ID: 404294
Cookbook: browseurl.jbs
Time: 21:51:52
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

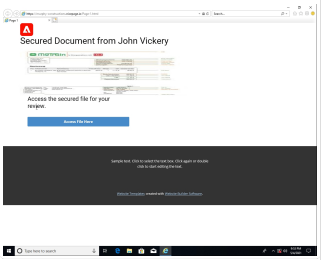
Analysis Report https://murphy-constructions.nicepage…

Overview

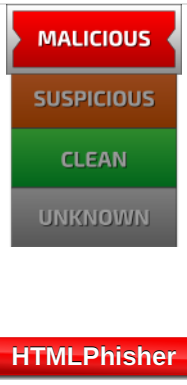
General Information

Sample URL:	http://https://murphy-constructions.nicepage.io/Page-1.html
Analysis ID:	404294
Infos:	

Most interesting Screenshot:



Detection



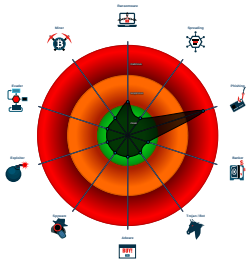
HTMLPhisher

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Phishing site detected (based on sh…
- Yara detected HtmlPhish10
- Yara detected HtmlPhish7
- HTML body contains low number of …
- HTML title does not match URL

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5440 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5752 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5440 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

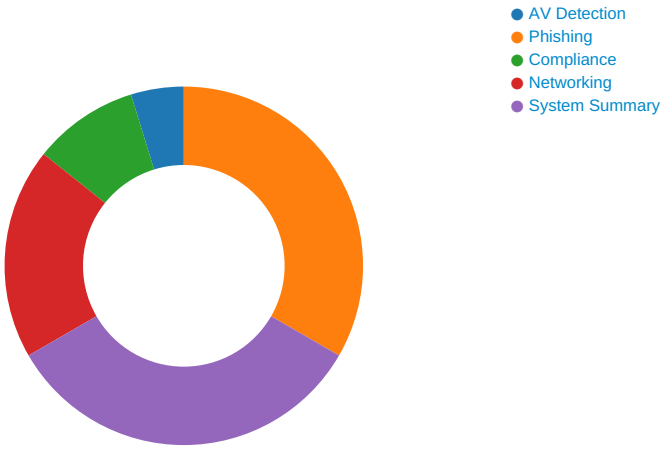
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\js[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\js[1].htm	JoeSecurity_HtmlPhish_7	Yara detected HtmlPhish_7	Joe Security	

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 shot template match)

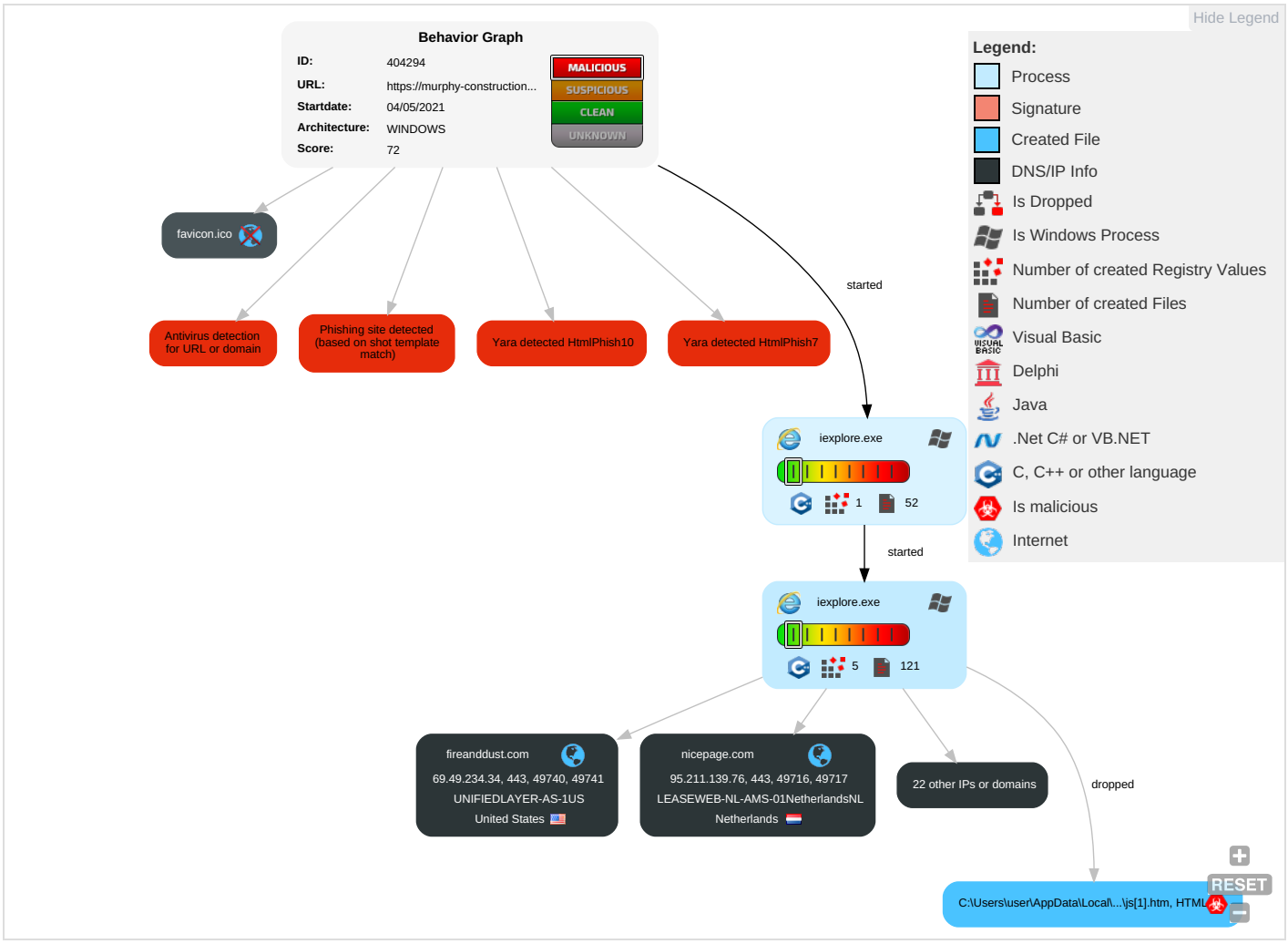
Yara detected HtmlPhish10

Yara detected HtmlPhish7

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

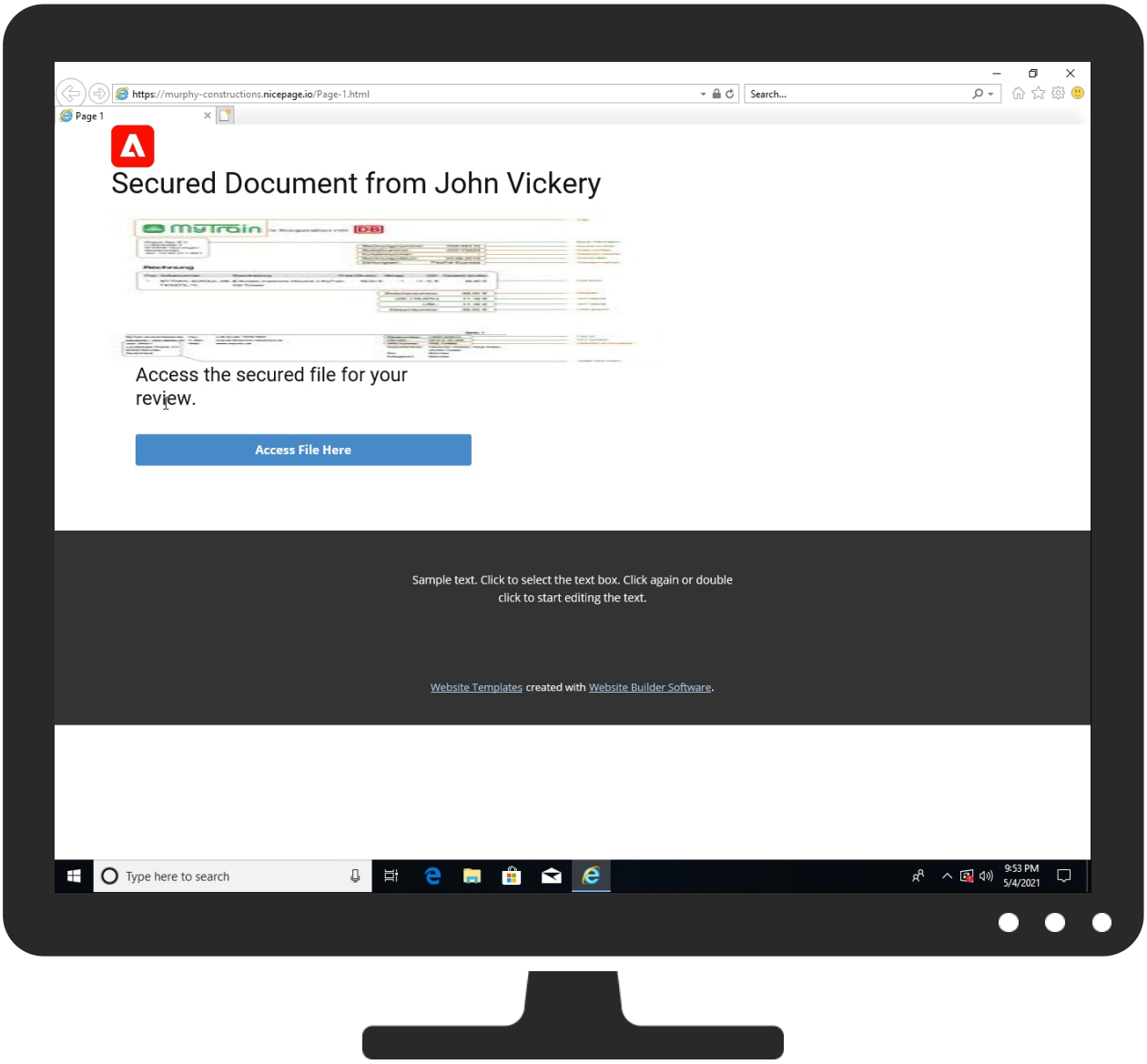
Behavior Graph



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://murphy-constructions.nicepage.io/Page-1.html	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://fireanddust.com/js/	100%	SlashNext	Fake Login Page type: Phishing & Social usering	
http://https://images01.nicepage.com/page/42/26/website-builder-software-42269.jpg	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://images01.nicepage.com/page/11/02/website-template-110215.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/32/18/website-template-full-32181.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/54/91/website-template-54915.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/33/84/website-builder-software-338486.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/23/80/website-builder-software-238078.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/42/34/website-template-42345.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/69/45/website-template-69459.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/42/41/website-builder-software-42414.jpg	0%	Avira URL Cloud	safe	
http://https://nicepage.com/ebsite-templates	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/29/64/website-template-29649.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/16/01/website-builder-software-160198.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/25/07/website-template-250747.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/10/76/website-builder-software-107655.jpg	0%	Avira URL Cloud	safe	
http://https://nicepage.com/de/website-vorlagen	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/27/91/website-builder-software-279124.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/10/49/website-builder-software-104927.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/22/28/website-builder-software-222893.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/11/88/website-template-118801.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/11/17/website-template-111762.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/21/18/website-builder-software-211836.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/20/68/website-template-206881.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/38/17/website-template-full-38174.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/96/14/website-template-96142.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/48/10/website-builder-software-48107.jpg	0%	Avira URL Cloud	safe	
http://https://csite.resource.nicepage.com/nicepage.css?version=2993d4e3-12ae-4eda-9125-86b9894223df	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/85/99/website-template-85994.jpg	0%	Avira URL Cloud	safe	
http://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/12/90/website-template-12905.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/10/35/website-template-103566.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/63/31/website-builder-software-63310.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/42/68/website-template-42682.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/58/36/website-template-58364.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/13/04/website-template-130486.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/17/19/website-builder-software-17195.jpg	0%	Avira URL Cloud	safe	
http://https://nicepage.com/Editor/Account/Register	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/10/77/website-template-107717.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/67/39/website-template-67398.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/92/92/website-template-92929.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/17/95/website-builder-software-17957.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/59/99/website-builder-software-59999.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/20/18/website-builder-software-201859.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/15/74/website-template-157494.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/32/56/website-builder-software-32565.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/10/73/website-template-107399.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/13/99/website-template-139905.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/44/08/website-template-44088.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/12/36/website-template-123679.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/65/94/website-template-65944.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/90/80/website-template-90807.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/87/40/website-template-87403.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/36/52/website-builder-software-365215.jpg	0%	Avira URL Cloud	safe	
http://https://nicepage.com	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/38/71/website-template-38710.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/96/87/website-template-full-96872.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/16/01/website-template-full-160154.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/31/03/website-template-full-310398.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/94/16/website-builder-software-94166.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/95/49/website-template-95498.jpg	0%	Avira URL Cloud	safe	
http://https://nicepage.com/website-templates?page=2	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/57/19/website-template-57195.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/96/20/website-template-96209.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/41/93/website-builder-software-41937.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/74/05/website-template-74057.jpg	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://images01.nicepage.com/page/85/56/website-template-85566.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/41/72/website-builder-software-41721.jpg	0%	Avira URL Cloud	safe	
http://https://fireanddust.com/js/.nicepage.io/Page-1.htmlX	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/10/18/website-template-101883.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/16/52/website-template-full-16526.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/15/75/website-builder-software-157509.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/41/35/website-template-41358.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/19/53/website-template-19530.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/66/49/website-builder-software-66499.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/20/17/website-builder-software-201724.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/10/81/website-builder-software-108127.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/96/52/website-template-full-96520.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/12/40/website-builder-software-12404.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/20/42/website-template-20428.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/46/60/website-builder-software-46609.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/24/79/website-template-full-247914.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/43/69/website-builder-software-43693.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/15/15/website-builder-software-151514.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/24/22/website-builder-software-242270.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/24/98/website-template-24984.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/55/34/website-builder-software-55345.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/81/13/website-template-81130.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/93/80/website-builder-software-93804.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/28/88/website-builder-software-288846.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/98/05/website-template-98054.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/31/86/website-template-31866.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/27/02/website-builder-software-27020.jpg	0%	Avira URL Cloud	safe	
http://https://images01.nicepage.com/page/43/33/website-builder-software-43333.jpg	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
1163043995.rsc.cdn77.org	89.187.165.8	true	false		unknown
www.google.de	142.250.185.227	true	false		high
1834444515.rsc.cdn77.org	89.187.165.7	true	false		unknown
stats.l.doubleclick.net	74.125.133.156	true	false		high
static.nicepage.com	95.211.139.76	true	false		unknown
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high
cdn.amplitude.com	13.32.23.71	true	false		high
1156509985.rsc.cdn77.org	89.187.165.8	true	false		unknown
murphy-constructions.nicepage.io	18.194.109.194	true	false		unknown
nicepage.com	95.211.139.76	true	false		unknown
fireanddust.com	69.49.234.34	true	false		unknown
1487879380.rsc.cdn77.org	89.187.165.7	true	false		unknown
d57e01lyo0mq2.cloudfront.net	13.32.23.99	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
1238657323.rsc.cdn77.org	89.187.165.7	true	false		unknown
ka-f.fontawesome.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high
favicon.ico	unknown	unknown	false		unknown
stats.g.doubleclick.net	unknown	unknown	false		high
images02.nicepage.com	unknown	unknown	false		unknown
images03.nicepage.com	unknown	unknown	false		unknown
code.jquery.com	unknown	unknown	false		high
csite.nicepage.com	unknown	unknown	false		unknown
capp.nicepage.com	unknown	unknown	false		unknown
csite.resource.nicepage.com	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://murphy-constructions.nicepage.io/Page-1.html	true		unknown
http://https://nicepage.com/website-templates	true		unknown

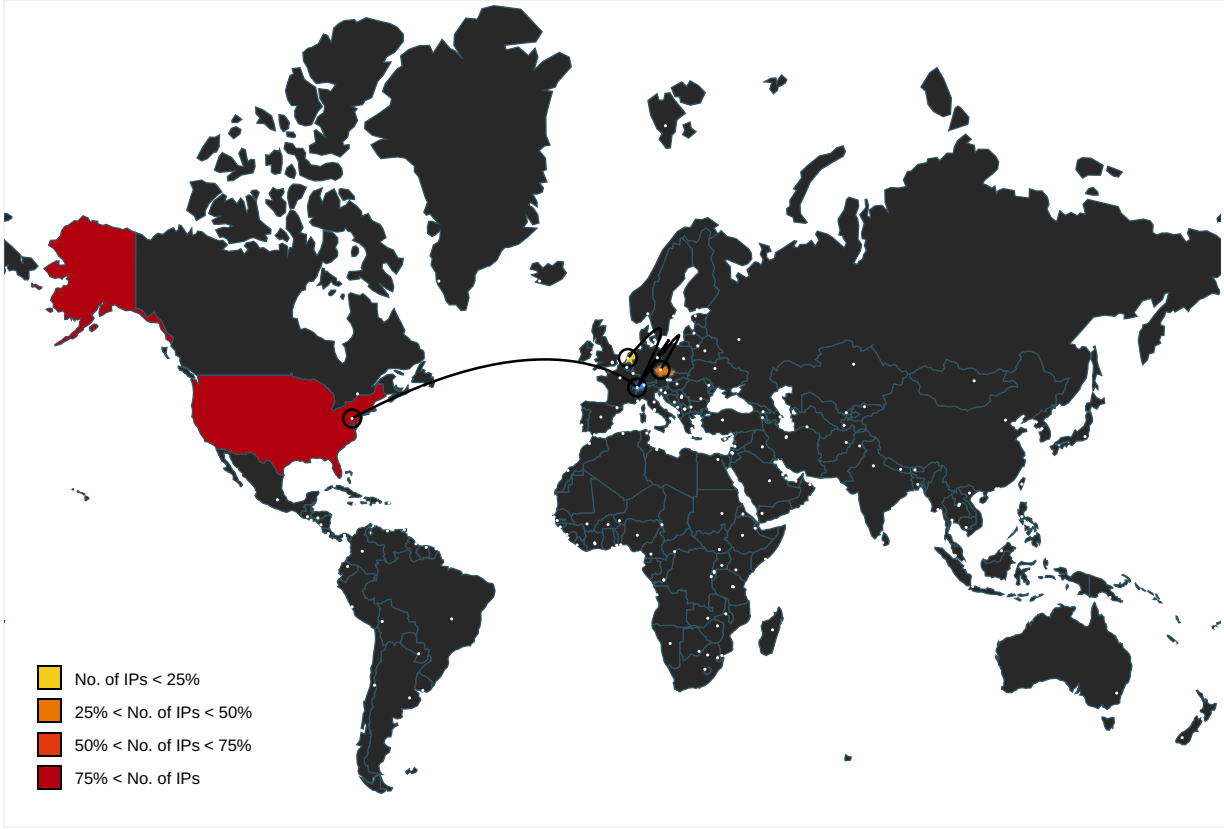
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://images01.nicepage.com/page/42/26/website-builder-software-42269.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/11/02/website-template-110215.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/32/18/website-template-full-32181.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/54/91/website-template-54915.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/33/84/website-builder-software-338486.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://twitter.com/NicepageApp	8ZU3LXBE.htm.3.dr	false		high
http://https://images01.nicepage.com/page/23/80/website-builder-software-238078.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/42/34/website-template-42345.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/69/45/website-template-69459.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/42/41/website-builder-software-42414.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://nicepage.com/ebsite-templates	~DFB4F288BC7A0B80AF.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/29/64/website-template-29649.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/16/01/website-builder-software-160198.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/25/07/website-template-250747.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/10/76/website-builder-software-107655.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://nicepage.com/de/website-vorlagen	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/27/91/website-builder-software-279124.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/10/49/website-builder-software-104927.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/22/28/website-builder-software-222893.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/11/88/website-template-118801.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/11/17/website-template-111762.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/21/18/website-builder-software-211836.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.froala.com/wysiwyg-editor)	nicepage[1].css0.3.dr	false		high
http://https://images01.nicepage.com/page/20/68/website-template-206881.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/38/17/website-template-full-38174.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/96/14/website-template-96142.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/48/10/website-builder-software-48107.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://csite.resource.nicepage.com/nicepage.css?version=2993d4e3-12ae-4eda-9125-86b9894223df	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/twbs/bootstrap/graphs/contributors)	bootstrap.min[1].js.3.dr	false		high
http://https://images01.nicepage.com/page/85/99/website-template-85994.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://getbootstrap.com)	site-common-libs[1].js.3.dr	false	• Avira URL Cloud: safe	low
http://https://images01.nicepage.com/page/12/90/website-template-12905.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/10/35/website-template-103566.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/63/31/website-builder-software-63310.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/42/68/website-template-42682.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/58/36/website-template-58364.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://images01.nicepage.com/page/13/04/website-template-130486.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/17/19/website-builder-software-17195.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://nicepage.com/Editor/Account/Register	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/10/77/website-template-107717.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/67/39/website-template-67398.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/92/92/website-template-92929.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/17/95/website-builder-software-17957.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/59/99/website-builder-software-59999.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/20/18/website-builder-software-201859.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/15/74/website-template-157494.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/32/56/website-builder-software-32565.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/10/73/website-template-107399.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/13/99/website-template-139905.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/44/08/website-template-44088.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/12/36/website-template-123679.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/65/94/website-template-65944.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/90/80/website-template-90807.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ct.pinterest.com/v3/?tid=2619058937406&pd	8ZU3LXBE.htm.3.dr	false		high
http://https://images01.nicepage.com/page/87/40/website-template-87403.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/36/52/website-builder-software-365215.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://nicepage.com	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/38/71/website-template-38710.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/96/87/website-template-full-96872.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/16/01/website-template-full-160154.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/31/03/website-template-full-310398.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/94/16/website-builder-software-94166.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/95/49/website-template-95498.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://nicepage.com/website-templates?page=2	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/57/19/website-template-57195.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/96/20/website-template-96209.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/41/93/website-builder-software-41937.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/74/05/website-template-74057.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/85/56/website-template-85566.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/41/72/website-builder-software-41721.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://fireanddust.com/js/.nicepage.io/Page-1.htmlX	~DFB4F288BC7A0B80AF.TMP.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/10/18/website-template-101883.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/16/52/website-template-full-16526.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/15/75/website-builder-software-157509.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/41/35/website-template-41358.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://images01.nicepage.com/page/19/53/website-template-19530.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/66/49/website-builder-software-66499.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/20/17/website-builder-software-201724.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/10/81/website-builder-software-108127.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/96/52/website-template-full-96520.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/12/40/website-builder-software-12404.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/20/42/website-template-20428.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/46/60/website-builder-software-46609.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/24/79/website-template-full-247914.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/43/69/website-builder-software-43693.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/15/15/website-builder-software-151514.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/24/22/website-builder-software-242270.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/24/98/website-template-24984.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/55/34/website-builder-software-55345.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/81/13/website-template-81130.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/93/80/website-builder-software-93804.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/28/88/website-builder-software-288846.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/98/05/website-template-98054.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://fontawesome.com/license/free	free.min[1].css.3.dr	false		high
http://https://images01.nicepage.com/page/31/86/website-template-31866.jpg	website-templates[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://images01.nicepage.com/page/27/02/website-builder-software-27020.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://widget.intercom.io/widget/vwx04wrq	8ZU3LXBE.htm.3.dr	false		high
http://https://images01.nicepage.com/page/43/33/website-builder-software-43333.jpg	8ZU3LXBE.htm.3.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
74.125.133.156	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
69.49.234.34	fireanddust.com	United States		46606	UNIFIEDLAYER-AS-1US	false
104.18.10.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
13.32.23.99	d57e01lyo0mq2.cloudfront.net	United States		7018	ATT-INTERNET4US	false
18.194.109.194	murphy-constructions.nicepage.io	United States		16509	AMAZON-02US	false
95.211.139.76	static.nicepage.com	Netherlands		60781	LEASEWEB-NL-AMS-01NetherlandsNL	false
89.187.165.7	1834444515.rsc.cdn77.org	Czech Republic		60068	CDN77GB	false
89.187.165.8	1163043995.rsc.cdn77.org	Czech Republic		60068	CDN77GB	false
13.32.23.71	cdn.amplitude.com	United States		7018	ATT-INTERNET4US	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404294
Start date:	04.05.2021
Start time:	21:51:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://murphy-constructions.nicepage.io/Page-1.html
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:	10
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:	mal72.phis.win@3/91@19/10
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://fireanddust.com/js/ • Browsing link: https://nicepage.com/website-templates • Browsing link: https://nicepage.com/
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 104.43.139.144, 2.20.157.220, 8.241.78.126, 8.252.5.126, 8.238.35.254, 8.238.29.126, 67.26.73.254, 23.5.103.140, 13.64.90.137, 142.250.184.234, 142.250.185.227, 69.16.175.10, 69.16.175.42, 142.250.185.106, 104.18.22.52, 104.18.23.52, 172.64.101.17, 172.64.100.17, 142.250.185.78, 142.250.184.196, 20.82.209.183, 152.199.19.161, 92.122.213.194, 92.122.213.247 • TCP Packets have been reduced to 100 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, fg.download.windowsupdate.com.c.footprint.net, cds.s5x3j6q5.hwcdn.net, arc.msn.com.nsatc.net, ka-f.fontawesome.com.cdn.cloudflare.net, 2-01-3cf7-0009.cdx.cedexis.net, store-images.s-microsoft.com-c.edgekey.net, wu-fg-shim.trafficmanager.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, go.microsoft.com, www.google.com, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, www.google-analytics.com, kit.fontawesome.com.cdn.cloudflare.net, skypedataprdcolwus17.cloudapp.net, fonts.googleapis.com, www-google-analytics.l.google.com, fonts.gstatic.com, ajax.googleapis.com, ie9comview.vo.msecnd.net, skypedataprdcolcus16.cloudapp.net, download.windowsupdate.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\EQAWN5DV\nicepage[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1743
Entropy (8bit):	4.91025881632775
Encrypted:	false
SSDEEP:	24:WUW9xLUW9xLUW9xLUW9xwlnlLUW9xwlnlLUW9xwlnlLUW9xwynyJ:LWjwWjwWjwWjClwWjClwWjClwWj5yJ
MD5:	25B7FF5042D44A3CE5189151F9D08592
SHA1:	4E7D24E8C5D6D77694C8C60212651B31EA5EB2B9
SHA-256:	24BADB56F85717DA10FAEA3D418E6AA031B8DACC2D385B54986A96999893FB0D
SHA-512:	C265059BB18C4F179124B01DA90CD1ACF9E856A1575179730F3C29A23455A8509E3867762EB61C43B344C56379544DE2C5A0328FB0B5A2EB5176D25B99A675B8
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="np_userId" value="429529157e18c1aa01c0243c52b44d7" ltime="2328882208" htime="30884202" /></root><root><item name="np_userId" value="429529157e18c1aa01c0243c52b44d7" ltime="2328882208" htime="30884202" /></root><root><item name="np_userId" value="429529157e18c1aa01c0243c52b44d7" ltime="2328882208" htime="30884202" /></root><root><item name="np_userId" value="429529157e18c1aa01c0243c52b44d7" ltime="2328882208" htime="30884202" /><item name="amplitude_unsent_878f4709123a5451aff838c1f870b849" value="[]" ltime="2336232208" htime="30884202" /><item name="amplitude_unsent_identify_878f4709123a5451aff838c1f870b849" value="[]" ltime="2336232208" htime="30884202" /></root><root><item name="np_userId" value="429529157e18c1aa01c0243c52b44d7" ltime="2328882208" htime="30884202" /><item name="amplitude_unsent_878f4709123a5451aff838c1f870b849" value="[]" ltime="2336232208" htime="30884202" /><item name="amplitude_unsent_identify_878f4709123a5451aff838c1f870b849" value="

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{B97F68A8-AD5D-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8535645016908495
Encrypted:	false
SSDEEP:	96:rDZQZo2nLWBtqAfgWq1MMyT6sRgi+fgY6W/lX:rDZQZo2LWBtdfgxMRvgHfgY6sX
MD5:	AC3CB78CDB965C15D77C80EDF44B6A81
SHA1:	2D4DBAF859498CBB90BDDD11441277D78011EC3F
SHA-256:	9488656F8C7BE3F1961CFF8D71EBDFFC6B2247C45752FDF44398D888BEF93F83
SHA-512:	623F0651448CECCFAF2E2F37167CEAB48646517139D5A2EBBA24E15558174798367CB80669EE1440A8900FD14434C08DB08A3A040DFFD0B38A119969592D5AF8
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\{B97F68AA-AD5D-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	63002
Entropy (8bit):	2.160821524779915
Encrypted:	false
SSDEEP:	384:r15Aw4znAbK9D/7JH9XHStnciPR1cJPISCVDg:a

