	49733	54.201.10.107	192.168.2.4
May 20, 2021 20:37:11.501337051 CEST	49733	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.501353979 CEST	49733	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.502037048 CEST	443	49734	54.201.10.107	192.168.2.4
May 20, 2021 20:37:11.502068996 CEST	443	49734	54.201.10.107	192.168.2.4
May 20, 2021 20:37:11.502093077 CEST	443	49734	54.201.10.107	192.168.2.4
May 20, 2021 20:37:11.502108097 CEST	49734	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.502118111 CEST	49734	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.502142906 CEST	49734	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.502151966 CEST	443	49734	54.201.10.107	192.168.2.4
May 20, 2021 20:37:11.502193928 CEST	49734	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.538626909 CEST	49734	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.538717985 CEST	49733	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.545386076 CEST	49734	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.545603991 CEST	49734	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.545708895 CEST	49733	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.755301952 CEST	443	49733	54.201.10.107	192.168.2.4
May 20, 2021 20:37:11.755347967 CEST	443	49733	54.201.10.107	192.168.2.4
May 20, 2021 20:37:11.755449057 CEST	49733	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.755480051 CEST	49733	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.755971909 CEST	443	49734	54.201.10.107	192.168.2.4
May 20, 2021 20:37:11.755990028 CEST	443	49734	54.201.10.107	192.168.2.4
May 20, 2021 20:37:11.756036997 CEST	49734	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.756051064 CEST	49734	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.757462978 CEST	49733	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.758215904 CEST	49734	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.761816978 CEST	443	49733	54.201.10.107	192.168.2.4
May 20, 2021 20:37:11.761890888 CEST	49733	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.762610912 CEST	443	49734	54.201.10.107	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 20, 2021 20:37:11.762671947 CEST	49734	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.764478922 CEST	443	49734	54.201.10.107	192.168.2.4
May 20, 2021 20:37:11.764502048 CEST	443	49734	54.201.10.107	192.168.2.4
May 20, 2021 20:37:11.764518023 CEST	443	49734	54.201.10.107	192.168.2.4
May 20, 2021 20:37:11.764569998 CEST	49734	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:11.766144991 CEST	49734	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:12.016315937 CEST	443	49733	54.201.10.107	192.168.2.4
May 20, 2021 20:37:12.018161058 CEST	443	49734	54.201.10.107	192.168.2.4
May 20, 2021 20:37:12.061511993 CEST	49736	443	192.168.2.4	151.101.1.0
May 20, 2021 20:37:12.063009024 CEST	49737	443	192.168.2.4	151.101.1.0
May 20, 2021 20:37:12.063509941 CEST	49734	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:12.069753885 CEST	49738	443	192.168.2.4	104.16.18.94
May 20, 2021 20:37:12.071137905 CEST	49739	443	192.168.2.4	104.18.10.207
May 20, 2021 20:37:12.073519945 CEST	49740	443	192.168.2.4	104.16.18.94
May 20, 2021 20:37:12.074234009 CEST	49741	443	192.168.2.4	104.18.10.207
May 20, 2021 20:37:12.075190067 CEST	49742	443	192.168.2.4	104.16.18.94
May 20, 2021 20:37:12.076486111 CEST	49743	443	192.168.2.4	104.16.18.94
May 20, 2021 20:37:12.092998028 CEST	49734	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:12.093249083 CEST	49734	443	192.168.2.4	54.201.10.107
May 20, 2021 20:37:12.096046925 CEST	49744	443	192.168.2.4	104.16.18.94
May 20, 2021 20:37:12.097026110 CEST	49745	443	192.168.2.4	104.18.10.207
