ID: 323112
Cookbook: browseurl.jbs
Time: 11:09:24
Date: 26/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report https://hosting-e899f.web.app/#ba11_go_coa_chf@emfa.pt 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
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 8
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 9
Public 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 11
Static File Info 16
No static file info 16
Network Behavior 16
Network Port Distribution 16
TCP Packets 16
UDP Packets 18
DNS Queries 19
DNS Answers 19
HTTPS Packets 19
Code Manipulations 21
Statistics 21
Behavior 21
System Behavior 21
Analysis Process: iexplore.exe PID: 5860 Parent PID: 800 21

General 21
File Activities 22
Registry Activities 22
Analysis Process: iexplore.exe PID: 3984 Parent PID: 5860 22
General 22
File Activities 22
Registry Activities 22
Disassembly 22

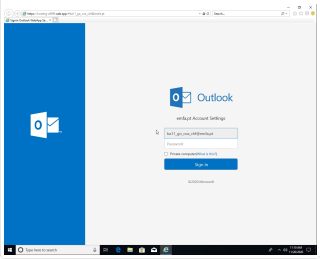
Analysis Report https://hosting-e899f.web.app/#ba11_g…

Overview

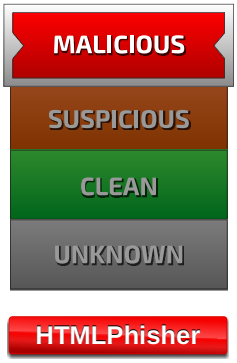
General Information

Sample URL:	http://https://hosting-e899f.web.app/#ba11_go_coa_chf@emfa.pt
Analysis ID:	323112

Most interesting Screenshot:



Detection

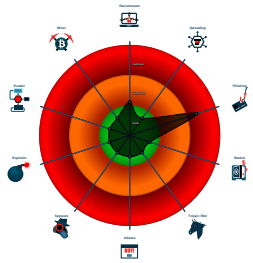


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for doma…
- Yara detected HtmlPhish_10
- Phishing site detected (based on log…
- Form action URLs do not match mai…
- HTML body contains low number of …
- HTML title does not match URL
- Suspicious form URL found
- URL contains potential PII (phishing…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5860 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 3984 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5860 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

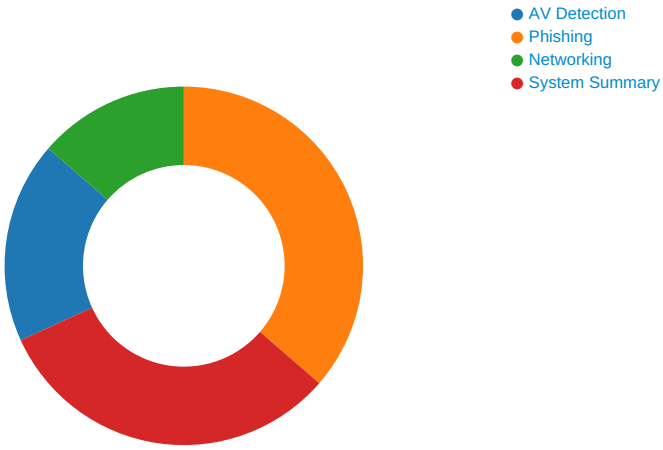
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\W3YTSHKB.htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for domain / URL

Phishing:

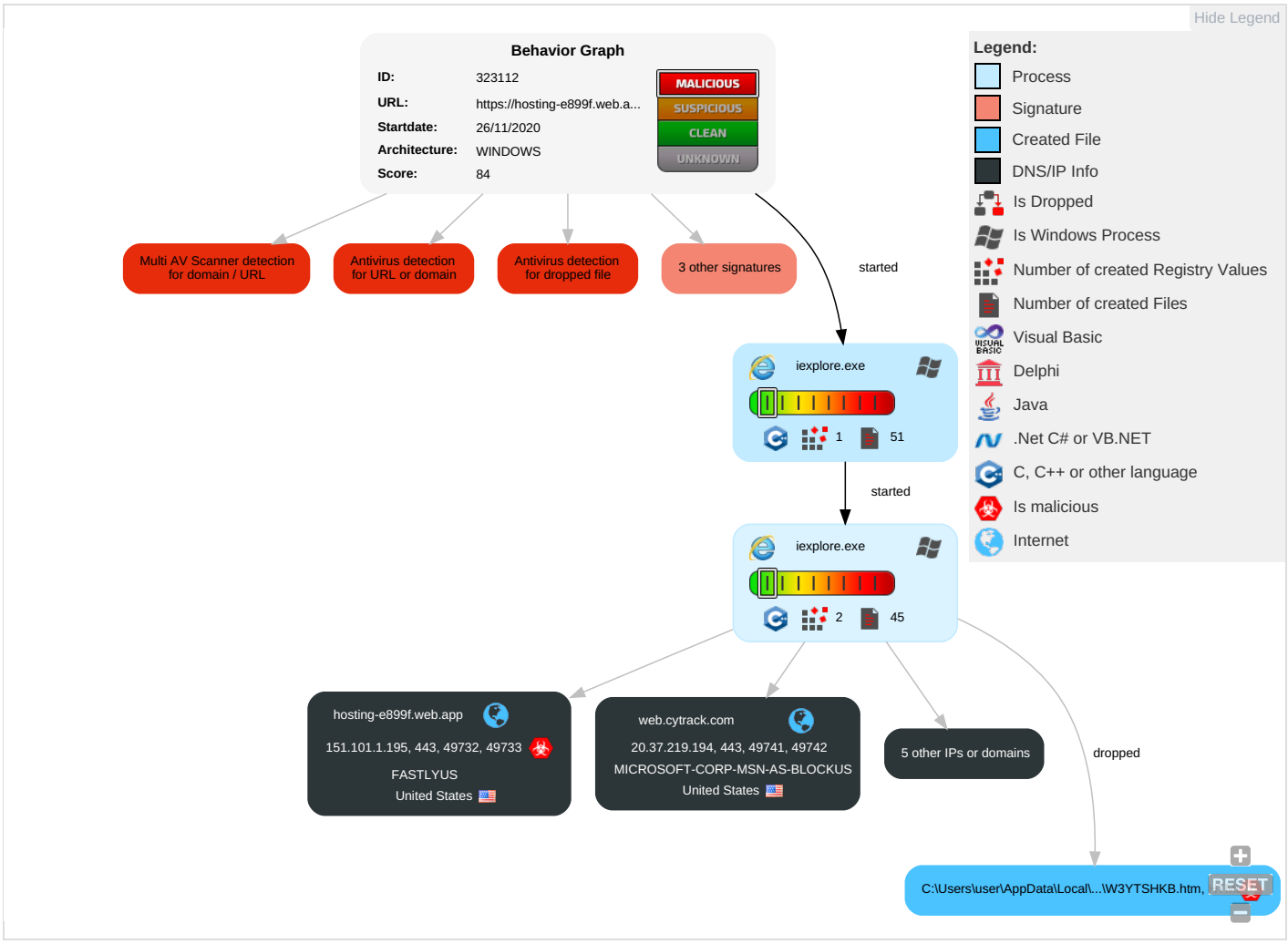
Yara detected HtmlPhish_10

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impac
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partiti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lockc
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data