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B97F68AA-AD5D-11EB-90E5-ECF4BB2D2496}.dat	
MD5:	0FDBD062B97AE94B7C946FCD9E394DA9
SHA1:	B6C12D5E715ADDE330C3BF23D1AA7F031AE6C892
SHA-256:	3E29B9C422D1A4CBA93829E66DBE9D1C716CCC03E5A20A622B25DC8150B7233D
SHA-512:	14CF0F4AC2B775B0D08CE68D43E484077207F3C8FD4B7E095E5847A787C6DBC78582DB08FEEEFD5FAF9990B2E264BE0BE1B52E453E398F829E4DF3BC964D37 4
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\{B97F68AB-AD5D-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5634365695270098
Encrypted:	false
SSDEEP:	48:IwbGcpruGwpayG4pQSGrapbSIZGQpKoG7HpRgaTGIpG:rBZGQC6UBSIzAzTgeA
MD5:	96EB1FABF6214D84EC0AB1A697CB96E4
SHA1:	C7F7004FAE5421EC26CB62459687B9B0F2BBE26D
SHA-256:	530720146E05F166E5071BF222E1C4F18036B651A1FB8E9CBAD18B880A3836C9
SHA-512:	4F6B6FB7877ACE5FC7172F7B0733D30807B9FDD6AFACAA9E696962CEC032A10ECE209285F4764C08D46C7218471CAE0E5BF758426F3DF20A73AFEC612262F8E 3
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y... ....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\wlm7n14\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1264
Entropy (8bit):	3.611102801746709
Encrypted:	false
SSDEEP:	12:VY1TYa8plOeRp3333333333ZOpRp333333333333g33333333333333333ypSrJ:VY1stOeyYhCCCeGsrDls3h9k1X
MD5:	0C9080D2E18D064B5D01EC84688FDAA7
SHA1:	1350852C69FD70212EB4C57C3C150A9CDADCA471
SHA-256:	4FDCC489B83ACBC524D23BE639D8A3F41739D8CA4EC6F3F8E844FA521FFD9BDB
SHA-512:	FCF98992CC9BFE1237C80E4164F8DFB1C21699BAEFDEB3A3164D06D3E778295FB4E63A42C41EF4505B696810EC2DA83CBDAAA598C8E8153CF1083ED796755C 3
Malicious:	false
Reputation:	low
Preview:	&.h.t.t.p.s.:././.c.s.i.t.e...n.i.c.e.p.a.g.e...c.o.m./.f.a.v.i.c.o.n...i.c.o.~.............. .h.......(....... ....@...................>. .>...U........B..>..>...G.........M..>..>..>..>..>..>...k...........I..>..>...U...........`..>..>..>..>..>..>...k...........I. .>..>...U...........`..>..>..>..>..>..>...k...........I..>..>...U...........`..>..>..>..>..>..>...k...........I..>..>...U...........`..>..>..>..>..>..>...k...........I..>..>...V...........`..>..>..>..>..>..>...k......... ..I..>..>...v...........]..>..>..>..>..>..>...k..............................C..>..>..>..>..>..>...k.................................>..>..>..>..>..>..>...S.....................b..>..>..>..>..>..>..>..>..>..>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\8[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=12, height=709, bps=0, PhotometricIntepretation=RGB, orientation=upper-left, width=1200], baseline, precision 8, 1200x646, frames 3
Category:	downloaded
Size (bytes):	161118
Entropy (8bit):	7.5594351594508185
Encrypted:	false
SSDEEP:	3072:WucfAcwuKGuN2q/gSsqnk4br5XUGpppLqfmazv7l04J:OMuKbYOF355XEuAv7lnJ
MD5:	F17B5B1163EFB6D2D47DE6BAE6D3A9CD
SHA1:	6D6964B34BC44C6D2B106ADE1AE675985B96D012
SHA-256:	7829F065E0E10C8466F3D57766E0719421B7B652F6A1082F21B98702F1B28A30
SHA-512:	7C0CBEF1D3CAE66A18C74544E593803C2EEC56817E762A385D54437BC7D597B2598886B0C0EDF72C6E934E9F146CEFC89392A492DB5425A1071E61CA1F15685
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\8[1].jpg	
Reputation:	low
IE Cache URL:	http://https://fireanddust.com/js/images/8.jpg
Preview:	......Exif..MM.*.....(.....1.....".....2.....i.....$.....'.....'.Adobe Photoshop CC 2015 (Windows).2020:01:21 13:41:42.....0221.....r.....z.(.....%.....H.....H.....Adobe_CM.....Adobe.d.....V....".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?.....q..KJG..x.."....]..TX...[^.m...R.....X.5..j?p.A.RI%0...MN.$..@.4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\JTUPjIg1_i6t8kCHKm459WxZSgnz_PZ2[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 24096, version 1.1
Category:	downloaded
Size (bytes):	24096
Entropy (8bit):	7.978949849579595
Encrypted:	false
SSDEEP:	384:0uponGPVx/956hA3UGTJO8WYRZ91cZlbNVpDY1fPmfl46wDNW/z3QtUBG9K7vwG5:0u5PVnoA3UF8WY/91clRCeflHgNW/jcS
MD5:	A8EC4957E1C24F5793305763AD9845B3
SHA1:	CC1C3AB955D78072362FF20259F2895DF5822631
SHA-256:	18EFFEC3306DDC4193B180E735A0E07A9B57FB1ECDC898438B586C65EDCDF0AD
SHA-512:	6962566699582FCF2C89BACDDE3E5D21D0B948CAD36773CE7E2D2CE8396D1ECD5096AB87161322CDA85EF865FE0B0BF22B7CFF0B7A624AAF9E71FA009B70AEF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTUPjIg1_i6t8kCHKm459WxZSgnz_PZ2.woff
Preview:	wOFF.....^ .....(.....GDEF.....G...X.f.^GPOS.....0*...GSUB...L.....,.OS/2.....Q...`U...cmap...d.....h.cvt ...(...e....6..`fpgm.....F...mM$.\|gasp.....glyf.....8...nb.%x.head..T....6...6..].hhea..T....#...$....hmtx..T....[...>H..loca..WP...$...(x...maxp..Yt... ... .[.Pname..Y.....,/.Lppost..Z.....D.-.prep..]d.....K..x.%....P.....@:D...$..]!....h.....2/.$.....D.^.F..ua.].N....%>.....x...p#...?..5.k8..;....0.c.3333cA.9q...I.#..).H...pU6..5...r*U8.W...Pk.wfD...1w.t...T.{>...b.....2@.Z+K..t.....:.,.5J...:....wP..'..0.&H..v..~5]IW..V.....m.V..j.m.".wK...c.4.$..zZ.b..1..]....h..O..d.*....b....\.,...s.n.=&.....u....-.3...5#L.m.U..W(0.4.9Wp.....r.P.)T..P.*....t.%....F.).x...la...C<WX..<_....:^(..n..{x/.x.P..|..>(TX..|X..#.(.....g.O.%>)L.)a.....P..B./.s|..K.Ma...F..0.w.y.'.,..}a...S...K.Ba.-~..[!.Ja.V.....3Q.....R.qL....%.,._...V9.,...Vz..2....Y..."..#b.....:..h8.....{U..y....(.G..k'.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\JTUQjIg1_i6t8kCHKm45_QpRyS7g[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22500, version 1.1
Category:	downloaded
Size (bytes):	22500
Entropy (8bit):	7.977478630884967
Encrypted:	false
SSDEEP:	384:qF14bCC33a2W8VT2+GTJO86XMfb0kqRQ6o7aaxESXN22ujw6lYkkjt9UwV:qF142Cy8VT2+F86XiwkoQNaaxLA2u0tt
MD5:	370318464551D5F25B0F0A78F374FAAC
SHA1:	20F4EC409A5E86EA89FE26BE42FDABFD11DC867C
SHA-256:	0B89EA33174D7ACB702309A88B66B3422189BDDC0BB5961A90116A21A98E848A
SHA-512:	B15A41753EF3AEB7355C647C5A40D30A65FBE9F347EFEAE9505D7C789B9447F2A58168F14F0BBC2CC8204274FF317F2305C35075833021C1308707796566FB24
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTUQjIg1_i6t8kCHKm45_QpRyS7g.woff
Preview:	wOFF.....W.....GDEF.....G...X.g.^GPOS.....2..1..7.GSUB.....,.OS/2.....L...`S..@cmap.....h.cvt .....\....,...fpgm...,...F...mM$.\|gasp...t.....glyf...\|..21.._.=.V.head..N....6...6.0.Yhhea..N.... ...$....hmtx..O.....>...]loca..Q$.....(>RU$maxp..SD... ... .h.\name..Sd.....)JD.post..TP.....D.z.prep..W(.....K..x.%....P.....@:D...$..]!....h.....2/.$.....D.^.F..ua.].N....%>./...x...l$...F..mw...=`.L/..13333333333.2.O...\|:.`yW~..O...)U.ny<^.....J.....d.'S....H.g.../d.....s.U.^.\E<P.)Sy..^.b...@..Zo.<..ThV.#'R...*..,].....jo....r`.....b...5....#.....]..}5.....N...s>.R..t.O]Z.((R...N.....r..R-..s._s..6e."tR)./.V.tm.z..W.. ..k..../...e%q.9"f=.4^b..X.....rQ..b....*\..r]..y"W.H....;.C.30...yw`....yo`....x.`;..l.{.2...L..@...c2~....@...2~.h..@..5c.&P.6..LpB`+'..rJ`..s&.....@.y.&..F. .d!0..2.....$K.I...&...+.%...;..B.?.g.JY).I...H.zI..Kz...n.uk....{..U..] '.X....Z..Y..(7W...?.9.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\JTURjIg1_i6t8kCHKm45_aZA3gnD-A[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23276, version 1.1
Category:	downloaded
Size (bytes):	23276
Entropy (8bit):	7.978722054298751
Encrypted:	false
SSDEEP:	384:boRxPu4aCGTJO87w6QBiPmWZRAtkRc44kjix7m8bRWca7ztugWPwV:bktu4aCF87mBibZRfRcVkOx5bRVa7ztp
MD5:	1FC98E126A3D152549240E6244D7E669
SHA1:	F77707F0EEB7086952F287C45E0FBA4FC01F1C53
SHA-256:	94221B9AB3055AB8D736B35D9D1573B89BB1EF89A37D4EDC395404E2EA5E4701
SHA-512:	B921DDAF4DEEE17899E67973F49E9EC0C45E50158180F794A115B386BA52CC0CE0DFA961E433624EB2E5F672AD94532F770CA355AB4B942FFA6C5B49C283B0C3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\JTURjIg1_i6t8kCHKm45_aZA3gnD-A[1].woff	
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTURjIg1_i6t8kCHKm45_aZA3gnD-A.woff
Preview:	wOFF.....Z.....l.....GDEF.....G...X.g.^GPOS.....P..2....hGSUB.....,.OS/2.....L...`S..Ecmap...(.....h.cvt .....\....-P.mfpgm...H...F...mM$.\|gasp..... ...glyf.....3...]R...head..Q....6...6.5._hhea..Q.... ...$....hmtx..R.....>...nloca..T(... ...(....maxp..VH... ... .h.Zname..Vh.....-ZG.post..WX.....D.z.prep..Z0.....K..x.%....P .....@:D...$..]!....h.....2/.$.....D.^.F..ua.].N....%>./...x...p[Y...'...$.%..43.2333333.,...3.4wW..q.cw...r.J...T.Ug.....H....sA...w.{&.r....%_.5.B....~.-?..s.B. .R].:..?....s.?:..qoe...A .....OS..A.....hB\..DD7.':.!..j.T.....?.s....<..!.A.b.\.N.*.r7Ib.=.d<O=.....Q..@....9..l.6....x.-..<.98....e..zZ..*.....tjgXz.d(...h...(.N.....e.i..[.%\RP.....r..,q..E...E..pR.Y.%....h...?...c Q.O.Z.T..31.....,_...J4.k.....y..YTx...mb...5.C..N..8..%.#j<&..(.(...^....b=..0G.(.%.8*F..c...../.....Xd.....8'r..I.....a<..Q.....1v.5...{b/.dq..hG.ft....SBe.P#W-.o...I.X.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\JTURjIg1_i6t8kCHKm45_c5H3gnD-A[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23872, version 1.1
Category:	downloaded
Size (bytes):	23872
Entropy (8bit):	7.9789410515218915
Encrypted:	false
SSDEEP:	384:WCPZ9khezoAK1PfDV/cGTJO8gpFu2KobVfXpH2h1AdWJ8OjcmB2SrOFbYvaUP5KR:WCPUwzj0jV/cF8CFubobVf5WEdCjvBFw
MD5:	9A9BEFCF50D64F9D2D19D8B1D1984ADD
SHA1:	1DAD9D9EFE7BC0B3BA089BE10B8F9741A02312A3
SHA-256:	2849C719C361F2EC1A04BF5B262BCBEDD3DF46BF35F5B4CAE8F75EA0AC500111
SHA-512:	5EC89892CC2453CBC6B9F64C3A261491B3EFF35EA65586B65200D8F3FFB31A727A4F7592D4BD86519EED54FDA35D6A79799300CB2537E5602D5D5AC908C5639
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTURjIg1_i6t8kCHKm45_c5H3gnD-A.woff
Preview:	wOFF.....]@.....l.....GDEF.....G...X.g.^GPOS.....2..=.GSUB.....,.OS/2.....O...`U6..cmap.....h.cvt .....e....56..fpgm.....F...mM$.\|gasp...D..... ..glyf...L..4...aZ-...head..S....6...6.t..hhea..T0... ...$....hmtx..TP...%...><..Eloca..Vx.....(y...maxp..X.... ... .[.Mname..X.....+.G.post..Y.....D.z.prep..\.....K..x.%....P .....@:D...$..]!....h.....2/.$.....D.^.F..ua.].N....%>./...x...p#.....c....L..33333333. .....y...T.u.Og.Y0t..rMY.s.....c. ..<.....'Rz..^.J._..7..[..0#.R_.>!.W.....B.l.yRmD.B.P..ap. Y.v.S....bC6m.m..YBd....m..6..W.@..Q....C..Uq.2.;.HH..N*..@.]D...Pb..... . ..[o'..*.{..x.*&uf.W.$@...U`.b.!.....W.=i.....T.....0.3V...)Q.S.`..{?....u\.0.....&$..\"`X.9&2. .L..."..... ..z>(.|H.....V>.z....G"....v~*....S..".....Q.L..Y...9.",.../.Xd.Td.\t.....[..W..'../Z8 .9(Z8$.....2....T...c....0)b..iL...,P.. ..0.Y...6.eZ....Ln..l;.D.BhU..k.O..... .by1..*.F.g..M.]...M...!.n.-.;.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\JTURjIg1_i6t8kCHKm45_epG3gnD-A[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23764, version 1.1
Category:	downloaded
Size (bytes):	23764
Entropy (8bit):	7.978500586551931
Encrypted:	false
SSDEEP:	384:4KIACx6AjGTJO8hB7wiraQlDvAnccLaDmU3hE5PeFcOm/IYdJnVtnwV:4KIh6AjF8hB7wiRceDmGhExUZ0nwV
MD5:	26D42C9428780E545A540BBB50C84BCE
SHA1:	DF9971D19E6F6C354DC0FA8FEC2E0EC899114726
SHA-256:	F0D96992E292218F917A5544A2CFF615C935494DBA791CB3E0E3D910A5F2EB34
SHA-512:	464C9ACC575AAFBCA8086581F412850AD35DB4F171E9DEF87086AFBE740536586B06623ECE28CE7A5ADC894E202657E82E19B9161179A1B2AEE96F83CE84EFF F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTURjIg1_i6t8kCHKm45_epG3gnD-A.woff
Preview:	wOFF.....\.....GDEF.....G...X.g.^GPOS.....|../...A.GSUB...D.....,.OS/2.....O...`U...cmap...X.....h.cvt .....e....6..Xfpgm.....F...mM$.\|gasp..... ...glyf.....6...l.7...head..S....6...6....hhea..S.... ...$....hmtx..S.... ...>F..loca..V....$...(A.[.maxp..X4... ... .\.Pname..XT.....(.EWpost..Y@.....D.z.prep..\.....K..x.%....P .....@:D...$..]!....h.....2/.$.....D.^.F..ua.].N....%>./...x...p#...?..6...im..w.....a.....\|.M.H.#.(...._..M...(...Vw.kxo...'2@....c.....C.~+.....m....Z...T.{....v.....K_U.O..../....<d..\O ..,&.....4.&!.%.%U...Uk..TM..$...M.m.T.89N3].D*_d.b.{..:..~..[_mB.....N..F.l..'....yM^O....b.-N-.m.{..(..M...d.....I..2T."..r.*.](HGZ.6>-.....|Q..K.(_.f..0./....W..k!.o.-..N(. (.9L..pa.#.a..(J.-.8F..Xa...,'.YN.&9.....a..A..F.@..Ba...)....#..{. .k.Yj..Y...E...+l....wJ.....S-.*|.Q..!Y..Br.e.....g..'U.....W...18.....s.Z...2.....=A.w.j.UzS.)...N]g..\..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\KFOjCnqEu92Fr1Mu51TjASc6CsI[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22280, version 1.1
Category:	downloaded
Size (bytes):	22280
Entropy (8bit):	7.9727639867534075
Encrypted:	false
SSDEEP:	384:P9oOx7sdtvlKnxdf5DGTHz3uPGia2ghi4OEiO+KdRialMgTC3YS95HbcW8Y:1lZsdKnxdBDwz++ia2l4OEi7KCquoS9J
MD5:	6E949B62AF2E8B6F705E35EE4DBC17F4
SHA1:	31BC06C0C932EC0176F42C6864C58D7450BBF97E
SHA-256:	917A5159BE44DE9A82072F6A1C52EF645844D6BEDF42F8FD1549CD99D6DB2CC5
SHA-512:	109EF637EF3C4FB1670DD328466BF1507F0E92D97153A71CA045F3F17F924CC92FF75777B3730CF722825C755D646A796F429F50973C64B543AA13C174D8921B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOjCnqEu92Fr1Mu51TjASc6CsI.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\KFOjCnqEu92Fr1Mu51TjASc6Csl[1].woff	
Preview:	wOFF.....W.....x.....GDEF.....G...d....GPOS.....!GSUB.....OS/2...L...N...`t6.<cmap.....#cvt .....X...X/...fpgm.....4.....".gasp...@..... ....glyf...L..C`..tP>.e%hdmx..O....m....$+.-head..P....6...6...mhhea..PT...#...$...zhmtx..Px.....3J.loca..S.....maxp..U.... ... .4..name..U0.....>.post..V..... .a.dprep..V $.....?.1 .x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x...l\..F..3...N..q)..a|.....^..33..c.....p"y.iT....<Gg...!.3...T1...{.g0.u.y.....m.|.k..NF.....mox. ;...7&.Y..C.R_[.T.c..-.=...9:...a*j.G.....O.Q".6...>...(?...~...._2:..K4....S%...jbr).....*....e.U..-..X.3.ILQ....z..!.f:...<.W.#...e.c=...&6...lc;;..3<.s<....H.i2..N..t..)Ns...#`..".).[... ._.T..T.....+l..=..O.....Z..F...r..eM.f.Y.....-...r.\.s6.r..,..:.<$..#.l..F.$.2#.e..].[.....yR...e.|{..O..`)..U.0.e.50.Z.b../cM..i.&O._..+.Y.W...;z....j.p._.o..[CL.)n'.UGx..>).X..MJ..Fr..v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\KFOlCnqEu92Fr1MmEU9fBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20532, version 1.1
Category:	downloaded
Size (bytes):	20532
Entropy (8bit):	7.966425322589798
Encrypted:	false
SSDEEP:	384:tfEIIA0zhnegvIQxhXmqd8lpP/FwL0cV8yP1JSRHbNHlZL7qwZkoEu3HTbpXcyKd:tr0zhnewHxRmqd8PdwLLeR/ZLGwZLbTA
MD5:	DA2721C68B4BC80DB8D4C404F76B118C
SHA1:	3A32E8B7EFBC9DFB52F024D657B8C8C0A80E5804
SHA-256:	BD811625271ACCA47F7DAC48B460F13E08EE947B2A8E17E278C4D5CCB5D9323C
SHA-512:	5110656E41A261BD2A06F8B5B2A362FF8836B4289E1DE0777D83DB8E9D709C4C4248B67653A28FA47AD4AE823021ADBFC587900E142BF6887C2A7C936F7F4C33
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmEU9fBBc-.woff
Preview:	wOFF.....P4.....l.....GDEF.....G...d....GPOS.....oGSUB.....OS/2...p...Q...`t...cmap.....#cvt .....\...\1..Kfpgm...8...2.....$.gasp...l.....glyf... x..<e..n..W..hdmx..H....m....+1.3head..IP...6...6...rhhea..I.... ...$....hmtx..I.....S.loca..L8.....maxp..N4... ... .4..name..NT.....:.post..O0..... .m.dprep..OD.....S.. .)x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x....%Y....Wm=..mo..k.m....rl...m.g"^..../..[.}.S...\.mD...1..G>..giz...=C..}.y....|o..c.x.R.r"B.....m...../.&./ 6..5D.AGX.....)<'.)....?.... .Y4>|1...ES.Gc...FO.>$.../...}RCl..T.zD..uZ4~D.._OK.$.Z.(..JR...\..\..\..\.\.....*'n..6:x...b,..$...?.g:./y.iLg.3..l.0.y.g..X..V...d.#O...0....b7{..>.n.iD.V....." e.\A..OR.kwp.].....6p..."ZE..%...e.u3..L..V...W.7b..L.3.L1K...Ts..$6.-b.....9...b@..!1,...v.C....{...dox.G(...|a%E:.Fn.Nn.^n.....Sf..E)...k....<g..){....|.....DT..N....Hy.F.Jez....._? 7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\KFOlCnqEu92Fr1MmWUlfBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20396, version 1.1
Category:	downloaded
Size (bytes):	20396
Entropy (8bit):	7.974131663185347
Encrypted:	false
SSDEEP:	384:SfXdUIIA0zhyKR28ePpAwxZ5M3py8wtshtdf45DEVTGdYb7H2Q/VEgm:Svdj0zhbRmjIQ8wtsV4lEVGdY3/i/
MD5:	68D6DABFE54E245E7D5D5C16C3C4B1A9
SHA1:	7FDAB895EAEBECEDB3FB5473EAB94A1B292CEF19
SHA-256:	A01A632E56731A854F35701AA8C3A6A19A113290D9032FF9048F8064C45383BD
SHA-512:	44EB151F85178A2F9600E85AD43FAE470FABE0F247C9A03E67931B36028E600C7550D9DE2D69B3576A06577A5DEAF54822EE4BDC9DCBB47588D1972C8A959D4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmWUlfBBc-.woff
Preview:	wOFF.....O.....GDEF.....G...d....GPOS.....oGSUB.....OS/2...p...Q...`u...cmap.....#cvt .....H...H+~..fpgm...$...3...._...gasp...X..... ...glyf...d..< ..l..C^]hdmx..H....m....03#7head..H....6...6...\hhea..I,... ...$.&..hmtx..IL....."J.loca..K.....maxp..M.... ... .4..name..M.....~..9.post..N..... .m.dprep..N.....)* v60x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x....%Y....Wm=..mo..k.m....rl...m.g"^..../..[.}.S...\.mD...1..G>..giz...=C..}.y....|o..c.x.R.r"B.....m...../.& /6..5D.AGX.....)<'.)....?.... .Y4>|1...ES.Gc...FO.>$.../...}RCl..T.zD..uZ4~D.._OK.$.Z.(..JR...\..\..\..\.\.....*'n..6:x...b,..$...?.g:./y.iLg.3..l.0.y.g..X..V...d.#O...0....b7{..>.n.iD.V....." e.\A..OR.kwp.].....6p..."ZE..%...e.u3..L..V...W.7b..L.3.L1K...Ts..$6.-b.....9...b@..!1,...v.C....{...dox.G(...|a%E:.Fn.Nn.^n.....Sf..E)...k....<g..){....|.....DT..N....Hy.F.Jez....._? 7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\KFOlCnqEu92Fr1MmYUtfBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20412, version 1.1
Category:	downloaded
Size (bytes):	20412
Entropy (8bit):	7.970834733902595
Encrypted:	false
SSDEEP:	384:af5t4IIA0zhLqV6fCjKK/bF+ituwbilrCG36/C4odv4QobGOo8y0rO+:arn0zhLqnDFbuwb0rCGPdv4QoKOByf+
MD5:	64BBA9C4E8156C152050C657E9D24BF1
SHA1:	90ECF87091FAABE7BC0FF54A43828FA4DD483278
SHA-256:	D33864E01E5103EBE439732BB606E694C73B6851F24DA25D41901EB17CB5D98E
SHA-512:	2456A688A4C51759293E482D434A324BA81EFAC9DC203226007C256D468E424A88C678D1B8BCAD9E3950C6AC4F7FF76CACAD71A730709A600CA45569586910C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmYUtfBBc-.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\KFOlCnqEu92Fr1MmYUtfBBc-[1].woff	
Preview:	wOFF.....O.....|.....GDEF.....G...d....GPOS.....oGSUB.....OS/2...p...O...`v...cmap.....#cvt .....Z...Z...=fpgm...4...3.....#.gasp...h.....glyf...t..<...lL....hdmx..H....n....47(;head..H....6...6...Rhhea..I,... ...$.]..hmtx..IL.....,A.loca..K.....Bs.maxp..M.... ... .4..name..M.....\|..9.post..N..... .m.dprep..N.....8...Cx...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x....%Y....Wm=..mo..k.m....rl...m.g"^..../..[.}.S...\.mD...1..G>..giz...=C..}.y....\|o..c.x.R.r"B.....m...../.&./6..5D.AGX.....)<'.)....?.... .Y4>\|1...ES.Gc...FO.>$.../...}RCl..T.zD..uZ4~D._OK.$.Z.(..JR...\..\..\.\.\.....*'n..6:x...b,..$...?.g:./y.iLg.3..l.0.y.g..X..V...d.#O...0....b7{..>.n.iD.V....."e.\A..OR.kwp.].....6p..."ZE..%...e.u3..L..V...W.7b..L.3.L1K...Ts..$6.-b.....9...b@..!1,...v.C....{...dox.G(...|a%E:..Fn.Nn.^n.....Sf..E)...k....<g..){....|.....DT..N....Hy.F.Jez....._?7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\adobe[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 400x400, frames 3
Category:	downloaded
Size (bytes):	30925
Entropy (8bit):	7.75667128400845
Encrypted:	false
SSDEEP:	768:nuowBuvTpjgz+wqrPZ2qh8fmyjlX6RqnxgYqwNL:nuPOpjgzPqrPZRYZGnYqYL
MD5:	BE5274AF7D8BD25B8148A190FF515399
SHA1:	B8D0850FD92EE935287E17988B89E53607808C8C
SHA-256:	26C62DBDF527B8DCBF378EA62F129CBBBA3B244730687909BA21ECD729C9D2E6
SHA-512:	64893C625BE72783088575E36EF26FF4573243F32601BDA754EDA72B7515063B5E4E4831697D16AC663529C910AE12CCD145BEC530F2A9BAE4D9324301C65667
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fireanddust.com/js/images/adobe.jpg
Preview:	.....JFIF.....C.....C.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..g.....\|?....".+....._.....4...R...'..q..~...n.7.....QXJ<...=...^.V'@U..E..5....Uz.....IE.PTe.}/p.y.....T.<...-T..\|...b.=.#IU..~....{O/...b..E.....X...G...?.....\|....._....M..g.....T~g.....<.....T~g.....3$.=._..IU.K..^.E...=.#U.._[X.R..=W...1.....QTr.\....*.7..?..6.9K..^.E.Ps.\.....%W..y...g)s[KX)<.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\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
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\3Y2ADQKS\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	4043
Entropy (8bit):	5.251768380802729
Encrypted:	false
SSDEEP:	96:SYgW9YgLZYgxTGYgC7Ygw6QOWGOLpOxTvOChOw6QYgS7NAYgWNkYgLNuYggNwYgN:Hl6k+2TpEIszezox37NBlNtkN7PNRpN+
MD5:	A71E111C7B550B1E8B8533CF6153EDFA
SHA1:	53A7A79A8C0DC2B1DCD357494FE3621C8771C4DC
SHA-256:	872ECF85DBCF3CAA926F3BF745999161E5B98F816A14D6FFFACEFE82810A0564
SHA-512:	94592FA0BF8C1093B181B5F3450A1309267A77E3A9A0A395DD4A02A399F2E08B084B4133FCE0414025AF0B25A35279CE5988C3FA2925D26DCD5929C88A7DB958
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\css[1].css	
Preview:	@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKWyV9hrIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/opensans/v18/mem6YaGs126MiZpBA-UFUK0Zdcs.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 600;. src: url(https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKXGUdhrIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKWiUNhrIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 800;. src: url(https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKW-U9hrIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\free-website-templates-1200[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1200x350, frames 3
Category:	downloaded
Size (bytes):	31280
Entropy (8bit):	7.917034343993739
Encrypted:	false
SSDEEP:	768:BkVqldrvuBDFB8/s0ND9tzfZr9V6Aiamv/:Pnrv0UpND9TBV6ALmX
MD5:	1314E610670FD6EC6464985284848579
SHA1:	A28F467E8BAEA59029E28574026F8FB3A61B2AF8
SHA-256:	276DD1DDE5EDCFFC6DE00130FE8758DE2B7CFE23E9FF8ABC54CF3860A6610F63
SHA-512:	16724FB7E53840B78CEC7718E2F806FB2670376691132F626A00986C24B7AD36BE1F7BCE3FE2EB42A8F167AE5751ED4E4282B53190FC6502BD83377F25AA8B89
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://csite.nicepage.com/Images/Site/free-website-templates-1200.jpg?v4
Preview:	......JFIF......"..."*%%*424DD\....."..."*%%*424DD\.....^...."..~..1....."....|.{.y.ku.z.|..%..51....33Q...!./Gm.#:'..'u3.....(.^.....0u..Y..uR|K.y..9.....w....h.}....z../.....eO.s..<..-L..Mv.;S..Y...+.Y.Ec.Y^/..u.....X..>...]X.....q..Z...s.D_g~...[XX....s.@..$'.g.\|I.j.w.dR.}.4..\.....5.....<.....~..{f.>k.....X..._..q..SU.4....2.....~....#&.....$z...u..t.Y...Q.....m6.O.^...>.}.. ..W.....X...m.....9....q-.3..Y.....2.....J.>(.....\.....-.,.....:.M.....FU...4C.6.....3.+..?..3x.....=7..5..3.1..f.n.In.|..;{+m...5.....}.&r~u.....$..UQ....+.h..T.he..#.,-u....U.....5.....1....>...:.f:.....Mb.T .....;L..^Z.m.....>m}.3..4;,....>...n.IF..Y..n...If...(.o.O....._.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\icon-input-search[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1271
Entropy (8bit):	6.619982248865804
Encrypted:	false
SSDEEP:	24:U1he91Wwh82lYSKwTjBZKkVZZKbT3ouyJ3Vfg6bGg+2gnYUCbdNm+Jb0:aqQvnLuZKkDZKblJ3B22gYUCbdc3
MD5:	1F9A746B0C450820A4ABB292A3606D80
SHA1:	0C0CCED0E3F7EB97D66EA5927B0B54CB673600B9
SHA-256:	161482EBC4EAC70FAF3B6CA1AB7C085A96300C5E04E9939B257A58E89B25D5E3
SHA-512:	E0033C7C93CE40CA826CC2F07FD4B9806705A4B417FB75BDDB29F13A34D437AE4BF5507DAD53A0A0CBB8BC443772863808FDD00569A901D219D0B7DCEC330EA6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://csite.nicepage.com/Images/Site/icon-input-search.png
Preview:	.PNG.....IHDR.....a....tEXtSoftware.Adobe ImageReadyq.e<...fiTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <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:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:CB551714F39DE311ACEF8E194F869962" xmpMM:DocumentID="xmp.did:C51195149E0F11E39EE9B7DBA95B409F" xmpMM:InstanceID="xmp.iid:C51195139E0F11E39EE9B7DBA95B409F" xmp:CreatorTool="Adobe Photoshop CS6 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:CC551714F39DE311ACEF8E194F869962" stRef:documentID="xmp.did:CB551714F39DE311ACEF8E194F869962"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?> V.....'IDATx...J.p...-Q.]..S}.....CTPP..uq....Dp.J

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\mem6YaGs126MiZpBA-UFUK0Zdcs[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17440, version 1.1
Category:	downloaded
Size (bytes):	17440
Entropy (8bit):	7.962704570077627
Encrypted:	false
SSDEEP:	384:2QHZz7pdg60gyjkXImq2+GTFGc+Hq8pMG2dKQWS:9HTyAYa+GIHzyKQX
MD5:	06B4BFDA4E139EAF3AB9872A6D66F42F
SHA1:	E5C5999D6AF4869BC60EEA92D1A8C328FB0E1378
SHA-256:	39EC493A5A688A85B60A1E889A22CFB93F23C900E0FDC0BE8AB8543DC9DAA783
SHA-512:	D6665B3CDD7E759D4A2B1BF916654A9C7FCA24ACBEBA1FB4A75668F5B451C7542B5683C097A6A62ACCE76B98694A4F6847CE2DC5193113D02200A04EC85A658
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\mem6YaGs126MiZpBA-UFUK0Zdcs[1].woff	
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem6YaGs126MiZpBA-UFUK0Zdcs.woff
Preview:	wOFF.....D .....d@.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....]...`~l.=cmap...`.....X..cvt .....W.....fpgm...l.....~a..gasp.....#glyf... ...4...M..o*.head..< ...6...6..z.hhea..<X..."...$. ..hmtx..<\|...*.....=A.loca..>.....\|.maxp..@h... ... .name..@.....%`@.post..At.....x.I..prep..C0.....T..... .....x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`f.f.....:.....Q.B3_dHcb```.fccfeabbi``P..x.....:.;302(...&.O.....)B..q>H..u..R``..?i.....x.\.!..q..... .#aff...#1Q@.'U..@5.".llt.Aa#.f\|c.W....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c..$KY...e@.,.."..... ...?.....g....Z...[..5..=.d.....p.a.C?C..L...FF~..,...x.uTGw.F.....)..)7.W.$`*.....G.Kz.)e....t.|.1.7...s.g...3.7mgf..~{1...s.3.S...co..o.~.Zy.u...kW.\.t...N.KG.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\memnYaGs126MiZpBA-UFUKWiUNhrIqU[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17452, version 1.1
Category:	downloaded
Size (bytes):	17452
Entropy (8bit):	7.960788191365059
Encrypted:	false
SSDEEP:	384:gVRT8VGShcBuPgTnSzgEuY86rgt710WmLonjMKsZMQAZ:s3ShcBuASzgEuYPNn0nDRQAZ
MD5:	BF72679CA22E53320BEAEA090E8BB07D
SHA1:	F3BAA33E986EC10D6F0C8211A826242441D52CC7
SHA-256:	1E742589D91A4B7E3888284A43A73675F312D3D6C4E78B3B76EBC36292646100
SHA-512:	F8FFC70E2E187EFBC785A52959BB26F605FEFB904D27B73EA4E1012DCC35569A78144751F761AA30D7B4AB0E5951B91322EA322BAF792C18E359C2ED79BBAF6E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKWiUNhrIqU.woff
Preview:	wOFF.....D,.....eT.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....]...`....cmap...`.....X..cvt .....b.....g.ifpgm...x.....s.ugasp.....glyf...(..3...NH7X..head..<....6...6..{.hhea..<T..."...$...ahmtx..<x...).....>/Sloca..>.....maxp..@l.. ... .x..name..@.....)/C.post..A.....x.I..prep..C<..... x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`f9.....u..1...<.f.....b.. 0t.vfPdP...M...C.G/S....\|..K..6 .....t.....x.\.!..q.....#aff...#1Q@ .'U..@5.".llt.Aa#.f\|c.W....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c..$KY...e@.,q.....x.....3... .....%..=.d.....#..6.e..L@6.3.e.....1._....#...x.TGw.F.....)..)7.W..`*.j.-...=*'_..sI...2...O>....[tt....TK]..|...G.....^.m..=..x.q...+./].p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\memnYaGs126MiZpBA-UFUKWyV9hrIqU[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17668, version 1.1
Category:	downloaded
Size (bytes):	17668
Entropy (8bit):	7.9576211916710635
Encrypted:	false
SSDEEP:	384:TQHZiJiLqdJVOpEbXHYV0cIeLg8hDHNbCqe+WQN:NWuV1X/eRHNbCqefQN
MD5:	793B1237017AEACD646FB80911425566
SHA1:	51E3023140BE407FD5FBFD27E0A5D2C30AE66F31
SHA-256:	5BB07410994C14D60F72CE3F6E19B172FCD7BC515F9BAEAF1F74C6CC2216E86A
SHA-512:	95C6644C1C1A2E369075D429E86736491451431C6046BA74545C0BF91C1CABEA1B1A4FCFD8FC5BB6A37269E4F80AF5B792BF80C968EC6A3B8B325F33EC66331
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKWyV9hrIqU.woff
Preview:	wOFF.....E.....c.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....]...`~...cmap...`.....X..cvt .....^.....M..fpgm...t.....~a..gasp.....#glyf... ..4...Lv$.#.head..<....6...6./{.hhea..=...."...$....hmtx..=4...@....}.K.loca..?t.....*maxp..A4... ... .name..AT.....*.D9post..BD.....x.I..prep..D.....$...J..... .....x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.%..@@.@.....T.2..Q.1dB...!.j@..}(../y..]...V....b.b.D#5/....(..v.p...'e.7.....@@?.9.....x.\.!..q..... #aff...#1Q@.'U..@5.".llt.Aa#.f\|c.W....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c.. .P...,..`....b`....C ..D@$P..)._.....a .p@.0.(.@.8. ..0....a8.....x.uTGw.F.....)..)7.W.$`*.....G.Kz.)e....t.|.1.7...s.g...3.7mgf..~{1...s.3.S...co..o.~.Zy.u...kW.\.t...N

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\outlook1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 26 x 26, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	771
Entropy (8bit):	7.682244426935498
Encrypted:	false
SSDEEP:	24:74yiH9yQmOntihdLl00qDeu1BcaDa0oljZG0:omOntO7v/uJDYG0
MD5:	C3FC46C5799C76F9107504028F39190F
SHA1:	519096AD3F03410CF9CE3C9B9FCCA6B439D97B23
SHA-256:	57898461712A639D119BDF88B7145919DCC8956C7A271D2E4A1084B29EAE6785
SHA-512:	DF4A0A2F78B2013035FB738BF405119B275D4CFEC31A23071EB9AF499D5F31FDC4BE22754CE791C975D7D417E908B5CAD16F962B0ADD3DFDCDE19844D74F668
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fireanddust.com/js/images/outlook1.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\outlook1[1].png	
Preview:	.PNG.....IHDR.....JL.....bKGD.....IDATH....k.A..k6.b.F1..H@...j@.aQ...(.. .. .. .A..D...I.....E.....1...W...;;.Y.d.}].U5]..x"3?....!..A..y..+R2\...m.NX.=..p.0... d.^.3.....J.Z.X.).....P\..x1.3.M.0....m.....F....?...n.....I.Fo)x._ R|.s..a.T?...?.=.9.Y..u....z..|.....Wz...h..<..P.. ...$.Y.....k`/4.y/.....L.C.....".....U....7....G...'h.....1j1E..%t..... @..a.....b.ED-.Tn.<..o.D...o..(.{1l>.....".4a.:k.l./.7t./.Q-'..>.. .....'3eb..d.@=4...C....A...;..N.X3.(.....,v...+...S...W..l...@,...j.).u<..@u..0...V&.b.yp.....0..o.?..V..B =.~&m"r (...6;EP.T.....h.m".[f.U)\|t..2.Q.....g.cP.W...D..[.O>..d;.yI.{/..#v.._..$.Q.....t\E..5i.q._.."/n...v.w..Uo ...#..S....^.....F..+._??.r.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\website-templates[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	286945
Entropy (8bit):	4.981372231207774
Encrypted:	false
SSDEEP:	1536:bHnIzpADNWNxbCejMvU4Lklc1DWWm77v7gOXkDQQqh7bwcVoUn+f+jguCDfblr7u:bozp4NWD7IBDGnY+Chyy8xZeCHR0vk
MD5:	FD1D4457A9869EEB867980BF180FB105
SHA1:	C08D66A7776094A283064D1526ADA647BFBAD73C
SHA-256:	16423AE04F40AA5D0817342A376AF64594A8B7A765AB57965DB4C2FB93D95A47
SHA-512:	E09DD11525F1DB648ECD790F88AB5D7AB2732CBF1E5E5494E9BC5946E8E163FA3C915D277E3F1C856CF738E2F53CE7317C6B31862363E886BC0507269258096E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://nicepage.com/website-templates
Preview:	<!DOCTYPE html>..<html lang="en">.. <head>.... <title>7000+ Website Templates | Free Website Templates</title>.... <link rel="shortcut icon" href="//csit e.nicepage.com/favicon.ico" type="image/x-icon">.. <meta name="Keywords" content="">.. <meta name="Description" content="Free Download the biggest collection of Free Website Templates, Layouts and Themes. 7000+ Website Design Ideas for your Inspiration. Responsive web page templates.">.. <meta prop erty="og:type" content="website">.. <meta property="og:url" content="https://nicepage.com/website-templates">.. <meta property="og:title" content="7000+ Web site Templates | Free Website Templates">.. <meta property="og:image" content="https://images01.nicepage.com/page/66/41/website-template-66419.jpg?versio n=b8951a15-39eb-44bc-9498-43ae92b97946">.. <meta property="og:description" content="Free Download the biggest collection of Free Website Templates, Layou ts and Themes. 7000+

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\JTUOjIg1_i6t8kCHKm459WxZqh7k29U[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22888, version 1.1
Category:	downloaded
Size (bytes):	22888
Entropy (8bit):	7.978328337821095
Encrypted:	false
SSDEEP:	384:Pdh/RzlrZ4jO2GTJO8pW1QYXMrABM+kM4HbEvfgRuni+zHftpi6t35p2CQtC5WD4:PrVlrSjO2F8pW7MrA+zbAnwui+bftp5t
MD5:	ECF7D49386E8F265878E735DB34A7C4B
SHA1:	D9CF54EA75107CE240E5042B96F712C24D16451D
SHA-256:	8216911F426DA25E3DC798C3E854996964BE8DD6FC5122C57D138B763B6997E1
SHA-512:	A8C7518FD04B7A57BC3FC24C6A9B364E7C2EFF60AB316D76F299AAEA3671ED3DEAF6EBD4A1A09FB2C992FC478BFDD9695398A927395FCD613D2FB8C096261 40
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTUOjIg1_i6t8kCHKm459WxZqh7k29U.woff
Preview:	wOFF.....Yh.....GDEF.....G...X.f.^GPOS.....1.....GSUB.....,.OS/2...t...O...`S..:cmap.....h.cvt .....\...,...fpgm.....F...mM$.\|gasp...,.....glyf... 4..3...`...Shead..O....6...6.<]ghhea..P0...#...$....hmtx..PT...E...>.../loca..R....!...(Y.p.maxp..T.... ... .f.fname..T.....$/.KVpost..U.....D.-.prep..X.....K..x.%....P.....@:D...$..]!....h.....2/.$.....D.^.F..ua.].N....%>.....x..up#I..."CI.d.dv.n.....;L.....>X.!.D.yv.....,...".$U.vz.}.Y....{.J".D<..Px.e..H....71.....p."@..ViZ.....T.k...Q<@.Jat...s.EQU..}.~.h ...g.....M....7.w.[...y.G%...Z!.]...h-M5...N...kJ...$D.S.*%RR.....$.g+I+...@.x.O.Tn?.....>.3....Fx.0.d.Y{....M.f.mN..B).....<.&....0..c..< ....."...J|.r|.....4.d.1...2...<u.@$..." .....j..U.ip..y....C....ZWKS...)...F(b.N.....J?G.. }.M.M.x..$.(.%*.I.z..1.R.?$.f(...E....N...=O..!',rhvr>..Qt...{..]}.V>..z]=.j.f.}l..@.0...A.&....k.....lm.U|...RX...~".64.]....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\JTUPjIg1_i6t8kCHKm459WxZBg_z_PZ2[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23756, version 1.1
Category:	downloaded
Size (bytes):	23756
Entropy (8bit):	7.978941742494386
Encrypted:	false
SSDEEP:	384:l42CoLobcXpoW0GTJO8ynXJGM5sMPbiHl3pLvgOzmtkUecUpXWD4:l4xKobOohF8U0M5sMP+xpD7ykUezpmD4
MD5:	FE46CF8B9462C820457D3BF537E4057F
SHA1:	9C78135EB4E84EFEF49139B64EA2D5A6D3A5F484
SHA-256:	219D08EEBC3A38B9E3DBCF90C2076911312625602D2D7942F3D2A4E7A36D50B6
SHA-512:	8C3F0CC3C9F5AF8FAC7DDF85CA9B17A9B57758317FA821219D35044A4877273DAA37494ADCB39FA51CA13798753A03E11FBBBDDDB057B50AE301B6C5BE0AD 9C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTUPjIg1_i6t8kCHKm459WxZBg_z_PZ2.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\JTUPjIg1_i6t8kCHKm459WxZBg_z_PZ2[1].woff	
Preview:	wOFF.....\.....8.....GDEF.....G...X.f.^GPOS.....2..).GSUB.....,.OS/2.....N...`S..@cmap.....h.cvt .....b....-Q.ofpgm.....F...mM$.\|gasp...`..... ..glyf...h..4...^vB..Rhead..SX...6...6.F]khhea..S....#...$....hmtx..S....L...>....loca..V.....(.o".maxp..X.... ... .a.fname..X<.....T5%Pepost..Y8.....D.-.prep..\.....K..x.%....P .....@:D...$..]!....h.....2/.$.....D.^.F..ua.].N...%>.....x...p[...+Kvt.$.....,333333.-.,...3.0.3.9o.Z.a.y..<.M...:..T.....4.n..W&.r>.od..?.....~?.}.....r;E.).R.Le..\|.w...R...D...kNw0...l.a... P....2c4@...I=.....R.....E...Z.n..$>.m@].....u...Q....P.#Tu..U..1....e.(%..H...Qm.o.=j...7#....nq>.....P.....-0.....u2.....8BAMp.V7ZP.B.Q..Z..Z+DN..1..49.EV..;...4G9k..b..l.lc+2~ ._g?evQe.{]...>.w..c..0G...;.d.,Ra7.-F ..Q..2...!..0*.,I.0....@....{...P.=.P|..GLs.P.#...e.L.L....u.~.|.L.Z.B.R.o..[....c.....A.,5 .)0.]y...@.U..Z@M.....6.B.a...<5.JZ}&AZ#.Ch..v.z ,..&R.....!..H(.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\JTUPjIg1_i6t8kCHKm459WxZOg3z_PZ2[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 24056, version 1.1
Category:	downloaded
Size (bytes):	24056
Entropy (8bit):	7.976695432056879
Encrypted:	false
SSDEEP:	384:C8tsJp6IXhrsDyZNGTJO8vEuvk1vaiQDSH20iB74ekoe1B2oO8Gzko9v5Mj9o1WU:C8tsJp6IwyZNF8dvr7DQ20iB72V15PGN
MD5:	72C01F753C3940C0B9CB6BF2389CADDF
SHA1:	FBE552AC4711EBE9F95281512BE46BE6E22B0422
SHA-256:	D7B2311364F2138610AD7DEC8BDB5EA8EC88E9B0B100CEAA8E59173B05FDD138
SHA-512:	94171B6D63B283622269F54F9D935F02E7B0BB69CDBD4D1A69D0734F9945A62470ACCF186FC4CCFC2FBD865D3BA4988430551F2C42E19126CFBC6E81C7B2983
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTUPjIg1_i6t8kCHKm459WxZOg3z_PZ2.woff
Preview:	wOFF.....]....GDEF.....G...X.f.^GPOS.....2..g.)GSUB...L.....,.OS/2.....Q...`T..\cmap...d.....h.cvt ...(...b....0...fpgm.....F...mM$.\|gasp..... ...glyf.....5...^...head..T....6...6.z].hhea..T....#...$...Nhmtx..T....J...>%u..loca..W(.....(3.J\maxp..YH... ... .f.fname..Yh.....41.L.post..Zd.....D.-.prep..]<.....K..x.%....P. .....@:D...$..]!....h.....2/.$.....D.^.F..ua.].N....%>.....x...P\Y.....!i..!t.L.a.....#..X...6L...a`.f)..W.^..&..~_.+..y....(.9...}.....~.~=... E.T6S.2..|.7.=..)XO....JF-...(.....W.....qz V.j.iFOh...]...guJK...:.....e..V..+Pa;. .+....#4.(..n.k..M.*L....#..`\-.O.t..2g.D..B.&..y7.lEnB...(.....H{.vN....MH..AM...a.h....J.Q.r..+f.t....`.Y.x.E..s.....R.*.....a..U..<...y.Q..C.....n .....A....$..^...n.O=...~..s...K ..=.R..Ez..t.o...@]..M.W2I.u.....j.%.5u.t....]..Y...M..h..r....7.Z..#@...l.....rw..4E72."..P.C.....g..ij..k..n+.5.X1.7....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\JTUPjIg1_i6t8kCHKm459WxZYgzz_PZ2[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23744, version 1.1
Category:	downloaded
Size (bytes):	23744
Entropy (8bit):	7.978176631397249
Encrypted:	false
SSDEEP:	384:yjzvJqgI7qBtvcyn4GTJO8U7QKwIbAHJTY+YUCXyrrQIRJuAmsvTTcxvWD4:yjzBqFW3cyn4F8QwjJl0gRP0xOD4
MD5:	3FE16939288856E8E828FA2661BF2354
SHA1:	38862D707B124D6CDC39825FD721ACA3888D76F2
SHA-256:	C65FB5E86DE426F12116089347F59809E92598936E37B1AB16587C4015E24184
SHA-512:	40762351F80C9E48D68FAD4C483A39080800CF66EAA78FF6C19380D8C7A14A1AA6D052FE3F7BEBD6C8414D10C6E167B3E4048965D92095A4D9AA1743C03FFFC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTUPjIg1_i6t8kCHKm459WxZYgzz_PZ2.woff
Preview:	wOFF.....\.....GDEF.....G...X.f.^GPOS.....w..2..g.^GSUB...@.....,.OS/2.....Q...`S7.Gcmap...X.....h.cvt .....b.....7.Efpgm.....F...mM$.\|gasp..... ...glyf.....4...\....Fhead..SX...6...6.U]shhea..S....#...$...+hmtx..S....H...>....loca..U.....(...=maxp..X.... ... .a.ename..X8.....,0.L.post..Y,.....D.-.prep..\.....K..x.%.... P.....@:D...$..]!....h.....2/.$.....D.^.F..ua.].N....%>.....x...p#I....$.j.H..X..xy.....!...~ffXf..ofgw..:.k:K..{."..CVxv..{.U.Y.U.U]M..\|)?H.....<.~.G~...."...r..uz(..O../R...v".w..~...v.o.' y'EH.J...:...jC.:...H..YM..H:c.=..F...I...@m..'..-e6..6Mq.P..T.!...;....9F1.?.....u.GMsFs$..R5.)..Q....e..B.KD.L....f?...J....z5...T+RP..V...Rb.5..KxN.....fy.y<.<a&L..\0..E. 7K.G..?./...N.....&....v.E..^.....E*..p....#....2.h. .JGN.0@ .5@...h{.....H....P...:..$.....u..Y...t...#....j...y?..0d....<.....,..D.i6A./.~.b.r].....H.D.....@.M....O$.. ....%..e.)..E...u..i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\JTUQjIg1_i6t8kCHKm459WxRyS7g[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 24012, version 1.1
Category:	downloaded
Size (bytes):	24012
Entropy (8bit):	7.97899710370432
Encrypted:	false
SSDEEP:	384:qwrKruFCJY76CwND0ENPGTJO8umTJLkhotpUGP0n01tDqrha0D0Q48Jy5PJkOfQX:qepv76C9ENPF8umTJLkhoUGP9D0Py0+G
MD5:	D191F22AF3BB50902B99AC577F81A322
SHA1:	8FF75A5A912739F74BC792CDCD96473E0AF9EC24
SHA-256:	A52BBF7F1149C3994896E372304C294BD156F1BED90AC5456902349C0E47C30D
SHA-512:	4890C57BCD108763FC970E7552E1FB81EB59C25D3D959B349A4DC3FDB2262EB7659AB1F79D0CE8B93E01D5C0E916A8DB03C079D05F684FEE3E65968A302751(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTUQjIg1_i6t8kCHKm459WxRyS7g.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\JTUQjIg1_i6t8kCHKm459WxRyS7g[1].woff	
Preview:	wOFF.....].....4.....GDEF.....G...X.f.^GPOS.....2....(GSUB...L.....,.OS/2.....Q...`S..Pcmap...d.....h.cvt ...(...b..../M.Dfpgm.....F...mM$.\|gasp..... ...glyf.....5...^.<.X.head..T`...6...6.f]\|hhea..T....#...$...<hmtx..T....G...>....loca..W....!...(B?X.maxp..Y(... ... .a.ename..YH.....,1G.post..Z8.....D.-.prep..]......K..x.%.... P.....@:D...$..]!....h.....2/.$.....D.^.F..ua.].N....%>.....x...t[G...z.l...Gv..q...B.....T.7e.7U.2$qb.J....9.N\|.....w....Q.r.....J.K.....o.zn.. E..6S.....o.z.W.@.Q._.;.J.C}#[.FV.W.... t.....Q.].!..E...4GE...:..:.-N.S..6..@m.Z).uk.t.%$h...1.....@....0....^.....%.O.p}.d....9..Mp..^.p%r....D*....N..@.....H.G.9`.....5!t..L8.....]...O0.qN.....u.....q..E.....U..)v..1. ..NF..x..q.Yf..g.._.V..e....5. d.....p.....f."?H .5.(..1..Q#+."e(..&...F.f...]L....._a]C...5K.....WC#..Z%F+.t..:Sd.X.L-r.....{u&.....W"..fA.vY.0@.t.w?..L.q.J.!4..^.tOJV....TIH.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\bars2[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 350 x 210, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	9312
Entropy (8bit):	7.911384467203007
Encrypted:	false
SSDEEP:	192:MiFSOBNtTb3Hd0FgjYu75Zqip3mogS0/Pv6fqP50H:LHPtTb36G0u7xZhgSKn6fq2
MD5:	AEAED8ED43D826D4095239D44B25698B
SHA1:	ADEC3F06FFB041E1A9FAA402D79BF38661282F94
SHA-256:	FD2BCEAA6DA1C6EDB2D60FCBBDF44153D33C5AB4D83526874DE32ACEA5671405
SHA-512:	82759395EC803465EF879F23790DA19524E88A87A5C1C493EFA643A3D5FD3EA7EB81F1E3D6002F5513DAFDF2F9899A714311C49D7A8F00AD1402A25482D4B614
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://images03.nicepage.com/a122014e1e8cdf24af08f98c/c6a4f9513b875aba994ff889/bars2.png
Preview:	.PNG.....IHDR...^.....5.X?....gAMA.....a.....PLTEt.&.G{..V'P.....6].?k/_...^.!j.H..;b'..Z..(.:g3g.c.C.=j.v.G... *T...%w.P.)H.?l(D..u.M.47o.,M.r.k.H.K...$..Z.:fN.4.L.e.EM../.....D.. [.=={.`.A.N.r.M...Br{.SG...% ...O.5r.M[.=}.Uq$>.6^a.Aw.Q.,.D..t[.@..].?8p.q$>. ..#.f.,J.H...S.|.T.3X.W.WD....Gw/T.9x.R.R.#..Y.<.J.8q.Y.<..("F...0U>h*7,.d.DZ@.H....Z|.T...3. (.."..C.....AP...%.v...V..#w.P#(..O.;<-C...Fx..&|.Tq.L.Ap\V.D..<x...'|.4X#..W.....WE...V9s..ApB2...#.I}.Ct(B*0Q .....".Fy..'..#?0.~.U;-.*..~.U:u...&.L.1R!_H..4'.Dv...fM.".....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\bootstrap.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	144877
Entropy (8bit):	5.049937202697915
Encrypted:	false
SSDEEP:	1536:GcoqwrUPyDHU7c7TcDEBi82NcuSELL4d/+oENM6HN26Q:VoPgPard2oENM6HN26Q
MD5:	450FC463B8B1A349DF717056FBB3E078
SHA1:	895125A4522A3B10EE7ADA06EE6503587CBF95C5
SHA-256:	2C0F3DCFE93D7E380C290FE4AB838ED8CADFF1596D62697F5444BE460D1F876D
SHA-512:	93BF1ED5F6D8B34F53413A86EFD4A925D578C97ABC757EA871F3F46F340745E4126C48219D2E8040713605B64A9ECF7AD986AA8102F5EA5ECF9228801D962F5D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css
Preview:	/*! * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors. * Copyright 2011-2018 Twitter, Inc.. * Licensed under MIT (https://github .com/twbs/bootstrap/blob/master/LICENSE). */:root{--blue:#007bff;--indigo:#6610f2;--purple:#6f42c1;--pink:#e83e8c;--red:#dc3545;--orange:#fd7e14;--yellow:#ffc107;-- green:#28a745;--teal:#20c997;--cyan:#17a2b8;--white:#fff;--gray:#6c757d;--gray-dark:#343a40;--primary:#007bff;--secondary:#6c757d;--success:#28a745;--info:#17a2b8;-- warning:#ffc107;--danger:#dc3545;--light:#f8f9fa;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:576px;--breakpoint-md:768px;--breakpoint-lg:992px;--breakpoint- xl:1200px;--font-family-sans-serif:-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,"Helvetica Neue",Arial,sans-serif,"Apple Color Emoji","Segoe UI Emoji","Segoe UI Symbol";--font-family-monospace:SFMono-Regular,Menlo,Monaco,Consolas,"Liberation Mono","Courier New",monospace}*,::after,::before{box-sizing:border-box}h tml{font-family:sans

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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):	3.351091276827269
Encrypted:	false
SSDEEP:	12:9Rp3333333333ZOpRp333333333333g3333333333333333333ypSr33332U3ax35:VyYhCCCeGsrDls3h/
MD5:	DF9125700DE49A3C7464E250830B212F
SHA1:	100EBEA44C82A14AFE1FBCD337CD0008D2CF8A31
SHA-256:	9241D4D83F3EE2C51CC17D3515E668ACEC2FBF0E0750751FC5BEAB14975488FF
SHA-512:	B6C1357A414243C0A36B4092B02F7240F632FE03B08C51C877FD2B924B6AE5F65A47B43E2E59EB748BE8619733144383410C28159BAF165D730E71457977A162
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://csite.nicepage.com/favicon.ico

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\favicon[1].ico

Preview:	.... .h.......(....... ....@....................>.. >..>...U........B..>..>...G.........M..>..>..>..>..>..>..>...k...........I..>..>...U...........`..>..>..>..>..>..>..>...k...........I..>..>...U...........`..>..>..>..>..>..>..>...k...........I..>..>...U...........`..>..>..>..>..> ..>...k...........I..>..>...U...........`..>..>..>..>..>..>..>...k...........I..>..>...V...........`..>..>..>..>..>..>..>...k...........I..>..>...v...........]..>..>..>..>..>..>..>...k..............................C..>..>..>..>. .>..>...k................................>..>..>..>..>..>..>..>...S....................b..>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\hover[1].css

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	114697
Entropy (8bit):	4.9296726009523
Encrypted:	false
SSDEEP:	1536:67O7EesvXIPRX4PT8aZv8qoXIoqbTFaFeTxvyAZ+D7M71D:qXIPRX4PT3
MD5:	FAC4178C15E5A86139C662DAFC809501
SHA1:	EF1481841399156A880EC31B07DDA9CFAA1ACE39
SHA-256:	BB88454962767EB6F2DDB1AABAAF844D8A57DE7E8F848D7F6928F81B54998452
SHA-512:	0902219B6E236FBF9D8173D1D452C8733C1BF67B0EB906CC9866EA0C27C2D08F6DA556D01475E9B54E2C6CE797B230BFBD5F39055CE0C71EA4D3E36872C378I 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fireanddust.com/js/css/hover.css
Preview:	/*!. * Hover.css (http://ianlunn.github.io/Hover/). * Version: 2.3.2. * Author: Ian Lunn @IanLunn. * Author URL: http://ianlunn.co.uk/. * Github: https://github.com/IanLunn/Hover.. * Hover.css Copyright Ian Lunn 2017. Generated with Sass.. */./* 2D TRANSITIONS */./* Grow */..hvr-grow {. display: inline-block;. vertical-align: middle;. -webkit-transform: perspective(1px) translateZ(0);. transform: perspective(1px) translateZ(0);. box-shadow: 0 0 1px rgba(0, 0, 0, 0);. -webkit-transition-duration: 0.3s;. transition-duration: 0.3s;. -webkit-transition-property: transform;. transition-property: transform;.}..hvr-grow:hover, .hvr-grow:focus, .hvr-grow:active {. -webkit-transform: scale(1.1);. transform: scale(1.1);.}../* Shrink */..hvr-shrink {. display: inline-block;. vertical-align: middle;. -webkit-transform: perspective(1px) translateZ(0);. transform: perspective(1px) translateZ(0);. box-shadow: 0 0 1px rgba(0, 0, 0, 0);. -webkit-transition-duration: 0.3s;. transition-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\jquery-3.1.1.min[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	86709
Entropy (8bit):	5.367391365596119
Encrypted:	false
SSDEEP:	1536:9NhEyjjTikEJO4edXXe9J578go6MWXqcVhrLyB4Lw13sh2bzrl1+iuH7U3gBORDT:jxcq0hrLZwpsYbmzORDU8Cu5
MD5:	E071ABDA8FE61194711CFC2AB99FE104
SHA1:	F647A6D37DC4CA055CED3CF64BBC1F490070ACBA
SHA-256:	85556761A8800D14CED8FCD41A6B8B26BF012D44A318866C0D81A62092EFD9BF
SHA-512:	53A2B560B20551672FBB0E6E72632D4FD1C7E2DD2ECF7337EBAAAB179CB8BE7C87E9D803CE7765706BC7FCBCF993C34587CD1237DE5A279AEA19911D69067I 65
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-3.1.1.min.js
Preview:	/*! jQuery v3.1.1 | (c) jQuery Foundation | jquery.org/license */.!function(a,b){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.1.1",r=function(a,b){return new r.fn.init(a,b)},s=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,t=/^-ms-/,u=/-([a-z])/g,v=function(a,b){return b.toUpperCase()};r.fn=r.prototype={jquery:q,constructor:r,length:0,toArray:function(){return f.call(this)},get:function(a){return null==a?f.call(this):a<0?this[a+this.length]:this[a]},pushStack:function(a){var b=r.merge(this.con

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\jquery-3.2.1.slim.min[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	69597
Entropy (8bit):	5.369216080582935
Encrypted:	false
SSDEEP:	1536:qNhEyjjTikEJO4edXXe9J578go6MWX2xkjVe4c4j2lI2Ac7pK3F71QDU8CuT:Exc2yjq4j2uYnQDU8CuT
MD5:	5F48FC77CAC90C4778FA24EC9C57F37D
SHA1:	9E89D1515BC4C371B86F4CB1002FD8E377C1829F
SHA-256:	9365920887B11B33A3DC4BA28A0F93951F200341263E3B9CEFD384798E4BE398
SHA-512:	CAB8C4AFA1D8E3A8B7856EE29AE92566D44CEEAD70C8D533F2C98A976D77D0E1D314719B5C6A473789D8C6B21EBB4B89A6B0EC2E1C9C618FB1437EBC77D3A 269
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-3.2.1.slim.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\jquery-3.2.1.slim.min[1].js	
Preview:	/*! jQuery v3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_evalUrl,-event/ajax,-effects,-effects/Tween,-effects/animatedSelector	(c) JS Foundation and other contributors	jquery.org/license */!function(a,b){"use strict";"object"==typeof module &&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	85578
Entropy (8bit):	5.366055229017455
Encrypted:	false
SSDEEP:	1536:EYE1JVoiB9JqZdXXe2pD3PgoIiulrUndZ6a4tfOR7WpfWBZ2BJda4w9W3qG9a986:v4J+OlfOhWppCW6G9a98Hr2
MD5:	2F6B11A7E914718E0290410E85366FE9
SHA1:	69BB69E25CA7D5EF0935317584E6153F3FD9A88C
SHA-256:	05B85D96F41FFF14D8F608DAD03AB71E2C1017C2DA0914D7C59291BAD7A54F8E
SHA-512:	0D40BCCAA59FEDECF7243D63B33C42592541D0330FEFC78EC81A4C6B9689922D5B211011CA4BE23AE22621CCE4C658F52A1552C92D7AC3615241EB640F8514B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js
Preview:	/*! jQuery v2.2.4 | (c) jQuery Foundation | jquery.org/license */!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="2.2.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return this.pushStack(n.map(this,function(b,c){return a.call

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\mem5YaGs126MiZpBA-UN_r8OUuhv[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18668, version 1.1
Category:	downloaded
Size (bytes):	18668
Entropy (8bit):	7.969106009002288
Encrypted:	false
SSDEEP:	384:Wv4QHZChiRh3lwLOf8cWN78NXpcr6gBUA9CD/q4cOPZmPO:WvwhNOkvvxC7qnc
MD5:	A7622F60C56DDD5301549A786B54E6E6
SHA1:	D55574524345932DB3968C675E1AEA08C68A456F
SHA-256:	6E8A28A0638C920E5B76177E5F03BA94FCDEDD3E3ECD347C333D82876B51C9C0
SHA-512:	1A842E5EDFFFFBAE353AD16545D9886E3E176755F22B86ECCC9B8B010FC79DB7194B7C5518CC190BF5B78B332C7D542B70A6A53B3BAF23366708DF348C2C2D9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UN_r8OUuhv.woff
Preview:	wOFF.....H.....n0.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....^...`}...cmap...`.....X..cvt .....].....fpgm...t.....~a..gasp.....#glyf... ..8...WP..M.head..@....6...6..F.hhea..A.....$...chmtx..A8....._{loca..CL.....K.4&maxp..E.... .. ....name..E0....."c?Jpost..F.....x.U..prep..G.....:..].....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\mem5YaGs126MiZpBA-UNirkOUuhv[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18696, version 1.1
Category:	downloaded
Size (bytes):	18696
Entropy (8bit):	7.96597476007567
Encrypted:	false
SSDEEP:	384:yeQHZsdOZKOIVrf0uvAxZEw5w7Yc3XGi/L6:dBbVwuvAYYw7THc
MD5:	449D681CD6006390E1BEE3C3A660430B
SHA1:	2A9777AFC07BF0BB4BB48F233ED7C4BCBDB60760
SHA-256:	57C79375B1419EE1D984F443CDA77C04B9B38C0BE5330B2D41D65103115FFD72
SHA-512:	8B8436670BB4D742AFA60ABA29D7A78F3788CBEF9353C2896AA492618CF1B22E9A0679972AB930E2F2D4732F3B979C023D25AA0FA86C813AC674524FD4ECA2BE
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\mem5YaGs126MiZpBA-UNirkOUuhv[1].woff	
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UNirkOUuhv.woff
Preview:	wOFF.....l.....m.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....^...`.-..cmap...`.....X..cvt .....[.....4fpgm...p.....~a..gasp.....glyf... ...8...W.J.4.head..A....6...6...Mhhea..A<.....$...#hmtx..A\... .....IT.loca..C\|.....6..umaxp..E@... ... .t..name..E`.....#.@Ppost..FP.....x.U..prep..H.....x..n..... .....x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`fy.....:....Q.B3_dHc.....@`...../..?....^..... 9. .m@J.....x.\.!..q.....#aff... #1Q@.'U..@5.".llt.Aa#.f\|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN...:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c..$KY...e@.,A.".m....x.....3 .....?.[.o...2...:...a..b.)@.Y.....v1.b4d...36 ..x.uTGw.F.....)..)7.W.$`*.....G.Kz.)e....t.|.1.7...s.g...3.7mgf..~{1...s.3.S...co..o.~.Zy.u...kW.\.t...N.KG.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\mem8YaGs126MiZpBA-UFVZ0d[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18100, version 1.1
Category:	downloaded
Size (bytes):	18100
Entropy (8bit):	7.962027637722169
Encrypted:	false
SSDEEP:	384:aHQHZuiZQFFlimUy1oml4hN2Vmw1Qa57YC74ObDDj08X0UJQiXc:1ZQT0UySml4bEmAP5EC7PbDH4U1M
MD5:	DE0869E324680C99EFA1250515B4B41C
SHA1:	8033A128504F11145EA791E481E3CF79DCD290E2
SHA-256:	81F0EC27796225EA29F9F1C7B74F083EDCD7BC97A09D5FC4E8D03C0134E62445
SHA-512:	CD616DB99B91C6CBF427969F715197D54287BAFA60C3B58B93FF7837C21A6AAC1A984451AEEB9E07FD5B1B0EC465FE020ACBE1BFF8320E1628E970DDF37B0F 0E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem8YaGs126MiZpBA-UFVZ0d.woff
Preview:	wOFF.....F.....i.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....^...`~]..cmap...`.....X..cvt .....Y.....M..fpgm...p.....~a..gasp.....#glyf... ...6...S...]head..>....6...6..cphhea..>.....$....hmtx..?.....[$loca..A4.....f..maxp..B.... ... .name..C.....&:A.post..D.....x.U..prep..E.....C..... ..x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`f..8.....u..1...<.f.....A.....5....1...A.._6..".-..L.....Ar,.....3..(....x.\.!..q.....#aff...#1Q@.'U..@5." .llt.Aa#.f|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c..$KY...e@.,.".....?....%.g....Z..... (".o..Y..Bu342.e.....0.....M=.....x.uTGw.F.....)..)7.W.$`*.....G.Kz.)e....t.|.1.7...s.g...3.7mgf..~{1...s.3.S...co..o.~.Zy.u...kW.\.t...N.KG.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\memnYaGs126MiZpBA-UFUKW-U9hrIqU[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17788, version 1.1
Category:	downloaded
Size (bytes):	17788
Entropy (8bit):	7.967181593577758
Encrypted:	false
SSDEEP:	384:Vp3UxvLq7eMDKdiXVYFbQk9YlD/XmhJGSiQ3L+CEW/9fE+QH:jgjq7ejOQMUeD/AGO6CB/98+QH
MD5:	92DA6F116D973BD334CF9B3AFDB29C4F
SHA1:	C7E59C92F4D8391276FB0A3A55528CF3965478E7
SHA-256:	49B6274BCCB5C6B31E20CEBB213D96197B522B1FB9C95B8649A0626EDB5BD9D8
SHA-512:	B3483F5137EAE074BDC95262B8C5D6049C4E7AF276F3EB1DDC3097ED3FBFB2C43110341B78E0B388E6B9B5D186168CD86DA324496CB08F909C60FEBFB3E207 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKW-U9hrIqU.woff
Preview:	wOFF.....E|.....f.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....]...`....cmap...`.....X..cvt .....o.....fpgm.....s.ugasp...(.....#glyf...8 ..4...N.-.W.head..=0...6...6....hhea..=h..."...$....hmtx..=....8.....\|&.loca..?.....P..maxp..A.... ... .name..A.....8Gtpost..B.....x.l..prep..D`.....@..R..... .x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.%..@0...?.%.N.O:Zg..TjL...Bk..-.a ..5.j.F...`...^..3.V.P..P.4..c....[..].9.... ..T(.q...x.\.!..q.....#aff...#1Q@.' U..@5.".llt.Aa#.f\|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c..$KY...e@.,,.".9....x.....3.....e.. =L.....`.Q..1.Q.....uF.F[F}Fe.....-.p..... ..x.TGw.F.....)..)7.W..`*.j.-...=*'_..sI...2...O>....[tt....TK]..|...G.....^.m..=..x

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\memnYaGs126MiZpBA-UFUKXGUdhrIqU[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17492, version 1.1
Category:	downloaded
Size (bytes):	17492
Entropy (8bit):	7.957749340429713
Encrypted:	false
SSDEEP:	384:bQHZhYs3a6PsVt9W9Z3owyC3bSZjyVO9Gz8W6EaJQgacXcK1cDVQgx:gq6PMK9Z3WCyc5z6lnXcYcxQU
MD5:	56E5756B696615D6164A625E1BCB1A9E
SHA1:	E2AEF56F577DBB78254066B73C2D0FBE30B40AE0
SHA-256:	BB87838929C15E1D0A05693C375323B95B6B4690FE207D3639E3A432C44AEF35
SHA-512:	BB998858AB9DF11375B0844EA008D31ABE4377826F6BE73C6F1DDE2E85C6F9A0404FADFDA9C081318F2F59614A22A1CF7F32376B25232887EDE8C7FBA323CB1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/memnYaGs126MiZpBA-UFUKXGUdhrIqU.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\memnYaGs126MiZpBA-UFUKXGUdhrIqU[1].woff	
Preview:	wOFF.....DT.....dD.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....]...`.7.rcmap...`.....X..cvt .....^.....fpgm...t.....~a..gasp.....glyf.....4 ..M4.]2.head..<<...6...6..zghhea..<t..."...$.{.@hmtx..<...,.....V9Vloca..>.....rimaxp..@.... ... .name..@.....,.G.post..A.....x.I..prep..CT.....x..%..... ..x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`f.....:....Q.B3_dHcb```.fgc.`abbi``P..x.....:.;302(...&.O.....)B..q>H.%.u..R``..<.....x.\.!..q.....#aff...# 1Q@.'U..@5.".llt.Aa#.f|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c..$KY...e@.,A.".m....x.....3 .....[.o....=.d...u.a.....S....G..3.b..h...."...x.uTGw.F.....)..)7.W.$`*.....G.Kz.)e....t.|.1.7...s.g...3.7mgf..~{1...s.3.S...co..o.~.Zy.u...kW.\.t...N

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\nicepage[1].css	
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):	1080138
Entropy (8bit):	5.0505805899494804
Encrypted:	false
SSDEEP:	12288:iUmo2qJ4FfbKmckQ2rJym5Dz6P5uXWXjmMULs5i6erDcY:X2rJrT
MD5:	B225C3AE6022C035CF3ECAAE9E51926E
SHA1:	05B0A8D07415370B7B3A3B4D33F7635F01E1449E
SHA-256:	0DD72FA3836BF24F07173E3B3D57FFCC3FBB068C20FC5E8C4736CA543AD343C1
SHA-512:	4FEE31FF748088958AFBE74B1650A52FB37BA619C12CF6E2F28ADCE03E8EC29768B94021C4306A7AE9BE6D1CA566D883D38898900D06FF9C5E0837BE585E5B5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://murphy-constructions.nicepage.io/nicepage.css?version=22baa169-ff2f-437c-8b06-732e40d9cb8d
Preview:	/*begin-commonstyles library*//*!.. * froala_editor v3.2.3 (https://www.froala.com/wysiwyg-editor).. * License https://froala.com/wysiwyg-editor/terms/.. * Copyright 2014-2020 Froala Labs.. */.....fr-clearfix::after {.. clear: both;.. display: block;.. content: "";.. height: 0; }.....fr-hide-by-clipping {.. position: absolute;.. width: 1px;.. height: 1px;.. padding: 0;.. margin: -1px;.. overflow: hidden;.. clip: rect(0, 0, 0, 0);.. border: 0; }.....fr-view img.fr-rounded, .fr-view .fr-img-caption.fr-rounded img {.. border-radius: 10px;.. -moz-border-radius: 10px;.. -webkit-border-radius: 10px;.. -moz-background-clip: padding;.. -webkit-background-clip: padding-box;.. background-clip: padding-box; }.....fr-view img.fr-shadow, .fr-view .fr-img-caption.fr-shadow img {.. -webkit-box-shadow: 10px 10px 5px 0px #cccccc;.. -moz-box-shadow: 10px 10px 5px 0px #cccccc;.. box-shadow: 10px 10px 5px 0px #cccccc; }.....fr-view img.fr-bordered, .fr-view .fr-img-caption.fr-bordered

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\nicepage[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):	159950
Entropy (8bit):	5.251567124483337
Encrypted:	false
SSDEEP:	3072:bowEUkhzz0XIMM4WakSPSLcxeghPIyq6cmN:bo58XDM4zS0ZIyH
MD5:	8799B3D4E1BF276C92BAC9BE63DC7554
SHA1:	76CAFFC0B171B0076EC95841F589642684CFBB43
SHA-256:	0FDD8ADBF5E7365F7AC6BD731A6760DDA0C680C5FC263781EA02DEAB2A913C8E
SHA-512:	61A51D2996A848BA20F7EDAA156EC2237BF55B9ED7E749A4DAF07C9161A50361AE1826D564CF287460218C5D011A22FF6A5833834A77D4F4CA73550793DECF2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://capp.nicepage.com/6ba8f9621eefd8f9e7050129b53e111985c3f5cb/nicepage.js
Preview:	!function(t){function e(n){if(i[n])return i[n].exports;var o=i[n]={i:n,l:false,exports:{}};return t[n].call(o.exports,o,o.exports,e),o.l=true,o.exports}var i={};return e.m=t,e.c=i, e.d=function(t,i,n){if(!e.o(t,i))Object.defineProperty(t,i,{configurable:false,enumerable:true,get:n})},e.n=function(t){var i=t&&t.__esModule?function e(){return t.default}:functio n e(){return t};return e.d(i,"a",i),i},e.o=function(t,e){return Object.prototype.hasOwnProperty.call(t,e)},e.p="/Content/BundledScripts/",e(e.s=5182)}({100:function(t,e,i){"use strict";function HorizontalLayoutSlider(slider,t){if(slider&&slider.length){var e=slider.children(".u-gallery-inner, .u-repeater");if(e.length){this.viewport=e;var i=slider.children(".u-gallery-nav");if(i.length){if(this.controls=i,this.data={offset:0,width:0,scrollWidth:0,maxOffset:0},t)this._onScroll=this.onScroll.bind(this),this.viewport.scroll(this._onScrol l);if(this.updateInnerData(),t)this.updateControls()}}}}t.exports=HorizontalLayoutSlider,HorizontalL

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\popper.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	19188
Entropy (8bit):	5.212814407014048
Encrypted:	false
SSDEEP:	384:+CbuG4xGNoDic2UjKPafxwC5b/4xQviOJU7QzxzivDdE3pcGdjkd/9jt3B+Kb964:zb4xGmiJfaf7gxQvVU7eziv+cSjknZ3f
MD5:	70D3FDA195602FE8B75E0097EED74DDE
SHA1:	C3B977AA4B8DFB69D651E07015031D385DED964B
SHA-256:	A52F7AA54D7BCAAFA056EE0A050262DFC5694AE28DEE8B4CAC3429AF37FF0D66
SHA-512:	51AFFB5A8CFD2F93B473007F6987B19A0A1A0FB970DDD59EF45BD77A355D82ABBBD60468837A09823496411E797F05B1F962AE93C725ED4C00D514BA40269D1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\popper.min[1].js	
Preview:	/*. Copyright (C) Federico Zivolo 2017. Distributed under the MIT License (license terms are at http://opensource.org/licenses/MIT).. */(function(e,t){'object'==typeof exports&&'undefined'!=typeof module?module.exports=t():'function'==typeof define&&define.amd?define(t):e.Popper=t()})(this,function(){'use strict';function e(e){return e&&'[object Function]'==={}.toString.call(e)}function t(e,t){if(1!==e.nodeType)return[];var o=getComputedStyle(e,null);return t?o[t]:o}function o(e){return'HTML'===e.nodeName?e:e.parentNode||e.host}function n(e){if(!e)return document.body;switch(e.nodeName){case'HTML':case'BODY':return e.ownerDocument.body;case'#document':return e.body;}var i=t(e),r=i.overflow,p=i.overflowX,s=i.overflowY;return /(auto|scroll)/.test(r+s+p)?e:n(o(e))}function r(e){var o=e&&e.offsetParent,i=o&&o.nodeName;return i&&'BODY'!==i&&'HTML'!==i?-1!==['TD','TABLE'].indexOf(o.nodeName)&&'static'===t(o,'position')?r(o):o:e?e.ownerDocument.documentElement:document.documentElement}functio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\585b051251[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	10866
Entropy (8bit):	5.182623714755422
Encrypted:	false
SSDEEP:	192:BgHN42S+9SZRvACpiIthFzoXnemF+shSGnZ+PPxQDqv7jh81Q5l8OcchIlzbCn:WRCfhFzevnEZ/h81Q5l8OsE
MD5:	D8CA71772D1E86D5FB9D5E2F6CC1AE70
SHA1:	9B043E60997FE552D652E4474E16AFF923D7AA76
SHA-256:	7D840153F02AD6D91D652354E35B590721916D16C33956631EEF0E7D3B5613EE
SHA-512:	8E9DA8E9AE10EC0EB854A6E488FB4568A960EE10AF46FE4AA49F22F227CB94997F40E49E10A81E341B99489256163A2C0E065730EEA642777061CDA61B4D56C1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://kit.fontawesome.com/585b051251.js
Preview:	window.FontAwesomeKitConfig = {"asyncLoading":{"enabled":true},"autoA11y":{"enabled":true},"baseUrl":"https://ka-f.fontawesome.com","baseUrlKit":"https://kit.fontawesome.com","detectConflictsUntil":null,"iconUploads":{},"id":132286382,"license":"free","method":"css","minify":{"enabled":true},"token":"585b051251","v4FontFaceShim":{"enabled":false},"v4shim":{"enabled":true},"version":"5.15.3"};.!function(t){"function"==typeof define&&define.amd?define("kit-loader",t):t()}((function(){"use strict";function t(e){return(t="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(t){return typeof t}:function(t){return t&&"function"==typeof Symbol&&t.constructor===Symbol&&t!==Symbol.prototype?"symbol":typeof t})(e)}function e(t,e,n){return e in t?Object.defineProperty(t,e,{value:n,enumerable:!0,configurable:!0,writable:!0}):t[e]=n,t}function n(t,e){var n=Object.keys(t);if(Object.getOwnPropertySymbols){var r=Object.getOwnPropertySymbols(t);e&&(r=r.filter((function(e){return Object.g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\8ZU3LXBE.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	386721
Entropy (8bit):	5.228239281792927
Encrypted:	false
SSDEEP:	6144:ybMbn4RC0EgxnJXiwn5SzdGRCxgVz/KfOYq50SzJzBp+t4a4844484J5t+FQGQMu:1bn4RC0EgxnJXiwn5SzdGRCxgVz/KfOd
MD5:	AD8CF2C821470C331DDD72E7E90B1960
SHA1:	CE270F040EC1A76E302234CF6DBBBC40CC0790C9
SHA-256:	E0B90DEE27CB16ED764DC7B1D8153FDD2B14223EE608FA1727BE24B17843C0A8
SHA-512:	3FE79EE875AD04C7C40DCC2BDFD9551E086B50CE502167FA1E14C7857674BB645ED02800CF60F1FC2E3D47549ABD02DEF4876EF492203BBE253D9B8F76BE2E1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://nicepage.com/
Preview:	<!DOCTYPE html>..<html lang="en">.. <head>.... <title>Free Website Builder Software | 7000+ Free Templates</title>.... <link rel="shortcut icon" href="//csite.nicepage.com/favicon.ico" type="image/x-icon">.. <meta name="Keywords" content="website builder, website designer, html5 templates, joomla templates, wordpress themes, web design">.. <meta name="Description" content="Nicepage is your website builder software breaking limitations common for website builders with revolutionary freehand positioning. 7000+ Free Templates. Easy Drag-n-Drop. No coding. Mobile-friendly. Clean HTML.">.. <meta property="og:type" content="website">.. <meta property="og:url" content="https://nicepage.com/">.. <meta property="og:title" content="Free Website Builder Software | 7000+ Free Templates">.. <meta property="og:image" content="https://static.nicepage.com/images/site/nicepage.jpg">.. <meta property="og:description" content="Nicepage is

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\KFOjCnqEu92Fr1Mu51TLBCc6CsI[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22360, version 1.1
Category:	downloaded
Size (bytes):	22360
Entropy (8bit):	7.975733480737877
Encrypted:	false
SSDEEP:	384:afBIIA0zhsqLW3UAI+x+VH9cxS8XwZtyOOCiKCu5s7YRKWIrfu/oiQfTO4TPg:aG0zhsqLSUAI+xi2s8XwZtuKJzE6/qfg
MD5:	C2E42D1EAC2DE2B58A2358686E6ED73C
SHA1:	24760369053031DF1F2BE831E067E3D9E37F0B3A
SHA-256:	B31B421BAFE532F6B6BDBB6F680FB11BD3968F23C7FE09A29B1A22F4C8DD2A7E
SHA-512:	BFB71B0B6DE51CD1E643733A14B5CD4342F4E93A1732E9AAF6F3A6012DD85EEC5F660F409474C55751B28D122BA202875A325D72F0B7CF327660577C7C1DC9D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\KFOjCnqEu92Fr1Mu51TLBCc6CsI[1].woff	
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOjCnqEu92Fr1Mu51TLBCc6CsI.woff
Preview:	wOFF.....WX.....h.....GDEF.....G...d....GPOS.....oGSUB.....OS/2...p...O...`v...cmap.....#cvt .....Z...Z...=fpgm...4...3.....#.gasp...h..... ...glyf...t..C...t.,..hdmx..O....n....25$8head..Pl...6...6.G.Whhea..P....#...$.H..hmtx..P.....B(Cloca..Sd.....maxp..Ud... ... .4..name..U.....>.post..Vd..... .a.dprep..V |.....8...Cx...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x....%Y....Wm=..mo..k.m....rl...m.g"^..../..[.}.S...\.mD...1..G>..giz...=C..}.y....|o..c.x.R.r"B.....m ...../.&./6..5D.AGX.....)<'.)....?.... .Y4>|1...ES.Gc...FO.>$.../...}RCl..T.zD..uZ4~D.._OK.$.Z.(..JR...\..\..\..\.\.....*'n..6:x...b,..$...?.g:./y.iLg.3..l.0.y.g..X..V...d.#O...0....b7{..> .n.iD.V....." e.\A..OR.kwp.].....6p..."ZE..%...e.u3..L..V...W.7b..L.3.L1K...Ts..$6.-b.....9...b@..!1,...v.C....{...dox.G(...|a%E:.Fn.Nn.^n.....Sf..E)...k....<g..){....|.....DT..N....H y.F.Jez....._?7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\KFOkCnqEu92Fr1MmgVxIIzQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20424, version 1.1
Category:	downloaded
Size (bytes):	20424
Entropy (8bit):	7.973322748597765
Encrypted:	false
SSDEEP:	384:UaoO8n3eceZ+fUC1WCz8P+IgjhYSHA/fFb4+hQC:Bl8nOcBfUqT/jOgAiC
MD5:	04B7FD97F88B82DCCCE5EC446CCC29E6
SHA1:	9A3C1CE2EAB659A91AF7016570287428CC82C458
SHA-256:	A38AD0B609E4D2039D18B0F9DC89E9060F2E2E05F2F42764A6A93354346A6C37
SHA-512:	4B71614F447F4E250AB8060026BA002F3F0DAA9286F207AA4B0652201D9053BD72865C09D1AB90155CF932E17D5897D7A1F659C98F1B1AACFDF6397D6DB47DA8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOkCnqEu92Fr1MmgVxIIzQ.woff
Preview:	wOFF.....O.....GDEF.....G...d....GPOS.....!GSUB.....OS/2...L...P...`t..{cmap.....#cvt .....H...H.2..fpgm.....3...._...gasp...0.....glyf... <..<...q....Lhdmx..H....q...."&.(head..l@...6...6.G..hhea..Ix... ...$...whmtx..I....y.....lCloca..L.....X.;.maxp..N.... ... .4..name..N4.....x..9.post..O..... .m.dprep..O..... +6.x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x...l\..F..3...N..q)..a\|....^..33..c.....p"y.iT....<Gg...!.3...T1...{.g0.u.y.....m.\|.k..NF.....mox.;...7&.Y.. C.R_[.T.c..-.=...9:...a*j.G.....O.Q".6...>...(?...~...._.2:..K4....S%...jbr).....*....e.U..-..X.3.ILQ....z..!.f:...<.W.#...e.c=...&6...lc;;..3<.s<....H.i2..N..t..)Ns...#`..".).[...._.T..T... ..+l..=..O.....Z..F...r..eM.f.Y.....-...r.\.s6.r..,...:.<$..#.l..F.$.2#.e..].[.....yR...e.\{..O..`)..U.0.e.50.Z.b../cM..i.&O._..+.Y.W...;z....j.p._.o..[CL.)n'.UGx..>).X..MJ..Fr..v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\KFOlCnqEu92Fr1MmSU5fBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20404, version 1.1
Category:	downloaded
Size (bytes):	20404
Entropy (8bit):	7.970248785137973
Encrypted:	false
SSDEEP:	384:8uFoOxqigBacqKz8RGLv6K5a+jZ/rFSyeM5B8r/WjRy0BsM16t/PJ:PFlIvUKz8R+t5N53eGar/gY0Bv6tp
MD5:	BF0F407102FAF3A0B521D3B545F547A5
SHA1:	CA357CD0DE5DD0242E8EFACFB8D24AB60FDC86AB
SHA-256:	855A06974032BB69157D469ABA6F63440E8BE47C421F45C3F396F4E0B87B6DE8
SHA-512:	85359028F7FE49B1DF90B72E48DC7DE4B21F1B65E8BF109595705A3F4EAF9FA79854B5AEF060FE266291C5ECE9D04FCEAD1DE09BAA2C5E20601E1579212520C 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmSU5fBBc-.woff
Preview:	wOFF.....O.....x.....GDEF.....G...d....GPOS.....!GSUB.....OS/2...L...P...`t6..cmap.....#cvt .....X...X/...fpgm.....4.....".gasp...@.....glyf.. .L..<'..m..]5Yhdmx..Ht...m....),..head..H....6...6.Y.ihhea..I.... ...$....hmtx..I<.....Dd.loca..K.....maxp..M.... ... .4.\name..M.....\|..9.post..N..... .m.dprep..N.....:z /.Wx...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x...l\..F..3...N..q)..a\|....^..33..c.....p"y.iT....<Gg...!.3...T1...{.g0.u.y.....m.\|.k..NF.....mox.;...7&.Y.. C.R_[.T.c..-.=...9:...a*j.G.....O.Q".6...>...(?...~...._.2:..K4....S%...jbr).....*....e.U..-..X.3.ILQ....z..!.f:...<.W.#...e.c=...&6...lc;;..3<.s<....H.i2..N..t..)Ns...#`..".).[...._.T..T... ..+l..=..O.....Z..F...r..eM.f.Y.....-...r.\.s6.r..,...:.<$..#.l..F.$.2#.e..].[.....yR...e.\{..O..`)..U.0.e.50.Z.b../cM..i.&O._..+.Y.W...;z....j.p._.o..[CL.)n'.UGx..>).X..MJ..Fr..v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\KFOmCnqEu92Fr1Mu4mxM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20332, version 1.1
Category:	downloaded
Size (bytes):	20332
Entropy (8bit):	7.970235088150752
Encrypted:	false
SSDEEP:	384:U0iwaxoOUPVkOJJSu6SsCKTIRDqG9oHKwZh98OSv+MsgkAOY:75mlUmOSu1guh+fZhLSxkAr
MD5:	DC3E086FC0C5ADDC09702E111D2ADB42
SHA1:	B1138B84FF19EAC5F43C4202297529D389BD09B7
SHA-256:	EA50AC7FDDB61A5CE248A7F8B3A31A98FE16285E076B16E6DA6B4E10910724BB
SHA-512:	10123C785C396CF0844751A014413ECF4D058AD0C00CAAEF5F8FFEF504C370F03EACD0B3C2A49211EEE0877B7AE7D0EF6E01264F04FC910C2660584B5E943BE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOmCnqEu92Fr1Mu4mxM.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\KFOmCnqEu92Fr1Mu4mxM[1].woff	
Preview:	wOFF.....Ol.....x.....GDEF.....G...d....GPOS.....!GSUB.....OS/2...L...P...`t...cmap.....#cvt .....T...T+...fpgm.....5....w.`.gasp...@.....glyf.. .L..;...m.&.x.hdmx..H....m..../.head..H....6...6.j.zhhea..H.... ...$....hmtx..H.....]uloca..Kp.....m,maxp..Mp... ... .4..name..M.....t.U9.post..N`..... .m.dprep..Nt.....I .f..x...1..P.....PB..U.=I.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x...l\..F..3...N..q)..a\|.....^..33..c.....p"y.iT....<Gg...!.3...T1...{.g0.u.y.....m.\|.k..NF.....mox.;...7&.Y. .C.R_[.T.c..-.=...9:...a*j.G.....O.Q".6...>...(?...~...._.2:..K4....S%...jbr).....*....e.U..-..X.3.ILQ....z..!.f:...<.W.#...e.c=...&6...lc;;..3<.s<....H.i2..N..t..)Ns...#`..").[...._.T..T.. ...+I..=..O.....Z..F...r..eM.f.Y.....-...r.\.s6.r..,...:.<$..#.I..F.$.2#.e..].[.....yR...e.\{..O..`)..U.0.e.50.Z.b../cM..i.&O._..+.Y.W...;z....j.p._.o..[CL.)n'.UGx..>).X..MJ..Fr..v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\amplitude-5.2.2-min.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	55079
Entropy (8bit):	5.461377460868851
Encrypted:	false
SSDEEP:	1536:oN41FHEay+rP6bX88uFrVjnDcz8q8zQVpSRcfRx:M4Pw+rPYuFhg7
MD5:	6BF28BD8C301A00C18C5F2CC7C895A3B
SHA1:	BCF9BD3D2F8606F398E0594C1FB672FB2AB33729
SHA-256:	2173F130CA59DC5554498343432F02F92ECCE45C4F9381EA12B203A2978F33D4
SHA-512:	0A7EEF8A7A9AAB8C50BA600BAC724402C0DA8E6DFC757FDC9B9D36D895044E94FA46A02B3965823C0DE57F72CCB2B04955A1E6D5C0FD95F0A9BBC0A06B884C7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.amplitude.com/libs/amplitude-5.2.2-min.gz.js
Preview:	!function(e,t){"object"==typeof exports&&"undefined"!=typeof module?module.exports=t():"function"==typeof define&&define.amd?define(t):(e=e||self).amplitude=t()}(this,function(){"use strict";function t(e){return(t="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(e){return typeof e}:function(e){return e&&"function"==typeof Symbol&&e.constructor===Symbol&&e!==Symbol.prototype?"symbol":typeof e})(e)}function r(e,t,n){return t in e?Object.defineProperty(e,t,{value:n,enumerable:!0,configurable:!0,writable:!0}):e[t]=n,e}function l(t){for(var e=1;e<arguments.length;e++){var n=null!=arguments[e]?arguments[e]:{},i=Object.keys(n);"function"==typeof Object.getOwnPropertySymbols&&(i=i.concat(Object.getOwnPropertySymbols(n).filter(function(e){return Object.getOwnPropertyDescriptor(n,e).enumerable}))),i.forEach(function(e){r(t,e,n[e])})}return t}var f="$default_instance",c=2,n=4096,a=1e3,h="$identify",g="$groupidentify",v="amplitude_lastEventId",m="amplitude_lastEventTime",y="amp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\bootstrap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	48944
Entropy (8bit):	5.272507874206726
Encrypted:	false
SSDEEP:	768:9VG5R15WbHVKZrycEHSYro34CrSLB6WU/6DqBf4l1B:9VIRuo53XiwWTvl1B
MD5:	14D449EB8876FA55E1EF3C2CC52B0C17
SHA1:	A9545831803B1359CFEED47E3B4D6BAE68E40E99
SHA-256:	E7ED36CEEE5450B4243BBC35188AFABDFB4280C7C57597001DE0ED167299B01B
SHA-512:	00D9069B9BD29AD0DAA0503F341D67549CCE28E888E1AFFD1A2A45B64A4C1BC460D81CFC4751857F991F2F4FB3D2572FD97FCA651BA0C2B0255530209B182F2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery"),require("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,n){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function s(t,e,n){return e&&i(t.prototype,e),n&&i(t,n),t}function r(){return(r=Object.assign||function(t){for(var e=1;e<arguments.length;e++){var n=arguments[e];for(var i in n)Object.prototype.hasOwnProperty.call(n,i)&&(t[i]=n[i])}return t}).apply(this,arguments)}e=e&&e.hasOwnProperty("default")?e.default:e,n=n&&n.hasOwnProp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	2156
Entropy (8bit):	5.19080971935771
Encrypted:	false
SSDEEP:	48:UY3QS7NAY3QWNkY3QLN0BY3QgNwY3QCNpY3QMNlOS7NhOWNROLNKCOgNbOCNGOMB:UYgS7NAYgWNkYgLNuYggNwYgCNpYgMNv
MD5:	BA388635492879BEED5961CDC10169DF
SHA1:	C18E6C4F02E3067CDD3A59938634B557D4676A47
SHA-256:	EC2841D6A61E2F5EC5741534296EAECBF8673442ED960D1FB1CB6918E7B5FDBD
SHA-512:	AD4F24D722083B733E1064ED3FC0848649299427774765 4F5E7E3EAB7A2849BD5D705FDB2C9665BA40786E90FD88D665CFE1268ECD529A5B36D2BA90EAD8432
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\css[1].css	
Preview:	@font-face {. font-family: 'Roboto';. font-style: italic;. font-weight: 100;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOiCnqEu92Fr1Mu51QrEzAdKQ.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: italic;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOjCnqEu92Fr1Mu51TjASc6CsI.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: italic;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOkCnqEu92Fr1Mu51xIIzQ.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: italic;. font-weight: 500;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOjCnqEu92Fr1Mu51S 7ACc6CsI.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: italic;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOjCnq Eu92Fr1Mu51TzBic6CsI.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: italic;. font-weight: 900;. src: url(http

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\css[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	5368
Entropy (8bit):	5.293785521126314
Encrypted:	false
SSDEEP:	96:nOYgS75OYgJqOYgWUOYgLmOYggLOYgxTwXEOYgCqOYgw6nOYgMiOOS7iOOJEOOWS:b37NiKl0kGPv2wXkpKIbTj7WzhSHXjvX
MD5:	6B5A429F165B4B47CEF7EA6E788358DA
SHA1:	0FCEB05C42BC345D9755D336F2ADFFE57CAA172B
SHA-256:	066CE428BCCFD823847EA75D3C68C0EE5A082D015CFA50CF4BD9050331DE6E30
SHA-512:	2AA15EC6DF91DA3C3984D62EC21381AC7569E1B37783620DC8C443664C6CA2C5528BB106A1D2800D5943DEA5AB87426ED49101F74617CAA54FD10290948AC47
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Montserrat';. font-style: italic;. font-weight: 100;. src: url(https://fonts.gstatic.com/s/montserrat/v15/JTUOjIg1_i6t8kCHKm459WxZqh7k29U. woff) format('woff');.}.@font-face {. font-family: 'Montserrat';. font-style: italic;. font-weight: 200;. src: url(https://fonts.gstatic.com/s/montserrat/v15/JTUPjIg1_i6t8kCHKm 459WxZBg_z_PZ2.woff) format('woff');.}.@font-face {. font-family: 'Montserrat';. font-style: italic;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/montserr at/v15/JTUPjIg1_i6t8kCHKm459WxZYgzz_PZ2.woff) format('woff');.}.@font-face {. font-family: 'Montserrat';. font-style: italic;. font-weight: 400;. src: url(https://fon ts.gstatic.com/s/montserrat/v15/JTUQjIg1_i6t8kCHKm459WxRyS7g.woff) format('woff');.}.@font-face {. font-family: 'Montserrat';. font-style: italic;. font-weight: 500;. src: url(https://fonts.gstatic.com/s/montserrat/v15/JTUPjIg1_i6t8kCHKm459WxZOg3z_PZ2.woff) format('woff');.}.@font-face {. font-family: 'M

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\free-v4-shims.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	26701
Entropy (8bit):	4.829823522211244
Encrypted:	false
SSDEEP:	192:dP6hT1bIl4w0QUmQ10PwKLaAu5CwWavpHo4O6wgLPbJVR8XD7mycP:0hal4w0QK+PwK05eavpmgPPeXD7mycP
MD5:	8A99CE81EC2F89FBCA03F2C8CF1A3679
SHA1:	58F9EF32D12A5DA52CBAB7BD518BCC998FC59EF9
SHA-256:	362DAEAF1F7E05FEE9A609E549F148AACBE518C166FBD96EAD69057E295742AF
SHA-512:	930F28449365FAED13718BB8F332625DB110ABB08C3778DC632FDF00A0187A61A086B5EB4765FFC1923B64E2584C02592A213914B024DE6890FF3DBFC3A12FE5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.3/css/free-v4-shims.min.css?token=585b051251
Preview:	/*!. * Font Awesome Free 5.15.3 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.fa.fa-glass:before{content:"\f000"}.fa.fa-meetup{font-family:"Font Awesome 5 Brands";font-weight:400}.fa.fa-star-o{font-family:"Font Awesome 5 F ree";font-weight:400}.fa.fa-star-o:before{content:"\f005"}.fa.fa-close:before,.fa.fa-remove:before{content:"\f00d"}.fa.fa-gear:before{content:"\f013"}.fa.fa-trash-o{font- family:"Font Awesome 5 Free";font-weight:400}.fa.fa-trash-o:before{content:"\f2ed"}.fa.fa-file-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-file-o:before{co ntent:"\f15b"}.fa.fa-clock-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-clock-o:before{content:"\f017"}.fa.fa-arrow-circle-o-down{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-arrow-circle-o-down:before{content:"\f358"}.fa.fa-arrow-circle-o-up{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-arro

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\free.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	60351
Entropy (8bit):	4.728641238865369
Encrypted:	false
SSDEEP:	768:0Uh31IPiyXNq4YxBowbgJlkwF//zMQyYJYX9Bft6VSz8:0U0PxXE4YXJgndFTfy9lt5Q
MD5:	390B4210E10C744C3C597500BCF0B31A
SHA1:	2600C7C2F25D7DBCBC668231601E426010DC6489
SHA-256:	C2819CA1F7AD1AF7BA53C4EDFDFD395C547BCB16D29892A234D7860C689ED929
SHA-512:	E8A7E466BE8CC092E12994B51A6A8A39E2FBB66DD48221BCF499BB89365B4004D73C1909F8FE0BBBBF13907D5901D76FFE127D92FDD7493853646F83F5985CB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.3/css/free.min.css?token=585b051251

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\free.min[1].css	
Preview:	/*!. * Font Awesome Free 5.15.3 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.fa,.fab,.fad,.fal,.far,.fas{-moz-osx-font-smoothing:grayscale;-webkit-font-smoothing:antialiased;display:inline-block;font-style:normal;font-variant:normal;text-rendering:auto;line-height:1}.fa-lg{font-size:1.33333em;line-height:.75em;vertical-align:-.0667em}.fa-xs{font-size:.75em}.fa-sm{font-size:.875em}.fa-1x{font-size:1em}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-6x{font-size:6em}.fa-7x{font-size:7em}.fa-8x{font-size:8em}.fa-9x{font-size:9em}.fa-10x{font-size:10em}.fa-fw{text-align:center;width:1.25em}.fa-ul{list-style-type:none;margin-left:2.5em;padding-left:0}.fa-ul>li{position:relative}.fa-li{left:-2em;position:absolute;text-align:center;width:2em;line-height:inherit}.fa-border{border:.08em solid #eee;border-radius:.1em;padding:.2em .25em .15em}.fa-pul

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\jquery-1.9.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	92629
Entropy (8bit):	5.303443527492463
Encrypted:	false
SSDEEP:	1536:dnu00HWWaRxkqJg09pYxoxDKMXJrg8hXXO4dK3kyfiLJBhdSZE+I+Qg7rbaN1RUx:ddkWgoBhcZRQgmW42qe
MD5:	397754BA49E9E0CF4E7C190DA78DDA05
SHA1:	AE49E56999D82802727455F0BA83B63ACD90A22B
SHA-256:	C12F6098E641AACA96C60215800F18F5671039AECF812217FAB3C0D152F6ADB4
SHA-512:	8C64754F77507AB2C24A6FC818419B9DD3F0CECCC9065290E41AFDBEE0743F0DA2CB13B2FBB00AFA525C082F1E697CB3FFD76EF9B902CB81D7C41CA1C641DFB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.nicepage.com/shared/assets/jquery-1.9.1.min.js
Preview:	/*! jQuery v1.9.1 | (c) 2005, 2012 jQuery Foundation, Inc. | jquery.org/license.//@ sourceMappingURL=jquery.min.map.*/(function(e,t){var n,r,i=typeof t,o=e.document,a=e.location,s=e.jQuery,u=e.$,l={},c=[],p="1.9.1",f=c.concat,d=c.push,h=c.slice,g=c.indexOf,m=l.toString,y=l.hasOwnProperty,v=p.trim,b=function(e,t){return new b.fn.init(e,t,r)},x=/[+-]?(?:\d*\.\|)\d+(?:[eE][+-]?\d+\|)/.source,w=/\S+/g,T=/^[\s\uFEFF\xA0]+\|[\s\uFEFF\xA0]+$/g,N=/^(?:(<[\w\W]+>)[^>]*|#([\w-]*))$/,C=/^<(\w+)\s*\/?>(?:<\/\1>\|)$/,k=/^[\],:{}\s]*$/,E=/(?:^|:|,)(?:\s*\[)+/g,S=/\\(?:["\\\/bfnrt]|u[\da-fA-F]{4})/g,A=/"[^"\\\r\n]*"|true|false|null|-?(?:\d+\.|)\d+(?:[eE][+-]?\d+|)/g,j=/^-ms-/,D=/-([\da-z])/gi,L=function(e,t){return t.toUpperCase()},H=function(e){(e.addEventListener||"load"===e.type||"complete"===o.readyState)&&(q(),b.ready())},q=function(){o.addEventListener?(o.removeEventListener("DOMContentLoaded",H,!1),e.removeEventListener("load",H,!1)):(o.detachEvent("onreadystatechange",H),e.detachEvent("onload",H)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\masonry.pkgd.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	28953
Entropy (8bit):	5.180056571790237
Encrypted:	false
SSDEEP:	768:S9+z0BFXYKby+HvOqvevgOkYtkdEvWBzigMPI0:SgKbbO0IkdEvPgI
MD5:	C54E75EDF5CBAF412BC16BA4145F6032
SHA1:	67638430C92C23CEDB89DB038627876D361135C0
SHA-256:	733D7C26A5FB7240E83E8AF2C822218B321B5143E28C2DD65AB2492297AC6BD7
SHA-512:	DCFA0ADEFBB8BF4B9CB2082D98B452DAEFAE51137315003AABD021805F8575FCCE8CCF0DB78A7AA0A35C6C485D529C37B9DE803BBC5A151A677A0E7E4012C55D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://csite.nicepage.com/Scripts/Site/Libs/masonry.pkgd.min.js?version=6ba8f9621eefd8f9e7050129b53e111985c3f5cb
Preview:	/*!. * Masonry PACKAGED v3.3.2. * Cascading grid layout library. * http://masonry.desandro.com. * MIT License. * by David DeSandro. */..!function(a){function b(){}function c(a){function c(b){b.prototype.option||(b.prototype.option=function(b){a.isPlainObject(b)&&(this.options=a.extend(!0,this.options,b))})}function e(b,c){a.fn[b]=function(e){if("string"==typeof e){for(var g=d.call(arguments,1),h=0,i=this.length;i>h;h++){var j=this[h],k=a.data(j,b);if(k)if(a.isFunction(k[e])&&"_"!==e.charAt(0)){var l=k[e].apply(k,g);if(void 0!==l)return l}else f("no such method '"+e+"' for "+b+" instance");else f("cannot call methods on "+b+" prior to initialization; attempted to call '"+e+"'")}return this}return this.each(function(){var d=a.data(this,b);d?(d.option(e),d._init()):(d=new c(this,e),a.data(this,b,d))})}}if(a){var f="undefined"==typeof console?b:function(a){console.error(a)};return a.bridget=function(a,b){c(b),e(a,b)},a.bridget}}var d=Array.prototype.slice;"function"==typeof define&&define.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\mem5YaGs126MiZpBA-UN7rgOUuhv[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18900, version 1.1
Category:	downloaded
Size (bytes):	18900
Entropy (8bit):	7.96514104643824
Encrypted:	false
SSDEEP:	384:nejx4dDcsFhu/3v79dEAUdH6XSw1fz9fKQm9LQNG/X1epB:ejadDrhYTf3Udaieza98Nbz
MD5:	1F85E92D8FF443980BC0F83AD7B23B60
SHA1:	EE8642C4FAE325BB460EC29C0C2C9AD8A4C7817D
SHA-256:	EA20E5DB3BA915C503173FAE268445FC2745FC9A5DCE2F58D47F5A355E1CDB18
SHA-512:	F34099C30F35F782C8BB2B92D7F44549013D90E9EEDE13816D4C7380147D5B2C8373CC4D858CDF3248AAA8A73948350340EE57DAE9734038FC80615848C7133E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\mem5YaGs126MiZpBA-UN7rgOUuhv[1].woff	
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UN7rgOUuhv.woff
Preview:	wOFF.....l.....p.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....^...`....cmap...`.....X..cvt .....]....-..fpgm...t.....s.ugasp.....glyf...$ ..9...Y..(.head..A....6...6.%l.hhea..B,.....$.)..hmtx..BL.....O,loca..D`.....9yfmaxp..F$... ... .q..name..FD.....#.>.post..G4.....x.U..prep..H.....k..... .....x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`f.g.....:....Q.B3_dHc.....@`...../..?....^..... 9.8.m@J....w..!..x.\.!..q.....#aff...#1Q@ .'U..@5.".llt.Aa#.f|c.W....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:....F....GG.g.s,x.>0....v..l;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g``..$KY...e@.,q@.j...o@<..O.H.t..... .....c .p@.....3lbd.....-.}.M...!...!....x.TGw.F.....)..)7.W..`*.j.-...=*'_..sI...2...O>....[tt....TK]..|...G.....^.m..=..x.q...+./].p...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\mem5YaGs126MiZpBA-UN8rsOUuhv[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19072, version 1.1
Category:	downloaded
Size (bytes):	19072
Entropy (8bit):	7.966673384993769
Encrypted:	false
SSDEEP:	384:UCwUC2nJxPRk+P/Qvm6DBM1W71wcdDmyBE+2fweE9m0aGuTeopiH:PJC2nJxP++P/36QWpwNyb2tqgk
MD5:	05EBDBE10796850F045FCD484F35788D
SHA1:	07744CFE76B8C37096443A6BCC3FBD04F93AD05B
SHA-256:	35EB714D45479FE35586513C7D372CED0AE3E26EB05883950BEA2669C6E802AA
SHA-512:	D4F293115640C05E3134D635AA077BC91BF35E80463C93C14646D97784CD9FC8D4CD4E10EEAA7BE621DBD9FA0DE5BE943328014ED505C217E61769F76BFA7F4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UN8rsOUuhv.woff
Preview:	wOFF.....J.....p.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....^...`...vcmap...`.....X..cvt .....g.....o.[fpgm...|.....s.ugasp... .....#glyf...0 ...".."..Yr....head..BT...6...6....hhea..B.....$....hmtx..B....*....#.C.loca..D.....n..maxp..F.... ... .name..F.....%.@cpost..G.....x.U..prep..lp.....1..S..... x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`f.cV``e``..j...(.../2.11s01qs.1s.01.400.300x.....:.;380(...&.O.....)B..q>H.%.u..R``.....x.\.!..q..... .#aff...#1Q@.'U..@5.".llt.Aa#.f\|c.W....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..l;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g``..$K..(..`.e.a.a`....C ..L..@t.....A..L..&.....1\gta.e....320.0...2.g.j...=...x.TGw.F.....)..)7.W..`*.j.-...=*'_..sI...2...O>....[tt....TK]..|...G.....^.m..=..x.q...+.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\nicepage[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):	159812
Entropy (8bit):	5.250908894425148
Encrypted:	false
SSDEEP:	3072:sTkENkhyzE/v5MM4WafSmSNc3eghXAySiQxG:sTEV/iM4LSoJAyh
MD5:	C11606198D6E63A6A54D8978A5885033
SHA1:	A3BEAAA1050D20D489BD7D74C75850573C787A67
SHA-256:	2051A823FB0E84FC333380A350F52E9F5817F68F01486CF01B69C597AF56C337
SHA-512:	D229700D36F2979AF468CD01987468DB285B50FD794D44E4E7A5BCB0649D324884881188F5B12AE534AA2BE06E92454E0F47BEF680C6EF74BBEBACF587322A2(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://capp.nicepage.com/1fd39372a624e5db9973af25d76427670e3deec8/nicepage.js
Preview:	!function(t){function e(n){if(i[n])return i[n].exports;var o=i[n]={i:n,l:false,exports:{}};return t[n].call(o.exports,o,o.exports,e),o.l=true,o.exports}var i={};return e.m=t,e.c=i, e.d=function(t,i,n){if(!e.o(t,i))Object.defineProperty(t,i,{configurable:false,enumerable:true,get:n})},e.n=function(t){var i=t&&t.__esModule?function e(){return t.default}:functio n e(){return t};return e.d(i,"a",i),i},e.o=function(t,e){return Object.prototype.hasOwnProperty.call(t,e)},e.p="/Content/BundledScripts/",e(e.s=5024)}({114:function(t,e){var e=void 0,t=void 0;(function(){/*!. * https://github.com/gilmoreorless/css-background-parser. * Copyright . 2015 Gilmore Davidson under the MIT license: http://gilmore orless.mit-license.org/. */.!function(t){function e(t){if(!(this instanceof e))return new e;this.backgrounds=t||[]}function Background(t){function e(e,n){i[e]=e in t?t[e]:n}if(!(this instanceof Background))return new Background(t);t=t||{};var i=this;e("color",""),e("image",""),e("attachment",""),e(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\site-common-libs[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	assembler source, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	100946
Entropy (8bit):	4.988897703730311
Encrypted:	false
SSDEEP:	768:mYqFD75Zfdel5faHT3QPv1E64YAG4iGGKgyYqwk7Ed1nAB7FU/JVuvl/SE1Jj8RA:mYq57k2EGlbf4nFdJt36UjXpBfaiwD
MD5:	B769F234EF123D126B48E9E10DC9F2D8
SHA1:	01A12DDAE7CBAEC8C7C98F9C282C3AD9503303BA
SHA-256:	7C5FFB9FD83844D9BDC3925A7CCBE1957AF18897F76BF2DA9BADA1A9EC990758
SHA-512:	B5FE3ABC524450138985F3DB5313A5484B78BCE4BF053BD9AF5E1532553619FD27FB792BBDDBD7AF96D793C2DCFC8F1DE86A179F489C1A6461862FF855F00EC 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://csite.nicepage.com/BundledScripts/site-common-libs.css?version=6ba8f9621eefd8f9e7050129b53e111985c3f5cb

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\site-common-libs[1].css	
Preview:	@charset "UTF-8";./*!. * 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;. -ms-text-size-adjust: 100%;. -webkit-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: bold;.}..dfn {. font-style: italic;.}..h1 {. font-size: 2em;. margin: 0.67em 0;.}..mark {. background: #ff0;. color: #000;.}..small {. font-siz

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\site-common-libs[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	144864
Entropy (8bit):	5.21739100600007
Encrypted:	false
SSDEEP:	1536:qCIRHCU3Y2FO8nIjIXwz6OvL8hJuJGmHdUhtGhoP1p1vEs+xaBYHRW8IeaxyWb1u:kCU3fgY6oR4clhesHQtDFJ
MD5:	F1103827F91AFA2536840FECFB2F083D
SHA1:	77171D484F17C99383CF40726626799E2BD5F340
SHA-256:	00AEF00EF7F80EFFEDFE97B176924E3E31B2B7C11AE0DBCE2586DAF0794E4CFD
SHA-512:	4AE722C8D5AA405F49312A0979607B96E6F77EE56ECF0455ED26975B65B2B44275486DC11B198B5DFEAC1A816ACC7EF5D8C2FEE92C049A06177527D18BEA478 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://csite.nicepage.com/BundledScripts/site-common-libs.js?version=6ba8f9621eefd8f9e7050129b53e111985c3f5cb
Preview:	!function(e){function t(i){if(n[i])return n[i].exports;var o=n[i]={i:i,l:false,exports:{}};return e[i].call(o.exports,o,o.exports,t),o.l=true,o.exports}var n={};return t.m=e,t.c=n, t.d=function(e,n,i){if(!t.o(e,n))Object.defineProperty(e,n,{configurable:false,enumerable:true,get:i})},t.n=function(e){var n=e&&e.__esModule?function t(){return e.defaul t}:function t(){return e};return t.d(n,"a",n),n},t.o=function(e,t){return Object.prototype.hasOwnProperty.call(e,t)},t.p="/Content/BundledScripts/",t(t.s=5173)}({12:function(e,t){v ar e=void 0;(function(){/*!. * jQuery Cookie Plugin v1.4.1. * https://github.com/carhartl/jquery-cookie. *. * Copyright 2013 Klaus Hartl. * Released under the MIT license. */.!function(factory){if("function"==typeof define&&define.amd)define(["jquery"],factory);else if("object"==typeof void 0)factory(require("jquery"));else factory(jQuery)}(functio n(e){function t(e){return l.raw?e:encodeURIComponent(e)}function n(e){return l.raw?e:decodeURIComponent(e)}function i(e)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\templates-page-libs[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	assembler source, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	135379
Entropy (8bit):	5.178274760565854
Encrypted:	false
SSDEEP:	1536:mYq57k2EGlbf4nFdJt36UjXpBfaiwvAjAOfrSDQaS2hd0vtl0vxuD:mB57k3qSLj1jnz5cO8Q
MD5:	3CF11616804E3965E6725EAB812BC50B
SHA1:	65A885281538079851F1CBE57C90F04B14C10606
SHA-256:	A39EB61DA4BE192504D41C3285C76DA59D7C597418EFF87984FE5CE798658FFF
SHA-512:	B4747D5BC36473977B88358695D2D54EB60692E2EC5E83C3C7C064DA7F6AAA3E2C2DA21E5ECD560C031766D19283FDE171C6F834D1356F6F9BFE0E77B3A7A1 5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://csite.nicepage.com/BundledScripts/templates-page-libs.css?version=6ba8f9621eefd8f9e7050129b53e111985c3f5cb
Preview:	@charset "UTF-8";./*!. * 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;. -ms-text-size-adjust: 100%;. -webkit-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: bold;.}..dfn {. font-style: italic;.}..h1 {. font-size: 2em;. margin: 0.67em 0;.}..mark {. background: #ff0;. color: #000;.}..small {. font-siz

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\Addd[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 227 x 222, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	2172
Entropy (8bit):	7.863141802289699
Encrypted:	false
SSDEEP:	48:JMaNj5WCun23d3qKhcMo0UKdSiKwmodowTErmkq9:Satz/3d3qU9FUKbKQdo3ix
MD5:	E95CB3DA20F97D8CBE507AFD010DD534
SHA1:	7E6FF45CC1B7D41C697AC1F1E82A674ADC22E0FD
SHA-256:	F5C2D070A6E782D9F597EFBAFF95D385E0F798D874E167C1477F34050A4BD822
SHA-512:	735F1D635EAB0634ACAE77FED7A3DF1069F06893777F5E181E014769894F42D5058E3D417B2089646467495020D1E8CBC6DA96D74E758C72DE3AB99044BCC3A9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\Addd[1].png	
IE Cache URL:	http://https://images02.nicepage.com/4a6432a7cb0551e103110d03/1f1493ca1973564fa5ccaabe/Addd.png
Preview:	.PNG.....IHDR.....G.....PLTE.....LG.....'....ID.....{x.SN.>8....}z.-&.E@....!.....hd.ok....70....VQ.....`\....[W.kg.$..uq....93..,%.....].....IDATx..i[.0...$..p$P..4@.R.....F...iW..k...h5..UT...f.Xn.+.O..v...G.....f..o.B.7{x..8.cM.U2..5..R..QD.K+..D.a"...f...$LDt?....&...j..Z.a".....7./.^D.r./....2.Y..1..qt..b.y?*`..1..22..A.!.&...c.<.yX.1..8..1..j....'..._.C.!_.....w.."P...2L.....q{d..2.....iL.+.b.q..1.x...4....0:V.8..2..r.3N.g...x8E.k.5..1.....T....*..1.=.E.....h.....1t..Z..B.Z+...v.>a.^.z.'*... ...y.6O.).*]:..gF_+..oa...1.~I..[..V0#.....\H*J...&..~...#...e.6b..a.k.....P{..O\.%s..>[..'.a.".d.B....l.[.....1.wKD.Ah.f.,.....,.4.m.....R5.(F.T.QX.;I..$..TM%.....<.UM.('.....tV.QJzO?*k.O2 ..yF.dx....Q.ISh..X"<..7Z...F.k.(!.^.TM.....).....W,.....=....#s.A...k.Ls.&b}V.L.....hX.....~.....+.#W.c.rA..[...{..v.....&l.....j!.....KBc.....c.I...Yz..v.nC...B..IA.C..%...<.R.Pl.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\JTUPjIg1_i6t8kCHKm459WxZFgrz_PZ2[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 24148, version 1.1
Category:	downloaded
Size (bytes):	24148
Entropy (8bit):	7.979296793493818
Encrypted:	false
SSDEEP:	384:xhcTbotJFmcbpWQoeNGTJO8X5Qj2dZaUsxIc4wexSiGepv4S1e2BVr9aqKbR9NPN:vcPo/50FeNF8JQidZaU64we3TQYdBVgd
MD5:	F3D4DE8D0AFB19E777C79032CE828E3D
SHA1:	45C3C0083806C9C6750E5B2EF77BAD73393E87B5
SHA-256:	681A53B9F5778E3F113955B991209A56F2B6C4951829A3683F71B77B5BE39BBB
SHA-512:	EB231920798F982554B4377D9F985938C3139B2C91C2F41AAC6B7DF85C7FC66C402EB2F94B76F9AC4BF660CE10A41E42B408178D63484F574971B0EC4F7F5465
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTUPjIg1_i6t8kCHKm459WxZFgrz_PZ2.woff
Preview:	wOFF.....^T.....GDEF.....G...X.f.^GPOS.....2..C..GSUB.....,.OS/2...L...P...`Tj.hcmap.....h.cvt ...`...d....2...fpgm.....F...mM$.\|gasp.....glyf.....6...b....Ihead..T....6...6..].hhea..U....#...$...chmtx..U0...S...>-O..loca..W.....(....maxp..Y.... ... .j.bname..Y.....D3.N.post..Z.....D.-.prep..]..... K..x.%....P.....@:D...$..]!....h.....2/.$.....D.^.F..ua.].N....%>.....x...p....".g....-x/.....3..(..1.n..t..K.[*;....MM".q8....O.LOO.3...3.Vj..._.....?.....Z.....B.S..C..?J..)...N4.t....=..Zy>u5....$m.g.6.....b1n.atU.gA...(]..(.N.....Tn.t..L..i.E...J:.zv.i.x).@.Z*/9.pB.....J.$s...*{...*)..&.<.AI...H.:..u.6..(.#;v..{4%...Vt)H...].F\.T...<."Op..Ye..+.....j<-.Y....W....8..{..$..or...<U8(.8 4....0.Pc.....#.I`>.....x_.{&J...%..C....9.Q..9u....kvq.r+...W)m..c.....R....>dR..)YO#...j...!..V..w2B..6...k.y.u0n.c.Z..4...en.)^Oc\6.1L.$r9...z....h.....#..}.dy.?

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\JTUPjIg1_i6t8kCHKm459WxZbgjz_PZ2[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 24404, version 1.1
Category:	downloaded
Size (bytes):	24404
Entropy (8bit):	7.978820197505777
Encrypted:	false
SSDEEP:	384:ALk/voi37GMyWTBYoWHGTJO8BFvW8Y+zcKpaLI+pVfCYGafTZqULGTNJk6K81EsW:ykXoiLGbWaoWHF8BYT+dpaLI+CYFqUqG
MD5:	897086F99F4E1F45E6B1E9368527D0BC
SHA1:	B397AD275B1C4CED4128813ECE16228053387911
SHA-256:	A6F84021BA6E28B3F691B98CD002F9243447CB542E00065AB46744BE67541AD6
SHA-512:	E07541367BB51F779410A46D0917DCDF978EDC0BC9170577EF2FB25AAD27CE9F318B966140A1E2E4E67D2E3FCB52AB0628CA303F3DD65D30CBB52E41D1D0AA5F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTUPjIg1_i6t8kCHKm459WxZbgjz_PZ2.woff
Preview:	wOFF......_T.....GDEF.....G...X.f.^GPOS.....2.....GSUB...t.....,.OS/2...8...Q...`U7..cmap.....h.cvt ...P...e....5=..fpgm.....F...mM$.\|gasp.....glyf.....6...c...B.head..U....6...6..].hhea..V....#...$....hmtx..V(...X...>?...loca..X....!...(.V.Amaxp..Z.... ... .[.Pname..Z.....L3.O.post..[.....D.-.prep..^.....K..x.%....P.....@:D...$..]!....h.....2/.$.....D.^.F..ua.].N....%>.....x...p.I...!i...H..A.IF-..[<ffffff.....L>...iY...eY.mY.....}..:..?.....3+.....=..s....1.g...\J. ..q..'O....+.eC ....s..2.*...o..}."......L....8F9..+N.8...8.b....\....H...wl.S.....gv.....P...5F.....Hi.<9Lq..I..c..]4..1...3$f...Yq.T!K...+..S#{w.R*.Rf.}qKK}.Lj...',V...;1..QW<.S5....bTes...vq....43H..B.Kh....~..Pb.r.....25.hg..,c1.O9...:..m.k..z..U..T"..!.60w.M.....)iJ.....S?ELn..\.S..x}...e%P.O..+b.c.%.q.q..+._...v.].>.S....RFc..7_..az.Q...*.i`...,.3...6.+Rmj.2...,..\..j..f=.U.r.H.I...Y.\....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\JTUPjIg1_i6t8kCHKm459WxZcgvz_PZ2[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 24440, version 1.1
Category:	downloaded
Size (bytes):	24440
Entropy (8bit):	7.981001599876889
Encrypted:	false
SSDEEP:	384:GYwxskWSMr5oYGTJO87S6IDTmODSmyEiWbjvkmve3POBpfRkwk2C5OWD4:GYk97MloYF87JIeOAEiWHvJmfMWyCPD4
MD5:	8C98142B425630821139C24BD1698700
SHA1:	0091B988D7DF56ECF357644E02988D66ADB89CBD
SHA-256:	C900E20BA36D01660CBF7BBD552B956C40B28C8532ABB012C0E6766A9F554DE6
SHA-512:	9A1EEA0B8B787B782465919892A4CA50FCA83E77016B29A4410B6BD9B1A3201AD614E1324ACCBDE3143053ED2691BFB7B9D7FA03A4B5EDF4A373BC4D0EC434F9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTUPjIg1_i6t8kCHKm459WxZcgvz_PZ2.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\JTUPJlg1_i6t8kCHKm459WxZcgvz_PZ2[1].woff	
Preview:	wOFF....._x.....GDEF.....G...X.f.^GPOS.....2.....GSUB...T.....,.OS/2.....Q...`T..cmap...l.....h.cvt ...0...c....3..Afpgm.....F...mM$.\|gasp..... ..glyf.....7...a...head..U....6...6..].hhea..V,...#...$...{hmtx..VP...V...>5...loca..X.....(....maxp..Z.... ... .[.Qname..Z.....$/.K.post..[.....D.-.prep..^.....K..x.%....P.....@:D...$..]!....h.....2/.$.....D.^.F..ua.].N....%>.....x...p.....H.Zl+.d..11.....X.ff.a8..X.a.[':.\|>....WS[s['.!.z=.{z..y..wI....d....?.....l!...[..B-O...^..WRI. 9..\.....I.~HVU.M.Q...a!..{..#.....X. %..N.....]V...%.BXvn..+.eI..Q.c...~M%...0..H.P.....u:.B....>...0.&5....U.*f.KR.$E@..D9K.d.h....!.pU]..Di.='T4.c.&..-.[..L.p,L.~...MQ.2.8..3.1...eB.1!.A!..eN.1.V)..G..m..Q..:.p. [..$.....i.2.....i0..e.s.%:.M...&Z..r....1.N...}.T"..4Y..5....F...6.;\.(yih.j8.SU....].^"]#>..er..-.&,.Ki.%..".n...C.f.{.c..3+|]l[..M.ck..<....p?.W.*.Q.C...U.|8.....L..e..+..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\JTURjIg1_i6t8kCHKm45_ZpC3gnD-A[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23576, version 1.1
Category:	downloaded
Size (bytes):	23576
Entropy (8bit):	7.979995638545985
Encrypted:	false
SSDEEP:	384:evykH+9E9B49CndLoAUlGTJO8OzoRb1Jrb7ZlZ/EYh93e1rRykMKAZir2k4lyPmo:eqP9sC2dXUlF8Ozc5JrbNr/EM93eZRhl
MD5:	8B763220218FFC11C57C84DDB80E7B26
SHA1:	E85E6898C8FD8B095BD694B3F1350342C7BB3F35
SHA-256:	299E5F2B6E651BFD7B4C74AA12B06BB10A1200757CC4EBD1FC4C0D9D1AAFA00D
SHA-512:	4A93693CDE6B4BAEAD17A78C6B3FF7BD9F7489D20E5BE3815751B4A1E4E034E7BB54249DEF7F8E06B3ADE41E4333F45FDB232E67971C1817F66151F1440BDE3 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTURjIg1_i6t8kCHKm45_ZpC3gnD-A.woff
Preview:	wOFF.....\.....GDEF.....G...X.g.^GPOS.....2....GSUB.....,.OS/2...I...O...`T..acmap.....h.cvt .....b....0...fpgm.....F...mM$.\|gasp...,..... ..glyf...4..3...\.)...head..R....6...6.P.xhhea..S.... ...$....hmtx..S,...'...>"...loca..UT.....(...maxp..Wt... ... .h.Wname..W.....*.EIpost..X.....D.z.prep..[\.....K..x.%....P.....@:D.. .$..]!....h.....2/.$.....D.^.F..ua.].N....%>./...x..ex#.....<..d.e.-.1..33333333..y...T.`.V^p.m._.{..9...z..z..5... .<....|...<.-.}9./..._....f.P.J?F.....d...b..DzFm.....&b...!...H..;a.XI.=6gEB..6 N.....]6.I...J..w.hU\6...I.u*ei..@..J.n. .2.D3.. .(ay.....<..j>....s@.n.....Z.U.H@.v..e.....!..s.`wW...u4.8P...x.r...z4...h.....H@.;.g.....,1..)..E.}".S.5..X.{E....._.....".D...=|D..Q... D7...q>.\ .\.E.s.Hp.Hr...r.....+..f..q...\+:.Q..,Bn...g#.l..l..l.i..&v.4;E..D=...I.....R.O.1-.fDDA.1+j8...A.D...?M..w.|.&F.f..1..z....j-o9.V.y.em...vRO.^..-.S..f.q.....j...c....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\JTURjIg1_i6t8kCHKm45_bZF3gnD-A[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23628, version 1.1
Category:	downloaded
Size (bytes):	23628
Entropy (8bit):	7.97652223541331
Encrypted:	false
SSDEEP:	384:aWXmwssTJH1/G6rbr24Jln5GTJO8XWSN2OyyW/nGGxnslEYe3cB68HOeHS9AVqmT:aW2wdx1/HPCQln5F8XL2frP5pMB68H/N
MD5:	7C839D15A6F54E7025BA8C0C4B333E8F
SHA1:	09FC9F1CA6B859952A3641EDBFB1424E1C873F5D
SHA-256:	46226ABFCDE5DB2598FED8FD0DE77AF9B96C8242DC0E72242971F0BBCF566A38
SHA-512:	239EDDCB1FE723077F1FDC76B265A3D5E6F946F5258C968B15AB99CDD817D0D67D85248DA13820D9EBF0EA256F1E29ADB975894707E1901BCBDB0C2908ABC8 C2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTURjIg1_i6t8kCHKm45_bZF3gnD-A.woff
Preview:	wOFF.....\L.....GDEF.....G...X.g.^GPOS.....2....!GSUB.....,.OS/2...|...M...`Ti.mcmap.....h.cvt .....d....2...fpgm.....F...mM$.\|gasp...<..... ...glyf...D..4..._.F.1.head..S....6...6.Z..hhea..S@... ...$....hmtx..S`...$...>*...loca..U....!...(N.e.maxp..W.... ... .h.Wname..W.....+.FOpost..X.....D.z.prep..[.....K..x.%.... P.....@:D...$..]!....h.....2/.$.....D.^.F..ua.].N....%>./...x...p.I....RK..Z-...m.-.= .a.....1.0..n.....-h....C!.....Wm.F3....J~/..\|.....*..._]F....Y.x.._.....s.w!.S...'..9d...(...5.).O. z.>...OQ..7J'....>...J.:..K$a6. .._P.lXP."....6....le.sY5.n.t'".C..-..5.2...4.}..H.P....w.....OX.....)8....7?..H..I.@|.....R.'..#R.:....{C}....V.%.i...v.L9K..C.....N".r.P.../..7.UN..'..0...- .Q..M..o.6.....-.&l..B.w..x.....e>....CB....&.....&..P.S....3..Y...Q>/..e...B.+..|.o0..I.#L.]a...../.....&..gLz....J...g!.,$..4#...2L..>.P...gF.67.@.}...IX.&....?Vi....ORR

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\JTURjIg1_i6t8kCHKm45_cJD3gnD-A[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23256, version 1.1
Category:	downloaded
Size (bytes):	23256
Entropy (8bit):	7.977753236160612
Encrypted:	false
SSDEEP:	384:2gMWysI22L2wL/yhGTJO87uvLzyBFvQ3dol9ET1Em9FOgBhkIkYaUpIJ8eQ0iUiJ:2gMWX12LvDyhF87GzUvSCjYD9FOgvsYl
MD5:	8DC95FAB9CF98D02CA8D76E97D3DFF60
SHA1:	FA51AFC9A31F67078FAA9124BEF881655DF4317B
SHA-256:	25F8F00A6FE95DED91A8E33E70154AEE1562760D0D969368D4BAD84BFE85F8D0
SHA-512:	992131CBE01D3DC13831557DD59368B6870BEE453D0C753A5814D001B11327DB60CDEB8D71E4B579E1A5C0238F08E07DF1267CB645738C96197C808E24443A4I
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTURjIg1_i6t8kCHKm45_cJD3gnD-A.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\JTURjIg1_i6t8kCHKm45_cJD3gnD-A[1].woff	
Preview:	wOFF.....Z.....@.....GDEF.....G...X.g.^GPOS.....2....yGSUB.....,.OS/2...L...O...`S6.Mcmap.....h.cvt ...`...b.....:.Gfpgm.....F...mM$.|gasp..... ...glyf.....2...[H.xz.head..Q....6...6.<.ehhea..Q.... ...$....hmtx..R.....>....loca..T.....(.J.-maxp..V8... ... .h.Zname..VX.....)!Etpost..WD.....D.z.prep..Z.....K..x.%.... P.....@:D...$..]!....h.....2/.$.....D.^.F..ua.].N....%>./...x...p[I...'=..3[.G._.....WpL..... `.#o.)g9g.....2._=..==._.D@..x.....o....~.....{..)N$.0.Q...M...?..OQ.X..xo.i..Z...s...n".hI.K .%.a...m..U..l.....6...s...6..<...Z....@myrT...q.${....@.Sl1.@.....N/...k=`?...X..3G$.Z.@=^WK.....c..[a..@[hG.T.I...jF...NVqB..V..+....(...7h.^.i.rB.k.`'{.>.W....B..B.n!.W.h.F. '.=a...r.@.....?.j..0...3....."?..s.....d*W.1Ws..\+d.N.....n....[h.V!.6!.....+.._..".h.e.TV.....X%4.Zh.]hf.PO..g#.4~.0.2]*w.u..".....$.....-Q.%4...C....hf>.....6"..A.)S.....dK...N. ..._X.G....3.....*.uA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\JTURjIg1_i6t8kCHKm45_dJE3gnD-A[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23836, version 1.1
Category:	downloaded
Size (bytes):	23836
Entropy (8bit):	7.979463633723131
Encrypted:	false
SSDEEP:	384:1JCJnpTwnH5O+5hR1GTJO8Ir7BxLJMmel49Ryt+3qiixubNtKBG2DWmkahwV:1w56nZO+5hbF8I5xLJ649MabNCpDkCwV
MD5:	80F10BD382F0DF1CD650FEC59F3C9394
SHA1:	46F6D60D4AC25FC1AA385513C42A58D89BAB45BA
SHA-256:	2A5AFDAC758F2E6A3FD3709719001951708D9F27E7E55ADF9C33B69814A4CD50
SHA-512:	0597EDDF1926C95D792772D3797646AA1E6A294BF023B179CDA1396690AB8B7EAB5394FC896D49A77C161B59D45AB69C53269D869EF40AE83812AC03AA6593B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTURjIg1_i6t8kCHKm45_dJE3gnD-A.woff
Preview:	wOFF.....].....GDEF.....G...X.g.^GPOS.....2....GSUB.....,.OS/2...I...O...`T.Ycmap.....h.cvt .....e....3..=fpgm.....F...mM$.|gasp...0..... .glyf...8..4..._..qhead..S....6...6.i..hhea..T.... ...$....hmtx..T8...&...>37.hloca..V`.....(Wjn.maxp..X.... ... .[.Mname..X.....*SE.post..Y.....D.z.prep..\`.....K..x.%....P.. ....@:D...$..]!....h.....2/.$.....D.^.F..ua.].N....%>./...x...p.I.E_..z.-....4f.....!.0..i.ye...5..I+.j.n..p.f.y.....*UuK.6....^B.Q.y.(....x.....w...D.f>+.E...{.....S[...g...Q...v.ap.....&....Q.T.. [...v.]o.v....P.....? K..l.|.HD.....e.Q....Yl.i...D, ...n.OR.|.[....p+.PF}....D@D3.{.....l..'Mv.bE.L.....E.0.....Hl.....~P+R.....Np.s..KH..''...9!r...=..^..U|B..b....|Z...(.Y1...|^..... .,~.B~./).+..k~C...1..<.:...\"....h.r.q.....kE..E.....:.N....nQ....^..>.H.hb....!.S.(..1.'D-gD.Y..#f.+j.d.. .....AtW.whb..`...M..Rb..Fo.....:..*.['y.y._.n...w....m...P..EV..I6..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\JTUSjIg1_i6t8kCHKm459WlhzQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23480, version 1.1
Category:	downloaded
Size (bytes):	23480
Entropy (8bit):	7.981253427621622
Encrypted:	false
SSDEEP:	384:lEfDbJfERirQlhTVld2GTJO8Z84zUE8EW3md2T0LuYXDbMdK3OLmvTHc5qawV:lEf3JPrQl8d2F8WDE9w0FLTbMdK+Cvj3
MD5:	8102C4838F9E3D08DAD644290A9CB701
SHA1:	5AF1938D1327395F47C84E57B6BA7756234D2262
SHA-256:	60CEBEA4C9183F51FBD323F14DD729E18768BE4F6395467013216AE36526CF9C
SHA-512:	E8A0D6B72163E407DE82170E4560044CAE90116D1DD3CFA20F140E4379C8AABDC5BEAC6DD965D0E925CA673E41C42A858975C47F1F8152637958569D239E91F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTUSjIg1_i6t8kCHKm459WlhzQ.woff
Preview:	wOFF.....[.....8.....GDEF.....G...X.g.^GPOS.....2.....GSUB.....,.OS/2...\...N...`S..Ucmap.....h.cvt ...p...\..../R.Hfpgm.....F...mM$.|gasp..... ...glyf.....3X..],,..$head..Rt...6...6.F.nhhea..R.... ...$....hmtx..R....%...>.x..loca..T.....(..*0maxp..W.... ... .h.Yname..W4.....-5H.post..X$.....D.z.prep..Z.....K..x.%.... P.....@:D...$..]!....h.....2/.$.....D.^.F..ua.].N....%>./...x..ut.I.....e+..o...g.^..13333333333.-.e/.cgYAs....R.{.G..^.L.....j.....R.z..D..o...~.....$.`.BY.21.W.....9...f.C..(..M.!..D....1rT ...w6cG.J....U.....]..>.....q..jhT\l..;,M.zYK..x:.n.R...(.....g)..~...Xl#`.....-.#..T...]..Tw.....k.7....I.....@..$..r....X.\..L....._.H.2".V... .1...".._d.#R..4c"...2> ..A..D;..e>".|Tt.1. .....8...._.K..+.....Y~'r.A.....D.../..W..ob.....[.8K.8Gtq..0...|....D.KE+..".V.....\vr.._-.Se..=..A.1$...<.E.CL..%QB.8.9.....,.Jv.=,...%.i..:U*V..U.b..]N.D..O..'...1.$.....<

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\KFOiCnqEu92Fr1Mu51QrEzAdKQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 21776, version 1.1
Category:	downloaded
Size (bytes):	21776
Entropy (8bit):	7.972467440478283
Encrypted:	false
SSDEEP:	384:G+oO9eMm6IbA7qJx9w3/TVd3fr5KjEid8pTN4TbOwyFPhgGRw9:zl9eMm6eKsHwpdPr5K+Pu6wsPaGRU
MD5:	E21019768EE6D334593AA1EBCA028ACF
SHA1:	DFE80B4CB13F47ECED9236E33AB360DB41711B0C
SHA-256:	75D75439F2A7EA1851A3E5B621320B9DFA1399861D2EC6D443A3C2919B93AFB7
SHA-512:	CFE0237C61D61CD630A1F9E05C2A00DEE1C2006811ADAB19162F2BCB890E2F126054EC01131CD2642D2D2398C0F56C7D2D9A25A56C2BAD6FF4BC6FB21029C 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOiCnqEu92Fr1Mu51QrEzAdKQ.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\KFOiCnqEu92Fr1Mu51QrEzAdKQ[1].woff	
Preview:	wOFF.....U.....GDEF.....G...d....GPOS.....!GSUB.....OS/2...L...O...`t..'cmap.....#cvt .....H...H.2..fpgm.....3...._...gasp...0.....glyf...<..A...u....hdmx..M....q.....#.&head..Np...6...6.|.hhea..N....#...$.}.[hmtx..N.....rQ.loca..QX..... ..._maxp..SP... ... .4..name..Sp..... G= post..TL..... .a.dprep..Td.....+6.x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x...l\..F..3...N..q)..a|.....^..33..c.....p"y.iT...<Gg...!.3...T1...{.g0.u.y.....m.|.k..NF.....mox.;...7&.Y..C.R_[.T.c..-.=...9:...a*j.G.....O.Q".6...>...(?...~...._2:..K4....S%...jbr).....*....e.U..-..X.3.ILQ....z..!.f:...<.W.#...e.c=...&6...lc;;..3<.s<....H.i2..N..t..)Ns...#`..").).[...._..T..T.....+l..=..O.....Z..F...r..eM.f.Y.....-...r.\.s6.r..,...:.<$..#.l..F.$.2#.e..].[.....yR...e.|{..O..`)..U.0.e.50.Z.b../cM..i.&O._..+.Y.W...;z....j.p._.o..[CL.)n'.UGx..>).X..MJ..Fr..v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\KFOjCnqEu92Fr1Mu51S7ACc6Csl[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22080, version 1.1
Category:	downloaded
Size (bytes):	22080
Entropy (8bit):	7.970620647480227
Encrypted:	false
SSDEEP:	384:BfnIIA0zhdg/5oXRAZDRsZObG141wGUaBgKYADioTCgZM6+HJtWjbmMbQMbL2nNQ:B00zhdW7ZDRsR141wYAoTCGUptzMbqnu
MD5:	FA8878D8872A2AC4BEB377CDAE15566A
SHA1:	34EE72B0E553C3EFA41A7E0DF4EB710596469A10
SHA-256:	8411023A027610AEB3DC333438E12A17222163AE78817C5395DA04548ED30150
SHA-512:	112ED53A4A18EB3378A57B154566C0F1AF438FF400EBE453253F5E2465B6A07370B447736EACB99114ED43E05CAE5A3A019BE6886D50EB15FA1E2D6F35D9AFBA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOjCnqEu92Fr1Mu51S7ACc6Csl.woff
Preview:	wOFF.....V@.....0.....GDEF.....G...d....GPOS.....oGSUB.....OS/2...p...N...`t..dcmap.....#cvt .....\...\1..Mfpgm...4...2.....$.gasp...h.....glyf...t..Bf..s...hdmx..N....l....(/./head..OH...6...6...vhhea..O....#...$....hmtx..O.....*:8loca..R@.....*.imaxp..T8... ... .4..name..TX.....!.>gpost..U4..... .a.dprep..UL.....X9..x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x....%Y....Wm=..mo..k.m....rl...m.g"^..../..[.}.S...\.mD...1..G>..giz...=C..}.y....|o..c.x.R.r"B.....m.../../.&./6..5D.AGX.....)<'.)....?.... .Y4>|1...ES.Gc...FO.>$.../...}RCl..T.zD..uZ4~D.._OK.$.Z.(..JR...\..\..\..\.\.....*'n..6:x...b,..$...?.g:./y.iLg.3..l.0.y.g..X..V...d.#O...0....b7{..>.n.iD.V....." e.\A..OR.kwp.].....6p..."ZE..%...e.u3..L..V...W.7b..L.3.L1K...Ts..$6.-b.....9...b@..!1,...v.C....{...dox.G(...|a%E:.Fn.Nn.^n.....Sf..E)...k....<g..)\{....|.....DT..N....Hy.F.Jez....._?7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\KFOjCnqEu92Fr1Mu51TzBic6Csl[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 21656, version 1.1
Category:	downloaded
Size (bytes):	21656
Entropy (8bit):	7.971138981009303
Encrypted:	false
SSDEEP:	384:vfqIIA0zh/VF0+5SLHCK+yo5HHx/KnMpljPSiQZxLZtspfA9JaXWWyBuM9rgaSJV:vJ0zh/VFv0Hm15HHtKnalaiQfZtsp49o
MD5:	147F4E11CE73A22AAC9C6C2822290953
SHA1:	EEFEA89A9C36F8B1A7CA99372A7E0E05C92EADD6
SHA-256:	A22585CFD64238EF14B1B383B5B9A8BAD7C89E354C09FC0886067E876687A38C
SHA-512:	3D7ADA26B281864CE394CB49974A9EA59D28FA8C2EFB006DF31DCAE66DB4684223BDB42B8234A5135BF1B4F834E91DE415E44558EB2CF2346086C8879397058
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOjCnqEu92Fr1Mu51TzBic6Csl.woff
Preview:	wOFF.....T.....GDEF.....G...d....GPOS.....oGSUB.....OS/2...p...O...`u...cmap.....#cvt .....J...J..,ofpgm...$...3....c...gasp...X.....glyf...d..@...o.H.6.hdmx..MD...n....,..0head..M....6...6...`hhea..M....#...$....hmtx..N.....1)loca..P.....maxp..R.... ... .4..name..R..... .=$post..S..... .a.dprep..S.....9..Bx...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x....%Y....Wm=..mo..k.m....rl...m.g"^..../..[.}.S...\.mD...1..G>..giz...=C..}.y....|o..c.x.R.r"B.....m...../.&./6..5D.AGX.....)<'.)....?.... .Y4>|1...ES.Gc...FO.>$.../...}RCl..T.zD..uZ4~D.._OK.$.Z.(..JR...\..\..\..\.\.....*'n..6:x...b,..$...?.g:./y.iLg.3..l.0.y.g..X..V...d.#O...0....b7{..>.n.iD.V....." e.\A..OR.kwp.].....6p..."ZE..%...e.u3..L..V...W.7b..L.3.L1K...Ts..$6.-b.....9...b@..!1,...v.C....{...dox.G(...|a%E:.Fn.Nn.^n.....Sf..E)...k....<g..)\{....|.....DT..N....Hy.F.Jez....._?7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\KFOkCnqEu92Fr1Mu51xIIzQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22036, version 1.1
Category:	downloaded
Size (bytes):	22036
Entropy (8bit):	7.974581575530646
Encrypted:	false
SSDEEP:	384:WhoOtWgD0GjcBsPSQSQhzT8EeFVJDOFKA3t1pLXhj8gGddsbnDX1F:4l30GI/cRMzqKA91pNj89WnDX1F
MD5:	522AECAD450B10CE647739BC8D9AA1C6
SHA1:	6C3528F1BDD5B980F41BDCD1D9FCD812FE0C6D61
SHA-256:	2B5FB1F0EE063320196A64157AE9A949BB4656BC48604914175F1EDA636DCE07
SHA-512:	33AAAE71C92278EE04102EE59B3856DB9EB7C6F187EC35BBD302492619CA47811FF379A2B469DAF670407ADEA10B3BCF56A7B883CD1241447957471263CF95B3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOkCnqEu92Fr1Mu51xIIzQ.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\KFOkCnqEu92Fr1Mu51xIlzQ[1].woff	
Preview:	wOFF.....V.....x.....GDEF.....G...d....GPOS.....!GSUB.....OS/2...L...O...`t..Rcmap.....#cvt .....R...R..-.fpgm.....4....s...gasp...<.....glyf.. .H..Bd..rp}..hdmx..N....m....#-.,head..O....6...6...ehhea..OT...#...$....hmtx..Ox.....cC.loca..R..... \|.maxp..T.... ... .4..name..T0.....:.post..U..... .a.dprep..U .....D. .].x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x...l\..F..3...N..q)..a\|....^..33..c.....p"y.iT....<Gg...!.3...T1...{.g0.u.y.....m.\|.k..NF.....mox.;...7&.Y.. C.R_[.T.c..-.=...9:...a*j.G.....O.Q".6...>...(?...~....._.2:..K4....S%...jbr).....*....e.U..-..X.3.ILQ....z..!.f:...<.W.#...e.c=...&6...lc;;..3<.s<....H.i2..N..t..)Ns...#`..".).[...._.T..T... ..+l..=..O.....Z..F...r..eM.f.Y.....-...r.\.s6.r..,...:.<$..#.l..F.$.2#.e..].[.....yR...e.\{..O..`)..U.0.e.50.Z.b../cM..i.&O._..+.Y.W...;z....j.p._.o..[CL.)n'.UGx..>).X..MJ..Fr..v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\Nyttt[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, 266x189, frames 3
Category:	downloaded
Size (bytes):	6975
Entropy (8bit):	7.910366047932427
Encrypted:	false
SSDEEP:	96:lhviVGCajAg3lDXX2UTiqpqPy1Qe/hK5tK+KEmguytrZr7kjMlMUHwPrMLGOYm0O:P+DajAgh3TiqpqPcQepOaSPwPKTYm0PG
MD5:	5CE5359184445C8A35D5C3CAED7E8993
SHA1:	3A79F02E68A594536997E700186F2A2D73EC9E7F
SHA-256:	B05E67ACDFE53D14B59E8EBF228156FA09B47466FAFD71DF6DD44855E65587A0
SHA-512:	807A23418840B1543ECB387BDD6D29D983B703EB30941D06E3236082802DFD0CEE71F2FF248AB89759AF3822DA74EEB46EB54B01FBE4F7078271D504F510CB90
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://images02.nicepage.com/4a6432a7cb0551e103110d03/056c8b253ee65a37aa77a49d/Nyttt.jpg
Preview:	.....JFIF..... (..%...!1!%*+....!383-7(-.+.....+%..------+2++---+7----------3-7----------++-----+-.....".....H.....!. .1.AQ.."RSa...2q....#B..3b..Ccr.....$4T...5D.....(.....a..Q!..1A....q...#.....?....B.8.....A:....L.BdP..o...-N.\|..<....S..).&Z.v.O..x+).C..].S.L.:..R\.VS".- N.\|...S1nfX.9N..{.M.++H..W..)..Z.fyO./.e:(2..3.~...Y.S.K.YN...z..e..g..R.VS..-^.<..j...?T.....W..)..Z.fyO./.'E.Z.fyO.2..3.~.x+).A..Y.S.L.z..^..tPe..g..S-^.<.....j...?U.0...[..~.[.IQU. +f..D. f#..ZH.&.DU.D@T.5.6....#.3.qV}0.=.G1...x+3.../.jS5v..P.1{....q_O....pxY.Z...7.....q..oU.....4.N.I...[.9...B.y...$...xly+..:...../.....|.IC...K..(...,..0'<.Tx..M.1....Kv..fA$8d.e. 9.u...8..W..~L.4.5..y...Z.....ZJ..t.z.#...S..6.&.Gm\Z*ScZ.uK$.7Sk{....._J.W.../.M.y.H.....[.....C*2"$T....U...s]Ls..T]..''..A..j....R4.H..O_.....E.i..V(6.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\Page-1[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	4559
Entropy (8bit):	5.115290234299837
Encrypted:	false
SSDEEP:	48:e7YBOrhCtkODyWpWQKyc5tL1Ot+EShoXQHZdPjSVv8t4MYBxeL:fOykJWpejmgXp4LBxeL
MD5:	FF42446F76DF060079027F1F49D5E5D6
SHA1:	1A564E5AC2EF2477267AA1E315B1E5643DA54A2D
SHA-256:	A5193B6B5D356CB0D288B9353641EC9AFFF32009C6A57AA9CE8A0227F0F982BB
SHA-512:	8C2C681395B6FC90E64A7B1D493745EA7590B875455F8F18AC104E5DF64749C0C216FF99580E0DE9AD16B4311AAFB6864D2AAA0EE3108D75648B0AB2A36F1F8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://murphy-constructions.nicepage.io/Page-1.html
Preview:	<!DOCTYPE html>.<html style="font-size: 16px;">. <head>. <meta name="viewport" content="width=device-width, initial-scale=1.0">. <meta charset="utf-8">. <meta name="keywords" content="Secured Document from John Vickery">. <meta name="description" content="">. <meta name="page_type" content="np-template-header-footer-from-plugin">. <title>Page 1</title>. <link rel="stylesheet" href="/nicepage.css?version=22baa169-ff2f-437c-8b06-732e40d9cb8d" media="screen">. <script class="u-script" type="text/javascript" src="//static.nicepage.com/shared/assets/jquery-1.9.1.min.js" defer=""></script>. <script class="u-script" type="text/java script" src="//capp.nicepage.com/6ba8f9621eefd8f9e7050129b53e111985c3f5cb/nicepage.js" defer=""></script>. <meta name="generator" content="Nicepage 3.13.5, n icepage.com">. <link id="u-theme-google-font" rel="stylesheet" href="https://fonts.googleapis.com/css?family=Roboto:100,100i,300,300i,400,400i,500,500i,700,7 00i,900,900i|Open+Sa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	211
Entropy (8bit):	5.026484232218891
Encrypted:	false
SSDEEP:	6:0IFFwKh+56ZRWHMqh7izlpdBEoKOEEJTONin:jFWmO6ZRoMqt6p3EondOY
MD5:	04F7435B2672FBE66984EA436E7087C6
SHA1:	44896875E69B297EB979CC0D3E8522D872656BA8
SHA-256:	F9088C15A062F0C7708C3864C5E261A2E4961DFEB0F150DF744FAEC2E3B74AD6
SHA-512:	9A1D01A7FAC3D6B205CFA37C05A93AFA9D903D4D35DCB16E31D3A31D19CD65B8DE5D66E626BC7F70D07841C779E20CD2C2DD6254824F96DE0E8E576E156F1 7D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Yellowtail&display=swap

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\css[1].css	
Preview:	@font-face {. font-family: 'Yellowtail';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/yellowtail/v11/OZpGg_pnoDtINPfRIlLohlvHxw.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\gmail[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1280 x 1280, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	66743
Entropy (8bit):	7.712342056984168
Encrypted:	false
SSDEEP:	1536:FxqKcVqezl0vLoYxEuKoYk5LHjGkT3b1mQOEj0+R+EH:FsK2qezl0zoYxEuKo7CYrOb+Rb
MD5:	DCE2F2B0E50CB1DBB0246D152791CB46
SHA1:	D0A69C159304EDC08DB005163E7A0DAF5A1E98A6
SHA-256:	ACF087C1757F08B0CFD53D59066544D7EF0BFCC50999E77C5813739CD9DC1479
SHA-512:	91054B36EF1673B24E4FE3DC324CBE339F4E9EB72785A6A4C355C7B2A11A9A7C6E188FF9BF5B34FFDD2805D4BBED71EF6CA4975EE3E330FD8D8E383ED64B28EE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fireanddust.com/js/images/gmail.png
Preview:	.PNG.....IHDR.....sBIT....|.d.....pHYs...../....tEXtSoftware.www.inkscape.org..<... .IDATx...{x.u.....I.sS..9Q(..J.L&.$..V\|.....#..''...Zw.eEQv.Q..U.A]9Vh..I8...H2)`....i.....).....f.y....L.pu...{n.....@Is..... mj=...X<65....U.l.b.t.U...mR...e..P.i.$.i2U..@N1.f...i.s...cf...../....2ev.`..%.|.o...s..j..l.B....V&..s;b..Pfg.....!...:..5....$.@...I0.=.IY.....a...B.4g... T.9Wif..R..o.R.t'.0...?G.9i...L...*..&..s.Vgnkhn...;p[.0.5.....$.....P.....^".HL.M...@.p..;04....9.&.(i....9.sK..=&.'$m.....f..1..'...f2.Uww.....PH....@..xq....k.2..l.Luf..s5..`.|

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\js[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	11777
Entropy (8bit):	4.816019894976133
Encrypted:	false
SSDEEP:	192:K2FI5vEJKnYmrDfG4RDwAOT+UY/t4IdtWPtY:1nmRsAKyt48tZ
MD5:	D162B0FF37D24C43E185D012250A0303
SHA1:	493210A8D7D5F033AD86920378A2800D2656C455
SHA-256:	92019D1A8FD2F8C5876863B91F8C71576656F71F84FD15453F93BFC0AF9FB05F
SHA-512:	603190096894C7564A7637EFA3E1AEB0CB8C44802744936B4C6D650C8D23AFEFD8B80467064EBA8E13797ECF2C02DA397EF4FE8BD7523C601BB316181DAE247
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\js[1].htm, Author: Joe Security • Rule: JoeSecurity_HtmlPhish_7, Description: Yara detected HtmlPhish_7, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\js[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://fireanddust.com/js/
Preview:	...<!doctype html>..<html lang="en">..<head>.. <script src="https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>.. <script src="https://code.jquery.com/jquery-3.1.1.min.js">.. <script src="https://code.jquery.com/jquery-3.3.1.js" integrity="sha256-2Kok7MbOyxpgUVvAk/HJ2jigOSYS2auK4Pfzbm7uH60=" crossorigin="anonymous"></script>.. Required meta tags -->.. <meta charset="utf-8">.. <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">.... Bootstrap CSS -->.. <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css" integrity="sha384-Gn5384xqQ1aoWXA+058RXPxPg6fy4IWvTNh0E263XmFcJlSAwiGgFAW/dAiS6JXm" crossorigin="anonymous">.. <link href="https://fonts.googleapis.com/css?family=Yellowtail&display=swap" rel="stylesheet">.. <script src="https://kit.fontawesome.com/585b051251.js" crossorigin="anonymous"></script>.. <title>Share Point Online</title>.. <link

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\logo-w[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 123 x 40, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	2326
Entropy (8bit):	7.557196740671305
Encrypted:	false
SSDEEP:	48:UwkNvnAbZIJ3PfTNPJpImD9uVHlttw3l4yzjeO7SF2NuTo:CNAFS19PteV4y+O7SRE
MD5:	3FEF24C6C26DF3CF768A82FDAD6EACB9
SHA1:	42D2F49769FEB458C47683301C9CE7CEC4216C6F
SHA-256:	5A382D39B099194A3C05A6AF16412AF0339D6A3833B88A1EAD3105C4562128AC
SHA-512:	7395CC7EBB182251551918B632BF832969CD2036DA92410013610ACA175AD09668A10B89723E142A0766F7250139608EF859FA1E7A948DBAC261C1CCC1E9E644
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://csite.nicepage.com/Images/logo-w.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\logo-w[1].png	
Preview:	.PNG.....IHDR...{...(.....&....tEXtSoftware.Adobe ImageReadyq.e<..."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:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:174C9D8F2DD611E9BBC2F5585045DBC5" xmpMM:InstanceID="xmp.iid:174C9D8E2DD611E9BBC2F5585045DBC5" xmp:CreatorTool="Adobe Photoshop CS6 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:D4BE73DC584211E8A406F483A57DA8D8" stRef:documentID="xmp.did:D4BE73DD584211E8A406F483A57DA8D8"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>9u.|....IDATx..[M..E...lV=h.ATPlO.x.9..tC..d..D.0}.".f.....M....*..Ar.n...Q..f.u3.....R...f;.....z...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\nicepage[1].css	
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):	1216236
Entropy (8bit):	5.012799133983897
Encrypted:	false
SSDEEP:	12288:iUmo2qJ4FfbKmckQ2rJym5Dz6P5uXWXjmMULs5i6erDcL:X2rJrA
MD5:	E5DEC9A30976D845B357D7E1ECD2BCD0
SHA1:	595745D2BE0C0CAEB6C2BE7B34C710CD3F7349D5
SHA-256:	568B5DF84E1F1D87BEA3F76471CCA82E55F7709A5AE52CF5817364FEDCDBFE5F
SHA-512:	59F884763271E411B8E89623E8C2E4C9DA0CD939943023C01C55F6A23C3D7AC09EBBE46CA34A8D5CBE26DCE2BA29E9867A56AC41C66F570EFABCF951E4DA7 14
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://csite.resource.nicepage.com/nicepage.css?version=2993d4e3-12ae-4eda-9125-86b9894223df
Preview:	/*begin-commonstyles library*//*!.. * froala_editor v3.2.3 (https://www.froala.com/wysiwyg-editor).. * License https://froala.com/wysiwyg-editor/terms/.. * Copyright 2014-2020 Froala Labs.. */.....fr-clearfix::after {.. clear: both;.. display: block;.. content: "";.. height: 0; }.....fr-hide-by-clipping {.. position: absolute;.. width: 1px;.. height: 1px;.. padding: 0;.. margin: -1px;.. overflow: hidden;.. clip: rect(0, 0, 0, 0);.. border: 0; }.....fr-view img.fr-rounded, .fr-view .fr-img-caption.fr-rounded img {.. border-radius: 10px;.. -moz-border-radius: 10px;.. -webkit-border-radius: 10px;.. -moz-background-clip: padding;.. -webkit-background-clip: padding-box;.. background-clip: padding-box; }.....fr-view img.fr-shadow, .fr-view .fr-img-caption.fr-shadow img {.. -webkit-box-shadow: 10px 10px 5px 0px #cccccc;.. -moz-box-shadow: 10px 10px 5px 0px #cccccc;.. box-shadow: 10px 10px 5px 0px #cccccc; }.....fr-view img.fr-bordered, .fr-view .fr-img-caption.fr-bordered

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\office3651[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 187 x 188, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	18025
Entropy (8bit):	3.011161251318808
Encrypted:	false
SSDEEP:	96:2S+WvkiqJq6Uq7NXrNG+GHhsc5yeFZV9D2Ydcx/NTV0K0VFDsCmm:2SJkiOq6Uq75shDs1kFP
MD5:	FE22440D79FFA34950F512EF4A718B2A
SHA1:	0E147E59544EE6580D3095353D4420849FA5EB8A
SHA-256:	A2F26B68A6C8810C1AEB4048C938F835A86BA83756A7A440F989B967E78F3BA8
SHA-512:	64218ECD4140DC05E50EB7BA4C9813794B8B5A4310C8308244205BA6ADA8EE7C2D1840121730A00800E41775241D8AFA02125A966064CD0EB2CC7D3E4605B81
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fireanddust.com/js/images/office3651.png
Preview:	.PNG.....IHDR..... .....pHYs.....<eiTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?>.<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c067 79.157747, 2015/03/30-23:40:42 ">. <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">. <rdf:Description rdf:about="". xmlns:xmp="http://ns.adobe.com/xap/1.0/". xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/". xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#". xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/". xmlns:dc="http://purl.org/dc/elements/1.1/". xmlns:tiff="http://ns.adobe.com/tiff/1.0/". xmlns:exif="http://ns.adobe.com/exif/1.0/">. <xmp:CreatorTool>Adobe Photoshop CC 2015 (Windows)</xmp:CreatorTool>. <xmp:CreateDate>2020-01-18T21:49:38+05:00</xmp:CreateDate>. <xmp:MetadataDate>2020-01-21T14:30:14+05:00</xmp:MetadataDate>. <x

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\other1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 190 x 187, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	21882
Entropy (8bit):	4.268463452779894
Encrypted:	false
SSDEEP:	192:ESCkiDw7e9Mg/wio0EYm9FWyo2XdJfXoOZdEDfmiIJQdiRVi/WTanY:DBiDw7eAdq+FWyo2/fXoZbDIJ0ci/BnY
MD5:	6843A244E12FAB158AA189680B5E7049
SHA1:	0E1C691F87CC4FA35C88344974F2829C40176B70
SHA-256:	3A9B144D6482B78AFC4E0A940A1D3C22240F14FA535B808CF4DAB9635339569F
SHA-512:	145010C45B6B83EA4005EB367C0507959FF0817E482F19E9973504081ACAE1B7827CBD1172CEC7732B13F4E0CEC058271BD6700444FBCF61FB6A3C068A3744C4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\other1[1].png	
IE Cache URL:	http://https://fireanddust.com/js/images/other1.png
Preview:	.PNG.....IHDR.....$.... cHRM..z&.....u0...`.:....p..Q<....sRGB.....gAMA.....a.....pHYs.....:.iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?>.<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c067 79.157747, 2015/03/30-23:40:42 ">. <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">. <rdf:Description rdf:about="". xmlns:xmp="http://ns.adobe.com/xap/1.0/". xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/". xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#". xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/". xmlns:dc="http://purl.org/dc/elements/1.1/". xmlns:tiff="http://ns.adobe.com/tiff/1.0/". xmlns:exif="http://ns.adobe.com/exif/1.0/">. <xmp:CreatorTool>Adobe Photoshop CC 2015 (Windows)</xmp:CreatorTool>. <xmp:CreateDate>2020-01-18T21:59:57+05:00</xmp:CreateDate>. <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\templates-page-libs[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	279421
Entropy (8bit):	5.239761527112776
Encrypted:	false
SSDEEP:	3072:vhQiLogL4QcBbmGSBabiTh5dXnh23LsFLyPDlBNFwXOwXz:2iog7cBbniaQLdXnhisFLy347Xz
MD5:	6228020B62C90D0A31CC5A9DA976EC91
SHA1:	D07F663ED8CF85DF2DE41DEAF8859943DE04E483
SHA-256:	4A9C86E7B83E0427B5469E0D72A637970D62B85FD033BB68C541B2F7C327924A
SHA-512:	A0E26F83BC6FAD60D86ACDAB4403457455C47A32EB86B5C7C0C76545B2198542C167F8CAE569770C6A46077A173C522BFF6C851A210B6A60501C8A1283FBD18
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://csite.nicepage.com/BundledScripts/templates-page-libs.js?version=6ba8f9621eefd8f9e7050129b53e111985c3f5cb
Preview:	!function(e){function t(n){if(i[n])return i[n].exports;var o=i[n]={i:n,l:false,exports:{}};return e[n].call(o.exports,o,o.exports,t),o.l=true,o.exports}var i={};return t.m=e,t.c=i,t.d=function(e,i,n){if(!t.o(e,i))Object.defineProperty(e,i,{configurable:false,enumerable:true,get:n})},t.n=function(e){var i=e&&e.__esModule?function t(){return e.default}:function t(){return e};return t.d(i,"a",i),i},t.o=function(e,t){return Object.prototype.hasOwnProperty.call(e,t)},t.p="/Content/BundledScripts/",t(t.s=5175)}({12:function(e,t){var e=void 0;(function(){/*!. * jQuery Cookie Plugin v1.4.1. * https://github.com/carhartl/jquery-cookie. *. * Copyright 2013 Klaus Hartl. * Released under the MIT license. */.!function(factory){if("function"==typeof define&&define.amd)define(["jquery"],factory);else if("object"==typeof void 0)factory(require("jquery"));else factory(jQuery)}(function(e){function t(e){return l.raw?e:encodeURIComponent(e)}function i(e){return l.raw?e:decodeURIComponent(e)}function n(e)

C:\Users\user\AppData\Local\Temp\~DFA7401578B30F75CD.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4774506596701812
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo89loM9lW3HovHnHs7YG:kBqoIHh3+HQYG
MD5:	81358899B93ACCDDF3857A4991A900F9
SHA1:	9AD848D1CFE12AE97FBCD5EBC87DF5B88B34D4FE
SHA-256:	908DD929DDEE86B8A9890DC5C03AC31A096C32E3ECFDB7ADD516DA875F4A9A7E
SHA-512:	8B697543295C2D62566250FCCA7D5B51FFF03E3799221921C9A70E43D055E54BD22FC968AF3960DB75C3D2F8E436180AA901A4ED2E1468186374FD17C35D599F
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFB4F288BC7A0B80AF.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	63351
Entropy (8bit):	0.8431570611266183
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+Px8Y8p8y85OuUQQUQiOrOzG0JOZOaKHAO8eOzd3tm:kBqoxKAuqR+PxzaBK9y4K0PgdPReKdd
MD5:	356F42749789EB2CBDE90F71A6C250A9
SHA1:	FD1C7C3F923CF01FEBF04B0FFEAA224079D73B86
SHA-256:	1CBD4DD4C1630AB3669F0A5129D0FD5023A06CC62AF503F293719DD1337C8D50
SHA-512:	00BFAA447CC943466CAFB0BF37B5C36E80C9D077F1F26E2CFC5F1955D12847C514C71396ED62072BF5620249FA5FCC9AC05AB0FFD65AF1718D09F604DC395A3B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DFB4F288BC7A0B80AF.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFDC6AE771C93B04EC.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

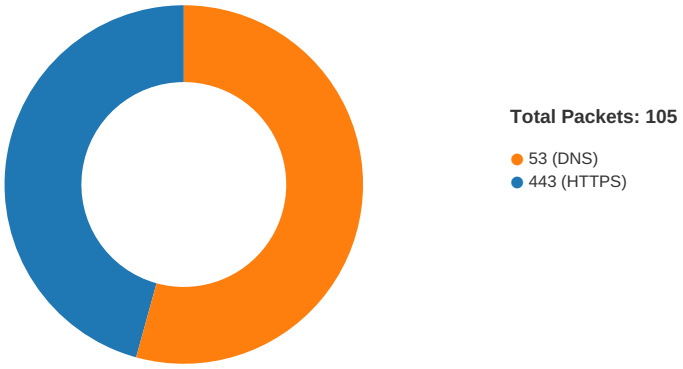
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-21:52:41.935670	ICMP	384	ICMP PING			192.168.2.6	8.241.78.126
05/04/21-21:52:41.972769	ICMP	449	ICMP Time-To-Live Exceeded in Transit			84.17.52.126	192.168.2.6
05/04/21-21:52:41.973300	ICMP	384	ICMP PING			192.168.2.6	8.241.78.126
05/04/21-21:52:42.008480	ICMP	449	ICMP Time-To-Live Exceeded in Transit			149.11.89.129	192.168.2.6
05/04/21-21:52:42.009359	ICMP	384	ICMP PING			192.168.2.6	8.241.78.126
05/04/21-21:52:42.045252	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.50.25	192.168.2.6
05/04/21-21:52:42.046520	ICMP	384	ICMP PING			192.168.2.6	8.241.78.126
05/04/21-21:52:42.087740	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.0.62	192.168.2.6
05/04/21-21:52:42.088588	ICMP	384	ICMP PING			192.168.2.6	8.241.78.126
05/04/21-21:52:42.137139	ICMP	449	ICMP Time-To-Live Exceeded in Transit			154.54.36.253	192.168.2.6
05/04/21-21:52:42.137626	ICMP	384	ICMP PING			192.168.2.6	8.241.78.126
05/04/21-21:52:42.229088	ICMP	449	ICMP Time-To-Live Exceeded in Transit			154.54.37.30	192.168.2.6
05/04/21-21:52:42.230327	ICMP	384	ICMP PING			192.168.2.6	8.241.78.126
05/04/21-21:52:42.279357	ICMP	449	ICMP Time-To-Live Exceeded in Transit			4.68.37.93	192.168.2.6

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-21:52:42.279781	ICMP	384	ICMP PING			192.168.2.6	8.241.78.126
05/04/21-21:52:42.325723	ICMP	449	ICMP Time-To-Live Exceeded in Transit			4.69.163.62	192.168.2.6
05/04/21-21:52:42.326724	ICMP	384	ICMP PING			192.168.2.6	8.241.78.126
05/04/21-21:52:45.953121	ICMP	384	ICMP PING			192.168.2.6	8.241.78.126
05/04/21-21:52:49.932735	ICMP	384	ICMP PING			192.168.2.6	8.241.78.126
05/04/21-21:52:53.933309	ICMP	384	ICMP PING			192.168.2.6	8.241.78.126
05/04/21-21:52:57.956118	ICMP	384	ICMP PING			192.168.2.6	8.241.78.126
05/04/21-21:53:01.936887	ICMP	384	ICMP PING			192.168.2.6	8.241.78.126
05/04/21-21:53:05.943665	ICMP	384	ICMP PING			192.168.2.6	8.241.78.126
05/04/21-21:53:09.937403	ICMP	384	ICMP PING			192.168.2.6	8.241.78.126
05/04/21-21:53:13.931656	ICMP	384	ICMP PING			192.168.2.6	8.241.78.126
05/04/21-21:53:18.120449	ICMP	384	ICMP PING			192.168.2.6	8.241.78.126
05/04/21-21:53:21.933970	ICMP	384	ICMP PING			192.168.2.6	8.241.78.126

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:52:45.335956097 CEST	49713	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.335972071 CEST	49714	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.380110979 CEST	443	49713	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.380136013 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.380346060 CEST	49713	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.381319046 CEST	49714	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.385605097 CEST	49714	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.385616064 CEST	49713	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.428565025 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.428591967 CEST	443	49713	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.428709984 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.428729057 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.428774118 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.428787947 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.428822994 CEST	49714	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.428853035 CEST	49714	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.437232018 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.437263012 CEST	443	49713	18.194.109.194	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:52:45.437308073 CEST	443	49713	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.437325001 CEST	443	49713	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.437347889 CEST	443	49713	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.437366962 CEST	49714	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.437444925 CEST	49713	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.437948942 CEST	49713	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.445738077 CEST	443	49713	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.445885897 CEST	49713	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.472626925 CEST	49713	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.472816944 CEST	49714	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.479933977 CEST	49714	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.517611980 CEST	443	49713	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.517730951 CEST	49713	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.517756939 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.517827988 CEST	49714	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.549154043 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.549205065 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.549273968 CEST	49714	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.549299002 CEST	49714	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.593630075 CEST	49714	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.672568083 CEST	49716	443	192.168.2.6	95.211.139.76
May 4, 2021 21:52:45.673589945 CEST	49717	443	192.168.2.6	95.211.139.76
May 4, 2021 21:52:45.676443100 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.689703941 CEST	49721	443	192.168.2.6	89.187.165.8
May 4, 2021 21:52:45.689994097 CEST	49720	443	192.168.2.6	89.187.165.8
May 4, 2021 21:52:45.707346916 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.707376003 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.707392931 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.707408905 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.707423925 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.707442999 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.707459927 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.707464933 CEST	49714	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.707475901 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.707493067 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.707508087 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.707528114 CEST	49714	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.707552910 CEST	49714	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.712243080 CEST	49722	443	192.168.2.6	89.187.165.7
May 4, 2021 21:52:45.713177919 CEST	49723	443	192.168.2.6	89.187.165.7
May 4, 2021 21:52:45.720473051 CEST	443	49716	95.211.139.76	192.168.2.6
May 4, 2021 21:52:45.720597029 CEST	49716	443	192.168.2.6	95.211.139.76
May 4, 2021 21:52:45.721455097 CEST	49716	443	192.168.2.6	95.211.139.76
May 4, 2021 21:52:45.722203970 CEST	443	49717	95.211.139.76	192.168.2.6
May 4, 2021 21:52:45.722312927 CEST	49717	443	192.168.2.6	95.211.139.76
May 4, 2021 21:52:45.723500967 CEST	49717	443	192.168.2.6	95.211.139.76
May 4, 2021 21:52:45.725869894 CEST	443	49721	89.187.165.8	192.168.2.6
May 4, 2021 21:52:45.725888968 CEST	443	49720	89.187.165.8	192.168.2.6
May 4, 2021 21:52:45.725960016 CEST	49721	443	192.168.2.6	89.187.165.8
May 4, 2021 21:52:45.726037025 CEST	49720	443	192.168.2.6	89.187.165.8
May 4, 2021 21:52:45.727102995 CEST	49721	443	192.168.2.6	89.187.165.8
May 4, 2021 21:52:45.727360964 CEST	49720	443	192.168.2.6	89.187.165.8
May 4, 2021 21:52:45.748728037 CEST	443	49722	89.187.165.7	192.168.2.6
May 4, 2021 21:52:45.748833895 CEST	49722	443	192.168.2.6	89.187.165.7
May 4, 2021 21:52:45.749176979 CEST	443	49723	89.187.165.7	192.168.2.6
May 4, 2021 21:52:45.749253988 CEST	49723	443	192.168.2.6	89.187.165.7
May 4, 2021 21:52:45.749561071 CEST	49722	443	192.168.2.6	89.187.165.7
May 4, 2021 21:52:45.749923944 CEST	49723	443	192.168.2.6	89.187.165.7
May 4, 2021 21:52:45.750225067 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.750248909 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.750264883 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.750282049 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.750297070 CEST	443	49714	18.194.109.194	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:52:45.750298023 CEST	49714	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.750318050 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.750319958 CEST	49714	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.750334978 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.750351906 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.750365019 CEST	49714	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.750368118 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.750384092 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.750391006 CEST	49714	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.750400066 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.750411034 CEST	49714	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.750415087 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.750431061 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.750442982 CEST	49714	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.750449896 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.750467062 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.750473976 CEST	49714	443	192.168.2.6	18.194.109.194
May 4, 2021 21:52:45.750483990 CEST	443	49714	18.194.109.194	192.168.2.6
May 4, 2021 21:52:45.750500917 CEST	443	49714	18.194.109.194	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:52:35.180538893 CEST	54513	53	192.168.2.6	8.8.8.8
May 4, 2021 21:52:35.241806984 CEST	53	54513	8.8.8.8	192.168.2.6
May 4, 2021 21:52:37.079054117 CEST	62044	53	192.168.2.6	8.8.8.8
May 4, 2021 21:52:37.121797085 CEST	63791	53	192.168.2.6	8.8.8.8
May 4, 2021 21:52:37.127762079 CEST	53	62044	8.8.8.8	192.168.2.6
May 4, 2021 21:52:37.181181908 CEST	53	63791	8.8.8.8	192.168.2.6
May 4, 2021 21:52:37.988540888 CEST	64267	53	192.168.2.6	8.8.8.8
May 4, 2021 21:52:38.037566900 CEST	53	64267	8.8.8.8	192.168.2.6
May 4, 2021 21:52:40.094664097 CEST	49448	53	192.168.2.6	8.8.8.8
May 4, 2021 21:52:40.143493891 CEST	53	49448	8.8.8.8	192.168.2.6
May 4, 2021 21:52:41.109123945 CEST	60342	53	192.168.2.6	8.8.8.8
May 4, 2021 21:52:41.161139011 CEST	53	60342	8.8.8.8	192.168.2.6
May 4, 2021 21:52:41.729099989 CEST	61346	53	192.168.2.6	8.8.8.8
May 4, 2021 21:52:41.933610916 CEST	53	61346	8.8.8.8	192.168.2.6
May 4, 2021 21:52:42.793939114 CEST	51774	53	192.168.2.6	8.8.8.8
May 4, 2021 21:52:42.842643023 CEST	53	51774	8.8.8.8	192.168.2.6
May 4, 2021 21:52:43.909099102 CEST	56023	53	192.168.2.6	8.8.8.8
May 4, 2021 21:52:43.967595100 CEST	53	56023	8.8.8.8	192.168.2.6
May 4, 2021 21:52:44.185235977 CEST	58384	53	192.168.2.6	8.8.8.8
May 4, 2021 21:52:44.238343954 CEST	53	58384	8.8.8.8	192.168.2.6
May 4, 2021 21:52:45.264508963 CEST	60261	53	192.168.2.6	8.8.8.8
May 4, 2021 21:52:45.326143980 CEST	53	60261	8.8.8.8	192.168.2.6
May 4, 2021 21:52:45.337804079 CEST	56061	53	192.168.2.6	8.8.8.8
May 4, 2021 21:52:45.387590885 CEST	53	56061	8.8.8.8	192.168.2.6
May 4, 2021 21:52:45.600625038 CEST	58336	53	192.168.2.6	8.8.8.8
May 4, 2021 21:52:45.607305050 CEST	53781	53	192.168.2.6	8.8.8.8
May 4, 2021 21:52:45.617609024 CEST	54064	53	192.168.2.6	8.8.8.8
May 4, 2021 21:52:45.640769005 CEST	52811	53	192.168.2.6	8.8.8.8
May 4, 2021 21:52:45.668538094 CEST	53	58336	8.8.8.8	192.168.2.6
May 4, 2021 21:52:45.675050974 CEST	53	53781	8.8.8.8	192.168.2.6
May 4, 2021 21:52:45.675873995 CEST	53	54064	8.8.8.8	192.168.2.6
May 4, 2021 21:52:45.709075928 CEST	53	52811	8.8.8.8	192.168.2.6
May 4, 2021 21:52:45.977682114 CEST	55299	53	192.168.2.6	8.8.8.8
May 4, 2021 21:52:46.039484978 CEST	53	55299	8.8.8.8	192.168.2.6
May 4, 2021 21:52:47.837779045 CEST	63745	53	192.168.2.6	8.8.8.8
May 4, 2021 21:52:47.886542082 CEST	53	63745	8.8.8.8	192.168.2.6
May 4, 2021 21:52:48.780472040 CEST	50055	53	192.168.2.6	8.8.8.8
May 4, 2021 21:52:48.829411983 CEST	53	50055	8.8.8.8	192.168.2.6
May 4, 2021 21:52:50.025861025 CEST	61374	53	192.168.2.6	8.8.8.8
May 4, 2021 21:52:50.083272934 CEST	53	61374	8.8.8.8	192.168.2.6
May 4, 2021 21:52:51.181265116 CEST	50339	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:52:51.230169058 CEST	53	50339	8.8.8.8	192.168.2.6
May 4, 2021 21:52:53.145299911 CEST	63307	53	192.168.2.6	8.8.8.8
May 4, 2021 21:52:53.194499969 CEST	53	63307	8.8.8.8	192.168.2.6
May 4, 2021 21:52:54.125835896 CEST	49694	53	192.168.2.6	8.8.8.8
May 4, 2021 21:52:54.174480915 CEST	53	49694	8.8.8.8	192.168.2.6
May 4, 2021 21:52:55.114291906 CEST	54982	53	192.168.2.6	8.8.8.8
May 4, 2021 21:52:55.163177013 CEST	53	54982	8.8.8.8	192.168.2.6
May 4, 2021 21:52:56.004842043 CEST	50010	53	192.168.2.6	8.8.8.8
May 4, 2021 21:52:56.056375027 CEST	53	50010	8.8.8.8	192.168.2.6
May 4, 2021 21:52:56.905102015 CEST	63718	53	192.168.2.6	8.8.8.8
May 4, 2021 21:52:56.955956936 CEST	53	63718	8.8.8.8	192.168.2.6
May 4, 2021 21:52:58.532438040 CEST	62116	53	192.168.2.6	8.8.8.8
May 4, 2021 21:52:58.586256981 CEST	53	62116	8.8.8.8	192.168.2.6
May 4, 2021 21:53:01.766747952 CEST	63816	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:01.823997021 CEST	53	63816	8.8.8.8	192.168.2.6
May 4, 2021 21:53:05.551525116 CEST	55014	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:05.612670898 CEST	53	55014	8.8.8.8	192.168.2.6
May 4, 2021 21:53:06.173854113 CEST	62208	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:06.177998066 CEST	57574	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:06.186069965 CEST	51818	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:06.189414024 CEST	56628	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:06.203919888 CEST	60778	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:06.226885080 CEST	53	57574	8.8.8.8	192.168.2.6
May 4, 2021 21:53:06.234081984 CEST	53	62208	8.8.8.8	192.168.2.6
May 4, 2021 21:53:06.247807026 CEST	53	51818	8.8.8.8	192.168.2.6
May 4, 2021 21:53:06.252616882 CEST	53	56628	8.8.8.8	192.168.2.6
May 4, 2021 21:53:06.261420965 CEST	53	60778	8.8.8.8	192.168.2.6
May 4, 2021 21:53:06.673530102 CEST	53799	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:06.737725019 CEST	53	53799	8.8.8.8	192.168.2.6
May 4, 2021 21:53:08.085237026 CEST	54683	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:08.145217896 CEST	53	54683	8.8.8.8	192.168.2.6
May 4, 2021 21:53:08.773221970 CEST	59329	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:08.834665060 CEST	53	59329	8.8.8.8	192.168.2.6
May 4, 2021 21:53:08.945614100 CEST	64021	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:08.952231884 CEST	56129	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:08.997596979 CEST	53	64021	8.8.8.8	192.168.2.6
May 4, 2021 21:53:09.041531086 CEST	53	56129	8.8.8.8	192.168.2.6
May 4, 2021 21:53:09.492098093 CEST	58177	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:09.552638054 CEST	53	58177	8.8.8.8	192.168.2.6
May 4, 2021 21:53:09.842360973 CEST	50700	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:09.892151117 CEST	53	50700	8.8.8.8	192.168.2.6
May 4, 2021 21:53:10.094986916 CEST	54069	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:10.095565081 CEST	61178	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:10.160665035 CEST	53	54069	8.8.8.8	192.168.2.6
May 4, 2021 21:53:10.177582026 CEST	53	61178	8.8.8.8	192.168.2.6
May 4, 2021 21:53:10.617420912 CEST	57017	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:10.700061083 CEST	53	57017	8.8.8.8	192.168.2.6
May 4, 2021 21:53:11.987194061 CEST	56327	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:12.050760031 CEST	53	56327	8.8.8.8	192.168.2.6
May 4, 2021 21:53:13.402019978 CEST	50243	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:13.453051090 CEST	53	50243	8.8.8.8	192.168.2.6
May 4, 2021 21:53:13.887995958 CEST	62055	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:13.937124968 CEST	53	62055	8.8.8.8	192.168.2.6
May 4, 2021 21:53:14.785948038 CEST	61249	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:14.835480928 CEST	53	61249	8.8.8.8	192.168.2.6
May 4, 2021 21:53:14.885354042 CEST	62055	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:14.934081078 CEST	53	62055	8.8.8.8	192.168.2.6
May 4, 2021 21:53:15.791148901 CEST	61249	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:15.849050045 CEST	53	61249	8.8.8.8	192.168.2.6
May 4, 2021 21:53:15.930834055 CEST	62055	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:15.979518890 CEST	53	62055	8.8.8.8	192.168.2.6
May 4, 2021 21:53:16.806665897 CEST	61249	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:16.863990068 CEST	53	61249	8.8.8.8	192.168.2.6
May 4, 2021 21:53:18.120158911 CEST	62055	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:53:18.168951988 CEST	53	62055	8.8.8.8	192.168.2.6
May 4, 2021 21:53:18.876082897 CEST	61249	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:18.926615000 CEST	53	61249	8.8.8.8	192.168.2.6
May 4, 2021 21:53:19.024039030 CEST	65252	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:19.082571030 CEST	53	65252	8.8.8.8	192.168.2.6
May 4, 2021 21:53:22.134913921 CEST	62055	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:22.183485031 CEST	53	62055	8.8.8.8	192.168.2.6
May 4, 2021 21:53:22.885144949 CEST	61249	53	192.168.2.6	8.8.8.8
May 4, 2021 21:53:22.936569929 CEST	53	61249	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 21:52:45.264508963 CEST	192.168.2.6	8.8.8.8	0x2f46	Standard query (0)	murphy-constructions.nicepage.io	A (IP address)	IN (0x0001)
May 4, 2021 21:52:45.600625038 CEST	192.168.2.6	8.8.8.8	0xde89	Standard query (0)	static.nicepage.com	A (IP address)	IN (0x0001)
May 4, 2021 21:52:45.607305050 CEST	192.168.2.6	8.8.8.8	0x847	Standard query (0)	capp.nicepage.com	A (IP address)	IN (0x0001)
May 4, 2021 21:52:45.640769005 CEST	192.168.2.6	8.8.8.8	0x427a	Standard query (0)	images02.nicepage.com	A (IP address)	IN (0x0001)
May 4, 2021 21:53:01.766747952 CEST	192.168.2.6	8.8.8.8	0x6404	Standard query (0)	favicon.ico	A (IP address)	IN (0x0001)
May 4, 2021 21:53:05.551525116 CEST	192.168.2.6	8.8.8.8	0x1328	Standard query (0)	fireanddust.com	A (IP address)	IN (0x0001)
May 4, 2021 21:53:06.177998066 CEST	192.168.2.6	8.8.8.8	0xe80a	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
May 4, 2021 21:53:06.186069965 CEST	192.168.2.6	8.8.8.8	0x703a	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
May 4, 2021 21:53:06.189414024 CEST	192.168.2.6	8.8.8.8	0x309	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
May 4, 2021 21:53:06.203919888 CEST	192.168.2.6	8.8.8.8	0x193a	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
May 4, 2021 21:53:06.673530102 CEST	192.168.2.6	8.8.8.8	0x491f	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
May 4, 2021 21:53:08.085237026 CEST	192.168.2.6	8.8.8.8	0x6a11	Standard query (0)	nicepage.com	A (IP address)	IN (0x0001)
May 4, 2021 21:53:08.773221970 CEST	192.168.2.6	8.8.8.8	0xc887	Standard query (0)	csite.nicepage.com	A (IP address)	IN (0x0001)
May 4, 2021 21:53:08.952231884 CEST	192.168.2.6	8.8.8.8	0x75ae	Standard query (0)	cdn.amplitude.com	A (IP address)	IN (0x0001)
May 4, 2021 21:53:09.492098093 CEST	192.168.2.6	8.8.8.8	0x1b73	Standard query (0)	d57e01lyo0mq2.cloudfront.net	A (IP address)	IN (0x0001)
May 4, 2021 21:53:09.842360973 CEST	192.168.2.6	8.8.8.8	0xb732	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
May 4, 2021 21:53:10.095565081 CEST	192.168.2.6	8.8.8.8	0x40d1	Standard query (0)	www.google.de	A (IP address)	IN (0x0001)
May 4, 2021 21:53:10.617420912 CEST	192.168.2.6	8.8.8.8	0x9b9f	Standard query (0)	csite.resource.nicepage.com	A (IP address)	IN (0x0001)
May 4, 2021 21:53:11.987194061 CEST	192.168.2.6	8.8.8.8	0xec6	Standard query (0)	images03.nicepage.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 21:52:45.326143980 CEST	8.8.8.8	192.168.2.6	0x2f46	No error (0)	murphy-constructions.nicepage.io		18.194.109.194	A (IP address)	IN (0x0001)
May 4, 2021 21:52:45.668538094 CEST	8.8.8.8	192.168.2.6	0xde89	No error (0)	static.nicepage.com		95.211.139.76	A (IP address)	IN (0x0001)
May 4, 2021 21:52:45.675050974 CEST	8.8.8.8	192.168.2.6	0x847	No error (0)	capp.nicepage.com	1156509985.rsc.cdn77.org		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:52:45.675050974 CEST	8.8.8.8	192.168.2.6	0x847	No error (0)	1156509985.rsc.cdn77.org		89.187.165.8	A (IP address)	IN (0x0001)
May 4, 2021 21:52:45.709075928 CEST	8.8.8.8	192.168.2.6	0x427a	No error (0)	images02.nicepage.com	1834444515.rsc.cdn77.org		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 21:52:45.709075928 CEST	8.8.8.8	192.168.2.6	0x427a	No error (0)	1834444515.rsc.cdn77.org		89.187.165.7	A (IP address)	IN (0x0001)
May 4, 2021 21:53:01.823997021 CEST	8.8.8.8	192.168.2.6	0x6404	Name error (3)	favicon.ico	none	none	A (IP address)	IN (0x0001)
May 4, 2021 21:53:05.612670898 CEST	8.8.8.8	192.168.2.6	0x1328	No error (0)	fireanddust.com		69.49.234.34	A (IP address)	IN (0x0001)
May 4, 2021 21:53:06.226885080 CEST	8.8.8.8	192.168.2.6	0xe80a	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:53:06.247807026 CEST	8.8.8.8	192.168.2.6	0x703a	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
May 4, 2021 21:53:06.247807026 CEST	8.8.8.8	192.168.2.6	0x703a	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
May 4, 2021 21:53:06.252616882 CEST	8.8.8.8	192.168.2.6	0x309	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:53:06.261420965 CEST	8.8.8.8	192.168.2.6	0x193a	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
May 4, 2021 21:53:06.261420965 CEST	8.8.8.8	192.168.2.6	0x193a	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
May 4, 2021 21:53:06.737725019 CEST	8.8.8.8	192.168.2.6	0x491f	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:53:08.145217896 CEST	8.8.8.8	192.168.2.6	0x6a11	No error (0)	nicepage.com		95.211.139.76	A (IP address)	IN (0x0001)
May 4, 2021 21:53:08.834665060 CEST	8.8.8.8	192.168.2.6	0xc887	No error (0)	csite.nicepage.com	1163043995.rsc.cdn77.org		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:53:08.834665060 CEST	8.8.8.8	192.168.2.6	0xc887	No error (0)	1163043995.rsc.cdn77.org		89.187.165.8	A (IP address)	IN (0x0001)
May 4, 2021 21:53:09.041531086 CEST	8.8.8.8	192.168.2.6	0x75ae	No error (0)	cdn.amplitude.com		13.32.23.71	A (IP address)	IN (0x0001)
May 4, 2021 21:53:09.041531086 CEST	8.8.8.8	192.168.2.6	0x75ae	No error (0)	cdn.amplitude.com		13.32.23.136	A (IP address)	IN (0x0001)
May 4, 2021 21:53:09.041531086 CEST	8.8.8.8	192.168.2.6	0x75ae	No error (0)	cdn.amplitude.com		13.32.23.160	A (IP address)	IN (0x0001)
May 4, 2021 21:53:09.041531086 CEST	8.8.8.8	192.168.2.6	0x75ae	No error (0)	cdn.amplitude.com		13.32.23.194	A (IP address)	IN (0x0001)
May 4, 2021 21:53:09.552638054 CEST	8.8.8.8	192.168.2.6	0x1b73	No error (0)	d57e01lyo0mq2.cloudfront.net		13.32.23.99	A (IP address)	IN (0x0001)
May 4, 2021 21:53:09.552638054 CEST	8.8.8.8	192.168.2.6	0x1b73	No error (0)	d57e01lyo0mq2.cloudfront.net		13.32.23.72	A (IP address)	IN (0x0001)
May 4, 2021 21:53:09.552638054 CEST	8.8.8.8	192.168.2.6	0x1b73	No error (0)	d57e01lyo0mq2.cloudfront.net		13.32.23.64	A (IP address)	IN (0x0001)
May 4, 2021 21:53:09.552638054 CEST	8.8.8.8	192.168.2.6	0x1b73	No error (0)	d57e01lyo0mq2.cloudfront.net		13.32.23.209	A (IP address)	IN (0x0001)
May 4, 2021 21:53:09.892151117 CEST	8.8.8.8	192.168.2.6	0xb732	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:53:09.892151117 CEST	8.8.8.8	192.168.2.6	0xb732	No error (0)	stats.l.doubleclick.net		74.125.133.156	A (IP address)	IN (0x0001)
May 4, 2021 21:53:09.892151117 CEST	8.8.8.8	192.168.2.6	0xb732	No error (0)	stats.l.doubleclick.net		74.125.133.155	A (IP address)	IN (0x0001)
May 4, 2021 21:53:09.892151117 CEST	8.8.8.8	192.168.2.6	0xb732	No error (0)	stats.l.doubleclick.net		74.125.133.157	A (IP address)	IN (0x0001)
May 4, 2021 21:53:09.892151117 CEST	8.8.8.8	192.168.2.6	0xb732	No error (0)	stats.l.doubleclick.net		74.125.133.154	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 21:53:10.177582026 CEST	8.8.8.8	192.168.2.6	0x40d1	No error (0)	www.google.de		142.250.185.227	A (IP address)	IN (0x0001)
May 4, 2021 21:53:10.700061083 CEST	8.8.8.8	192.168.2.6	0x9b9f	No error (0)	csite.resource.nicepage.com	1238657323.rsc.cdn77.org		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:53:10.700061083 CEST	8.8.8.8	192.168.2.6	0x9b9f	No error (0)	1238657323.rsc.cdn77.org		89.187.165.7	A (IP address)	IN (0x0001)
May 4, 2021 21:53:12.050760031 CEST	8.8.8.8	192.168.2.6	0xec6	No error (0)	images03.nicepage.com	1487879380.rsc.cdn77.org		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:53:12.050760031 CEST	8.8.8.8	192.168.2.6	0xec6	No error (0)	1487879380.rsc.cdn77.org		89.187.165.7	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 4, 2021 21:52:45.437232018 CEST	18.194.109.194	443	192.168.2.6	49714	CN=*.nicepage.io, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Feb 17 16:46:40 CET 2021 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014	Mon Mar 21 16:46:40 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
May 4, 2021 21:52:45.445738077 CEST	18.194.109.194	443	192.168.2.6	49713	CN=*.nicepage.io, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Feb 17 16:46:40 CET 2021 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014	Mon Mar 21 16:46:40 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 21:52:45.763767004 CEST	89.187.165.8	443	192.168.2.6	49721	CN=1156509985.rsc.cdn77.org CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Apr 14 09:14:50 CEST 2021	Tue Jul 13 09:14:50 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 4, 2021 21:52:45.764287949 CEST	89.187.165.8	443	192.168.2.6	49720	CN=1156509985.rsc.cdn77.org CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Apr 14 09:14:50 CEST 2021	Tue Jul 13 09:14:50 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 4, 2021 21:52:45.786742926 CEST	89.187.165.7	443	192.168.2.6	49722	CN=1834444515.rsc.cdn77.org CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat May 01 12:19:31 CEST 2021	Fri Jul 30 12:19:31 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 4, 2021 21:52:45.786921024 CEST	89.187.165.7	443	192.168.2.6	49723	CN=1834444515.rsc.cdn77.org CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat May 01 12:19:31 CEST 2021	Fri Jul 30 12:19:31 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 4, 2021 21:53:05.936166048 CEST	69.49.234.34	443	192.168.2.6	49740	CN=fireanddust.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue May 04 02:00:00 CEST 2021	Tue Aug 03 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
							Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
May 4, 2021 21:53:05.936315060 CEST	69.49.234.34	443	192.168.2.6	49741	CN=fireanddust.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue May 04 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Tue Aug 03 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
May 4, 2021 21:53:06.360188961 CEST	104.18.10.207	443	192.168.2.6	49750	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 4, 2021 21:53:06.360982895 CEST	104.18.10.207	443	192.168.2.6	49751	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 4, 2021 21:53:06.381593943 CEST	104.16.19.94	443	192.168.2.6	49755	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 21:53:06.382924080 CEST	104.16.19.94	443	192.168.2.6	49754	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 4, 2021 21:53:08.919872999 CEST	89.187.165.8	443	192.168.2.6	49760	CN=1163043995.rsc.cdn77.org CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Apr 14 09:14:52 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Jul 13 09:14:52 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 4, 2021 21:53:08.919918060 CEST	89.187.165.8	443	192.168.2.6	49762	CN=1163043995.rsc.cdn77.org CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Apr 14 09:14:52 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Jul 13 09:14:52 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 4, 2021 21:53:08.920017004 CEST	89.187.165.8	443	192.168.2.6	49761	CN=1163043995.rsc.cdn77.org CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Apr 14 09:14:52 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Jul 13 09:14:52 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 4, 2021 21:53:09.143898964 CEST	13.32.23.71	443	192.168.2.6	49765	CN=cdn.amplitude.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 Nov 18 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Dec 18 00:59:59 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 4, 2021 21:53:09.152522087 CEST	13.32.23.71	443	192.168.2.6	49766	CN=cdn.amplitude.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 Nov 18 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Dec 18 00:59:59 CET 2021 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 4, 2021 21:53:09.641525984 CEST	13.32.23.99	443	192.168.2.6	49767	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 4, 2021 21:53:09.641875982 CEST	13.32.23.99	443	192.168.2.6	49768	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 4, 2021 21:53:10.001624107 CEST	74.125.133.156	443	192.168.2.6	49769	CN=*.g.doubleclick.net, 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 12:11:12 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:11:11 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		
May 4, 2021 21:53:10.003920078 CEST	74.125.133.156	443	192.168.2.6	49770	CN=*.g.doubleclick.net, 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 12:11:12 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:11:11 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		
May 4, 2021 21:53:10.781812906 CEST	89.187.165.7	443	192.168.2.6	49776	CN=1238657323.rsc.cdn77.org CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Apr 14 07:14:48 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Jul 13 07:14:48 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 21:53:10.782293081 CEST	89.187.165.7	443	192.168.2.6	49775	CN=1238657323.rsc.cdn77.org CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Apr 14 07:14:48 CEST 2021	Tue Jul 13 07:14:48 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 4, 2021 21:53:12.125647068 CEST	89.187.165.7	443	192.168.2.6	49778	CN=1487879380.rsc.cdn77.org CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Apr 16 07:17:50 CEST 2021	Thu Jul 15 07:17:50 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 4, 2021 21:53:12.126075029 CEST	89.187.165.7	443	192.168.2.6	49777	CN=1487879380.rsc.cdn77.org CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Apr 16 07:17:50 CEST 2021	Thu Jul 15 07:17:50 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5440 Parent PID: 792

General

Start time:	21:52:42
Start date:	04/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff721e20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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: 5752 Parent PID: 5440

General

Start time:	21:52:43
Start date:	04/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5440 CREDAT:17410 /prefetch:2
Imagebase:	0x1080000
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