May 20, 2021 20:37:12.105756998 CEST	443	49738	104.16.18.94	192.168.2.4
May 20, 2021 20:37:12.105842113 CEST	443	49736	151.101.1.0	192.168.2.4
May 20, 2021 20:37:12.105914116 CEST	49736	443	192.168.2.4	151.101.1.0
May 20, 2021 20:37:12.105916977 CEST	49738	443	192.168.2.4	104.16.18.94
May 20, 2021 20:37:12.107297897 CEST	443	49737	151.101.1.0	192.168.2.4
May 20, 2021 20:37:12.107391119 CEST	49737	443	192.168.2.4	151.101.1.0
May 20, 2021 20:37:12.107831001 CEST	443	49739	104.18.10.207	192.168.2.4
May 20, 2021 20:37:12.107899904 CEST	49739	443	192.168.2.4	104.18.10.207
May 20, 2021 20:37:12.109484911 CEST	443	49740	104.16.18.94	192.168.2.4
May 20, 2021 20:37:12.109610081 CEST	49740	443	192.168.2.4	104.16.18.94
May 20, 2021 20:37:12.110198975 CEST	443	49741	104.18.10.207	192.168.2.4
May 20, 2021 20:37:12.110260010 CEST	49741	443	192.168.2.4	104.18.10.207
May 20, 2021 20:37:12.111922026 CEST	443	49742	104.16.18.94	192.168.2.4
May 20, 2021 20:37:12.112009048 CEST	49742	443	192.168.2.4	104.16.18.94
May 20, 2021 20:37:12.112808943 CEST	443	49743	104.16.18.94	192.168.2.4
May 20, 2021 20:37:12.112890005 CEST	49743	443	192.168.2.4	104.16.18.94
May 20, 2021 20:37:12.120271921 CEST	49743	443	192.168.2.4	104.16.18.94
May 20, 2021 20:37:12.120861053 CEST	49736	443	192.168.2.4	151.101.1.0
May 20, 2021 20:37:12.121522903 CEST	49738	443	192.168.2.4	104.16.18.94
May 20, 2021 20:37:12.132986069 CEST	443	49744	104.16.18.94	192.168.2.4
May 20, 2021 20:37:12.133099079 CEST	49744	443	192.168.2.4	104.16.18.94
May 20, 2021 20:37:12.134207010 CEST	443	49745	104.18.10.207	192.168.2.4
May 20, 2021 20:37:12.134475946 CEST	49745	443	192.168.2.4	104.18.10.207
May 20, 2021 20:37:12.156425953 CEST	443	49743	104.16.18.94	192.168.2.4
May 20, 2021 20:37:12.157001019 CEST	443	49743	104.16.18.94	192.168.2.4
May 20, 2021 20:37:12.157016993 CEST	443	49743	104.16.18.94	192.168.2.4
May 20, 2021 20:37:12.157073021 CEST	49743	443	192.168.2.4	104.16.18.94
May 20, 2021 20:37:12.157098055 CEST	49743	443	192.168.2.4	104.16.18.94
May 20, 2021 20:37:12.157407999 CEST	443	49738	104.16.18.94	192.168.2.4
May 20, 2021 20:37:12.158011913 CEST	443	49738	104.16.18.94	192.168.2.4
May 20, 2021 20:37:12.158030987 CEST	443	49738	104.16.18.94	192.168.2.4
May 20, 2021 20:37:12.158128977 CEST	49738	443	192.168.2.4	104.16.18.94
May 20, 2021 20:37:12.159939051 CEST	49744	443	192.168.2.4	104.16.18.94
May 20, 2021 20:37:12.159951925 CEST	49738	443	192.168.2.4	104.16.18.94
May 20, 2021 20:37:12.159986019 CEST	49745	443	192.168.2.4	104.18.10.207

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 20, 2021 20:37:01.293910980 CEST	65298	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:01.343472004 CEST	53	65298	8.8.8.8	192.168.2.4
May 20, 2021 20:37:02.534190893 CEST	59123	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:02.583895922 CEST	53	59123	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 20, 2021 20:37:03.247298002 CEST	54531	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:03.306991100 CEST	53	54531	8.8.8.8	192.168.2.4
May 20, 2021 20:37:03.766758919 CEST	49714	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:03.817869902 CEST	53	49714	8.8.8.8	192.168.2.4
May 20, 2021 20:37:04.844306946 CEST	58028	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:04.893342018 CEST	53	58028	8.8.8.8	192.168.2.4
May 20, 2021 20:37:06.265876055 CEST	53097	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:06.317991018 CEST	53	53097	8.8.8.8	192.168.2.4
May 20, 2021 20:37:07.466182947 CEST	49257	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:07.518456936 CEST	53	49257	8.8.8.8	192.168.2.4
May 20, 2021 20:37:08.600732088 CEST	62389	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:08.652883053 CEST	53	62389	8.8.8.8	192.168.2.4