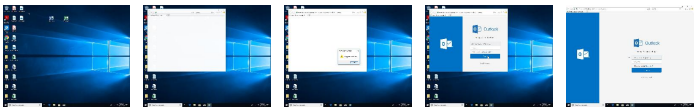
Behavior Graph

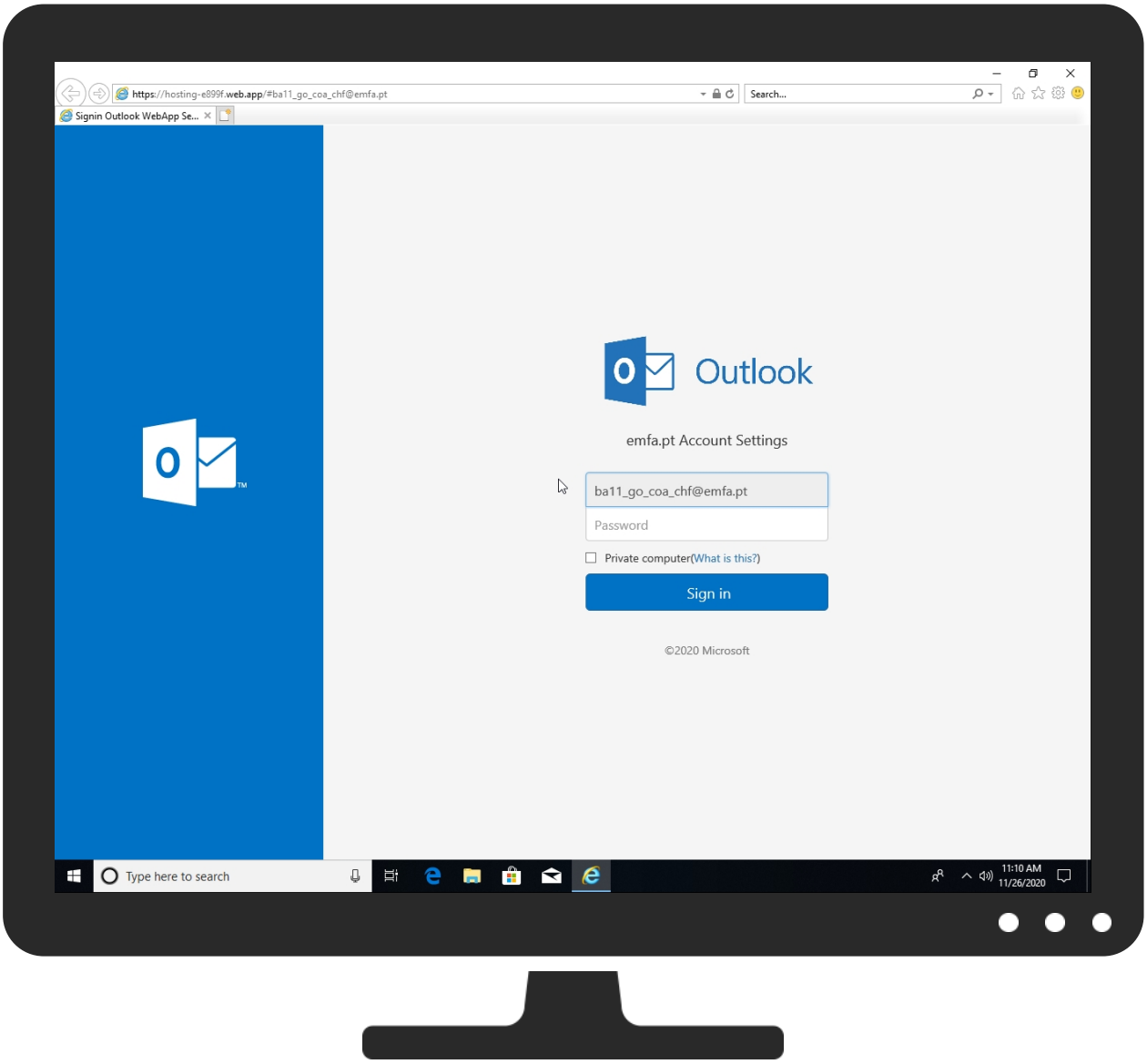


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://hosting-e899f.web.app/#ba11_go_coa_chf@emfa.pt	1%	Virustotal		Browse
http://https://hosting-e899f.web.app/#ba11_go_coa_chf@emfa.pt	100%	Avira URL Cloud	phishing	
http://https://hosting-e899f.web.app/#ba11_go_coa_chf@emfa.pt	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://hosting-e899f.web.app/#ba11_go_coa_chf@emfa.pt	100%	UrlScan	phishing brand: outlook web access	Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\W3YTSHKB.htm	100%	Avira	HTML/Infected.WebPage.Gen	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
hosting-e899f.web.app	11%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
web.cytrack.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://hosting-e899f.web.app/	1%	Virustotal		Browse
http://https://hosting-e899f.web.app/	100%	Avira URL Cloud	phishing	
http://https://hosting-e899f.web.app/#ba11_go_coa_chf@emfa.pt	1%	Virustotal		Browse
http://https://web.cytrack.com/wpv1/wp-content/uploads/microsoft-outlook-logo.jpg	0%	Avira URL Cloud	safe	
http://fontawesome.iohttp://fontawesome.iohttp://fontawesome.io/license/http://fontawesome.io/licens	0%	Avira URL Cloud	safe	
http://https://aogtechnics.cc/aa.php	0%	Avira URL Cloud	safe	
http://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://https://hosting-e899f.web.app/#ba11_go_coa_chf	100%	Avira URL Cloud	phishing	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hosting-e899f.web.app	151.101.1.195	true	true	• 11%, Virustotal, Browse	unknown
cdnjs.cloudflare.com	104.16.18.94	true	false		high
web.cytrack.com	20.37.219.194	true	false	• 0%, Virustotal, Browse	unknown
stackpath.bootstrapcdn.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
cdn.jsdelivr.net	unknown	unknown	false		high
maxcdn.bootstrapcdn.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://hosting-e899f.web.app/#ba11_go_coa_chf@emfa.pt	true	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://hosting-e899f.web.app/	~DFCEAC2B6E86150DAD.TMP.1.dr	true	• 1%, Virustotal, Browse • Avira URL Cloud: phishing	unknown
http://fontawesome.io	fontawesome-webfont[1].eot.2.dr, font-awesome.min[1].css.2.dr	false		high
http://fontawesome.io/license/	fontawesome-webfont[1].eot.2.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.0/umd/popper.min.js	W3YTSHKB.htm.2.dr	false		high
http://https://github.com/twbs/bootstrap/graphs/contributors)	bootstrap.min[1].js.2.dr	false		high
http://https://code.jquery.com/jquery-migrate-3.1.0.min.js	W3YTSHKB.htm.2.dr	false		high
http://https://web.cytrack.com/wpv1/wp-content/uploads/microsoft-outlook-logo.jpg	W3YTSHKB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://fontawesome.iohttp://fontawesome.iohttp://fontawesome.io/license/http://fontawesome.io/licens	fontawesome-webfont[1].eot.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css	W3YTSHKB.htm.2.dr	false		high
http://https://stackpath.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css	W3YTSHKB.htm.2.dr	false		high
http://https://stackpath.bootstrapcdn.com/bootstrap/4.1.0/js/bootstrap.min.js	W3YTSHKB.htm.2.dr	false		high
http://https://aogtechnics.cc/aa.php	W3YTSHKB.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.jsdelivr.net/npm/sweetalert2	W3YTSHKB.htm.2.dr	false		high
http://getbootstrap.com)	bootstrap.min[1].css.2.dr	false	• Avira URL Cloud: safe	low
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap.min[1].js.2.dr, bootstrap.min[1].css.2.dr	false		high
http://https://hosting-e899f.web.app/#ba11_go_coa_chf	~DFCEAC2B6E86150DAD.TMP.1.dr, {914E1A2B-2FCF-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: phishing	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://opensource.org/licenses/MIT).	popper.min[1].js.2.dr	false		high
http://https://getbootstrap.com/)	bootstrap.min[1].js.2.dr	false		high
http://https://code.jquery.com/jquery-3.3.1.min.js	W3YTSHKB.htm.2.dr	false		high
http://fontawesome.io/license	font-awesome.min[1].css.2.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
20.37.219.194	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
104.16.18.94	unknown	United States		13335	CLOUDFLARENETUS	false
151.101.1.195	unknown	United States		54113	FASTLYUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323112
Start date:	26.11.2020
Start time:	11:09:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://hosting-e899f.web.app/#ba11_go_coa_chf@emfa.pt
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:	4
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:	• EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.phis.win@3/16@7/3
