



ID: 356347
Cookbook: browseurl.jbs
Time: 23:44:48
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2

Analysis Report https://firebasestorage.googleapis.com/v0/b/speed-fc307.appspot.com/o/index.html?alt=media&token=bfb5fce8-3814-4fce-b15b-c1fb6db81c34#brnchadvrt@pella.com 4

- Overview 4
  - General Information 4
  - Detection 4
  - Signatures 4
  - Classification 4
- Startup 4
- Malware Configuration 4
- Yara Overview 4
  - Dropped Files 4
- Sigma Overview 4
- Signature Overview 4
  - AV Detection: 5
  - Phishing: 5
  - Compliance: 5
- Mitre Att&ck Matrix 5
- Behavior Graph 5
- Screenshots 6
  - Thumbnails 6
- Antivirus, Machine Learning and Genetic Malware Detection 7
  - Initial Sample 7
  - Dropped Files 7
  - Unpacked PE Files 7
  - Domains 7
  - URLs 7
- Domains and IPs 8
  - Contacted Domains 8
  - URLs from Memory and Binaries 8
  - Contacted IPs 8
  - Public 9
- General Information 9
- Simulations 10
  - Behavior and APIs 10
- Joe Sandbox View / Context 10
  - IPs 10
  - Domains 10
  - ASN 10
  - JA3 Fingerprints 11
  - Dropped Files 11
- Created / dropped Files 11
- Static File Info 18
  - No static file info 18
- Network Behavior 18
  - Network Port Distribution 18
  - TCP Packets 18
  - UDP Packets 19
  - DNS Queries 20
  - DNS Answers 21
  - HTTPS Packets 21
- Code Manipulations 21
- Statistics 21

Behavior 21
System Behavior 22
Analysis Process: iexplore.exe PID: 5816 Parent PID: 792 22
General 22
File Activities 22
Registry Activities 22
Analysis Process: iexplore.exe PID: 5556 Parent PID: 5816 22
General 22
File Activities 23
Registry Activities 23
Disassembly 23

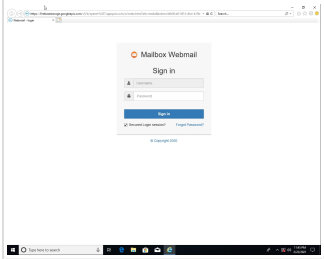
Analysis Report https://firebasestorage.googleapis.com…

Overview

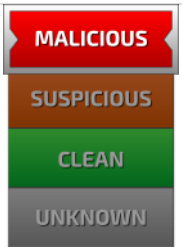
General Information

Sample URL:	https://firebasestorage.googleapis.com/v0/b/speed-fc307.appspot.com/o/index...l?alt=media&token=bfb5fce8-3814-4fce-b15b-c1fb6db81c34#brnchadvrt@pella.com
Analysis ID:	356347

Most interesting Screenshot:



Detection



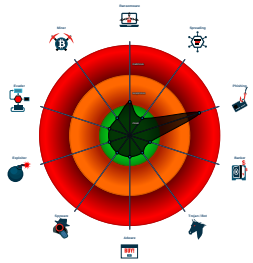
HTMLPhisher

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Phishing URL detected (based on va…
- Yara detected HtmlPhish_10
- HTML body contains low number of …
- Invalid 'forgot password' link found
- No HTML title found
- URL contains potential PII (phishing…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5816 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5556 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5816 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

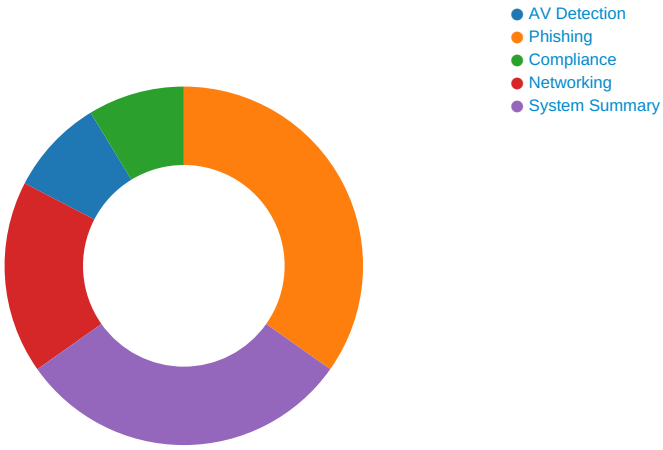
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\index[1].html	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

Antivirus detection for URL or domain

Phishing:

Phishing URL detected (based on various patterns)

Yara detected HtmlPhish_10

Compliance:

