ID: 356142
Cookbook: browseurl.jbs
Time: 16:30:55
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

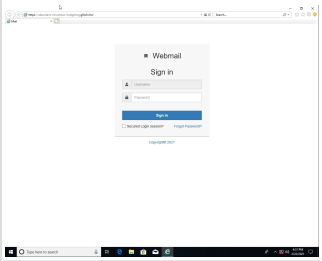
Analysis Report https://abundant-chivalrous-hedgehog....

Overview

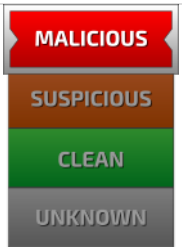
General Information

Sample URL:	http://https://abundant-chivalrous-hedgehog.glitch.me/
Analysis ID:	356142

Most interesting Screenshot:



Detection



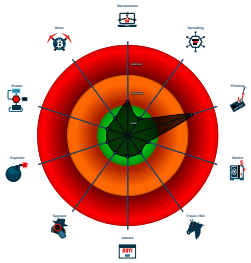
HTMLPhisher

Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected HtmlPhish_10
- Form action URLs do not match mai…
- HTML body contains low number of …
- Invalid 'forgot password' link found
- No HTML title found
- Suspicious form URL found

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 4368 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4532 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4368 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

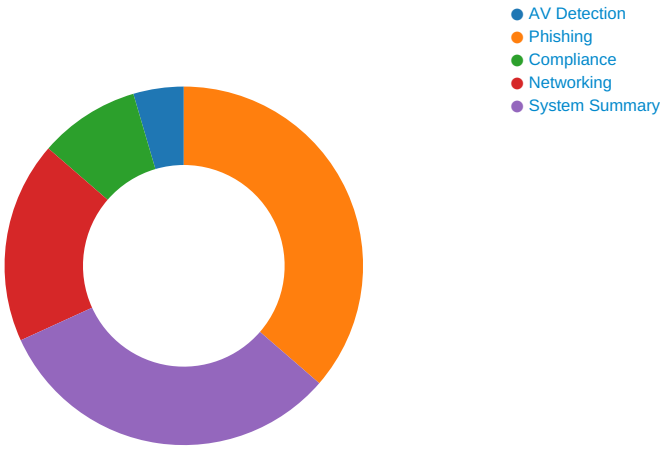
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\3YFB622I.htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Phishing:

Yara detected HtmlPhish_10

Compliance:

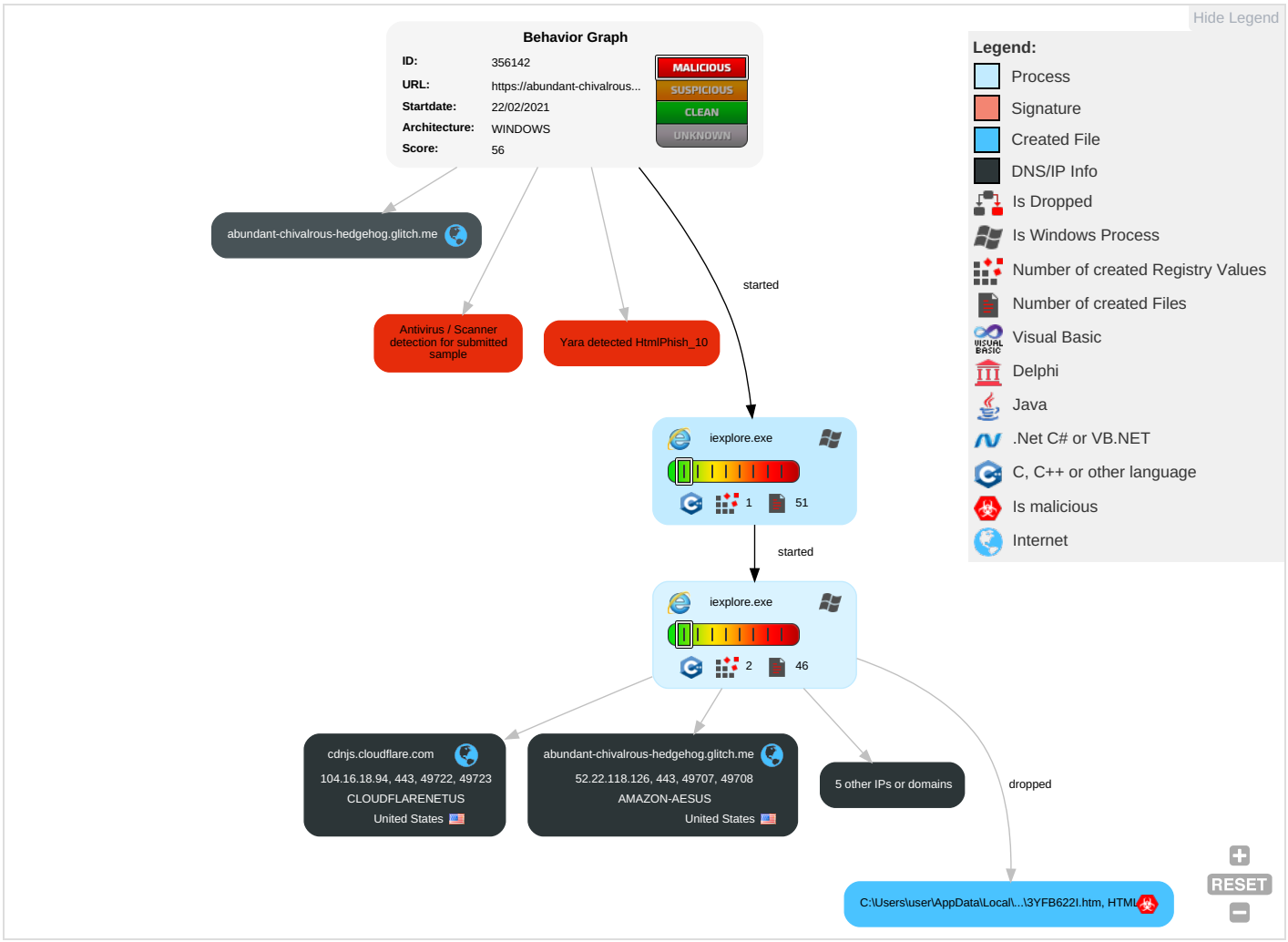
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