May 20, 2021 20:37:09.690025091 CEST	49910	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:09.744159937 CEST	53	49910	8.8.8.8	192.168.2.4
May 20, 2021 20:37:09.935540915 CEST	55854	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:09.997637987 CEST	53	55854	8.8.8.8	192.168.2.4
May 20, 2021 20:37:10.983257055 CEST	64549	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:11.048470020 CEST	53	64549	8.8.8.8	192.168.2.4
May 20, 2021 20:37:11.407054901 CEST	63153	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:11.466578007 CEST	53	63153	8.8.8.8	192.168.2.4
May 20, 2021 20:37:11.833252907 CEST	52991	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:11.840239048 CEST	53700	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:11.877557993 CEST	51726	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:11.892868042 CEST	53	52991	8.8.8.8	192.168.2.4
May 20, 2021 20:37:11.895452023 CEST	53	53700	8.8.8.8	192.168.2.4
May 20, 2021 20:37:11.932503939 CEST	53	51726	8.8.8.8	192.168.2.4
May 20, 2021 20:37:12.079370975 CEST	56794	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:12.099045038 CEST	56534	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:12.136205912 CEST	53	56794	8.8.8.8	192.168.2.4
May 20, 2021 20:37:12.159962893 CEST	53	56534	8.8.8.8	192.168.2.4
May 20, 2021 20:37:12.233066082 CEST	56627	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:12.294070959 CEST	53	56627	8.8.8.8	192.168.2.4
May 20, 2021 20:37:12.590106964 CEST	56621	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:12.644171000 CEST	53	56621	8.8.8.8	192.168.2.4
May 20, 2021 20:37:13.119201899 CEST	63116	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:13.154325008 CEST	64078	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:13.169322014 CEST	53	63116	8.8.8.8	192.168.2.4
May 20, 2021 20:37:13.214128971 CEST	53	64078	8.8.8.8	192.168.2.4
May 20, 2021 20:37:13.402614117 CEST	64801	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:13.451798916 CEST	53	64801	8.8.8.8	192.168.2.4
May 20, 2021 20:37:15.055172920 CEST	61721	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:15.107384920 CEST	53	61721	8.8.8.8	192.168.2.4
May 20, 2021 20:37:16.178339005 CEST	51255	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:16.228578091 CEST	53	51255	8.8.8.8	192.168.2.4
May 20, 2021 20:37:17.350894928 CEST	61522	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:17.403191090 CEST	53	61522	8.8.8.8	192.168.2.4
May 20, 2021 20:37:19.988082886 CEST	52337	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:20.040615082 CEST	53	52337	8.8.8.8	192.168.2.4
May 20, 2021 20:37:21.084177971 CEST	55046	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:21.139416933 CEST	53	55046	8.8.8.8	192.168.2.4
May 20, 2021 20:37:22.436830044 CEST	49612	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:22.489995003 CEST	53	49612	8.8.8.8	192.168.2.4
May 20, 2021 20:37:28.522547960 CEST	49285	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:28.576898098 CEST	53	49285	8.8.8.8	192.168.2.4
May 20, 2021 20:37:28.853568077 CEST	50601	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:28.939729929 CEST	53	50601	8.8.8.8	192.168.2.4
May 20, 2021 20:37:29.843955994 CEST	60875	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:29.896855116 CEST	53	60875	8.8.8.8	192.168.2.4
May 20, 2021 20:37:31.494093895 CEST	56448	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:31.552158117 CEST	53	56448	8.8.8.8	192.168.2.4
May 20, 2021 20:37:32.632900953 CEST	59172	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:32.702054977 CEST	53	59172	8.8.8.8	192.168.2.4