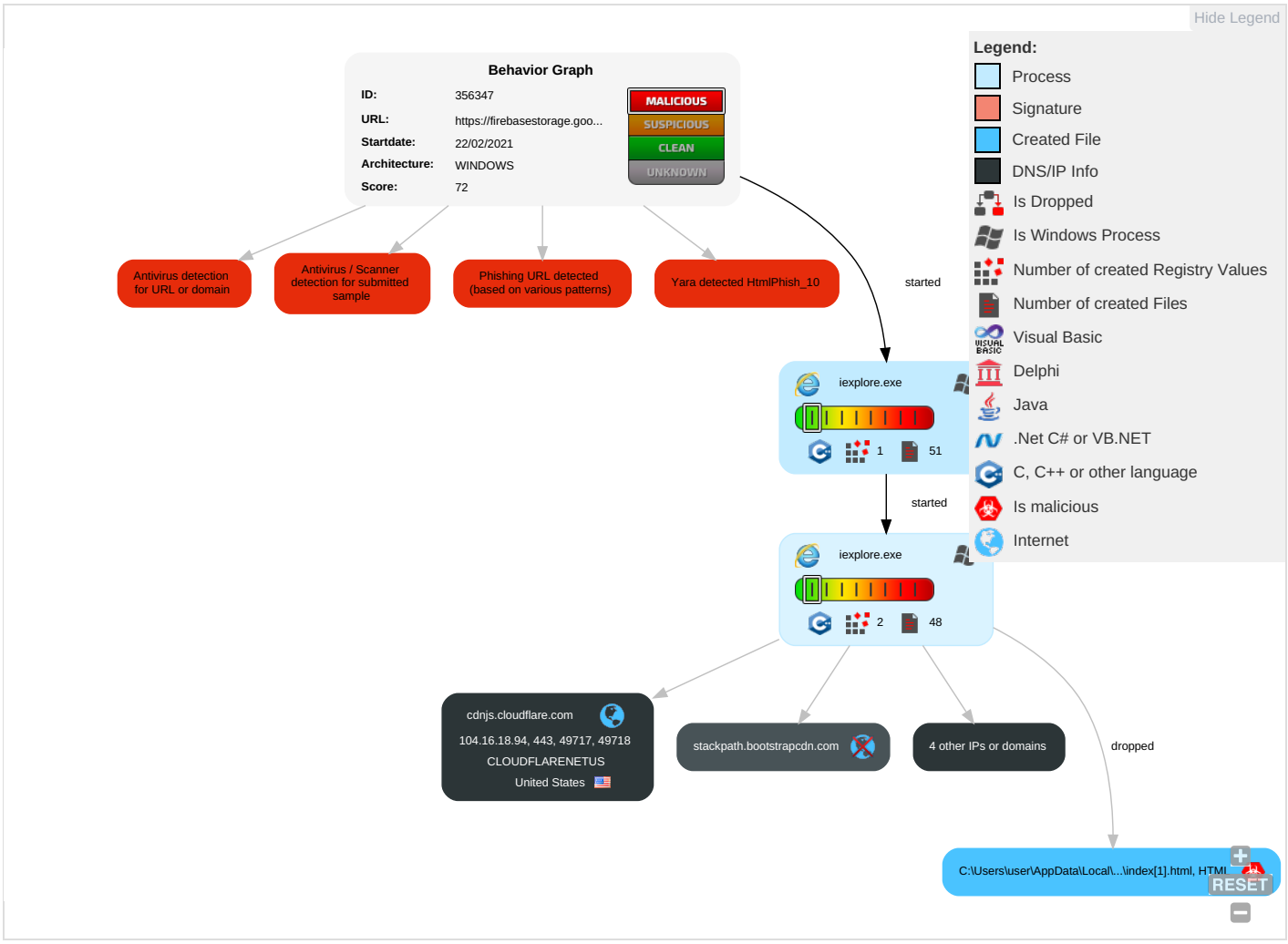
Uses new MSVCR Dlls

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	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