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 1	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

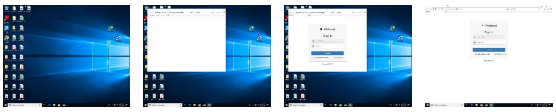
Behavior Graph

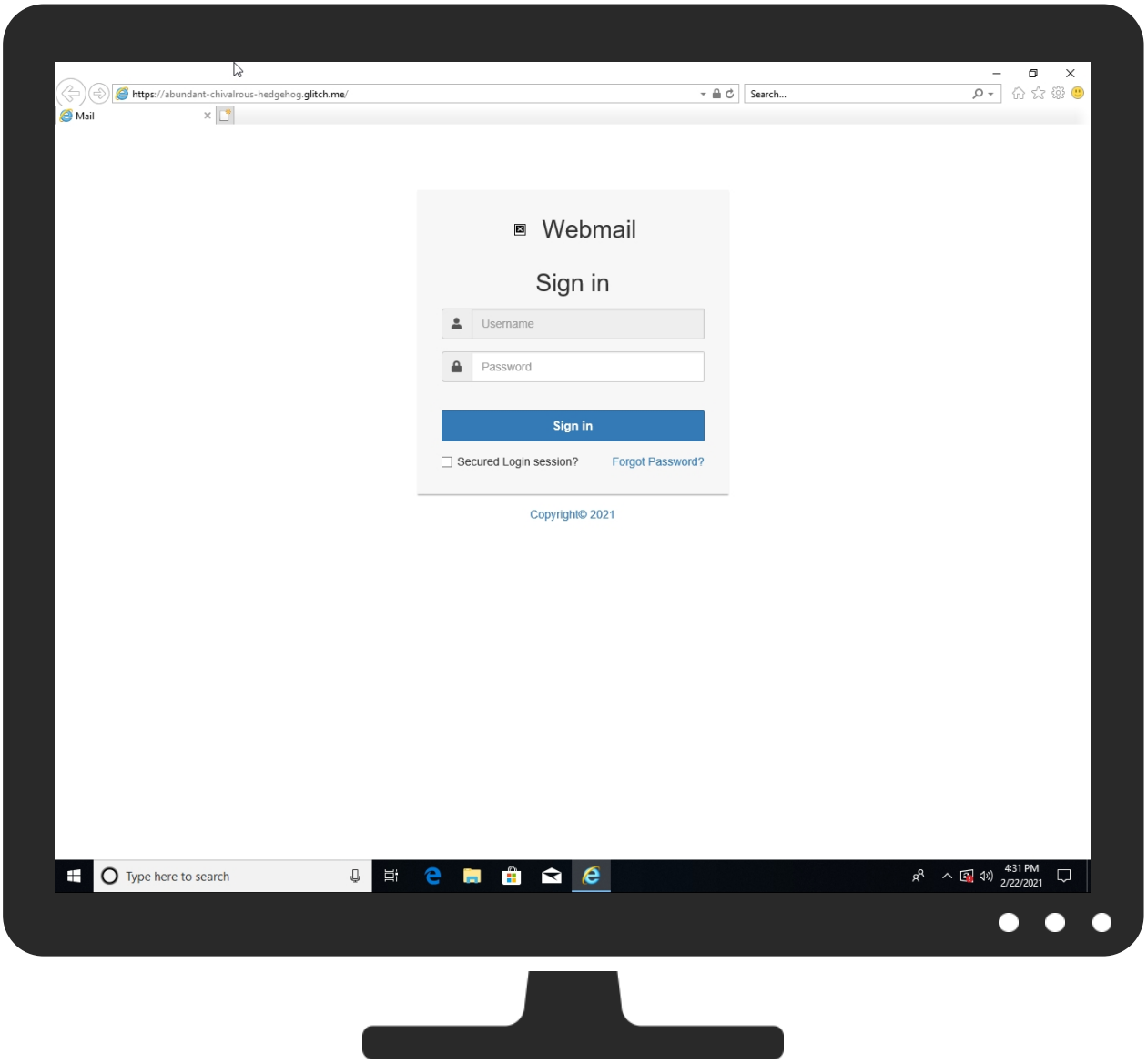


Screenshots

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://abundant-chivalrous-hedgehog.glitch.me/	2%	Virustotal		Browse
http://https://abundant-chivalrous-hedgehog.glitch.me/	0%	Avira URL Cloud	safe	
http://https://abundant-chivalrous-hedgehog.glitch.me/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
http://https://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://https://valvulasthermovalve.cl/wpxmp/index.php	0%	Avira URL Cloud	safe	
http://https://fontawesome.comhttps://fontawesome.comFont	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdnjs.cloudflare.com	104.16.18.94	true	false		high
abundant-chivalrous-hedgehog.glitch.me	52.22.118.126	true	false		high
stackpath.bootstrapcdn.com	unknown	unknown	false		high
ka-f.fontawesome.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high
maxcdn.bootstrapcdn.com	unknown	unknown	false		high