May 20, 2021 20:37:32.793450117 CEST	62420	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:32.845967054 CEST	53	62420	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 20, 2021 20:37:39.768549919 CEST	60579	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:39.830842972 CEST	53	60579	8.8.8.8	192.168.2.4
May 20, 2021 20:37:40.697268963 CEST	50183	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:40.747443914 CEST	53	50183	8.8.8.8	192.168.2.4
May 20, 2021 20:37:40.757601976 CEST	60579	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:40.819761992 CEST	53	60579	8.8.8.8	192.168.2.4
May 20, 2021 20:37:41.701647997 CEST	50183	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:41.759553909 CEST	53	50183	8.8.8.8	192.168.2.4
May 20, 2021 20:37:41.765623093 CEST	60579	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:41.817841053 CEST	53	60579	8.8.8.8	192.168.2.4
May 20, 2021 20:37:42.807245970 CEST	50183	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:42.860780954 CEST	53	50183	8.8.8.8	192.168.2.4
May 20, 2021 20:37:43.771012068 CEST	60579	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:43.824383974 CEST	53	60579	8.8.8.8	192.168.2.4
May 20, 2021 20:37:44.810633898 CEST	50183	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:44.862648964 CEST	53	50183	8.8.8.8	192.168.2.4
May 20, 2021 20:37:47.796600103 CEST	60579	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:47.848485947 CEST	53	60579	8.8.8.8	192.168.2.4
May 20, 2021 20:37:48.919727087 CEST	50183	53	192.168.2.4	8.8.8.8
May 20, 2021 20:37:48.977791071 CEST	53	50183	8.8.8.8	192.168.2.4
May 20, 2021 20:38:10.486989021 CEST	61531	53	192.168.2.4	8.8.8.8
May 20, 2021 20:38:10.545785904 CEST	53	61531	8.8.8.8	192.168.2.4
May 20, 2021 20:38:36.565789938 CEST	49228	53	192.168.2.4	8.8.8.8
May 20, 2021 20:38:36.637556076 CEST	53	49228	8.8.8.8	192.168.2.4
May 20, 2021 20:38:38.930824041 CEST	59794	53	192.168.2.4	8.8.8.8
May 20, 2021 20:38:38.990345001 CEST	53	59794	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 20, 2021 20:37:10.983257055 CEST	192.168.2.4	8.8.8.8	0xee6e	Standard query (0)	risefundraiser.com	A (IP address)	IN (0x0001)
May 20, 2021 20:37:11.833252907 CEST	192.168.2.4	8.8.8.8	0x7d9d	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
May 20, 2021 20:37:11.840239048 CEST	192.168.2.4	8.8.8.8	0xec33	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
May 20, 2021 20:37:11.877557993 CEST	192.168.2.4	8.8.8.8	0xb8bc	Standard query (0)	cdn.quilljs.com	A (IP address)	IN (0x0001)
May 20, 2021 20:37:12.079370975 CEST	192.168.2.4	8.8.8.8	0xb3b2	Standard query (0)	dqy0ngl1d5798.cloudfront.net	A (IP address)	IN (0x0001)
May 20, 2021 20:37:12.233066082 CEST	192.168.2.4	8.8.8.8	0xd4fb	Standard query (0)	js.hsforms.net	A (IP address)	IN (0x0001)
May 20, 2021 20:37:12.590106964 CEST	192.168.2.4	8.8.8.8	0x3589	Standard query (0)	s3-us-west-2.amazonaws.com	A (IP address)	IN (0x0001)
May 20, 2021 20:37:13.154325008 CEST	192.168.2.4	8.8.8.8	0x9329	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
May 20, 2021 20:37:28.853568077 CEST	192.168.2.4	8.8.8.8	0x262b	Standard query (0)	dqy0ngl1d5798.cloudfront.net	A (IP address)	IN (0x0001)
May 20, 2021 20:38:36.565789938 CEST	192.168.2.4	8.8.8.8	0xdf09	Standard query (0)	lh3.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 20, 2021 20:37:11.048470020 CEST	8.8.8.8	192.168.2.4	0xee6e	No error (0)	risefundraiser.com		54.201.10.107	A (IP address)	IN (0x0001)
May 20, 2021 20:37:11.048470020 CEST	8.8.8.8	192.168.2.4	0xee6e	No error (0)	risefundraiser.com		54.186.33.74	A (IP address)	IN (0x0001)
May 20, 2021 20:37:11.892868042 CEST	8.8.8.8	192.168.2.4	0x7d9d	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