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): ielowutil.exe, backgroundTaskHost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.193.48, 104.83.120.32, 13.88.21.125, 209.197.3.15, 209.197.3.24, 151.101.2.109, 151.101.66.109, 151.101.130.109, 151.101.194.109, 51.104.139.180 • Excluded domains from analysis (whitelisted): e11290.dspg.akamaiedge.net, cds.s5x3j6q5.hwcdn.net, go.microsoft.com, arc.msn.com.nsatc.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, cds.j3z9t3p6.hwcdn.net, watson.telemetry.microsoft.com, skypedataprdcolwus15.cloudapp.net, arc.msn.com, dualstack.f3.shared.global.fastly.net, skypedataprdcolcus15.cloudapp.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{914E1A29-2FCF-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33368
Entropy (8bit):	1.8693600818176375
Encrypted:	false
SSDEEP:	192:rCZFZM2Z9WTt2if4g6zMsyBdsDiyBcytqgJj3:r+r7ZURHBz05DV
MD5:	8D90D300BFF877DB3F79063721DED3AB
SHA1:	8317DA19166839C93666DD1A57FC14B640773031
SHA-256:	C47CEDB3C5300EF0FA60E89827BA35DFF7F0DA35121A0F3C7CF4047DB0BD811C
SHA-512:	4DC7EFA74EE5ABB4796356247B312DD5C3A61C58670A64FC77176FDE0396111E667AE3DCC4EA381C057B89461B70F628A1D8E7BF375337B79589C566DFCF292
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\{914E1A2B-2FCF-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27794
Entropy (8bit):	1.8264769621143095
Encrypted:	false
SSDEEP:	192:rrZoQw6P7kPFjp29kW1/MUxYF1u1G1rS+ir:r9RbPAPh4hu4Q111rSp
MD5:	46C83BCECEB5A1CB14E55929705C4707
SHA1:	38DEFED1B04794F213027519466DDF97DEC813A4
SHA-256:	E2B9FDDA268D69BFE66639831604173149CAE35978528B61726D3FC4A693FC7F
SHA-512:	11CE403B5F21A32E65B5372B7E3EC592096D6CEBA2E0F7F1656CD4505B5EC12EF870489DDE6DF1E10B17732C858AF240E5663702ADB9A0DFB509FEC5EDC070 0
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\{9A14E6E9-2FCF-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5663805649023126
Encrypted:	false
SSDEEP:	48:IwEGcprBGwpa+WG4pQcQhGrapbSdrGQpKLG7HpRVsTGIpG:rYZbQ96dxBSdFAKTV4A
MD5:	BB83D06ABD79FDECEDC1FC1176C4B001
SHA1:	46F2DF672037C184060AA639C6FF4FD82BD1B893
SHA-256:	3147801780D70A53E413629A29AC21BE0317B6DCC7BA7BDFC8D321AEAAC5E6DC
SHA-512:	41CA487D425847C50A0496DA3746507AC7240446FC3C72A29F47B1166E55790B07E8ED01D3492E378F3F096FEA6AED0C9DAFD506C46BCFCD1EFABBDD7CCE4 C
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\W3YTSHKB.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	46606

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\W3YTSHKB.htm

Entropy (8bit):	5.558251906424499
Encrypted:	false
SSDEEP:	384:VxkmkDmJnN+klvXFk2JHfgPD5uh1xjHEZJhCt8fIzIAKNePhd7As6eBMLNHgsHYW:F+wWE7fw8ePpJkCuYA/N
MD5:	DA583C1806EF55AA22B603C88C86677E
SHA1:	02B54F8E8872DFB50B0C3900114C968408398A88
SHA-256:	9777D2C3F99F378EA8A3B20CBD84349E7639277CA946D010868548AE730A2839
SHA-512:	DF24772ED382D1E4CF4D35BCDEBA68DD9F4717821292F1DDDE24D1EC8FFA561692D873F80C5CD2CC579017E9C36238557C4FD98FF0741CB9DB3076D4EC7AD 6
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\W3YTSHKB.htm, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
IE Cache URL:	http://https://hosting-e899f.web.app/
Preview:	<html lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. .. <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">.. <meta name="description" content="">.. <meta name="author" content="">.. .... <title>Signin Outlook WebApp Settings</title>..<script>..alert ('Confirm session to view')..</script>.. Bootstrap core CSS -->..<link rel="shortcut icon" href=" AAANgAAABgYAAABACAAiAkAAN4QAAAQEAAAAQAgAGgEAABmGgAAKAAAACAAAABAAAAAAQAgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAMJsABsAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAxG8ADMRvADbDbgBmw20AlsNtAMPDbADtwmwA/wAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAx3MAMMdzAFrFcgCHxXEAtMVwA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\fontawesome-webfont[1].eot

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), FontAwesome family
Category:	downloaded
Size (bytes):	165742
Entropy (8bit):	6.705073372195656
Encrypted:	false
SSDEEP:	3072:qbhEnD+IzsU9z9QJ6/P3Xe2iEiEPGFCMW1JVJG6wVTDsk6BmG6S1yKshojskO+b2:qenD+IzsU9z9QJ6/PO2FiEP2C/DVJG6I
MD5:	674F50D287A8C48DC19BA404D20FE713
SHA1:	D980C2CE873DC43AF460D4D572D441304499F400
SHA-256:	7BFCAB6DB99D5CFBF1705CA0536DDC78585432CC5FA41BBD7AD0F009033B2979
SHA-512:	C160D3D77E67EFF986043461693B2A831E1175F579490D7F0B411005EA81BD4F5850FF534F6721B727C002973F3F9027EA960FAC4317D37DB1D4CB53EC9D343A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://stackpath.bootstrapcdn.com/font-awesome/4.7.0/fonts/fontawesome-webfont.eot?
Preview:	n................................LP........................Yx.....................F.o.n.t.A.w.e.s.o.m.e.....R.e.g.u.l.a.r...$.V.e.r.s.i.o.n. .4...7...0. .2.0.1.6.....F.o.n.t.A.w.e.s.o.m.e................PFFTMk .G.........GDEF.......p... OS/2.2z@...X...`cmap..:.........gasp.......h....glyf...M......L.head...-.......6hhea...........$hmtxEy..........loca...\........maxp.,.....8... name....gh....post......k.... u.........xY_.<..........3.2.....3.2..'...............@.........i.........3.......3...s...............................pyrs.@. ....p.....U.................... ....]...y...n.......................................2.......................................@.. ....z.............................

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\microsoft-outlook-logo[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1275 x 550, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	17498
Entropy (8bit):	7.629418772586848
Encrypted:	false
SSDEEP:	384:Q9eLWV38uPhyQp4Y9t4h7iJQ+rjk6aq8F8jK1EmuM2w:Q9eLWTy0vtciq+rjLTM8jKOmuBw
MD5:	F29CA798184F9DCF518C0F235CAA0BDB
SHA1:	8C7D869A15A74AEC6623EAB97739ADE716390CF7
SHA-256:	09F2AF8997DCF4C4754B78BF337519D137537F5E08A3E31FBE989FF1E4DEC6BA
SHA-512:	BD71463BDF0525A17A8341F25854676D276CF3BB6C925BC67D28641E1F088DD0084DB28D1C47DBB06F810267BFA8EED9292E632714F66DFB7375686AE459D9E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://web.cytrack.com/wpv1/wp-content/uploads/microsoft-outlook-logo.jpg
Preview:	.PNG........IHDR.......&.....%.......pHYs...#...#.x.?v....tEXtSoftware.Adobe ImageReadyq.e<..C.IDATx...Ol..'......$...eD.)@.>...aga.f.f..H.{..FT6.x#.'$./.i8.iC.i.L6...d..i`z.f..^.. ...g'@...K.. ..B...d..).d..w.y..........{...O?........./5......A.............@&.}......a.....dB.............@&.}......a.....dB.............@&.}......a.....dB.............@&.}......a.....dB.............@&.}..... .a.....dB.............@&.}......a.....dB.............@&.}......a.....dB.............@&.}......a.....dB.............@&.}......a.....dB.............@&.}......a.....dB.............@& .}......a.....dB.............@&.}......a.....dB.............@&.}......a.....dB.............@&.}......a.....dB.............@&.}......a.....dB.............@&.}......a.....dB........ .....@&.}......a.....dB.............@&.}......a.....dB.............@&.}......a.....dB.............@&.}......a.....dB............:.85~X....."....J..d....}...6*.po..[...4........

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\jquery-3.3.1.min[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\jquery-3.3.1.min[1].js	
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	86927
Entropy (8bit):	5.289226719276158
Encrypted:	false
SSDEEP:	1536:jLiBdiaWLOczCmZx6+VWuGzQNOzdn6x2RZd9SEnk9HB96c9Yo/NWLbVj3kC6t3:5kn6x2xe9NK6nC69
MD5:	A09E13EE94D51C524B7E2A728C7D4039
SHA1:	0DC32DB4AA9C5F03F3B38C47D883DBD4FED13AAE
SHA-256:	160A426FF2894252CD7CEBBDD6D6B7DA8FCD319C65B70468F10B6690C45D02EF
SHA-512:	F8DA8F95B6ED33542A88AF19028E18AE3D9CE25350A06BFC3FBF433ED2B38FEFA5E639CDDFDAC703FC6CAA7F3313D974B92A3168276B3A016CEB28F27DB071 4A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-3.3.1.min.js
Preview:	/*! jQuery v3.3.1 | (c) JS Foundation and other contributors | jquery.org/license */!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery requires a window with a document");return t(e)}:t(e)}("undefined"!=typeof window?window:this,function(e,t){"use strict";var n=[],r=e.document,i=Object.getPrototypeOf,o=n.slice,a=n.concat,s=n.push,u=n.indexOf,l={},c=l.toString,f=l.hasOwnProperty,p=f.toString,d=p.call(Object),h={},g=function e(t){return"function"==typeof t&&"number"!=typeof t.nodeType},y=function e(t){return null!=t&&t===t.window},v={type:!0,src:!0,noModule:!0};function m(e,t,n){var i,o=(t=t||r).createElement("script");if(o.text=e,n)for(i in v)n[i]&&(o[i]=n[i]);t.head.appendChild(o).parentNode.removeChild(o)}function x(e){return null==e?e+"":"object"==typeof e||"function"==typeof e?l[c.call(e)]||"object":typeof e}var b="3.3.1",w=function(e,t){return new w.fn.init(e,t)},

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\jquery-migrate-3.1.0.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	8990
Entropy (8bit):	5.183972790029302
Encrypted:	false
SSDEEP:	96:5r3UrDAWhTAETMu3QXveMIIa8JdFFh7MyAgxr3KFBF/s++EHzDFvsiMAg:5rkrDNhTeeMIIa8J/Eg96DBs+hl8
MD5:	FB30815EC2C19CCADB318BA4E225F1FB
SHA1:	84B5946817F8C166BFA2D6F881E3462297CDF02F
SHA-256:	C9C25E5DB965F66EDD1CA79A3DB5C19191FC06E3FDF5298F9BFF2AE4EF926C17
SHA-512:	00DD08E4FDD0D608D987871CC1E1368BEB536DD7CF495401A88759E4A547FA3EF225E47DD3B80A70B19921C138E839651DC21D5C22A7C7F49B16DDE7008933
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-migrate-3.1.0.min.js
Preview:	/*! jQuery Migrate v3.1.0 | (c) OpenJS Foundation and other contributors | jquery.org/license */."undefined"==typeof jQuery.migrateMute&&(jQuery.migrateMute=!0),function(t){"function"==typeof define&&define.amd?define(["jquery"],function(e){return t(e,window)}):"object"==typeof module&&module.exports?module.exports=t(require("jquery"),window):t(jQuery,window)}(function(s,n){"use strict";function e(e){return 0<=function(e,t){for(var r=/^(\d+)\.(\d+)\.(\d+)/,n=r.exec(e)||[],o=r.exec(t)||[],i=1;i<=3;i++){if(+n[i]>+o[i])return 1;if(+n[i]<+o[i])return-1}return 0}(s.fn.jquery,e)}s.migrateVersion="3.1.0",n.console&&n.console.log&&(s&&e("3.0.0")||n.console.log("JQMIGRATE: jQuery 3.0.0+ REQUIRED"),s.migrateWarnings&&n.console.log("JQMIGRATE: Migrate plugin loaded multiple times"),n.console.log("JQMIGRATE: Migrate is installed"+(s.migrateMute?"":" with logging active")+", version "+s.migrateVersion));var r={};function u(e){var t=n.console;r[e]||(r[e]=!0,s.migrateWarnings.push(e),t&&t.warn&&!s.mi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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):	20495
Entropy (8bit):	5.217693761954058
Encrypted:	false
SSDEEP:	384:f5LFrVVVnCQvIR/CFU4hHPV4kdxXvYqo2D75zCx+vI2am3MxGpGTgd/9jt9+Db9A:hNVVVnyiU41xXvlD7wx+v0xyGTgnZO9A
MD5:	6B08DDC901000D51FA1F06A35518F302
SHA1:	BAFE987C18CBE0587DE3E6360E7DA40A2885614B
SHA-256:	02835066969199E9924F1332F7172A5D7E552F023A20C3D8BA03BB6C51CE5BE5
SHA-512:	7A97FA1CF4A12D0F338090F8A4FFAD48D91843D6955304DE5F6208DE394642B0B412D6FD30D7A880CAD92200A8F7F2005C40324BCCE3CFEDA7B14A57DFF098(A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.0/umd/popper.min.js
Preview:	/*. Copyright (C) Federico Zivolo 2018. 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|overlay)/.test(r+s+p)?e:n(o(e))}function r(e){if(!e)return document.documentElement;for(var o=ie(10)?document.body:null,n=e.offsetParent;n===o&&e.nextElementSibling;)n=(e=e.nextElementSibling).offsetParent;var i=n&&n.nodeName;return i&&'BODY'!==i&&'HTM

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\sweetalert2@9[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	67061
Entropy (8bit):	5.291009976660428
Encrypted:	false
SSDEEP:	768:La+DIKBK6bAQ145wPkXuzZuY3fNwodZeW9RuRdmPu4uqrHiWQ4ewoLw3cOcNBfwX:LaOBrL45wNgY3FwgkWaRdfsVe9wCO
MD5:	5F896C5A35E509118ADD8FDCE8577B90
SHA1:	228678EF16B656AB01F2CE84AA563D85DA36A516
SHA-256:	2950BC3FD628CB8A8C6B1367F664E31353A6FF9EDD99C3F2831CE548610A05B0
SHA-512:	8D74E0000B2173F05106F0DD1162A4746DFF25A9FDA8C92D278F7834176099FB3BD72720F152DF18A2654F93E86516C169379607D4388CAD48E18BC18C618FAB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.jsdelivr.net/npm/sweetalert2@9
Preview:	!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?module.exports=e():"function"==typeof define&&define.amd?define(e):(t=t||self).Sweetalert2=e()}(this,function(){"use strict";function r(t){return(r="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})(t)}function a(t,e){if(!(t instanceof e))throw new TypeError("Cannot call a class as a function")}function o(t,e){for(var n=0;n<e.length;n++){var o=e[n];o.enumerable=o.enumerable||!1,o.configurable=!0,"value"in o&&(o.writable=!0),Object.defineProperty(t,o.key,o)}}function c(t,e,n){return e&&o(t.prototype,e),n&&o(t,n),t}function s(){return(s=Object.assign||function(t){for(var e=1;e<arguments.length;e++){var n=arguments[e];for(var o in n)Object.prototype.hasOwnProperty.call(n,o)&&(t[o]=n[o])}return t}).apply(this,arguments)}function u(t){return(u=Object.setPrototypeOf?Object.ge

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\bootstrap.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	121200
Entropy (8bit):	5.0982146191887106
Encrypted:	false
SSDEEP:	768:Vy3Gxw/Vc/QWlJxtQOIuiHlq5mzI4X8OAduFKbv2ctg2Bd8JP7ecQVvH1FS:nw/a1fIuiHlq5mN8lDbNmPbh
MD5:	EC3BB52A00E176A7181D454DFFAEA219
SHA1:	6527D8BF3E1E9368BAB8C7B60F56BC01FA3AFD68
SHA-256:	F75E846CC83BD11432F4B1E21A45F31BC85283D11D372F7B19ACCD1BF6A2635C
SHA-512:	E8C5DAF01EAE68ED7C1E277A6E544C7AD108A0FA877FB531D6D9F2210769B7DA88E4E002C7B0BE3B72154EBF7CBF01A795C8342CE2DAD368BD6351E956195F8B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css
Preview:	/*!. * Bootstrap v3.3.7 (http://getbootstrap.com). * Copyright 2011-2016 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). *//*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */html{font-family:sans-serif;-webkit-text-size-adjust:100%;-ms-text-size-adjust:100%}body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background-color:transparent}a:active,a:hover{outline:0}abbr[title]{border-bottom:1px dotted}b,strong{font-weight:700}dfn{font-style:italic}h1{margin:.67em 0;font-size:2em}mark{color:#000;background:#ff0}small{font-size:80%}sub,sup{position:relative;font-size:75%;line-height:0;vertical-align:baseline}sup{top:-.5em}sub{bottom:-.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:1em 40px}hr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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):	50676
Entropy (8bit):	5.276454699305197
Encrypted:	false
SSDEEP:	768:D2Ybgh0GBxTHVmcmjWSLsynS/zZ/AcyUenY8yiKKdHPPm26Ro1FH4nx46:D2jh02Lh+SbZ/AbYqdm2mx46
MD5:	CE6E785579AE4CB555C9DE311D1B9271
SHA1:	5EF2C15B47D7290698C737676BA9C3056B45F2E8
SHA-256:	0BCA10549DF770AB6790046799E5A9E920C286453EBBB2AFB0D3055339245339
SHA-512:	A601871568C1B5B2874D30D6E5BB8667D994D2719FC4D6AF7F99162BF39DDAE800FFFF45B8C1C0BA790088C7B98DE2FFE565B5AF4531C0A8BA0F92E930E243DF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://stackpath.bootstrapcdn.com/bootstrap/4.1.0/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v4.1.0 (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,c){"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 o(t,e,n){return e&&i(t.prototype,e),n&&i(t,n),t}function h(r){for(var t=1;t<arguments.length;t++){var s=null!=arguments[t]?arguments[t]:{},e=Object.keys(s);"function"==typeof Object.getOwnPropertySymbols&&(e=e.concat(Object.getOwnPropertySymbols(s).filter(function(t){return Object.getOwnPropertyDescriptor(s,t).enum

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\font-awesome.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	31000
Entropy (8bit):	4.746143404849733
Encrypted:	false
SSDEEP:	384:wHu5yWeTUKW+KlkJ5de2UYDyVfwYUas2l8yQ/8dwmaU8G:wwlr+Klk3Yi+fwYUf2l8yQ/e9vf
MD5:	269550530CC127B6AA5A35925A7DE6CE
SHA1:	512C7D79033E3028A9BE61B540CF1A6870C896F8
SHA-256:	799AEB25CC0373FDEE0E1B1DB7AD6C2F6A0E058DFADAA3379689F583213190BD
SHA-512:	49F4E24E55FA924FAA8AD7DEBE5FFB2E26D439E25696DF6B6F20E7F766B50EA58EC3DBD61B6305A1ACACD2C80E6E659ACCEE4140F885B9C9E71008E9001FBF4B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://stackpath.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css
Preview:	/*!. * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome. * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License). */@font-face{font-family:'FontAwesome';src:url('../fonts/fontawesome-webfont.eot?v=4.7.0');src:url('../fonts/fontawesome-webfont.eot?#iefix&v=4.7.0') format('embedded-opentype'),url('../fonts/fontawesome-webfont.woff2?v=4.7.0') format('woff2'),url('../fonts/fontawesome-webfont.woff?v=4.7.0') format('woff'),url('../fonts/fontawesome-webfont.ttf?v=4.7.0') format('truetype'),url('../fonts/fontawesome-webfont.svg?v=4.7.0#fontawesomeregular') format('svg');font-weight:normal;font-style:normal}.fa{display:inline-block;font:normal normal normal 14px/1 FontAwesome;font-size:inherit;text-rendering:auto;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}.fa-lg{font-size:1.33333333em;line-height:.75em;vertical-align:-15%}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-fw{width:1.