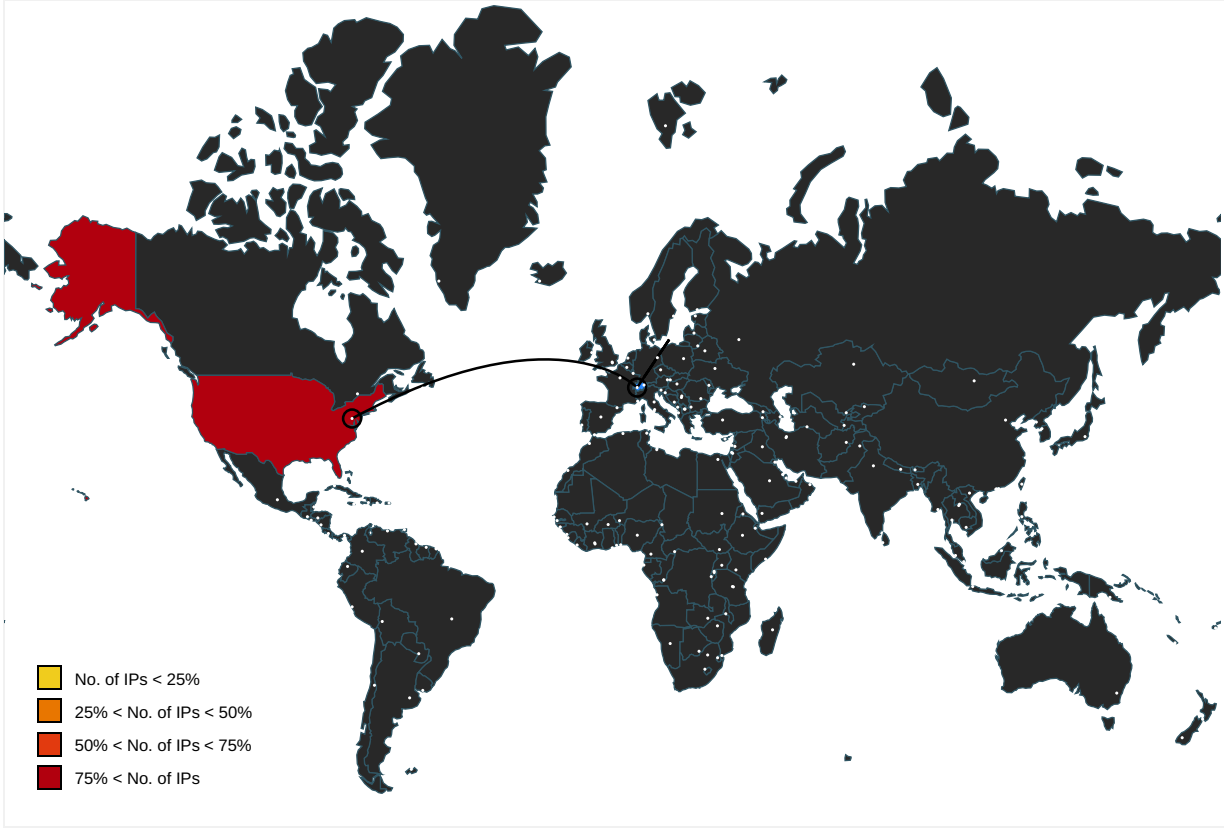
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://abundant-chivalrous-hedgehog.glitch.me/	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://fontawesome.com	free-fa-regular-400[1].eot.3.dr, free.min[1].css.3.dr	false		high
http://https://kit.fontawesome.com	585b051251[1].js.3.dr	false		high
http://https://github.com/twbs/bootstrap/graphs/contributors)	bootstrap.min[1].js.3.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js	3YFB622I.htm.3.dr	false		high
http://https://getbootstrap.com)	bootstrap.min[1].js.3.dr	false	• Avira URL Cloud: safe	low
http://https://abundant-chivalrous-hedgehog.glitch.me/	~DFDD73DA9B157391E8.TMP.2.dr	false		high
http://https://ka-f.fontawesome.com	585b051251[1].js.3.dr	false		high
http://https://code.jquery.com/jquery-3.2.1.slim.min.js	3YFB622I.htm.3.dr	false		high
http://https://code.jquery.com/jquery-3.1.1.min.js	3YFB622I.htm.3.dr	false		high
http://getbootstrap.com)	3YFB622I.htm.3.dr	false	• Avira URL Cloud: safe	low
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	3YFB622I.htm.3.dr, bootstrap.min[1].js.3.dr	false		high
http://https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js	3YFB622I.htm.3.dr	false		high
http://https://valvulasthermovalve.cl/wpxmp/index.php	3YFB622I.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://opensource.org/licenses/MIT).	popper.min[1].js.3.dr	false		high
http://https://kit.fontawesome.com/585b051251.js	3YFB622I.htm.3.dr	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js	3YFB622I.htm.3.dr	false		high
http://https://getbootstrap.com/)	bootstrap.min[1].js0.3.dr	false		high
http://https://fontawesome.comhttps://fontawesome.comFont	free-fa-regular-400[1].eot.3.dr, free-fa-solid-900[1].eot.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://abundant-chivalrous-hedgehog.glitch.me/Root	{7DA4CA46-756E-11EB-90E5-ECF4BB570DC9}.dat.2.dr	false		high
http://https://code.jquery.com/jquery-3.3.1.js	3YFB622I.htm.3.dr	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css	3YFB622I.htm.3.dr	false		high
http://https://fontawesome.com/license/free	free.min[1].css.3.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.22.118.126	unknown	United States		14618	AMAZON-AESUS	false
104.16.18.94	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356142
Start date:	22.02.2021
Start time:	16:30:55
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://abundant-chivalrous-hedgehog.glitch.me/
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:	8
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:	mal56.phis.win@3/19@8/2
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 93.184.220.29, 52.255.188.83, 51.103.5.159, 51.104.139.180, 52.147.198.201, 13.64.90.137, 104.42.151.234, 88.221.62.148, 92.122.145.220, 142.250.185.138, 209.197.3.24, 142.250.185.202, 104.18.22.52, 104.18.23.52, 209.197.3.15, 172.64.202.28, 172.64.203.28, 184.30.24.56 • Excluded domains from analysis (whitelisted): cds.s5x3j6q5.hwcdn.net, cs9.wac.phicdn.net, arc.msn.com.nsatc.net, ka-f.fontawesome.com.cdn.cloudflare.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, go.microsoft.com, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, www.bing.com, kit.fontawesome.com.cdn.cloudflare.net, client.wns.windows.com, skypedataprdcolwus17.cloudapp.net, fonts.googleapis.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ajax.googleapis.com, e1723.g.akamaiedge.net, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, cds.j3z9t3p6.hwcdn.net, skypedataprdcolwus16.cloudapp.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{7DA4CA44-756E-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8473470094036497
Encrypted:	false
SSDEEP:	96:rHZMZul2jWuztZbfrslxKMwdxqcPxQlxfRsqx6X:rHZMZ82jW2tdfrBMzTDfRMX
MD5:	3420C688BCF552B9AE76923F3F7FCD46
SHA1:	F6C706234D4C966FE6151EC8EB3B78B610DB5F82