May 20, 2021 20:37:11.892868042 CEST	8.8.8.8	192.168.2.4	0x7d9d	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 20, 2021 20:37:11.895452023 CEST	8.8.8.8	192.168.2.4	0xec33	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
May 20, 2021 20:37:11.895452023 CEST	8.8.8.8	192.168.2.4	0xec33	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
May 20, 2021 20:37:11.932503939 CEST	8.8.8.8	192.168.2.4	0xb8bc	No error (0)	cdn.quilljs.com	cdn-quilljs-com-7quy.onrender.com		CNAME (Canonical name)	IN (0x0001)
May 20, 2021 20:37:11.932503939 CEST	8.8.8.8	192.168.2.4	0xb8bc	No error (0)	cdn-quilljs-com-7quy.onrender.com	render.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 20, 2021 20:37:11.932503939 CEST	8.8.8.8	192.168.2.4	0xb8bc	No error (0)	render.map.fastly.net		151.101.1.0	A (IP address)	IN (0x0001)
May 20, 2021 20:37:11.932503939 CEST	8.8.8.8	192.168.2.4	0xb8bc	No error (0)	render.map.fastly.net		151.101.65.0	A (IP address)	IN (0x0001)
May 20, 2021 20:37:11.932503939 CEST	8.8.8.8	192.168.2.4	0xb8bc	No error (0)	render.map.fastly.net		151.101.129.0	A (IP address)	IN (0x0001)
May 20, 2021 20:37:11.932503939 CEST	8.8.8.8	192.168.2.4	0xb8bc	No error (0)	render.map.fastly.net		151.101.193.0	A (IP address)	IN (0x0001)
May 20, 2021 20:37:12.136205912 CEST	8.8.8.8	192.168.2.4	0xb3b2	No error (0)	dqy0ngl1d5798.cloudfront.net		13.224.89.71	A (IP address)	IN (0x0001)
May 20, 2021 20:37:12.136205912 CEST	8.8.8.8	192.168.2.4	0xb3b2	No error (0)	dqy0ngl1d5798.cloudfront.net		13.224.89.17	A (IP address)	IN (0x0001)
May 20, 2021 20:37:12.136205912 CEST	8.8.8.8	192.168.2.4	0xb3b2	No error (0)	dqy0ngl1d5798.cloudfront.net		13.224.89.190	A (IP address)	IN (0x0001)
May 20, 2021 20:37:12.136205912 CEST	8.8.8.8	192.168.2.4	0xb3b2	No error (0)	dqy0ngl1d5798.cloudfront.net		13.224.89.44	A (IP address)	IN (0x0001)
May 20, 2021 20:37:12.294070959 CEST	8.8.8.8	192.168.2.4	0xd4fb	No error (0)	js.hsforms.net		104.17.182.73	A (IP address)	IN (0x0001)
May 20, 2021 20:37:12.294070959 CEST	8.8.8.8	192.168.2.4	0xd4fb	No error (0)	js.hsforms.net		104.17.186.73	A (IP address)	IN (0x0001)
May 20, 2021 20:37:12.294070959 CEST	8.8.8.8	192.168.2.4	0xd4fb	No error (0)	js.hsforms.net		104.17.185.73	A (IP address)	IN (0x0001)
May 20, 2021 20:37:12.294070959 CEST	8.8.8.8	192.168.2.4	0xd4fb	No error (0)	js.hsforms.net		104.17.184.73	A (IP address)	IN (0x0001)
May 20, 2021 20:37:12.294070959 CEST	8.8.8.8	192.168.2.4	0xd4fb	No error (0)	js.hsforms.net		104.17.183.73	A (IP address)	IN (0x0001)
May 20, 2021 20:37:12.644171000 CEST	8.8.8.8	192.168.2.4	0x3589	No error (0)	s3-us-west-2.amazonaws.com		52.218.236.192	A (IP address)	IN (0x0001)
May 20, 2021 20:37:13.214128971 CEST	8.8.8.8	192.168.2.4	0x9329	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
May 20, 2021 20:37:13.214128971 CEST	8.8.8.8	192.168.2.4	0x9329	No error (0)	scontent.xx.fbcdn.net		31.13.92.14	A (IP address)	IN (0x0001)
May 20, 2021 20:37:28.939729929 CEST	8.8.8.8	192.168.2.4	0x262b	No error (0)	dqy0ngl1d5798.cloudfront.net		13.224.89.17	A (IP address)	IN (0x0001)
May 20, 2021 20:37:28.939729929 CEST	8.8.8.8	192.168.2.4	0x262b	No error (0)	dqy0ngl1d5798.cloudfront.net		13.224.89.190	A (IP address)	IN (0x0001)
May 20, 2021 20:37:28.939729929 CEST	8.8.8.8	192.168.2.4	0x262b	No error (0)	dqy0ngl1d5798.cloudfront.net		13.224.89.71	A (IP address)	IN (0x0001)
May 20, 2021 20:37:28.939729929 CEST	8.8.8.8	192.168.2.4	0x262b	No error (0)	dqy0ngl1d5798.cloudfront.net		13.224.89.44	A (IP address)	IN (0x0001)
May 20, 2021 20:38:36.637556076 CEST	8.8.8.8	192.168.2.4	0xdf09	No error (0)	lh3.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