C:\Users\user\AppData\Local\Temp\~DFA016103DA3E62CDB.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\~DFCEAC2B6E86150DAD.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	35491
Entropy (8bit):	0.5159577453577496
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+Ye0F5l5p1nxH9WsH0xgsHx9H+yUV019:kBqoxKAuvScS+Ye0FOD1rexbH
MD5:	D1CC12ED85E5726CF650C7320CF5F8AA
SHA1:	A941F4031687E8EB965A0D17993E73F94B3EC3D1
SHA-256:	764C5D516454C3984059A038DB3AFE7F67A1C10CDF6D5B75D79F6AF714F20EFE
SHA-512:	A69EE9BE30CDAA588AC947C6112A3782A141E21E756D911274A2450547803F6FE2710FE0B31A89B3D26BBC2D4814D1D6507F9B58986ECDF109AA6C8ABC17B0F4
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFD904113CBEB3043B.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13077

C:\Users\user\AppData\Local\Temp\~DFD904113CBEB3043B.TMP	
Entropy (8bit):	0.5107925601985209
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loO9lo+9lWpKtKhog:kBqoIJfpakog
MD5:	8947C183AE0CC5D13D7851930D2EEBED
SHA1:	03800A883A8421136DF3CEB3E5D4A83F6A48F70F
SHA-256:	305B549287158E8EE6E5E876EF950B2CD1656D3554EC4A70B24A8F4BE3A5A538
SHA-512:	71BDD4E3F3EB34FFD914F2A14A75F23EB54F7F4E464A8C68B6C003C8F2C4A26EAE80FDF6D1F5F289707C5FCB1409CF16C1BD1E1CBFC3AD1EA308DBF91288F 9A
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
Nov 26, 2020 11:10:13.214504957 CET	49733	443	192.168.2.4	151.101.1.195
Nov 26, 2020 11:10:13.214777946 CET	49732	443	192.168.2.4	151.101.1.195
Nov 26, 2020 11:10:13.233553886 CET	443	49733	151.101.1.195	192.168.2.4
Nov 26, 2020 11:10:13.233660936 CET	443	49732	151.101.1.195	192.168.2.4
Nov 26, 2020 11:10:13.233702898 CET	49733	443	192.168.2.4	151.101.1.195
Nov 26, 2020 11:10:13.233758926 CET	49732	443	192.168.2.4	151.101.1.195
Nov 26, 2020 11:10:13.240789890 CET	49733	443	192.168.2.4	151.101.1.195
Nov 26, 2020 11:10:13.240869999 CET	49732	443	192.168.2.4	151.101.1.195
Nov 26, 2020 11:10:13.259911060 CET	443	49732	151.101.1.195	192.168.2.4
Nov 26, 2020 11:10:13.259953022 CET	443	49733	151.101.1.195	192.168.2.4
Nov 26, 2020 11:10:13.261313915 CET	443	49732	151.101.1.195	192.168.2.4
Nov 26, 2020 11:10:13.261370897 CET	443	49732	151.101.1.195	192.168.2.4
Nov 26, 2020 11:10:13.261430979 CET	443	49732	151.101.1.195	192.168.2.4
Nov 26, 2020 11:10:13.261470079 CET	443	49733	151.101.1.195	192.168.2.4
Nov 26, 2020 11:10:13.261468887 CET	49732	443	192.168.2.4	151.101.1.195

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 11:10:13.261507034 CET	443	49733	151.101.1.195	192.168.2.4
Nov 26, 2020 11:10:13.261526108 CET	49732	443	192.168.2.4	151.101.1.195
Nov 26, 2020 11:10:13.261543036 CET	443	49733	151.101.1.195	192.168.2.4
Nov 26, 2020 11:10:13.261631966 CET	49733	443	192.168.2.4	151.101.1.195
Nov 26, 2020 11:10:13.303335905 CET	49733	443	192.168.2.4	151.101.1.195
Nov 26, 2020 11:10:13.303493023 CET	49732	443	192.168.2.4	151.101.1.195
Nov 26, 2020 11:10:13.310501099 CET	49733	443	192.168.2.4	151.101.1.195
Nov 26, 2020 11:10:13.310714006 CET	49733	443	192.168.2.4	151.101.1.195
Nov 26, 2020 11:10:13.311014891 CET	49732	443	192.168.2.4	151.101.1.195
Nov 26, 2020 11:10:13.323400021 CET	443	49732	151.101.1.195	192.168.2.4
Nov 26, 2020 11:10:13.323527098 CET	49732	443	192.168.2.4	151.101.1.195
Nov 26, 2020 11:10:13.323904037 CET	443	49733	151.101.1.195	192.168.2.4
Nov 26, 2020 11:10:13.324011087 CET	49733	443	192.168.2.4	151.101.1.195
Nov 26, 2020 11:10:13.329402924 CET	443	49733	151.101.1.195	192.168.2.4
Nov 26, 2020 11:10:13.329602957 CET	49733	443	192.168.2.4	151.101.1.195
Nov 26, 2020 11:10:13.329931021 CET	443	49732	151.101.1.195	192.168.2.4
Nov 26, 2020 11:10:13.329987049 CET	49733	443	192.168.2.4	151.101.1.195
Nov 26, 2020 11:10:13.330061913 CET	49732	443	192.168.2.4	151.101.1.195
Nov 26, 2020 11:10:13.330914021 CET	49732	443	192.168.2.4	151.101.1.195
Nov 26, 2020 11:10:13.349139929 CET	443	49733	151.101.1.195	192.168.2.4
Nov 26, 2020 11:10:13.392190933 CET	443	49732	151.101.1.195	192.168.2.4
Nov 26, 2020 11:10:13.775377035 CET	443	49733	151.101.1.195	192.168.2.4
Nov 26, 2020 11:10:13.775418043 CET	443	49733	151.101.1.195	192.168.2.4
Nov 26, 2020 11:10:13.775446892 CET	443	49733	151.101.1.195	192.168.2.4
Nov 26, 2020 11:10:13.775469065 CET	443	49733	151.101.1.195	192.168.2.4
Nov 26, 2020 11:10:13.775490046 CET	443	49733	151.101.1.195	192.168.2.4
Nov 26, 2020 11:10:13.775512934 CET	443	49733	151.101.1.195	192.168.2.4
Nov 26, 2020 11:10:13.775535107 CET	443	49733	151.101.1.195	192.168.2.4
Nov 26, 2020 11:10:13.775557041 CET	443	49733	151.101.1.195	192.168.2.4
Nov 26, 2020 11:10:13.775578976 CET	443	49733	151.101.1.195	192.168.2.4
Nov 26, 2020 11:10:13.775777102 CET	49733	443	192.168.2.4	151.101.1.195
Nov 26, 2020 11:10:13.929409027 CET	49741	443	192.168.2.4	20.37.219.194
Nov 26, 2020 11:10:13.931085110 CET	49742	443	192.168.2.4	20.37.219.194
Nov 26, 2020 11:10:13.958470106 CET	49743	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:13.958775043 CET	49744	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:13.974642038 CET	443	49743	104.16.18.94	192.168.2.4
Nov 26, 2020 11:10:13.974772930 CET	49743	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:13.974853039 CET	443	49744	104.16.18.94	192.168.2.4
Nov 26, 2020 11:10:13.974915981 CET	49744	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:13.975682974 CET	49744	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:13.980380058 CET	49743	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:13.991864920 CET	443	49744	104.16.18.94	192.168.2.4
Nov 26, 2020 11:10:13.995945930 CET	443	49744	104.16.18.94	192.168.2.4
Nov 26, 2020 11:10:13.995982885 CET	443	49744	104.16.18.94	192.168.2.4
Nov 26, 2020 11:10:13.996042967 CET	49744	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:13.996076107 CET	49744	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:13.996423960 CET	443	49743	104.16.18.94	192.168.2.4
Nov 26, 2020 11:10:13.998498917 CET	443	49743	104.16.18.94	192.168.2.4
Nov 26, 2020 11:10:13.998532057 CET	443	49743	104.16.18.94	192.168.2.4
Nov 26, 2020 11:10:13.998572111 CET	49743	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:13.998599052 CET	49743	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:14.018486023 CET	49744	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:14.018872976 CET	49744	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:14.019009113 CET	49744	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:14.020313978 CET	49743	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:14.020708084 CET	49743	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:14.034667015 CET	443	49744	104.16.18.94	192.168.2.4
Nov 26, 2020 11:10:14.035007000 CET	443	49744	104.16.18.94	192.168.2.4
Nov 26, 2020 11:10:14.035082102 CET	443	49744	104.16.18.94	192.168.2.4
Nov 26, 2020 11:10:14.036257029 CET	443	49744	104.16.18.94	192.168.2.4
Nov 26, 2020 11:10:14.036345005 CET	49744	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:14.036530018 CET	443	49743	104.16.18.94	192.168.2.4
Nov 26, 2020 11:10:14.037127018 CET	443	49743	104.16.18.94	192.168.2.4
Nov 26, 2020 11:10:14.037813902 CET	443	49743	104.16.18.94	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 11:10:14.037882090 CET	49743	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:14.037888050 CET	443	49743	104.16.18.94	192.168.2.4
Nov 26, 2020 11:10:14.037914991 CET	443	49744	104.16.18.94	192.168.2.4
Nov 26, 2020 11:10:14.037946939 CET	49743	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:14.037976027 CET	49744	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:14.038371086 CET	49744	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:14.038717031 CET	49743	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:14.046627998 CET	443	49744	104.16.18.94	192.168.2.4
Nov 26, 2020 11:10:14.046658039 CET	443	49744	104.16.18.94	192.168.2.4
Nov 26, 2020 11:10:14.046694040 CET	443	49744	104.16.18.94	192.168.2.4
Nov 26, 2020 11:10:14.046709061 CET	49744	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:14.046727896 CET	443	49744	104.16.18.94	192.168.2.4
Nov 26, 2020 11:10:14.046730042 CET	49744	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:14.046741962 CET	49744	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:14.046768904 CET	443	49744	104.16.18.94	192.168.2.4
Nov 26, 2020 11:10:14.046777964 CET	49744	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:14.046807051 CET	443	49744	104.16.18.94	192.168.2.4
Nov 26, 2020 11:10:14.046822071 CET	49744	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:14.046838045 CET	443	49744	104.16.18.94	192.168.2.4
Nov 26, 2020 11:10:14.046863079 CET	49744	443	192.168.2.4	104.16.18.94
Nov 26, 2020 11:10:14.046875000 CET	443	49744	104.16.18.94	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 11:10:07.712003946 CET	53097	53	192.168.2.4	8.8.8.8
Nov 26, 2020 11:10:07.739326954 CET	53	53097	8.8.8.8	192.168.2.4
Nov 26, 2020 11:10:09.011113882 CET	49257	53	192.168.2.4	8.8.8.8
Nov 26, 2020 11:10:09.038132906 CET	53	49257	8.8.8.8	192.168.2.4
Nov 26, 2020 11:10:10.104419947 CET	62389	53	192.168.2.4	8.8.8.8
Nov 26, 2020 11:10:10.131508112 CET	53	62389	8.8.8.8	192.168.2.4
Nov 26, 2020 11:10:10.889187098 CET	49910	53	192.168.2.4	8.8.8.8
Nov 26, 2020 11:10:10.916388988 CET	53	49910	8.8.8.8	192.168.2.4
Nov 26, 2020 11:10:11.860346079 CET	55854	53	192.168.2.4	8.8.8.8
Nov 26, 2020 11:10:11.887475967 CET	53	55854	8.8.8.8	192.168.2.4
Nov 26, 2020 11:10:12.183099031 CET	64549	53	192.168.2.4	8.8.8.8
Nov 26, 2020 11:10:12.219897032 CET	53	64549	8.8.8.8	192.168.2.4
Nov 26, 2020 11:10:13.160981894 CET	63153	53	192.168.2.4	8.8.8.8
Nov 26, 2020 11:10:13.204593897 CET	53	63153	8.8.8.8	192.168.2.4
Nov 26, 2020 11:10:13.457982063 CET	52991	53	192.168.2.4	8.8.8.8
Nov 26, 2020 11:10:13.493746996 CET	53	52991	8.8.8.8	192.168.2.4
Nov 26, 2020 11:10:13.845880985 CET	53700	53	192.168.2.4	8.8.8.8
Nov 26, 2020 11:10:13.853771925 CET	51726	53	192.168.2.4	8.8.8.8
Nov 26, 2020 11:10:13.872951031 CET	53	53700	8.8.8.8	192.168.2.4
Nov 26, 2020 11:10:13.880796909 CET	53	51726	8.8.8.8	192.168.2.4
Nov 26, 2020 11:10:13.886550903 CET	56794	53	192.168.2.4	8.8.8.8
Nov 26, 2020 11:10:13.898910046 CET	56534	53	192.168.2.4	8.8.8.8
Nov 26, 2020 11:10:13.914287090 CET	56627	53	192.168.2.4	8.8.8.8
Nov 26, 2020 11:10:13.925924063 CET	53	56534	8.8.8.8	192.168.2.4
Nov 26, 2020 11:10:13.926657915 CET	53	56794	8.8.8.8	192.168.2.4
Nov 26, 2020 11:10:13.934348106 CET	56621	53	192.168.2.4	8.8.8.8
Nov 26, 2020 11:10:13.941194057 CET	53	56627	8.8.8.8	192.168.2.4
Nov 26, 2020 11:10:13.971112967 CET	53	56621	8.8.8.8	192.168.2.4
Nov 26, 2020 11:10:14.670855999 CET	63116	53	192.168.2.4	8.8.8.8
Nov 26, 2020 11:10:14.697931051 CET	53	63116	8.8.8.8	192.168.2.4
Nov 26, 2020 11:10:15.495791912 CET	64078	53	192.168.2.4	8.8.8.8
Nov 26, 2020 11:10:15.522854090 CET	53	64078	8.8.8.8	192.168.2.4
Nov 26, 2020 11:10:16.359572887 CET	64801	53	192.168.2.4	8.8.8.8
Nov 26, 2020 11:10:16.395101070 CET	53	64801	8.8.8.8	192.168.2.4
Nov 26, 2020 11:10:17.410773993 CET	61721	53	192.168.2.4	8.8.8.8
Nov 26, 2020 11:10:17.446626902 CET	53	61721	8.8.8.8	192.168.2.4
Nov 26, 2020 11:10:21.745234966 CET	51255	53	192.168.2.4	8.8.8.8
Nov 26, 2020 11:10:21.772262096 CET	53	51255	8.8.8.8	192.168.2.4
Nov 26, 2020 11:10:23.132600069 CET	61522	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 11:10:23.160042048 CET	53	61522	8.8.8.8	192.168.2.4
Nov 26, 2020 11:10:24.258807898 CET	52337	53	192.168.2.4	8.8.8.8
Nov 26, 2020 11:10:24.285890102 CET	53	52337	8.8.8.8	192.168.2.4
Nov 26, 2020 11:10:25.066437006 CET	55046	53	192.168.2.4	8.8.8.8
Nov 26, 2020 11:10:25.093611002 CET	53	55046	8.8.8.8	192.168.2.4
Nov 26, 2020 11:10:26.107953072 CET	49612	53	192.168.2.4	8.8.8.8
Nov 26, 2020 11:10:26.135150909 CET	53	49612	8.8.8.8	192.168.2.4
Nov 26, 2020 11:10:30.766973972 CET	49285	53	192.168.2.4	8.8.8.8
Nov 26, 2020 11:10:30.794354916 CET	53	49285	8.8.8.8	192.168.2.4
Nov 26, 2020 11:10:31.661400080 CET	50601	53	192.168.2.4	8.8.8.8
Nov 26, 2020 11:10:31.688523054 CET	53	50601	8.8.8.8	192.168.2.4
Nov 26, 2020 11:10:31.904859066 CET	60875	53	192.168.2.4	8.8.8.8
Nov 26, 2020 11:10:31.931792021 CET	53	60875	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 26, 2020 11:10:13.160981894 CET	192.168.2.4	8.8.8.8	0x23b5	Standard query (0)	hosting-e8 99f.web.app	A (IP address)	IN (0x0001)
Nov 26, 2020 11:10:13.845880985 CET	192.168.2.4	8.8.8.8	0x8105	Standard query (0)	maxcdn.boo tstrapcdn.com	A (IP address)	IN (0x0001)
Nov 26, 2020 11:10:13.853771925 CET	192.168.2.4	8.8.8.8	0x6a52	Standard query (0)	stackpath. bootstrapc dn.com	A (IP address)	IN (0x0001)
Nov 26, 2020 11:10:13.886550903 CET	192.168.2.4	8.8.8.8	0xe447	Standard query (0)	web.cytrack.com	A (IP address)	IN (0x0001)
Nov 26, 2020 11:10:13.898910046 CET	192.168.2.4	8.8.8.8	0x8ffa	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Nov 26, 2020 11:10:13.914287090 CET	192.168.2.4	8.8.8.8	0x1c02	Standard query (0)	cdnjs.clou dflare.com	A (IP address)	IN (0x0001)
Nov 26, 2020 11:10:13.934348106 CET	192.168.2.4	8.8.8.8	0x6207	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 11:10:13.204593897 CET	8.8.8.8	192.168.2.4	0x23b5	No error (0)	hosting-e8 99f.web.app		151.101.1.195	A (IP address)	IN (0x0001)
Nov 26, 2020 11:10:13.204593897 CET	8.8.8.8	192.168.2.4	0x23b5	No error (0)	hosting-e8 99f.web.app		151.101.65.195	A (IP address)	IN (0x0001)
Nov 26, 2020 11:10:13.872951031 CET	8.8.8.8	192.168.2.4	0x8105	No error (0)	maxcdn.boo tstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 11:10:13.880796909 CET	8.8.8.8	192.168.2.4	0x6a52	No error (0)	stackpath. bootstrapc dn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 11:10:13.925924063 CET	8.8.8.8	192.168.2.4	0x8ffa	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 11:10:13.926657915 CET	8.8.8.8	192.168.2.4	0xe447	No error (0)	web.cytrack.com		20.37.219.194	A (IP address)	IN (0x0001)
Nov 26, 2020 11:10:13.941194057 CET	8.8.8.8	192.168.2.4	0x1c02	No error (0)	cdnjs.clou dflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Nov 26, 2020 11:10:13.941194057 CET	8.8.8.8	192.168.2.4	0x1c02	No error (0)	cdnjs.clou dflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Nov 26, 2020 11:10:13.971112967 CET	8.8.8.8	192.168.2.4	0x6207	No error (0)	cdn.jsdelivr.net	dualstack.f3.shared.globa l.fastly.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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 26, 2020 11:10:13.261370897 CET	151.101.1.195	443	192.168.2.4	49732	CN=web.app, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Apr 16 00:30:23 CEST 2020 Thu Jun 15 02:00:42 CEST 2017	Thu Apr 15 00:30:23 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Nov 26, 2020 11:10:13.261507034 CET	151.101.1.195	443	192.168.2.4	49733	CN=web.app, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Apr 16 00:30:23 CEST 2020 Thu Jun 15 02:00:42 CEST 2017	Thu Apr 15 00:30:23 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Nov 26, 2020 11:10:13.995982885 CET	104.16.18.94	443	192.168.2.4	49744	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 26, 2020 11:10:13.998532057 CET	104.16.18.94	443	192.168.2.4	49743	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 26, 2020 11:10:14.482079983 CET	20.37.219.194	443	192.168.2.4	49742	CN=web.cytrack.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Oct 20 01:30:37 CEST 2020 Thu Mar 17 17:40:46 CET 2016	Mon Jan 18 00:30:37 CET 2021 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 26, 2020 11:10:14.483596087 CET	20.37.219.194	443	192.168.2.4	49741	CN=web.cytrack.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Oct 20 01:30:37 CEST 2020 Thu Mar 17 17:40:46 CET 2016	Mon Jan 18 00:30:37 CET 2021 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5860 Parent PID: 800

General

Start time:	11:10:11
Start date:	26/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7e3950000
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: 3984 Parent PID: 5860

General

Start time:	11:10:12
Start date:	26/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5860 CREDAT:17410 /prefetch:2
Imagebase:	0x2f0000
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