SHA-256:	DDBA7299E631BF05CF885F9D524FAAF11A4278BAEE5ED9B67B1AF9EE44EC7C34
SHA-512:	36C0FC576C3C1A3A94BB74DF4737F6F0AAD8AAE99E498D4940096822A0ADDDA0C81C3D528A63B6F7FE41603F7227A0F7CE489ED7E256E3AB6809E1212EBD3E FF
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\{7DA4CA46-756E-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27730
Entropy (8bit):	1.812511282304039
Encrypted:	false
SSDEEP:	48:Iw7GcprGGwpamG4pQihGrapbSUGQpBfWGHHpcHTGUp8VUGzYpmC7GopZ0mNEvG+X:rhZeQW6ixBSMjfV2RWVQM2vq0SOE9tr
MD5:	06CD2A984DFACBD10BAA8E5F1C3B3351
SHA1:	F4AD663B60466ADBF1F1A62C87C507FB97C75F2E
SHA-256:	D56F4826633FFD6C923E47A3C6C03E2081878C59D5CC4574030F9B7C2D03018E
SHA-512:	9EA9D3DE37EAD59B62EF0B5F84A016DFBB03726F9DC0FCF7186C55DDD1885DC6BD8669E17AF3FB9D32231A90D06756F61D77B43B5BE0CDD3A63B1273518DA 33
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\{7DA4CA47-756E-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5620116672067232
Encrypted:	false
SSDEEP:	48:IwRGcprYGwpalG4pQpGrapbSFGQpKLG7HpRiTGIpG:rnZAQ36JBSvAKT2A
MD5:	D92AC4C57CE9B0BDC2A6EAFB8457C4C4
SHA1:	B022B6471DFC091961982FB5366D13BC991B7234
SHA-256:	1F8968376F62ADAD481AB53E3B3B316A1A2A43DD79DC96A5F1E172CE0D242B44
SHA-512:	5E22437836626C95BFE4AEFDE7ABBEB850975774E7A0273B51D6BC83410B9521E8C1D6F36C796337D43889592207A42D35B92D6AB60A44B5CA88C2E02559C409
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r. y.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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"),requir e("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.pro totype.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\4PB7FJMT\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	223
Entropy (8bit):	5.142612311542767
Encrypted:	false
SSDEEP:	6:0IFFDK+Q+56ZRWHMqh7izlpdRSRk68k3tg9EFNin:jFI+QO6ZRoMqt6p3Tk9g9CY
MD5:	72C5D331F2135E52DA2A95F7854049A3
SHA1:	572F349BB65758D377CCBAE434350507341ACD7B
SHA-256:	C3A12D7E8F6B2B1F5E4CD0C9938DFC79532AEF90802B424EE910093F156586DA
SHA-512:	9EA12CC277C9858524083FEBBE1A3E61FDECE5268F63B14C9FFAFE29396C7CCDB3B07BE10E829936BCCD8F3B9E39DCFA6BC4316F189E4CEA914F1D06916DB 66B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Archivo+Narrow&display=swap
Preview:	@font-face {. font-family: 'Archivo Narrow';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/archivonarrow/v12/tss 0ApVBdCYD5Q7hcxTE1ArZ0bbwiXo.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\3YFB622I.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	144732
Entropy (8bit):	5.452333629536582
Encrypted:	false
SSDEEP:	768:Zdy3Gxw/Vc/QWlJxtQOIuiHlq5mzI4X8OAduFKbv2ctg2Bd8JP7ecQVvH1FLRfkl:xw/a1fluiHlq5mN8lDbNmPbbyP1R0
MD5:	4904A2876C4D803200D421CCCD8FB04F
SHA1:	99C80A176C6A832F71AB3CE6E54F2C90A921DBD2
SHA-256:	36065137A28B0771079E7DE9FA7F2BB55C0F9990342DDF5A1055173BD3BB8EE5
SHA-512:	D79D37994991EE58E9B0BF1725C0115680AC2808EF394654C6FF4F7CEF4DE51DC238DBBD34FA661691C58875107B88C83DFE929E01DE40E0EF9FBF852363C06
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\3YFB622I.htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://abundant-chivalrous-hedgehog.glitch.me/
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.co m/jquery-3.1.1.min.js">. <script src="https://code.jquery.com/jquery-3.3.1.js" integrity="sha256-2Kok7MbOyxpgUVvAk/HJ2jigOSYS2auK4Pfzbm7uH60=" crossorigin="a nonymous"></script>. Required meta tags -->. <meta charset="utf-8">. <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">. <link rel="icon" type="image/png" sizes="192x192" class="logoimg" href="">.. Bootstrap CSS -->. <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com /bootstrap/4.0.0/css/bootstrap.min.css" integrity="sha384-Gn5384xqQ1aoWXA+058RXPxPg6fy4IWvTNh0E263XmFcJlSAwiGgFAW/dAiS6JXm" crossorigin="ano nymous"> -->. <link href="https://fonts.googleapis.com/css?family=Archivo+Narrow&display=swap" rel="stylesheet">. <script src="https://kit.fontawesome.com /585b051251.js" crossori