May 20, 2021 20:38:36.637556076 CEST	8.8.8.8	192.168.2.4	0xdf09	No error (0)	googlehosted.l.googleusercontent.com		172.217.20.1	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 20:37:11.501306057 CEST	54.201.10.107	443	192.168.2.4	49733	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 20:37:11.502151966 CEST	54.201.10.107	443	192.168.2.4	49734	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		

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 20:37:12.157016993 CEST	104.16.18.94	443	192.168.2.4	49743	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 20:37:12.158030987 CEST	104.16.18.94	443	192.168.2.4	49738	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 20:37:12.166270971 CEST	151.101.1.0	443	192.168.2.4	49736	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 20:37:12.196551085 CEST	104.16.18.94	443	192.168.2.4	49744	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 20:37:12.196927071 CEST	104.18.10.207	443	192.168.2.4	49745	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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 20:37:12.197562933 CEST	104.16.18.94	443	192.168.2.4	49742	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 20:37:12.198477030 CEST	104.18.10.207	443	192.168.2.4	49741	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 20:37:12.199806929 CEST	104.16.18.94	443	192.168.2.4	49740	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 20:37:12.203237057 CEST	104.18.10.207	443	192.168.2.4	49739	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 20:37:12.228564978 CEST	151.101.1.0	443	192.168.2.4	49737	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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 20:37:12.291444063 CEST	13.224.89.71	443	192.168.2.4	49746	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 20:37:12.312565088 CEST	13.224.89.71	443	192.168.2.4	49747	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 20:37:12.372056961 CEST	104.17.182.73	443	192.168.2.4	49751	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		

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 20:37:12.373173952 CEST	104.17.182.73	443	192.168.2.4	49750	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 20:37:12.431097984 CEST	13.224.89.71	443	192.168.2.4	49752	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 20:37:12.481929064 CEST	13.224.89.71	443	192.168.2.4	49753	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 20:37:12.523864031 CEST	13.224.89.71	443	192.168.2.4	49754	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 20:37:13.324176073 CEST	52.218.236.192	443	192.168.2.4	49756	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 20:37:13.325144053 CEST	52.218.236.192	443	192.168.2.4	49755	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 20:37:13.436635971 CEST	31.13.92.14	443	192.168.2.4	49759	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	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 20:37:13.436844110 CEST	31.13.92.14	443	192.168.2.4	49760	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		
May 20, 2021 20:38:24.430504084 CEST	52.218.236.192	443	192.168.2.4	49782	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 20:38:36.770054102 CEST	172.217.20.1	443	192.168.2.4	49783	CN=*.googleusercontent.com , O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Apr 13 12:15:39 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:15:38 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 2480 Parent PID: 800

General

Start time:	20:37:09
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:	0x7ff7e8ad0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	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: 1496 Parent PID: 2480

General

Start time:	20:37:10
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:2480 CREDAT:17410 /prefetch:2
Imagebase:	0xf10000
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