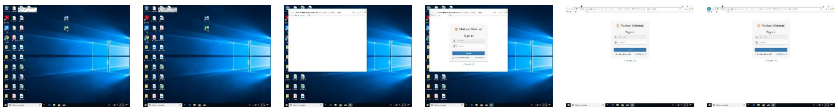
Behavior Graph

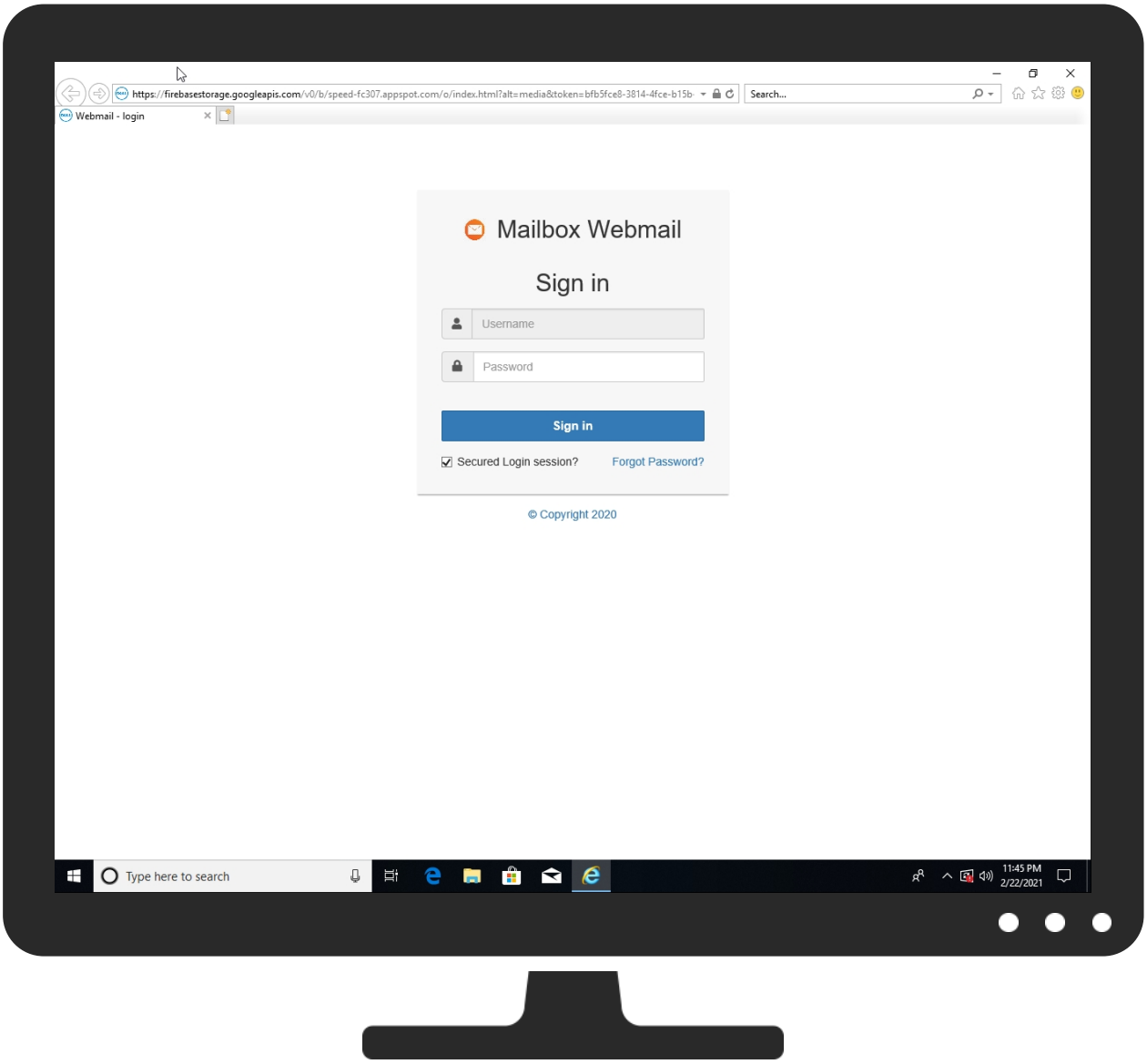


Screenshots

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://firebasestorage.googleapis.com/v0/b/speed-fc307.appspot.com/o/index.html?alt=media&token=bfb5fce8-3814-4fce-b15b-c1fb6db81c34#brnchadvrt@pella.com	1%	Virustotal		Browse
http://https://firebasestorage.googleapis.com/v0/b/speed-fc307.appspot.com/o/index.html?alt=media&token=bfb5fce8-3814-4fce-b15b-c1fb6db81c34#brnchadvrt@pella.com	0%	Avira URL Cloud	safe	
http://https://firebasestorage.googleapis.com/v0/b/speed-fc307.appspot.com/o/index.html?alt=media&token=bfb5fce8-3814-4fce-b15b-c1fb6db81c34#brnchadvrt@pella.com	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
http://https://firebasestorage.googleapis.com/v0/b/speed-fc307.appspot.com/o/index.html?alt=media&token=bfb5fce8-3814-4fce-b15b-c1fb6db81c34#	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://logosistemis.com/speed/mynewupdate/logged.php	0%	Avira URL Cloud	safe	
http://https://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://https://fontawesome.comhttps://fontawesome.comFont	0%	Avira URL Cloud	safe	

Domains and IPs

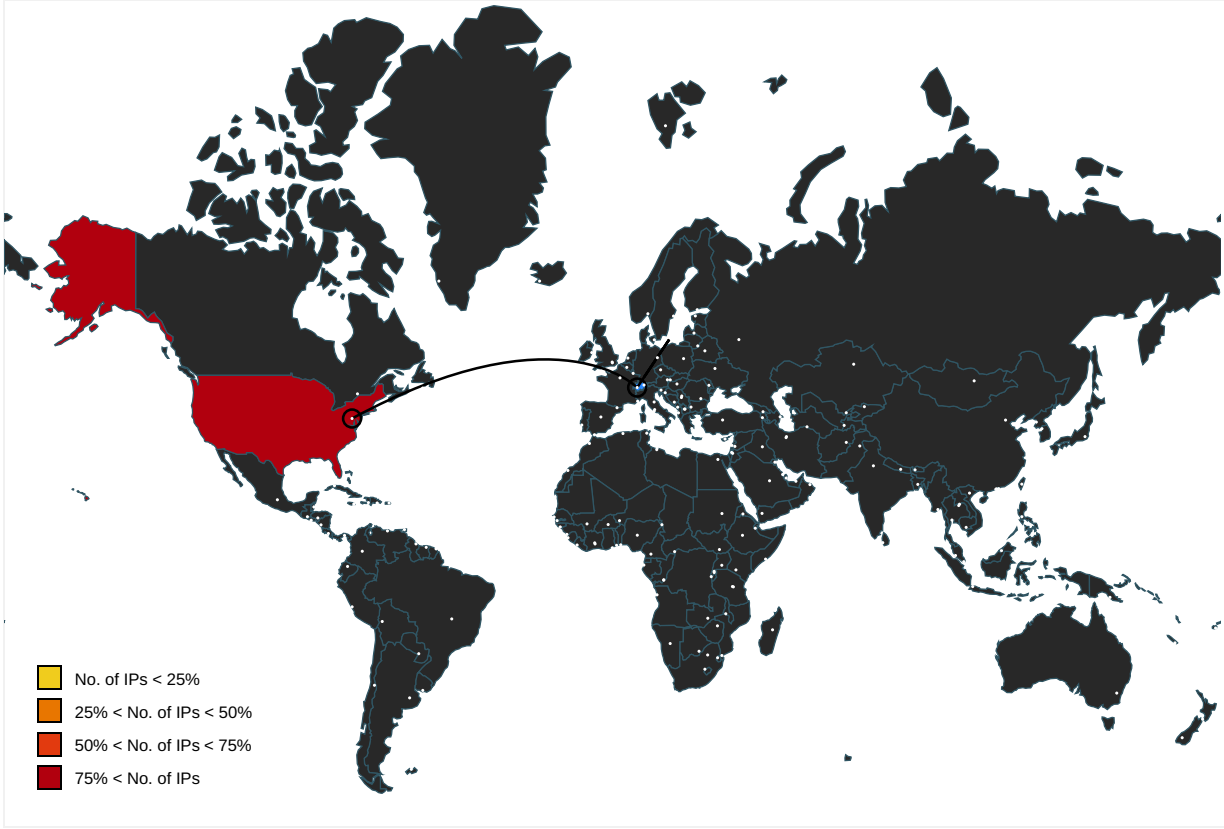
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdnjs.cloudflare.com	104.16.18.94	true	false		high
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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://fontawesome.com	free.min[1].css.2.dr, free-fa-solid-900[1].eot.2.dr	false		high
http://https://kit.fontawesome.com	585b051251[1].js.2.dr	false		high
http://https://logosistemis.com/speed/mynewupdate/logged.php	index[1].html.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/twbs/bootstrap/graphs/contributors)	bootstrap.min[1].js.2.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js	index[1].html.2.dr	false		high
http://https://getbootstrap.com)	bootstrap.min[1].js.2.dr	false	• Avira URL Cloud: safe	low
http://https://ka-f.fontawesome.com	585b051251[1].js.2.dr	false		high
http://https://code.jquery.com/jquery-3.2.1.slim.min.js	index[1].html.2.dr	false		high
http://https://code.jquery.com/jquery-3.1.1.min.js	index[1].html.2.dr	false		high
http://getbootstrap.com)	index[1].html.2.dr	false	• Avira URL Cloud: safe	low
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap.min[1].js.2.dr, index[1].html.2.dr	false		high
http://https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js	index[1].html.2.dr	false		high
http://https://logo.clearbit.com/	index[1].html.2.dr	false		high
http://opensource.org/licenses/MIT).	popper.min[1].js.2.dr	false		high
http://https://kit.fontawesome.com/585b051251.js	index[1].html.2.dr	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js	index[1].html.2.dr	false		high
http://https://getbootstrap.com/)	bootstrap.min[1].js0.2.dr	false		high
http://https://fontawesome.comhttps://fontawesome.comFont	free-fa-solid-900[1].eot.2.dr, free-fa-regular-400[1].eot.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://code.jquery.com/jquery-3.3.1.js	index[1].html.2.dr	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css	index[1].html.2.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
104.16.18.94	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356347
Start date:	22.02.2021
Start time:	23:44:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://firebasestorage.googleapis.com/v0/b/speed-fc307.appspot.com/o/index.html?alt=media&token=bfb5fce8-3814-4fce-b15b-c1fb6db81c34#brnchadvrt@pella.com
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:	9
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.phis.win@3/21@6/1

Copyright null 2021

Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://firebasestorage.googleapis.com/v0/b/speed-fc307.appspot.com/o/index.html?alt=media&token=bfb5fce8-3814-4fce-b15b-c1fb6db81c34#
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 51.11.168.160, 104.43.193.48, 104.43.139.144, 104.42.151.234, 92.122.145.220, 168.61.161.212, 88.221.62.148, 142.250.186.74, 209.197.3.24, 172.217.23.106, 142.250.185.202, 104.18.23.52, 104.18.22.52, 209.197.3.15, 172.64.203.28, 172.64.202.28, 142.250.185.164, 23.218.208.56, 152.199.19.161 • Excluded domains from analysis (whitelisted): 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, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, go.microsoft.com, www-bing-com.dual-a-0001.a-msedge.net, www.google.com, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, firebasestorage.googleapis.com, www.bing.com, kit.fontawesome.com.cdn.cloudflare.net, fonts.googleapis.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ajax.googleapis.com, ie9comview.vo.msecnd.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.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, 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.{1A2936D7-75AB-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8532132999216613
Encrypted:	false
SSDEEP:	192:rgZ3Z7M27WW7Et7diif7yluIzM7tGIB7aUID7LJsf7LgylZIjX:rQJPhUBLFNswDKvsvge8
MD5:	8D37613BDE2C2AE3DE909332A49F9DD7
SHA1:	5A7301F6AF6AAEF0D9E30793A718B2FFB1F906B7
SHA-256:	C1028AC836E0FAE6B54457896E9C14F4994D3DD4124686332E8ACFAD014561B6
SHA-512:	D0EBE8B36FFC6DA55B6F68CAB0B7FCC623D50429A6A88CFB9450395BD6B90F9763E081F46966D5CD2383B825A2002BEBE2FB7755EEFD5286DA386984E1F3310B
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\{1A2936D9-75AB-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	39942
Entropy (8bit):	2.1949541397113803
Encrypted:	false
SSDEEP:	384:rgJgnWONQ8oj9TE1oH6RmCE1/gZ17W51v:kMmOE
MD5:	C6FD7E3D03538F5D9F583563C28AFA8E
SHA1:	06AAD253BA3ED9032C069213EE6A50D15F725992
SHA-256:	5F07E7AD2759E4CD9192189339A5B28192E5793E6A3E7B2820D01A57483CCC53
SHA-512:	3728D3CE61E4412434F7CAD5EE509085F75059FACAE9D494B99A2F98C025C709BDEB0877D2C756DE906E95700652FA424B59590312D50EA0A320F874E7CD8948
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\{1A2936DA-75AB-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5638176258691519
Encrypted:	false
SSDEEP:	48:IwlGcprQGwpa5G4pQxGrapbS8GQpKVG7HpRKTGIpG:r7Z4Qb6BBSUAETuA
MD5:	0AE91401B4DB39BE21A5090D9BC45073
SHA1:	5C2FE2D5FC5F5DE76B13E9866EE279D56EB02B3E
SHA-256:	93D7EA1666DC2E9754615A55301E84F7FD4C6B0BB47679E1D33CF5569C6BBC80
SHA-512:	E608F734CF3F0CC3FB8CA2658594D53AC0A0652577B7859381877E863ED322803F27E49F7FE75C27C511227F5B4351A920B0C9A58C1C51BD668F92F6684EF2A6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{1A2936DA-75AB-11EB-90E6-ECF4BB82F7E0}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\po60zt0\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	853
Entropy (8bit):	7.162430469491424
Encrypted:	false
SSDEEP:	24:EwD7SByEH9bArPVO/XfF1NjjkJGHSE8ITJj:EwD7SUEdsTgfd1eJGHrdj
MD5:	CBDD6ED412FD7F5A3A3786C3BA4C0092
SHA1:	22D02CA4C4C5EF10E90B7CD67D6972D54E5638C5
SHA-256:	516823E34BBE0CBFB5EA0F858BE664049D5F0D6E229530DCA47DF3ECB5DC23D7
SHA-512:	4099BE978CC070FD4454CBB6126AF9F6C9EACF55EF0352C56FB0BCFAB059A580BAD3B14E572F95A77B7055E779B5F465C73A3CB80E2128EAD7CBFD1E3BB2FE 69
Malicious:	false
Reputation:	low
Preview:	?.h.t.t.p.s.:././.w.w.w...g.o.o.g.l.e...c.o.m./.s.2./.f.a.v.i.c.o.n.s.?.d.o.m.a.i.n.=.d.e.l.l...c.o.m.?.v.=.B.U.I.L.D._.H.A.S.H.....PNG.....IHDR.....a....sBIT....|.d....hIDAT8... [H.a....&..0i.B.E`.YJ...Q.Mt..^H.B.;+\.D*K1...:8...B...7g....Xf.P..:.s.-.t...h/<7...^^..{...Z=..y.=pw.6zr....3.k..>.2.t.@.$...Bh..C...i6.D.=.HtN...>.....0.1.$..P.*3.I...Tf..Uf."...d...~....t..... $0..}T.._8>z..C.T..B.n.....Mb%B.n.t.I-.....sj.9ht...+.i..(.....k...Q..U^...V.$\..G.7&!...T.B...3UqQ.I....k*.4...2..... I.O.. dik.pD...Q$..&.IF./S(w...8{)...S.5.T....;....\|hu#....'C.NI.@@.+g. Qr.t~.....@..7....!.:.:...O..../."#LH...%...B..].a....*.....$KA....."....."..6p:.s .....h_..{.b.@.}]3...O$.+z.$.[#. ....]..&.e!&..mP.x..v...c+T..Pe.....v...:...v.y9...x.r|.`.3#…c...$#.O.(- i.2...>..._....IEND.B`.....4`.....4`....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\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:	53A2B560B20551672FBB0E6E72632D4FD1C7E2DD2ECF7337EBAAAB179CB8BE7C87E9D803CE7765706BC7FCBCF993C34587CD1237DE5A279AEA19911D69067E 65
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-3.1.1.min.js
Preview:	/*! jQuery v3.1.1 | (c) jQuery Foundation | jquery.org/license */!function(a,b){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=a.do cument?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.c all(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,t oArray: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\0MX4YUS9\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\jquery-3.2.1.slim.min[1].js	
Preview:	/*! jQuery v3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_evalUrl,-event/ajax,-effects,-effects/Tween,-effects/animatedSelector | (c) JS Foundation and other contributors | jquery.org/license */!function(a,b){"use strict";"object"==typeof module &&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\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\2K7JPOQS\bootstrap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	48944
Entropy (8bit):	5.272507874206726
Encrypted:	false
SSDEEP:	768:9VG5R15WbHVKZrycEHSYro34CrSLB6WU/6DqBf4l1B:9VIRuo53XiwWTvl1B
MD5:	14D449EB8876FA55E1EF3C2CC52B0C17
SHA1:	A9545831803B1359CFEED47E3B4D6BAE68E40E99
SHA-256:	E7ED36CEEE5450B4243BBC35188AFABDFB4280C7C57597001DE0ED167299B01B
SHA-512:	00D9069B9BD29AD0DAA0503F341D67549CCE28E888E1AFFD1A2A45B64A4C1BC460D81CFC4751857F991F2F4FB3D2572FD97FCA651BA0C2B0255530209B182F2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js
Preview:	/*! * Bootstrap v4.0.0 (https://getbootstrap.com) * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors) * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE) */!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery"),require("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,n){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function s(t,e,n){return e&&i(t.prototype,e),n&&i(t,n),t}function r(){return(r=Object.assign||function(t){for(var e=1;e<arguments.length;e++){var n=arguments[e];for(var i in n)Object.prototype.hasOwnProperty.call(n,i)&&(t[i]=n[i])}return t}).apply(this,arguments)}e=e&&e.hasOwnProperty("default")?e.default:e,n=n&&n.hasOwnProp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\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:	572F349BB65758D377CCBAE4343505073 41ACD7B
SHA-256:	C3A12D7E8F6B2B1F5E4CD0C9938DFC79532AEF90802B424EE910093F156586DA
SHA-512:	9EA12CC277C9858524083FEBBE1A3E61FDECE5268F63B14C9FFAFE29396C7CCDB3B07BE10E829936BCCD8F3B9E39DCFA6BC4316F189E4CEA914F1D06916DB66B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\css[1].css	
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\2K7JPOQS\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/oOkKQB3l+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\2K7JPOQS\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\6M6D1PMD\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:	24E0AF4EC32A9AAB61D9E1AF9B2083F2D13CC98961B5E32BB613A02FEEF63F5F30C3B21C6308A4A204D981D77C86F09E221D0DB7B051A3538ACE07E727F29F5 8
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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\free-v4-shims.min[1].css	
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\6M6D1PMD\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\6M6D1PMD\index[1].html	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	144378
Entropy (8bit):	5.452012980543805
Encrypted:	false
SSDEEP:	768:REy3Gxw/Vc/QWlJxtQOIuiHlq5mzI4X8OAduFKbv2ctg2Bd8JP7ecQLvH1FLRfkR:Ruw/a1fIuiHlq5mN8lDbNmPbSNyHtRL
MD5:	15BE93CB46E09471239C8982526CA285
SHA1:	83E76D0E1F694447E6B46C07750AB4C320B7C6A2
SHA-256:	B315431D16638DED00CF1B2F9557CCBC41DCD6F34A9ECF2B023753BCDC51A94A
SHA-512:	C7ECA825FBFB3EAD54FF0B999E1F1F4BA58B7FACF9D17CFDC67603BCFAFCB61AE6F5AC5708397785D98368F7EB182D89E6E8B3BED7CA19C5402B7D8B48D58 4A0
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\index[1].html, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://firebasestorage.googleapis.com/v0/b/speed-fc307.appspot.com/o/index.html?alt=media&token=bfb5fce8-3814-4fce-b15b-c1fb6db81c34
Preview:	..<!doctype html>.<html lang="en">.<head>. <script src="https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>. <script src="https://code.jquery.com/jquery-3.1.1.min.js">. <script src="https://code.jquery.com/jquery-3.3.1.js" integrity="sha256-2Kok7MbOyxpgUVvAk/HJ2jigOSYS2auK4Pfzbm7uH60=" . crossorigin="anonymous"/></script>. Required meta tags -->. <meta charset="utf-8">. <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">. <link rel="icon" type="image/png" sizes="192x192" href="https://www.google.com/s2/favicons?domain=dell.com?v=BUILD_HASH">.. Bootstrap CSS -->. <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css" integrity="sha384-Gn5384xqQ1aoWXA+058RXPxPg6fy4IWvTNh0E263XmFcJlSAwiGgFAW/dAiS6JXm" crossorigin="anonymous"> -->. <link href="https://fonts.googleapis.com/css?family=Archivo+Narrow&display=swap" rel="stylesheet">. < script src="ht

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\popper.min[1].js	
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\VAHFWDJC\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:	2CD82E0DCD1381447522CFFD610136513323E5D2980FAE730801FE8BBA580FF7FDF9CB8D2E9AC794D6F2FB59C724EDA71BECE7CAA72C775BC963E1A54B30EBCB
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\VAHFWDJC\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:	9FA75814E1B9F7DB38FE61A503A13E60B82D83DB8F4CE30351BD08A6B48C0D854BAF472D891AF23C443C8293380C2325C7B3361B708AF9971AA0EA09A25CDDCA
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\VAHFWDJC\favicons[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	689
Entropy (8bit):	7.547514317403399
Encrypted:	false
SSDEEP:	12:6v/7aH90mJv85rPVOlNXbmMFb6IL9LjjPcQOJPQqG+GS+tVpAiz+1O4MbsDN:hH9bArPVO/XfF1NjjkJGHSE8ITG
MD5:	6F45B2E7280E12B8D0DF8280FDE4C155
SHA1:	7F4912503B0710270A047F0D1F2820FAE7B849E0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\favicons[1].png	
SHA-256:	B5BA52047193427D28D3F169FB3E4A2835C0FA1CA6F59192381BAA79CE74FBFB
SHA-512:	5C8C9114C682080337FD2BD2067D8C58C5E0D7E5B2DDEF64AE735E95AA5392AD15AE84153D7E15A113FF509B19B929616D74F5C65E2E583C2C7E3D122062F39
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a....sBIT....|.d....hIDAT8...[H.a....&..0i.B.E`.YJ...Q.Mt..^H.B.;+\.D*K1...:8...B...7g....Xf.P..:.s.-.t...h/<7...^^..{...Z=..y.=pw.6zr....3.k..>.2.t.@.$...Bh. .C...i6.D.=.HtN...>.....0.1.$..P.*3.l...Tf..Uf."...d...~....t.....$0..}T.._8>z..C.T..B.n.....Mb%B.n.t.l-.....sj.9ht...+.i..(.....k...Q..U^...V.$\..G.7&!...T.B...3UqQ.l....k*.4...2..... I.O.. dik.pD. ..Q$..&.lF./S(w...8{)...S.5.T....;....\|hu#....'C.NI.@@.+g.Qr.t~.....@..7....!.:..:...O..../."#LH...%...B..].a....*.....$KA....."....".6p:.s .....h_..{.b.@.}]3...O$.+z.$.[#. ....]..&.e!&.. mP.x..v...c+T..Pe.....v...:...v.y9...x.r|.`.3#...c...$#.O.(-i.2...>..._....IEND.B`.

C:\Users\user\AppData\Local\Temp\~DF75C49756B6172DCE.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.480980712209576
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo7B9lo7h9lW7zgP:kBqoI7q707zgP
MD5:	7CC87CE12A0C9A074ABEC92D2A71411A
SHA1:	CB2C91E64B21783DFB908E4613123EE286C4CBA5
SHA-256:	F7D353FBF664177AC708785CBF782D4F9921E4E944483503EB2D7C8D9AB4D2FC
SHA-512:	134B1CC33FAF6DBD957E0D8F83B3A0A5FC2E16F4A584083BF70A60C378218B73D736A03DFE60130EB26947E985D52AC989C5C248EDE961DF9B35F8452884E25
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFBC299770CFB6D2F4.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...(..... ....

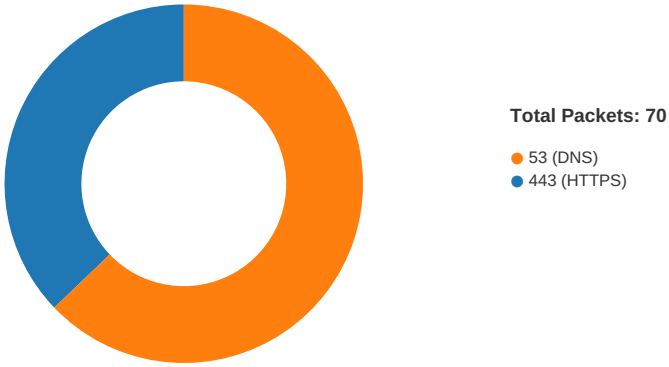
C:\Users\user\AppData\Local\Temp\~DFF0455DC76069C657.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	45869
Entropy (8bit):	0.9792235808693253
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+MqwRat91oH6RmL/yZRm4+:
MD5:	22E8365B621D07C3C9FEABA430A3101A
SHA1:	A2A0FBC4C3532C5248743488154C5F9818DD3A68
SHA-256:	101BAD0C44D4B61ABFF29B8727CB165A2CCC92DCF58E52937E9051948081FFEB
SHA-512:	625EEBA567943FC337C5C152AC523D7407B4437A51ABE2B52A165A6E8C45CB38050DB02C63D6F33387EDAFF53657051EC6844C63313A97BA7F113CD2C8CA59(
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 23:45:34.932363033 CET	49717	443	192.168.2.7	104.16.18.94
Feb 22, 2021 23:45:34.933594942 CET	49718	443	192.168.2.7	104.16.18.94
Feb 22, 2021 23:45:34.977018118 CET	443	49717	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:34.977205038 CET	49717	443	192.168.2.7	104.16.18.94
Feb 22, 2021 23:45:34.978166103 CET	443	49718	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:34.978271961 CET	49718	443	192.168.2.7	104.16.18.94
Feb 22, 2021 23:45:34.980340958 CET	49717	443	192.168.2.7	104.16.18.94
Feb 22, 2021 23:45:34.980540991 CET	49718	443	192.168.2.7	104.16.18.94
Feb 22, 2021 23:45:35.025038004 CET	443	49717	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:35.025115013 CET	443	49718	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:35.025628090 CET	443	49717	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:35.025650024 CET	443	49717	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:35.025667906 CET	443	49718	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:35.025684118 CET	443	49718	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:35.025767088 CET	49718	443	192.168.2.7	104.16.18.94
Feb 22, 2021 23:45:35.025784016 CET	49717	443	192.168.2.7	104.16.18.94
Feb 22, 2021 23:45:35.025818110 CET	49717	443	192.168.2.7	104.16.18.94
Feb 22, 2021 23:45:35.036624908 CET	49717	443	192.168.2.7	104.16.18.94
Feb 22, 2021 23:45:35.037020922 CET	49717	443	192.168.2.7	104.16.18.94
Feb 22, 2021 23:45:35.037233114 CET	49717	443	192.168.2.7	104.16.18.94
Feb 22, 2021 23:45:35.040606022 CET	49718	443	192.168.2.7	104.16.18.94
Feb 22, 2021 23:45:35.041280031 CET	49718	443	192.168.2.7	104.16.18.94
Feb 22, 2021 23:45:35.084115982 CET	443	49717	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:35.084134102 CET	443	49717	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:35.084150076 CET	443	49717	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:35.084347963 CET	443	49717	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:35.084456921 CET	49717	443	192.168.2.7	104.16.18.94
Feb 22, 2021 23:45:35.084801912 CET	443	49717	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:35.084887981 CET	49717	443	192.168.2.7	104.16.18.94
Feb 22, 2021 23:45:35.086127043 CET	49717	443	192.168.2.7	104.16.18.94

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 23:45:35.087340117 CET	443	49718	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:35.087435007 CET	443	49718	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:35.087505102 CET	49718	443	192.168.2.7	104.16.18.94
Feb 22, 2021 23:45:35.087588072 CET	443	49718	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:35.087641001 CET	49718	443	192.168.2.7	104.16.18.94
Feb 22, 2021 23:45:35.087754965 CET	443	49718	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:35.087773085 CET	443	49718	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:35.087827921 CET	49718	443	192.168.2.7	104.16.18.94
Feb 22, 2021 23:45:35.088809967 CET	49718	443	192.168.2.7	104.16.18.94
Feb 22, 2021 23:45:35.090461969 CET	443	49717	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:35.090483904 CET	443	49717	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:35.090509892 CET	443	49717	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:35.090526104 CET	443	49717	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:35.090562105 CET	443	49717	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:35.090588093 CET	443	49717	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:35.090603113 CET	49717	443	192.168.2.7	104.16.18.94
Feb 22, 2021 23:45:35.090624094 CET	49717	443	192.168.2.7	104.16.18.94
Feb 22, 2021 23:45:35.090728998 CET	49717	443	192.168.2.7	104.16.18.94
Feb 22, 2021 23:45:35.091447115 CET	443	49717	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:35.091490984 CET	443	49717	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:35.091536045 CET	49717	443	192.168.2.7	104.16.18.94
Feb 22, 2021 23:45:35.091558933 CET	49717	443	192.168.2.7	104.16.18.94
Feb 22, 2021 23:45:35.132426977 CET	443	49717	104.16.18.94	192.168.2.7
Feb 22, 2021 23:45:35.176886082 CET	443	49718	104.16.18.94	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 23:45:24.547091961 CET	61242	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:24.595805883 CET	53	61242	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:24.656646967 CET	58562	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:24.710457087 CET	53	58562	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:24.866457939 CET	56590	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:24.919217110 CET	53	56590	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:25.843972921 CET	60501	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:25.892643929 CET	53	60501	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:26.815551996 CET	53775	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:26.869354963 CET	53	53775	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:27.438141108 CET	51837	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:27.497509003 CET	53	51837	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:27.941450119 CET	55411	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:27.989973068 CET	53	55411	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:29.079828978 CET	63668	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:29.128274918 CET	53	63668	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:30.117470980 CET	54640	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:30.165993929 CET	53	54640	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:31.410054922 CET	58739	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:31.458826065 CET	53	58739	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:32.256298065 CET	60338	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:32.315119028 CET	53	60338	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:32.676990032 CET	58717	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:32.725694895 CET	53	58717	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:33.674144983 CET	59762	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:33.739300013 CET	53	59762	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:34.128448009 CET	54329	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:34.185643911 CET	53	54329	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:34.502650023 CET	58052	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:34.510937929 CET	54008	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:34.518580914 CET	59451	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:34.559346914 CET	53	54008	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:34.559674978 CET	53	58052	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:34.580409050 CET	53	59451	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:34.596898079 CET	52914	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:34.645443916 CET	53	52914	8.8.8.8	192.168.2.7

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 23:45:34.756093979 CET	64569	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:34.804636002 CET	53	64569	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:34.957295895 CET	52816	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:35.008737087 CET	53	52816	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:35.075237036 CET	50781	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:35.128606081 CET	53	50781	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:35.259963989 CET	54230	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:35.313216925 CET	53	54230	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:36.192677021 CET	54911	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:36.258470058 CET	53	54911	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:36.526453018 CET	49958	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:36.577496052 CET	53	49958	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:39.178020954 CET	50860	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:39.229490995 CET	53	50860	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:40.639101028 CET	50452	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:40.687737942 CET	53	50452	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:41.640733004 CET	59730	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:41.692147970 CET	53	59730	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:42.611717939 CET	59310	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:42.664643049 CET	53	59310	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:43.575654984 CET	51919	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:43.624202967 CET	53	51919	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:44.673677921 CET	64296	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:44.723680019 CET	53	64296	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:49.738421917 CET	56680	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:49.787132978 CET	53	56680	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:49.967075109 CET	58820	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:50.018532991 CET	53	58820	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:50.712666988 CET	60983	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:50.764086962 CET	53	60983	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:51.704313040 CET	49247	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:51.754908085 CET	53	49247	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:52.730870962 CET	52286	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:52.789962053 CET	53	52286	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:53.779633999 CET	56064	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:53.839694023 CET	53	56064	8.8.8.8	192.168.2.7
Feb 22, 2021 23:45:54.241528034 CET	63744	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:45:54.303189039 CET	53	63744	8.8.8.8	192.168.2.7
Feb 22, 2021 23:46:01.241362095 CET	61457	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:46:01.295388937 CET	53	61457	8.8.8.8	192.168.2.7
Feb 22, 2021 23:46:02.235168934 CET	58367	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:46:02.286770105 CET	53	58367	8.8.8.8	192.168.2.7
Feb 22, 2021 23:46:03.031439066 CET	60599	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:46:03.090854883 CET	53	60599	8.8.8.8	192.168.2.7
Feb 22, 2021 23:46:03.241189003 CET	58367	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:46:03.292980909 CET	53	58367	8.8.8.8	192.168.2.7
Feb 22, 2021 23:46:04.038353920 CET	60599	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:46:04.095463037 CET	53	60599	8.8.8.8	192.168.2.7
Feb 22, 2021 23:46:04.256990910 CET	58367	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:46:04.309086084 CET	53	58367	8.8.8.8	192.168.2.7
Feb 22, 2021 23:46:05.061655045 CET	60599	53	192.168.2.7	8.8.8.8
Feb 22, 2021 23:46:05.110346079 CET	53	60599	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 23:45:34.510937929 CET	192.168.2.7	8.8.8.8	0x9be2	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Feb 22, 2021 23:45:34.596898079 CET	192.168.2.7	8.8.8.8	0x5087	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Feb 22, 2021 23:45:34.756093979 CET	192.168.2.7	8.8.8.8	0xd014	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Feb 22, 2021 23:45:34.957295895 CET	192.168.2.7	8.8.8.8	0x4ba6	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 23:45:35.075237036 CET	192.168.2.7	8.8.8.8	0x8cba	Standard query (0)	stackpath.bootstrapcdn.com	A (IP address)	IN (0x0001)
Feb 22, 2021 23:45:35.259963989 CET	192.168.2.7	8.8.8.8	0x2948	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 23:45:34.559346914 CET	8.8.8.8	192.168.2.7	0x9be2	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 23:45:34.645443916 CET	8.8.8.8	192.168.2.7	0x5087	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 23:45:34.804636002 CET	8.8.8.8	192.168.2.7	0xd014	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Feb 22, 2021 23:45:34.804636002 CET	8.8.8.8	192.168.2.7	0xd014	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Feb 22, 2021 23:45:35.008737087 CET	8.8.8.8	192.168.2.7	0x4ba6	No error (0)	maxcdn.bootstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 23:45:35.128606081 CET	8.8.8.8	192.168.2.7	0x8cba	No error (0)	stackpath.bootstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 23:45:35.313216925 CET	8.8.8.8	192.168.2.7	0x2948	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	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 23:45:35.025650024 CET	104.16.18.94	443	192.168.2.7	49717	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 22, 2021 23:45:35.025684118 CET	104.16.18.94	443	192.168.2.7	49718	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

● iexplore.exe
● iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5816 Parent PID: 792

General

Start time:	23:45:31
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:	0x7ff7106a0000
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: 5556 Parent PID: 5816

General

Start time:	23:45:31

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:5816 CREDAT:17410 /prefetch:2
Imagebase:	0xaa0000
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