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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):	51039
Entropy (8bit):	5.247253437401007
Encrypted:	false
SSDEEP:	768:E9Yw7GuJM+HV0cen/7Kh5rM7V4RxCKg8FW/xsXQUd+FiID65r48Hgp5HRl+:E9X7PMIM7V4R5LFAxTWyuHHgp5HRl+
MD5:	67176C242E1BDC20603C878DEE836DF3
SHA1:	27A71B00383D61EF3C489326B3564D698FC1227C
SHA-256:	56C12A125B021D21A69E61D7190CEFA168D6C28CE715265CEA1B3B0112D169C4
SHA-512:	9FA75814E1B9F7DB38FE61A503A13E60B82D83DB8F4CE30351BD08A6B48C0D854BAF472D891AF23C443C8293380C2325C7B3361B708AF9971AA0EA09A25CDD0A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v4.1.3 (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,h){"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 l(r){for(var t=1;t<arguments.length;t++){var o=null!=arguments[t]?arguments[t]:{},e=Object.keys(o);"function"==typeof Object.getOwnPropertySymbols&&(e=e.concat(Object.getOwnPropertySymbols(o).filter(function(t){return Object.getOwnPropertyDescriptor(o,t).enum

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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):	4.82979949483045
Encrypted:	false
SSDEEP:	192:SP6hT1bIl4w0QUmQ10PwKLaAu5CwWavpHo4O6wgLPbJVR8XD7mycP:5hal4w0QK+PwK05eavpmgPPeXD7mycP
MD5:	1848E71668F42835079E5FA2AF6CF4A8
SHA1:	6AE345E2FEB8C2A524E7CF9E22A3A87BAEE60593
SHA-256:	D7CC3C57F9BDA4C6DCB83BB3C19F2F2AA86ECEC6274E243CD4EC315AE8E30101
SHA-512:	24E0AF4EC32A9AAB61D9E1AF9B2083F2D13CC98961B5E32BB613A02FEEF63F5F30C3B21C6308A4A204D981D77C86F09E221D0DB7B051A3538ACE07E727F29F58
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.2/css/free-v4-shims.min.css?token=585b051251
Preview:	/*!. * Font Awesome Free 5.15.2 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 Free";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{content:"\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\B87Z87FM\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):	4.728636851806783
Encrypted:	false
SSDEEP:	768:5Uh31IPiyXNq4YxBowbgJlkwF//zMQyYJYX9Bft6VSz8:5U0PxXE4YXJgndFTfy9lt5Q
MD5:	4ECC071B77D6B1790FA9FB8A5173F972
SHA1:	B44FCBAAC4F3AA7381D71DE20064AC84B0B729D1
SHA-256:	8C7BBA7DEB64FF95E98F7AC8CD0D3B675A4BCF02F302E57EDC5A1D6FA3D6CF94
SHA-512:	7CC1D04078B5917269025B6F37C7DDD83A0A5A0C5840E2A6E99ADFE2FB3E2242C626F25315480ADCD725C855AD2881DDF672B6FC1D793377C2D16FF38EAF69
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.2/css/free.min.css?token=585b051251
Preview:	/*!. * Font Awesome Free 5.15.2 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\B87Z87FM\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\NUEPGTR9\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:	53A2B560B20551672FBB0E6E72632D4FD1C7E2DD2ECF7337EBAAAB179CB8BE7C87E9D803CE7765706BC7FCBCF993C34587CD1237DE5A279AEA19911D69067B65
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\NUEPGTR9\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:qNhEyjjTikEJO4edXXe9J578go6MWX2xkjVe4c4j2ll2Ac7pK3F71QDU8CuT:Exc2yjq4j2uYnQDU8CuT
MD5:	5F48FC77CAC90C4778FA24EC9C57F37D
SHA1:	9E89D1515BC4C371B86F4CB1002FD8E377C1829F
SHA-256:	9365920887B11B33A3DC4BA28A0F93951F200341263E3B9CEFD384798E4BE398
SHA-512:	CAB8C4AFA1D8E3A8B7856EE29AE92566D44CEEAD70C8D533F2C98A976D77D0E1D314719B5C6A473789D8C6B21EBB4B89A6B0EC2E1C9C618FB1437EBC77D3A269
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-3.2.1.slim.min.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\PEJLKQA8\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):	5.182477446178365
Encrypted:	false
SSDEEP:	192:BBHN42S+9SZRvACpiIthFzoXnemF+shSGnZ+PPxQDqv7jh81Q5l8OcchIlzbCn:HRCfhFzevnEZ/h81Q5l8OsE
MD5:	4B900F0AF3BBDA85E1077C8EC8C83831
SHA1:	7E7015965195F25AFA3A47BE2108278AD6A0A4AC
SHA-256:	7943D6D067DB8587E9FB675F0D2CC78D6C90C91B187CF8642A3F52FF91381685
SHA-512:	2CD82E0DCD1381447522CFFD6101365133323E5D2980FAE730801FE8BBA580FF7FDF9CB8D2E9AC794D6F2FB59C724EDA71BECE7CAA72C775BC963E1A54B30E CB
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.fo ntawesome.com","detectConflictsUntil":null,"iconUploads":{},"id":132286382,"license":"free","method":"css","minify":{"enabled":true},"token":"585b051251","v4Fon tFaceShim":{"enabled":false},"v4shim":{"enabled":true},"version":"5.15.2"};.!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,writ able:!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\PEJLKQA8\free-fa-regular-400[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Font Awesome 5 Free Regular family
Category:	downloaded
Size (bytes):	34350
Entropy (8bit):	6.319416398409097
Encrypted:	false
SSDEEP:	384:2TILSQt3owpXUazLuDULbNVTH/oOkKQB3I+89AyI6WcRwkw8cQUtR:2ULSe3yy6DOP/oDB29uc5w8cQUL
MD5:	73570FCA80D5237954C19C20BDA58A70
SHA1:	E27F09071CA6B858A1B96B1CD02B2B34BCE85178
SHA-256:	75BAC9C568E4B2DF8C25F96513A92FA4740D4B11E58FB0ADB88E2F4DADC7FFCD
SHA-512:	60632D9B3893631C82FDC7D56741A8EFA52BA9333BF4FECA083330B9B1454CC6F4A1AEEDF621EBF92CFF634A0BA91F4EB1F0DF6009A69C6BD14A0A39908E8B 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.2/webfonts/free-fa-regular-400.eot?
Preview:	.....LP.....w.....6.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .R.e.g.u.l.a.r.....R.e.g.u.l.a.r...L.3.3.1...5.2.2. .(.F.o.n.t. .A.w.e.s.o.m.e. .v.e.r. s.i.o.n.:. .5...1.5...2.)...6.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .R.e.g.u.l.a.r.....PFFTM.4.....GDEF.*.....OS/2A.S....X...`cmap.....gasp.....glyf|.7.... ..n.head.& .....6hhea.5.....$hmtx...t.....Tloca.e.....6maxp.....8... name9.;"..w....[post.iA...}.....K...w._.<.....$.Z.....$.`..... ..@.....L.f...G.L.f.....PfEd.....T.....:..... .....@.....@.....@.....@.....@...@.....@...@..... .....`.....@.....@.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\free-fa-solid-900[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Font Awesome 5 Free Solid family
Category:	downloaded
Size (bytes):	204814
Entropy (8bit):	6.343269877413605
Encrypted:	false
SSDEEP:	6144:9t+zd6McnODzpN2BDXTIRSwRKSK3NC59M4:iELnODze58Rjg+5b
MD5:	AD5381B40F2857CE48DC73585FC92294
SHA1:	B404BB9916EDFD272560C27CFD09C032EC9F9B96
SHA-256:	2D45F4A3844BEFB918111DF65049A4FA71577D5E8FF009934B62E647E4702AB0
SHA-512:	69409725FE954403937CA22F5CDE811574FA2EBDBE24BF7CD5566826259A2427692251BFC90E663696C6A425F6C2DB95C8946495B4A5228B3BA8FEA10F79C2F5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.2/webfonts/free-fa-solid-900.eot?
Preview:	. .....LP.....F.....2.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .S.o.l.i.d.....S.o.l.i.d...L.3.3.1...5.2.2. .(.F.o.n.t. .A.w.e.s.o.m.e. .v.e.r.s.i.o.n.:. .5...1. 5...2.)...2.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .S.o.l.i.d.....PFFTM.4.....GDEF.*.....OS/23.V`...X...`cmap.j.4...h....gasp.....glyfh.....-....dhead.4.....6hhea.C.-... ....$hmtx.Q.....loca.....8....maxp.N.`...8... name#./....P...+post..Fa...|..1.....K..F...._.<.....$.\....$.`.....]. .....@..... L.f...G.L.f.....PfEd.....T.....:..... .....@.....@. .....@.....@..... @.....`.....@.....@.....@.....@....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\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
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\Temp\~DFDD73DA9B157391E8.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	35491
Entropy (8bit):	0.5071976319420638
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+j9PGCICT0mNEDQNE5cQNEGNEgNEjNE/0E9:kBqoxKAuvScS+j9PGNSyOE9
MD5:	626D7202C1A82CF618D35C8F11524951
SHA1:	B590EAF5CEB369B46716EBE362507001CA541606
SHA-256:	274D0208D5EE1A22CEAC5B80F167E19AF8F5B6A578379CE8305F7830088384B0
SHA-512:	D876B47100201C9639509383165C825886F82D3B91CC34F6DB5E240C3C0EBD21AA34172C9A29CCFE7EC1D333130DD9B0A1D3F48748E701FF4AEC7B3C1EC6AE2
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFDFF883BFB1B0276F.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4793734107392196
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fRvI9l8fRvY9lTqvD1CDi1efXecX/iX/p:c9lLh9lLh9lIn9lIn9loQ9log9lWYPaB
MD5:	CC556D0FD2F6FA93A8D2291C1B64A93E
SHA1:	07A317740C5308A1B9F363BD85978C1A3A360586
SHA-256:	72B4B597C9D7EACAF63DDA6126DFA6EC75168C0089D411C573E41F084FFD01FA
SHA-512:	A7D4AD463FFD71CCF9D1AC07B66FF84822C6A2BFAABFC315F9D8C9BB107DF25400839B3846DCBB8B13030B2ED409AB371319C74B457152F84E5DD71E2737303
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFEA48C588E0A2E738.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped

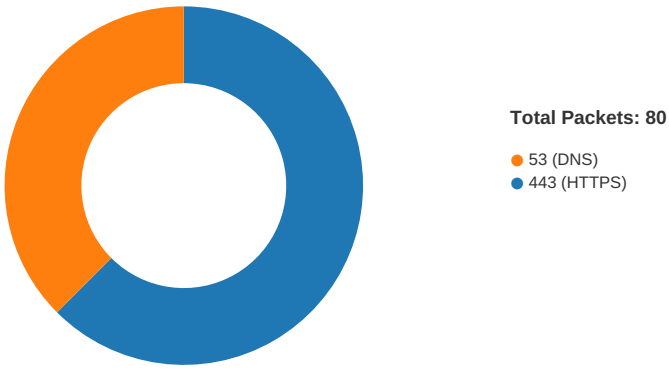
C:\Users\user\AppData\Local\Temp\~DFEA48C588E0A2E738.TMP	
Size (bytes):	25441
Entropy (8bit):	0.2977403157331066
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA+mml:kBqoxxJhHWSVSEab+
MD5:	054FBD285767F0A92295ADC313A9D5A3
SHA1:	CC621C016B7CA5DA0CB72C288B623C9628E38BDD
SHA-256:	BA024EB78232AB58864112ACB00D58B4CDADCA1AE02FC0B7F2233F9C823261AB
SHA-512:	C73D33EF85BE8887590BF0005345ABB3AC03B8E34A8992C7D954A7DF50A46609866C178BB7CBA7491F2678928145D18A196DEED845D05367B6F87C6E6A47FFB
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 16:31:40.418378115 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.419375896 CET	49708	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.547672987 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.547776937 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.548598051 CET	443	49708	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.548722029 CET	49708	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.553586960 CET	49708	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.553667068 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.682365894 CET	443	49708	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.682411909 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.683198929 CET	443	49708	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.683222055 CET	443	49708	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.683239937 CET	443	49708	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.683255911 CET	443	49708	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.683273077 CET	443	49707	52.22.118.126	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 16:31:40.683284998 CET	49708	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.683290005 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.683306932 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.683321953 CET	49708	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.683325052 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.683351994 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.683368921 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.717628002 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.717835903 CET	49708	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.723854065 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.723988056 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.724031925 CET	49708	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.844254971 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.844289064 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.844347000 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.844366074 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.844513893 CET	443	49708	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.844552040 CET	443	49708	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.844647884 CET	49708	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.844696999 CET	49708	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.845284939 CET	49708	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.845338106 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.850326061 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.850435972 CET	443	49708	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.850450039 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.850508928 CET	49708	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.892841101 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.971738100 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.992973089 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.993041992 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.993083000 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.993160009 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.996982098 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.997020006 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.997051001 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.997114897 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.997153044 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.997157097 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.997198105 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.997268915 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.997294903 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.997308016 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.997373104 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:40.997492075 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:40.997566938 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:41.012847900 CET	443	49708	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:41.119468927 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:41.119520903 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:41.119573116 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:41.119590998 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:41.119618893 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:41.119668961 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:41.119688034 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:41.119720936 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:41.122857094 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:41.123897076 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:41.123944044 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:41.123985052 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:41.124007940 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:41.124023914 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:41.124061108 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:41.124082088 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:41.124126911 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:41.124142885 CET	49707	443	192.168.2.5	52.22.118.126

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 16:31:41.124171019 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:41.124198914 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:41.124243975 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:41.124254942 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:41.124290943 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:41.124311924 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:41.124352932 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:41.124370098 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:41.124407053 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:41.124425888 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:41.124464989 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:41.124480963 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:41.124517918 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:41.124535084 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:41.124582052 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:41.124593019 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:41.124628067 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:41.124654055 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:41.124696016 CET	443	49707	52.22.118.126	192.168.2.5
Feb 22, 2021 16:31:41.124712944 CET	49707	443	192.168.2.5	52.22.118.126
Feb 22, 2021 16:31:41.124747038 CET	49707	443	192.168.2.5	52.22.118.126

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 16:31:31.036736012 CET	52212	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:31.096919060 CET	53	52212	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:31.202008009 CET	54302	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:31.250919104 CET	53	54302	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:31.791153908 CET	53784	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:31.839829922 CET	53	53784	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:32.082638979 CET	65307	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:32.144129038 CET	53	65307	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:32.875243902 CET	64344	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:32.926532030 CET	53	64344	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:33.021528006 CET	62060	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:33.071028948 CET	53	62060	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:33.136549950 CET	61805	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:33.210441113 CET	53	61805	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:33.644208908 CET	54795	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:33.704052925 CET	53	54795	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:34.848712921 CET	49557	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:34.900336027 CET	53	49557	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:35.659008026 CET	61733	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:35.707987070 CET	53	61733	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:37.281812906 CET	65447	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:37.333599091 CET	53	65447	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:38.418390989 CET	52441	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:38.477488995 CET	53	52441	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:39.244396925 CET	62176	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:39.303349018 CET	53	62176	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:39.559989929 CET	59596	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:39.614506960 CET	53	59596	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:40.347254992 CET	65296	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:40.409357071 CET	53	65296	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:40.815978050 CET	63183	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:40.874720097 CET	53	63183	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:40.923230886 CET	60151	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:40.976378918 CET	53	60151	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:41.042182922 CET	56969	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:41.058099985 CET	55161	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:41.102128029 CET	53	56969	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:41.105117083 CET	54757	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:41.109791994 CET	53	55161	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 16:31:41.139417887 CET	49992	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:41.174927950 CET	53	54757	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:41.189409971 CET	53	49992	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:41.427743912 CET	60075	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:41.479260921 CET	53	60075	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:41.599956989 CET	55016	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:41.648545980 CET	53	55016	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:41.685659885 CET	64345	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:41.709222078 CET	57128	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:41.734364033 CET	53	64345	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:41.757931948 CET	53	57128	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:42.995790005 CET	54791	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:43.057534933 CET	53	54791	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:43.785615921 CET	50463	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:43.837239981 CET	53	50463	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:44.935564041 CET	50394	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:44.984468937 CET	53	50394	8.8.8.8	192.168.2.5
Feb 22, 2021 16:31:56.745100021 CET	58530	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:31:56.809459925 CET	53	58530	8.8.8.8	192.168.2.5
Feb 22, 2021 16:32:03.793961048 CET	53813	53	192.168.2.5	8.8.8.8
Feb 22, 2021 16:32:03.852885008 CET	53	53813	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 16:31:40.347254992 CET	192.168.2.5	8.8.8.8	0xb096	Standard query (0)	abundant-chivalrous-hedgehog.glitch.me	A (IP address)	IN (0x0001)
Feb 22, 2021 16:31:41.058099985 CET	192.168.2.5	8.8.8.8	0xd5d4	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Feb 22, 2021 16:31:41.139417887 CET	192.168.2.5	8.8.8.8	0x86e6	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Feb 22, 2021 16:31:41.427743912 CET	192.168.2.5	8.8.8.8	0xd386	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Feb 22, 2021 16:31:41.599956989 CET	192.168.2.5	8.8.8.8	0xd475	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Feb 22, 2021 16:31:41.685659885 CET	192.168.2.5	8.8.8.8	0x1f0c	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Feb 22, 2021 16:31:41.709222078 CET	192.168.2.5	8.8.8.8	0x8f81	Standard query (0)	stackpath.bootstrapcdn.com	A (IP address)	IN (0x0001)
Feb 22, 2021 16:31:56.745100021 CET	192.168.2.5	8.8.8.8	0xc38f	Standard query (0)	abundant-chivalrous-hedgehog.glitch.me	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 16:31:40.409357071 CET	8.8.8.8	192.168.2.5	0xb096	No error (0)	abundant-chivalrous-hedgehog.glitch.me		52.22.118.126	A (IP address)	IN (0x0001)
Feb 22, 2021 16:31:40.409357071 CET	8.8.8.8	192.168.2.5	0xb096	No error (0)	abundant-chivalrous-hedgehog.glitch.me		34.196.60.73	A (IP address)	IN (0x0001)
Feb 22, 2021 16:31:40.409357071 CET	8.8.8.8	192.168.2.5	0xb096	No error (0)	abundant-chivalrous-hedgehog.glitch.me		18.215.10.11	A (IP address)	IN (0x0001)
Feb 22, 2021 16:31:40.409357071 CET	8.8.8.8	192.168.2.5	0xb096	No error (0)	abundant-chivalrous-hedgehog.glitch.me		54.237.41.217	A (IP address)	IN (0x0001)
Feb 22, 2021 16:31:41.109791994 CET	8.8.8.8	192.168.2.5	0xd5d4	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 16:31:41.189409971 CET	8.8.8.8	192.168.2.5	0x86e6	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 16:31:41.479260921 CET	8.8.8.8	192.168.2.5	0xd386	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Feb 22, 2021 16:31:41.479260921 CET	8.8.8.8	192.168.2.5	0xd386	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Feb 22, 2021 16:31:41.648545980 CET	8.8.8.8	192.168.2.5	0xd475	No error (0)	maxcdn.bootstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 16:31:41.734364033 CET	8.8.8.8	192.168.2.5	0x1f0c	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 16:31:41.757931948 CET	8.8.8.8	192.168.2.5	0x8f81	No error (0)	stackpath.bootstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 16:31:56.809459925 CET	8.8.8.8	192.168.2.5	0xc38f	No error (0)	abundant-chivalrous-hedgehog.glitch.me		34.196.60.73	A (IP address)	IN (0x0001)
Feb 22, 2021 16:31:56.809459925 CET	8.8.8.8	192.168.2.5	0xc38f	No error (0)	abundant-chivalrous-hedgehog.glitch.me		52.22.118.126	A (IP address)	IN (0x0001)
Feb 22, 2021 16:31:56.809459925 CET	8.8.8.8	192.168.2.5	0xc38f	No error (0)	abundant-chivalrous-hedgehog.glitch.me		18.215.10.11	A (IP address)	IN (0x0001)
Feb 22, 2021 16:31:56.809459925 CET	8.8.8.8	192.168.2.5	0xc38f	No error (0)	abundant-chivalrous-hedgehog.glitch.me		54.237.41.217	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
Feb 22, 2021 16:31:40.683255911 CET	52.22.118.126	443	192.168.2.5	49708	CN=glitch.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	Mon Jan 18 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Wed Feb 16 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 22, 2021 16:31:40.683325052 CET	52.22.118.126	443	192.168.2.5	49707	CN=glitch.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	Mon Jan 18 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Wed Feb 16 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Feb 22, 2021 16:31:41.643861055 CET	104.16.18.94	443	192.168.2.5	49722	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Feb 22, 2021 16:31:41.644309044 CET	104.16.18.94	443	192.168.2.5	49723	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		

Code Manipulations

Statistics

Behavior

● iexplore.exe
● iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 4368 Parent PID: 792

General

Start time:	16:31:38
Start date:	22/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6a0080000
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: 4532 Parent PID: 4368

General

Start time:	16:31:39

Start date:	22/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4368 CREDAT:17410 /prefetch:2
Imagebase:	0xc0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly