ID: 298795
Cookbook: browseurl.jbs
Time: 17:58:20
Date: 15/10/2020
Version: 30.0.0 Red Diamond

Table of Contents

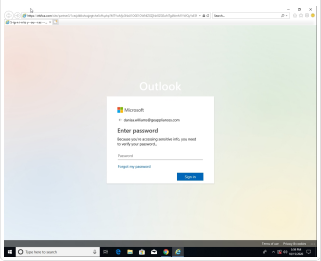
Analysis Report http://wuftzayaebbtzem.activeinernatio…

Overview

General Information

Sample URL:	http://wuftzayaebbtzem.activeinernational.com/espnx/ZGFuaXNhLndpbGxpYW1zQGdlYXBwbGlhbmNlcy5jb20=
Analysis ID:	298795

Most interesting Screenshot:



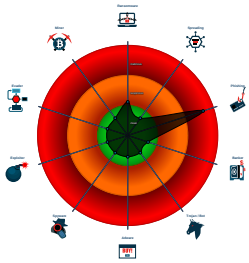
Detection

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

Signatures

- Antivirus / Scanner detection for sub…
- Phishing site detected (based on fav…
- Yara detected HtmlPhish_10
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- Invalid T&C link found

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 1876 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6392 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1876 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

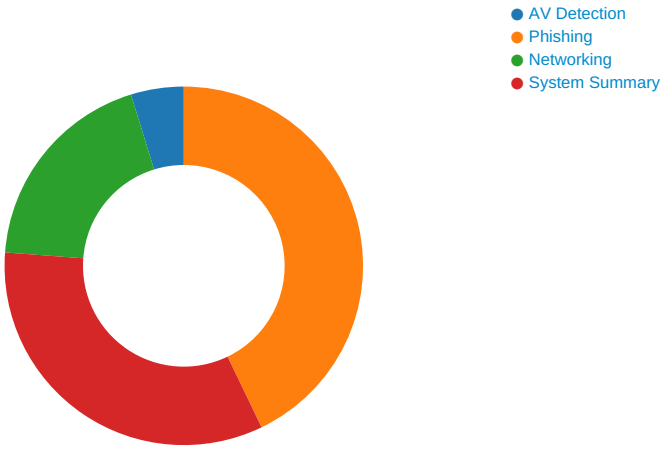
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\1cexjdblkshxqjegtvhe5cfh[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish_10

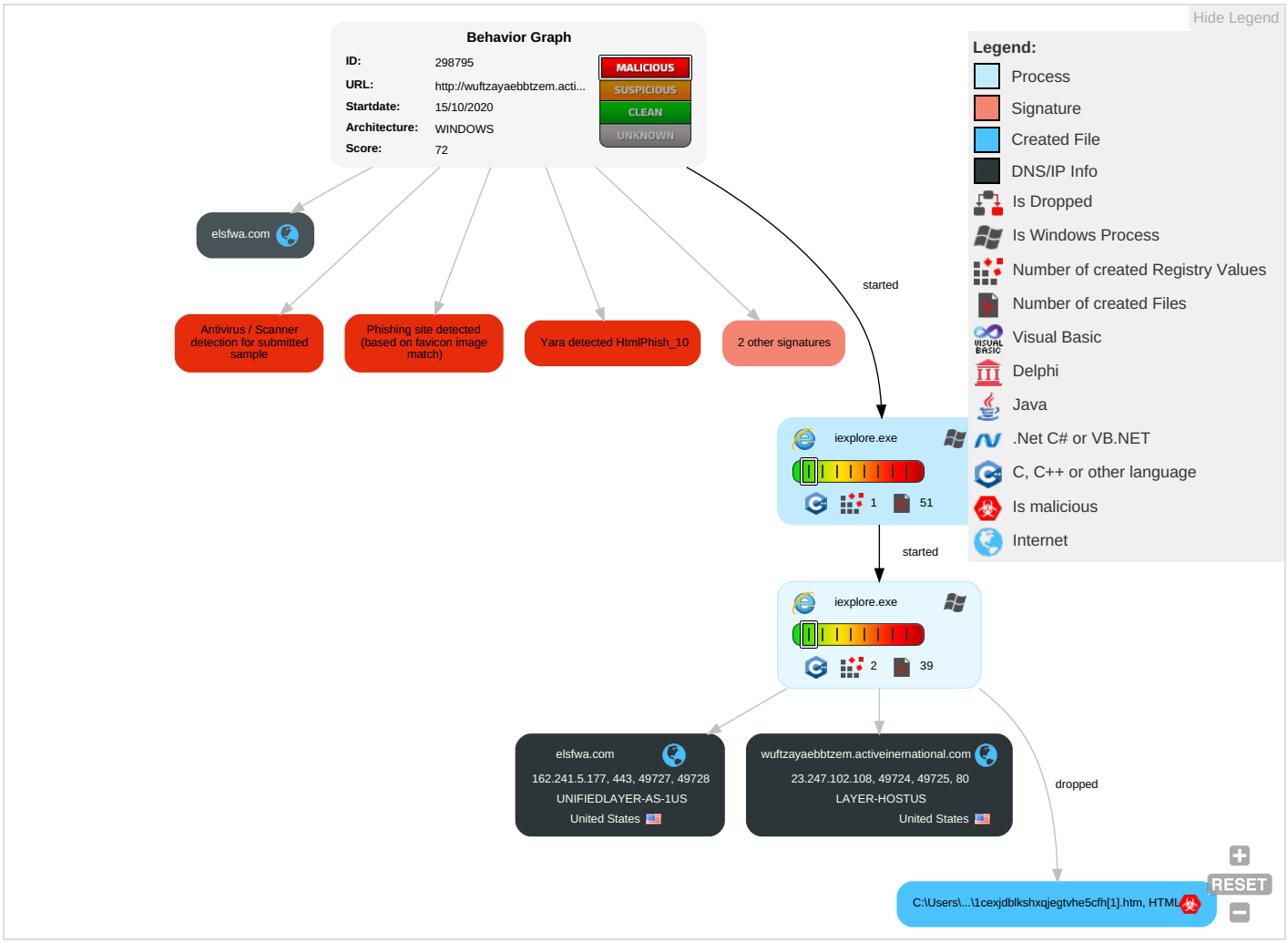
Phishing site detected (based on image similarity)

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

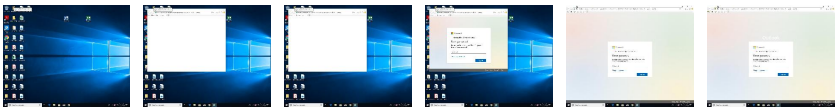
Behavior Graph

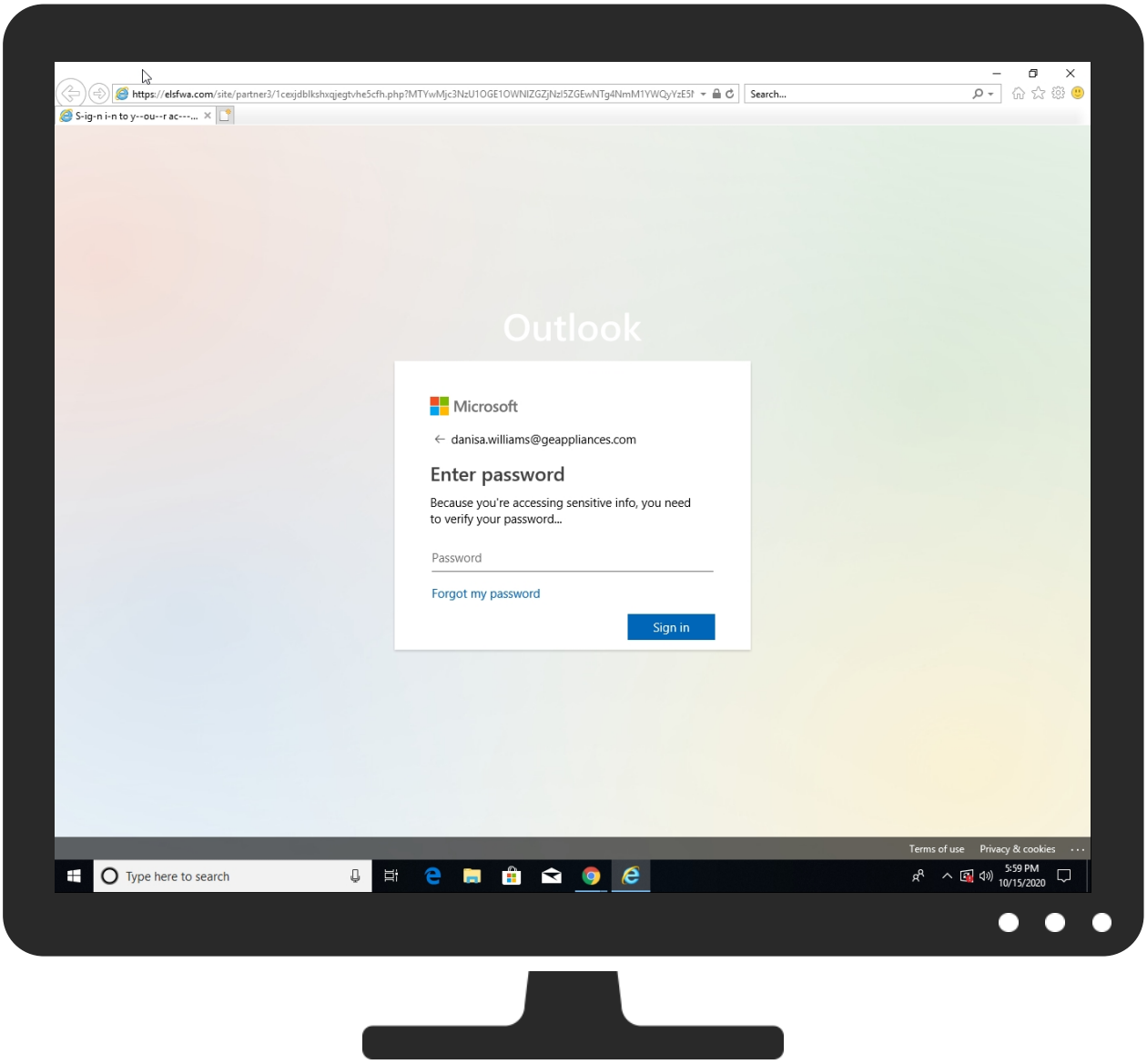


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://wuftzayaebbtzem.activeinernational.com/espnxx/ZGFuaXNhLndpbGxpYW1zQGdlYXBwbGlhbmNlcy5jb20=	0%	Virustotal		Browse
http://wuftzayaebbtzem.activeinernational.com/espnxx/ZGFuaXNhLndpbGxpYW1zQGdlYXBwbGlhbmNlcy5jb20=	0%	Avira URL Cloud	safe	
http://wuftzayaebbtzem.activeinernational.com/espnxx/ZGFuaXNhLndpbGxpYW1zQGdlYXBwbGlhbmNlcy5jb20=	100%	SlashNext	Fake Login Page type: Phishing & Social usering	
http://wuftzayaebbtzem.activeinernational.com/espnxx/ZGFuaXNhLndpbGxpYW1zQGdlYXBwbGlhbmNlcy5jb20=	100%	UrlScan	phishing brand: onedrive microsoft	Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
elsfwa.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://elsfwa.com/site/partner3/lib/img/favicon.ico~	0%	Avira URL Cloud	safe	
http://https://elsfwa.com/site/partner3/?danisa.williams	0%	Avira URL Cloud	safe	
http://https://elsfwa.com/site/partner3/1cexjdblkshxqjegtvhe5cfh.php?MTYwMjc3NzU1OGE1OWNlZGZjNzI5ZGEwNTg4Nm	0%	Avira URL Cloud	safe	
http://https://elsfwa.com/site/partner3/lib/img/favicon.ico	0%	Avira URL Cloud	safe	
http://https://elsfwa.com/site/partner3/lib/img/favicon.ico~(	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
wuftzayaebbtzem.activeinernational.com	23.247.102.108	true	false		unknown
elsfwa.com	162.241.5.177	true	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://elsfwa.com/site/partner3/lib/img/favicon.ico~	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://elsfwa.com/site/partner3/?danisa.williams	ZGFuaXNhLndpbGxpYW1z QGdlYXBwbGlhbmNlcy5jb20=[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://elsfwa.com/site/partner3/1cexjdblkshxqjegtvhe5cfh.php?MTYwMjc3NzU1OGE1OWNlZGZjNzI5ZGEwNTg4Nm	{CD180BEF-0F4A-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://elsfwa.com/site/partner3/lib/img/favicon.ico	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://elsfwa.com/site/partner3/lib/img/favicon.ico~(	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Country	Flag	ASN	ASN Name	Malicious
162.241.5.177	United States		46606	UNIFIEDLAYER-AS-1US	false
23.247.102.108	United States		46573	LAYER-HOSTUS	false

General Information

Joe Sandbox Version:	30.0.0 Red Diamond
Analysis ID:	298795
Start date:	15.10.2020
Start time:	17:58:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://wuftzayaebbtzem.activeinernational.com/espnxx/ZGFuaXNhLndpbGxpYW1zQGdlYXBwbGlhbmNlcy5jb20=
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:	6
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@3/16@3/2
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 13.88.21.125, 184.85.150.82, 104.43.193.48, 51.104.144.132, 23.10.249.43, 23.10.249.26 • Excluded domains from analysis (whitelisted): e11290.dspg.akamaiedge.net, umwatsonrouting.trafficmanager.net, go.microsoft.com, arc.msn.com.nsatc.net, go.microsoft.com.edgekey.net, skypedataprdcolcus16.cloudapp.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, a1449.dscg2.akamai.net, skypedataprdcolwus15.cloudapp.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net

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.{CD180BED-0F4A-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8585783778246776
Encrypted:	false
SSDEEP:	96:rXoZRpZK2b9WCtJUrAfJAUAo81MWAjET0AdqR0c7+f0cXodlX:r4ZDZK2b9WCtpfcVMYICfnMX
MD5:	4DC6FF55C1CF15726A1FFA4FCBF2A7CD
SHA1:	B80F791E7070CF1681C5AEA43183899D6858BFF9
SHA-256:	699596D059D5F56A1A98B64E33887B18C8CD43101170FACA78B7FA82F7319B8B
SHA-512:	9C040EFFF667FA5F39070AAFC70C9041121BA5E8D696386827A19C65FD2143893C43D93BD01613746CB19B1B945F9E737D7B8AA4CB597F102E443CE2CBA1126E
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\{CD180BEF-0F4A-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	32608
Entropy (8bit):	2.1506771677357603
Encrypted:	false
SSDEEP:	192:r8Z3Qn60kTFjF/2FSkWFTMFFYL3xt32aYi0fSoWedg:r8g6ZThFuFmFQFFe3D32fM
MD5:	B663BB1638D4ADC9CFC4489A41F4ECAF
SHA1:	F77BD594A5548A7354C4C51DD9F2B2D906B48A88
SHA-256:	79FF769035F80AA50FEB3BD9C1BA365404555927AC08489629AD6096E8B8659A
SHA-512:	CEF9C1C5846414375C69BC85DAF1B3049DAFC1C997F292300AB7CE5B187F951462219B95B4C74F5913A8E7BC74904E9018333B26B5BF07BFA9ACA15EE111A10
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\{D7602CEB-0F4A-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.56666623880916
Encrypted:	false
SSDEEP:	48:IwjGcpr+GwpazG4pQpZGrapbSArGQpKukOG7HpRtsTGIpG:rZZ2QF6LBSAFAuKTt4A
MD5:	445C4B3975D6574A7564ADAE48C1FB25
SHA1:	99198AF8C0EED530B883C9BD326C8A11B2AE24D3
SHA-256:	7E59DC77B3E504730C30E4990A9B8836315852601ED6899AA5DDCFD10B8781B1
SHA-512:	EC960FB8488487AA8672A83214B07EE454B596974C014EEDB54B6B5B5B167A4EA36771AAA43A54BA8A1177E2EB40B0D7A2764D7EB2AB93577B4CFBE0256D6EB1
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\wlm7n14\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	18056
Entropy (8bit):	3.0609555086887297
Encrypted:	false
SSDEEP:	48:30E/LS0E/+S0E/2S0E/tgyyyyyyyyyyyyyfS0E/DiS0E/GQQQQQo4:aQQQQQN
MD5:	5959ECBB5136E892F298766BB5F81572
SHA1:	69AC3A3A0FE348B8F06EC89F2AC4CB7A395D5DC5
SHA-256:	D5FFEC74D0C4A85352EA4F1B3F16A45F70EF85EA7211D6EAEC4771D7759DF7A9
SHA-512:	FDDBBE6AD797ED7540BF59ED9E27BABAAEEEE6B8B8CBAACE5376A54A1917C53D57D8C2645E03393E3380FA8223A5CA6DF857FC5CBE1A109BCD65A9D1B1668E7E
Malicious:	false
Reputation:	low
Preview:	4.h.t.t.p.s.:././.e.l.s.f.w.a...c.o.m./.s.i.t.e./.p.a.r.t.n.e.r.3./.l.i.b./.i.m.g./.f.a.v.i.c.o.n...i.c.o.~(.....h(.....(.....("P.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\1cexjdblkshxqjegtvhe5cfh[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	4887
Entropy (8bit):	3.5038495050598293
Encrypted:	false
SSDEEP:	48:Ul53h2BAfWmvAavqWRt5pkf1A/GvIT7iUzdmv:CUBAfl7fpkmAupmv
MD5:	83CB6730AADA4FF0F7303D28543B675A
SHA1:	546DAF2A5FD075B7D545DEFA415B7CAF100D361C
SHA-256:	A4A9DE98E35CAD5783C533A32C757D5432E2A19300983C25519177B3D4AA083B
SHA-512:	8FD8F3A54B69BED66A292BC07C7354E03124C3BD7A7D95C5E3D5A901D320816C8BF85626B51943EF89213E2F84AF40B11D828F945A3CC70E58ACC4F5A8D4AD6
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\1cexjdblkshxqjegtvhe5cfh[1].htm, Author: Joe Security
Reputation:	low
Preview:	<html dir=ltr lang=en>..<title>S.ig.n i.n to y..ou..r ac...cou.nt</title>..<link href=lib/img/favicon.ico rel="shortcut icon">..<link href=lib/css/login.css rel=stylesheet>.. .. .. <form method=post action=process>.. .. .. ..<img src=lib/img/logo3.png class=background-logo>.. .. ..<img src=lib/img/logo2.svg class=logo>.. .. ..<img src=lib/img/arrow.svg>......<div class=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\background[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\background[1].jpg	
File Type:	[TIFF image data, big-endian, direntries=4, xresolution=62, yresolution=70, resolutionunit=2], progressive, precision 8, 1920x1080, frames 3
Category:	downloaded
Size (bytes):	31419
Entropy (8bit):	7.838593850267985
Encrypted:	false
SSDEEP:	768:B2CG6sPLHj1DDtLEHZwbz0yDEr+q5jc0T7KEE:4CG6sTDFRLKZwbzpDEr+Zc7e
MD5:	B204756661AE1F820ACDBF507B2C0FE7
SHA1:	8BCC62CD820991FE0C4D35C2E397E9D2E225D4A0
SHA-256:	A33593E9043EFEFBAF94D9CA220C885CE1C42DD2A7707F30ED072D7D71587DA5
SHA-512:	F115CD7216716F759575B0411028CFA56049150F54D2692CF8998E47D82959BA1521CB9462DF6E5496C51B08ED736FFC0CF4BB70C0328099143293CDDB4B570E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://elsfwa.com/site/partner3/lib/img/background.jpg
Preview:	.....JFIF.....`.`.....VExif..MM.*.....>.....F.(.....`.....`.....! !,,;.....! !,,;.....8. ..."....&`...n.... .Z...&.P....UZ. .....%`....d.j...[@.....@.....C9kD...4..k@.Z36-jP..Y...2...f....4.....b...*....uA..t..b.....3 .T....n....f... .+"KR..A.FC.`.d&..f. !t...@]P]P...b...g ....d.t...@.-.&..)."..D.i.J.....2X@.H.HR.....T.`...0.D..0.....3.....@.....hH....sL.. ...r[I.Am.U.]Pn.@..0.kL.&`.2.n.L....h.5..@bS[U.$-f@.1.ee5...."..$...E.....k L..w 9.....`h.....m..e..f.....$S9-&a...`.U..R....7B..... ....P.:.....V..Z..P.U.# .s...$.&...&.....Ahk@.....9].....V..B,u%R...h.7r.w6....,.a5-.....@."f..J..]...{.uCt..b...rD.4$l@.....i2]..... ..%...&..a0.....h....7rkE.LCy.9...$.*..u@.oi..]Vd7B.T...3fE....."..].H.M..uQ.QjK.sg&....%.$...@n....5)M.eu@.U(....H..*`3.&a2hFi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\login[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	101788
Entropy (8bit):	5.304944776832708
Encrypted:	false
SSDEEP:	1536:QpHDglbuhw+ExmazA/PWrF7qvEAFiQcpmNtuhPyJRD:l74wyJZ
MD5:	4DB4A299AE7E73B3CB53351867416D0C
SHA1:	36C0DFF7A6742EAD3229E476F05C559069C3080F
SHA-256:	10C50B88EBF99FDF813A4CCE86BA218A6E2EA3D266146520529F1E1BDDC5EBD3
SHA-512:	8EB086FC241C314DDD4B15AC6F34DBD61B838E2D7C2B535A02AF2A83A92294AB1C79EB122EFCA8FF648346F4515B35EDEEB13DC5E79EBC2C7E9ACCC4AC5B AA76
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://elsfwa.com/site/partner3/lib/css/login.css
Preview:	/*! Copyright (C) Microsoft Corporation. All rights reserved. *//*!.---------- START OF THIRD PARTY NOTICE ----------..This file based on or incorporates material from the projects listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise..//----------.twbs-bootstrap-sass (3.3.0).//----------..The MIT License (MIT)..Copyright (c) 2013 Tw Inc..Permission is hereby granted, free of charge, to any person

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\ZGFuaXNhLndpbGxpYW1zQGdlYXBwbGlhbmNlcy5jb20=[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	132
Entropy (8bit):	4.621797789578561
Encrypted:	false
SSDEEP:	3:gnkAqRAdu6/GY7voOkADFoHDGLRW9way4XSWYJrcK5UYLn:7AqJm7+mmHmWSG9YJrcK5UYL
MD5:	B32A4339B861CD0A93E17C9E13598AB1
SHA1:	B3D809E3B0643168E06EEB549863294E33FF57F3
SHA-256:	800DB6C82C3854E3239E31F9342394BB10A10FBB3EA58E6A241C5231FDC7EE83
SHA-512:	5D9F7B2B77B16E20C336C2753F71C4EC43291244EDED0534C57C7892512CBFB18D900D20917CA755A2AC1B6E129E3A813CC67BF7148B8B45D6A58251F995392
Malicious:	false
Reputation:	low
IE Cache URL:	http://wuftzayaebbtzem.activeinernational.com/espnxx/ZGFuaXNhLndpbGxpYW1zQGdlYXBwbGlhbmNlcy5jb20=
Preview:	<script type="text/javascript">window.location.href = "https://elsfwa.com/site/partner3/?danisa.williams@geappliances.com"</script>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 6 icons, 128x128, 16 colors, 72x72, 16 colors
Category:	downloaded
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\favicon[1].ico	
Encrypted:	false
SSDEEP:	24:QSNTmTFxg4lyyyyyyyyyyyyyio7eeeeeeeeekzgsLsLsLsLsLsQZp:nfgyyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://elsfwa.com/site/partner3/lib/img/favicon.ico
Preview:	.............h(..f...HH..........(..00......h....6.. ....=..............@.........(....A..(...................(....................................."P.."" ...3 333333333333333333333333333333"" ...333333333333333333333333333333"" ...333333333333333333333333333333"""" "" ...333333333333333333333333333333"" ...333333333333333333333333333333"" ...33333333333 3333333333333333333"" ...333333333333333333333333333333"" ...333333333333333333333333333333"""""""""""""""""""""""""""""""""" """""""""" ...333333333333333333333333333333"" ...333333333333333333333333333333"" ...333333333333333333333 333333333"" ...333333333333333333333333333333""""""""""""""""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\white_ellipsis[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	915
Entropy (8bit):	3.877322891561989
Encrypted:	false
SSDEEP:	24:t4CvnAVRf83f1QqCSzGUdiHTVtpRduf1QqCWbVHTVeUV0Uv6f1QqCWbVHTVeUV0W:fnL1QqC4GuiHFXS1QqCWRHQ3V1QqCWRV
MD5:	5AC590EE72BFE06A7CECFD75B588AD73
SHA1:	DDA2CB89A241BC424746D8CF2A22A35535094611
SHA-256:	6075736EA9C281D69C4A3D78FF97BB61B9416A5809919BABE5A0C5596F99AAEA
SHA-512:	B9135D934B9EA50B51BB0316E383B114C8F24DFE75FEF11DCBD1C96170EA59202F6BAFE11AAF534CC2F4ED334A8EA4DBE96AF2504130896D6203BFD2DA6913 F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://elsfwa.com/site/partner3/lib/img/white_ellipsis.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path fill="#ffffff" d="M1.143,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,.7,9.054a1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893A1.164,1.164,0,0,1,.7,6.946a1.107,1.107,0,0,1,.446-.089M8,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,8,6.857m6.857,0a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,14.857,6.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\arrow[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	513
Entropy (8bit):	4.720499940334011
Encrypted:	false
SSDEEP:	12:t4BdU/uRqv6DLfBHKFWJCDLfBSU1pRXIFl+MJ4bADc:t4TU/uRff0EcfIU1XXU+t2c
MD5:	A9CC2824EF3517B6C4160DCF8FF7D410
SHA1:	8DB9AEBAD84CA6E4225BFDD2458FF3821CC4F064
SHA-256:	34F9DB946E89F031A80DFCA7B16B2B686469C9886441261AE70A44DA1DFA2D58
SHA-512:	AA3DDAB0A1CFF9533F9A668ABA4FB5E3D75ED9F8AFF8A1CAA4C29F9126D85FF4529E82712C0119D2E81035D1CE1CC491FF9473384D211317D4D00E0E234AD9 F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://elsfwa.com/site/partner3/lib/img/arrow.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="24" height="24" viewBox="0 0 24 24"><title>assets</title><path d="M18,11.578v.844H7.617l3.921,3.928-.594.594L6,12 l4.944-4.944.594.594L7.617,11.578Z" fill="#404040"/><path d="M10.944,7.056l.594.594L7.617,11.578H18v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944m0-.141-.071.07L5.929,11.929,5.858,12l.071.071,4.944,4.944.071.07.071-.07.594-.595.071-.07-.071-.071L7.858,12.522H18.1V11.478H7.858l3.751-3.757.071-.071-.071-.07-.594-.595-.071-.07Z" fill="#404040"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\logo2[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3651
Entropy (8bit):	4.094801914706141

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\logo2[1].svg	
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://elsfwa.com/site/partner3/lib/img/logo2.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38 .119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392, 1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47. 081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.707,4.707,0, 0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.61 1,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.9 52,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\logo3[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 342 x 72, 4-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1750
Entropy (8bit):	7.784821733371315
Encrypted:	false
SSDEEP:	24:W6Yai7i2Tz46sC7PbpHZMYYsOWFzyKgXW0n9/ND1LCgz7AXtew1pcv8m5PRlQXt+:9KtTzx/HxRF+KKWE/B1LCgYXtIZRlN
MD5:	533E293F0C8947ADA653B47C00E394E2
SHA1:	0F507BB89C42F937A290D0EEDA3F2E0DBFCAD5C1
SHA-256:	B5D587F6C48A9B22BBE97150249E0C0655AC1780BD273431480A22F8A5BFEF6C
SHA-512:	B91127D6C27E270F7AAB0A83054451FFF4719C587A425F36EC32F4E532CF4E4D74505AAC71ED3629769552924BC9A9C8CB7F73667B0D20EA5AAED587BCD3E17
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://elsfwa.com/site/partner3/lib/img/logo3.png
Preview:	.PNG.....IHDR...V...H....._*.....gAMA.....a.....sRGB.....0PLTEGpL.....D>.....tRNS.w.D...3f..".U...1;...)IDATh..ZMh\U...t&...L#..:I(.P..7..T$V ....1h....Eq!..Q.....q.....&Bq.Up.".B..$.L..Os...}..s...%3.w.....=..s...a....T.9.i.....'...\.7X...~.....c.....3.`.6.Z.T.....m..U.YM*.....K-..Y..g...<..-.z...Bs.....uZ;.F.w...Y..m.....m... ..jMYl..RkzQ.{]..V...i..i.R.V...e..yj....Mk..[g.y#h..,.u.].K.f..d.....b.u..L.a..Kk...5r....Rk...v.\../..Ekz.....i..,.K..?F.....).<..x...=o.k..}'g.0.o...n.....K.L..l..B...5.....4..`.CD+...-1...E. ((.=k.....}.H.dqe.Q..b.%.C.\.e..=...m.\k.".4_.....Y5.S.....U....j.ZV.*wY;..^.X.....&.1.!.*..;m,..?..`.<t.Z....3@...../...j..rC>x>.e.,.=...F.....p..U...J...5d....>.~d._\.....o.....j...\.z8.8..a... <.MI8.]...3.V.Z.G....V.S..ta.c.m..Z."k.&y....a....p..Z.h..q..a.#.....s>4O}.F.&9....R.$....\....>..0....F.."....8f.....i-X....".aX.1....j..#k.c.U.9).ta.#K..!..z..zXD...&8.

C:\Users\user\AppData\Local\Temp\~DF1D2A2AD58E32361C.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	42289
Entropy (8bit):	0.8193126232720831
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+FwF2FsFtF2Fl3c353ZU0fSoW:kBqoxKAuqR+FwF2FsFtF2Fl3c3539
MD5:	BC2BAA037426983E0E8D6AF986D26AE8
SHA1:	3B0E664BAF3D9803DF564C61F99AB0879B8A910B
SHA-256:	FD0F865D0952465893ABC9EA4A8D9C14D913698651306O2F0AC24AE6291213F6
SHA-512:	359E863FA46288BD950635497CD969CE2B65DFFC00FF24D169B8079227A9EDE7151C15FB822F4F1A5D1C7F397B17B04416CF4C79C737BA0B5A293BE2F2DDF83
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF1E9F711CF262AE1C.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.3813998364528575
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAvdml/oHgRg:kBqoxxJhHWSVSEab0Eo4g
MD5:	234DA60EF502CAC29829E6EEFE817BE3

C:\Users\user\AppData\Local\Temp\~DF1E9F711CF262AE1C.TMP	
SHA1:	0F80A314011FDFF52C3FD8B4AF14BE95866389E1
SHA-256:	231194AF3395E98C7E69D82CC0ABED72ACD4446EFD2C9643A1F8207D89A68AF0
SHA-512:	0DADAE2F8ED55384EA2A2CD95F65FA56DE8574180E3B0DFD232A4E262A10FAEDEAC544CFC3BED8D7AC202F085C6E11B88316DE0B953FF75CC053DB6C10B4 745
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

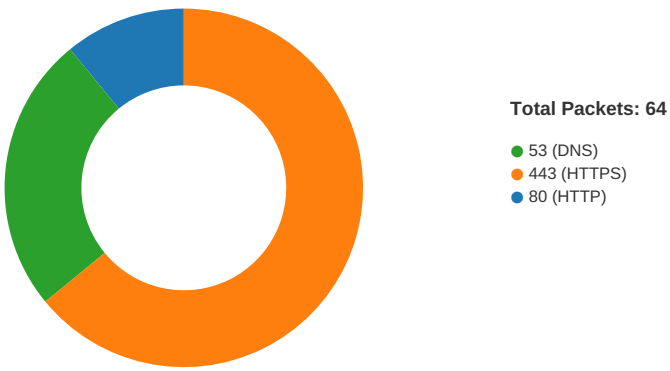
C:\Users\user\AppData\Local\Temp\~DF31150979467F106C.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47873306332546967
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loK9lo69lWVbR0IW7s:kBqoIVDr3
MD5:	A3269B4158F6C98631F144135E2BFDF9
SHA1:	F7422BF3C83F3FA9AE26298EB97AD9F292EDB022
SHA-256:	D975EFF2E1DE6CDCD5D10F47C732EF3C0A5E063762D1D34E05D072E194DA5300
SHA-512:	CE391183034FFE8DA03B8B8BB8364BA1032AEC318356EB312809F099A5446D07713C0A22BC05C222486DB53C4267F46236F24F4D8D1D5533DF8020272E7DB50C
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
Oct 15, 2020 17:59:13.206693888 CEST	49724	80	192.168.2.6	23.247.102.108

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 15, 2020 17:59:13.206871986 CEST	49725	80	192.168.2.6	23.247.102.108
Oct 15, 2020 17:59:13.384520054 CEST	80	49724	23.247.102.108	192.168.2.6
Oct 15, 2020 17:59:13.384561062 CEST	80	49725	23.247.102.108	192.168.2.6
Oct 15, 2020 17:59:13.384687901 CEST	49724	80	192.168.2.6	23.247.102.108
Oct 15, 2020 17:59:13.384747982 CEST	49725	80	192.168.2.6	23.247.102.108
Oct 15, 2020 17:59:13.385870934 CEST	49724	80	192.168.2.6	23.247.102.108
Oct 15, 2020 17:59:13.622908115 CEST	80	49724	23.247.102.108	192.168.2.6
Oct 15, 2020 17:59:13.894201040 CEST	80	49724	23.247.102.108	192.168.2.6
Oct 15, 2020 17:59:13.894284010 CEST	49724	80	192.168.2.6	23.247.102.108
Oct 15, 2020 17:59:14.110471964 CEST	49727	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:14.111742973 CEST	49728	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:14.255549908 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:14.255752087 CEST	49727	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:14.258697033 CEST	443	49728	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:14.258830070 CEST	49728	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:14.302052975 CEST	49728	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:14.302813053 CEST	49727	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:14.447771072 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:14.448776960 CEST	443	49728	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:14.449069977 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:14.449094057 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:14.449173927 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:14.449177980 CEST	49727	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:14.449201107 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:14.449223042 CEST	49727	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:14.449227095 CEST	49727	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:14.449234962 CEST	49727	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:14.449786901 CEST	443	49728	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:14.449852943 CEST	443	49728	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:14.449877024 CEST	49728	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:14.449892044 CEST	443	49728	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:14.449898005 CEST	49728	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:14.449908018 CEST	443	49728	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:14.449958086 CEST	49728	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:14.449966908 CEST	49728	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:14.451807022 CEST	443	49728	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:14.451838970 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:14.451905966 CEST	49727	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:14.452719927 CEST	49728	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:14.651654005 CEST	49727	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:14.657605886 CEST	49727	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:14.661725044 CEST	49728	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:14.797434092 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:14.797544956 CEST	49727	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:14.809920073 CEST	443	49728	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:14.810026884 CEST	49728	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:14.843676090 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:18.710210085 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:18.710370064 CEST	49727	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:18.725095987 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:18.725447893 CEST	49727	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:18.729123116 CEST	49727	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:18.874102116 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:19.429027081 CEST	80	49724	23.247.102.108	192.168.2.6
Oct 15, 2020 17:59:19.429203033 CEST	49724	80	192.168.2.6	23.247.102.108
Oct 15, 2020 17:59:19.671101093 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:19.671269894 CEST	49727	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:19.690821886 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:19.691076040 CEST	49727	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:19.693631887 CEST	49727	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:19.838423014 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:20.251710892 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:20.251739979 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:20.251758099 CEST	443	49727	162.241.5.177	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 15, 2020 17:59:20.251791000 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:20.251817942 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:20.252024889 CEST	49727	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:20.252144098 CEST	49727	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:20.264877081 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:20.265065908 CEST	49727	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:20.267827034 CEST	49727	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:20.270411968 CEST	49728	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:20.273808956 CEST	49733	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:20.274017096 CEST	49734	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:20.274151087 CEST	49735	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:20.412842989 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:20.414849043 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:20.414874077 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:20.414901018 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:20.414921045 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:20.414982080 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:20.415005922 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:20.415045977 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:20.415090084 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:20.415115118 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:20.415179968 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:20.415209055 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:20.415229082 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:20.415254116 CEST	49727	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:20.415291071 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:20.415316105 CEST	443	49727	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:20.415330887 CEST	49727	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:20.415417910 CEST	49727	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:20.419096947 CEST	443	49735	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:20.419222116 CEST	49735	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:20.419810057 CEST	443	49734	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:20.420023918 CEST	49734	443	192.168.2.6	162.241.5.177
Oct 15, 2020 17:59:20.420186996 CEST	443	49733	162.241.5.177	192.168.2.6
Oct 15, 2020 17:59:20.420325994 CEST	49733	443	192.168.2.6	162.241.5.177

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 15, 2020 17:59:07.232144117 CEST	52811	53	192.168.2.6	8.8.8.8
Oct 15, 2020 17:59:07.244131088 CEST	53	52811	8.8.8.8	192.168.2.6
Oct 15, 2020 17:59:08.161478043 CEST	55299	53	192.168.2.6	8.8.8.8
Oct 15, 2020 17:59:08.173677921 CEST	53	55299	8.8.8.8	192.168.2.6
Oct 15, 2020 17:59:09.438813925 CEST	63745	53	192.168.2.6	8.8.8.8
Oct 15, 2020 17:59:09.450901031 CEST	53	63745	8.8.8.8	192.168.2.6
Oct 15, 2020 17:59:10.469255924 CEST	50055	53	192.168.2.6	8.8.8.8
Oct 15, 2020 17:59:10.482812881 CEST	53	50055	8.8.8.8	192.168.2.6
Oct 15, 2020 17:59:11.461631060 CEST	61374	53	192.168.2.6	8.8.8.8
Oct 15, 2020 17:59:11.474459887 CEST	53	61374	8.8.8.8	192.168.2.6
Oct 15, 2020 17:59:11.947694063 CEST	50339	53	192.168.2.6	8.8.8.8
Oct 15, 2020 17:59:11.965848923 CEST	53	50339	8.8.8.8	192.168.2.6
Oct 15, 2020 17:59:13.153090954 CEST	63307	53	192.168.2.6	8.8.8.8
Oct 15, 2020 17:59:13.195255995 CEST	53	63307	8.8.8.8	192.168.2.6
Oct 15, 2020 17:59:13.209882975 CEST	49694	53	192.168.2.6	8.8.8.8
Oct 15, 2020 17:59:13.222754002 CEST	53	49694	8.8.8.8	192.168.2.6
Oct 15, 2020 17:59:14.087312937 CEST	54982	53	192.168.2.6	8.8.8.8
Oct 15, 2020 17:59:14.108285904 CEST	53	54982	8.8.8.8	192.168.2.6
Oct 15, 2020 17:59:14.854605913 CEST	50010	53	192.168.2.6	8.8.8.8
Oct 15, 2020 17:59:14.866822958 CEST	53	50010	8.8.8.8	192.168.2.6
Oct 15, 2020 17:59:16.326761007 CEST	63718	53	192.168.2.6	8.8.8.8
Oct 15, 2020 17:59:16.339991093 CEST	53	63718	8.8.8.8	192.168.2.6
Oct 15, 2020 17:59:17.453567028 CEST	62116	53	192.168.2.6	8.8.8.8
Oct 15, 2020 17:59:17.466500044 CEST	53	62116	8.8.8.8	192.168.2.6
Oct 15, 2020 17:59:18.408546925 CEST	63816	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 15, 2020 17:59:18.421484947 CEST	53	63816	8.8.8.8	192.168.2.6
Oct 15, 2020 17:59:31.487868071 CEST	55014	53	192.168.2.6	8.8.8.8
Oct 15, 2020 17:59:31.529014111 CEST	53	55014	8.8.8.8	192.168.2.6
Oct 15, 2020 17:59:33.366946936 CEST	62208	53	192.168.2.6	8.8.8.8
Oct 15, 2020 17:59:33.379645109 CEST	53	62208	8.8.8.8	192.168.2.6
Oct 15, 2020 17:59:36.853730917 CEST	57574	53	192.168.2.6	8.8.8.8
Oct 15, 2020 17:59:36.872031927 CEST	53	57574	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 15, 2020 17:59:13.153090954 CEST	192.168.2.6	8.8.8.8	0xedda	Standard query (0)	wuftzayaebbtzem.activeinernational.com	A (IP address)	IN (0x0001)
Oct 15, 2020 17:59:14.087312937 CEST	192.168.2.6	8.8.8.8	0x7713	Standard query (0)	elsfwa.com	A (IP address)	IN (0x0001)
Oct 15, 2020 17:59:31.487868071 CEST	192.168.2.6	8.8.8.8	0xa1d2	Standard query (0)	elsfwa.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 15, 2020 17:59:13.195255995 CEST	8.8.8.8	192.168.2.6	0xedda	No error (0)	wuftzayaebbtzem.activeinernational.com		23.247.102.108	A (IP address)	IN (0x0001)
Oct 15, 2020 17:59:14.108285904 CEST	8.8.8.8	192.168.2.6	0x7713	No error (0)	elsfwa.com		162.241.5.177	A (IP address)	IN (0x0001)
Oct 15, 2020 17:59:31.529014111 CEST	8.8.8.8	192.168.2.6	0xa1d2	No error (0)	elsfwa.com		162.241.5.177	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- wuftzayaebbtzem.activeinernational.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49724	23.247.102.108	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Oct 15, 2020 17:59:13.385870934 CEST	488	OUT	GET /espnxx/ZGFuaXNhLndpbGxpYW1zQGdlYXBwbGlhbmNlcy5jb20= HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: wuftzayaebbtzem.activeinernational.com Connection: Keep-Alive
Oct 15, 2020 17:59:13.894201040 CEST	500	IN	HTTP/1.1 200 OK Date: Thu, 15 Oct 2020 22:59:12 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.2.33 X-Powered-By: PHP/7.2.33 Content-Length: 132 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 20 3d 20 22 68 74 74 70 73 3a 2f 2f 65 6c 73 66 77 61 2e 63 6f 6d 2f 73 69 74 65 2f 70 61 72 74 6e 65 72 33 2f 3f 64 61 6e 69 73 61 2e 77 69 6c 6c 69 61 6d 73 40 67 65 61 70 70 6c 69 61 6e 63 65 73 2e 63 6f 6d 22 3c 2f 73 63 72 69 70 74 3e 0a Data Ascii: <script type="text/javascript">window.location.href = "https://elsfwa.com/site/partner3/?danisa.williams@geappliances.com"</script>

HTTPS Packets

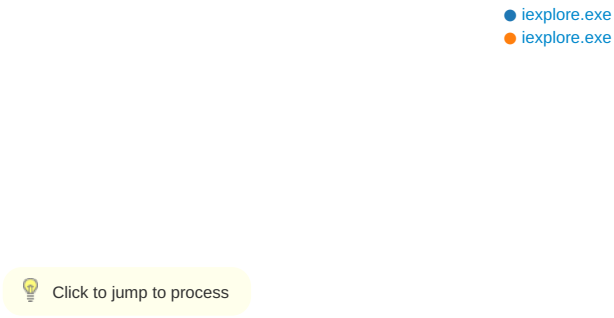
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Oct 15, 2020 17:59:14.451807022 CEST	162.241.5.177	443	192.168.2.6	49728	CN=elsfwa.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Sep 28 02:00:00 CEST 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Mon Dec 28 00:59:59 CET 2020 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Oct 15, 2020 17:59:14.451838970 CEST	162.241.5.177	443	192.168.2.6	49727	CN=elsfwa.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Sep 28 02:00:00 CEST 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Mon Dec 28 00:59:59 CET 2020 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Oct 15, 2020 17:59:31.832271099 CEST	162.241.5.177	443	192.168.2.6	49736	CN=elsfwa.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Sep 28 02:00:00 CEST 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Mon Dec 28 00:59:59 CET 2020 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 1876 Parent PID: 792

General

Start time:	17:59:11
Start date:	15/10/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff721e20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 6392 Parent PID: 1876

General

Start time:	17:59:12
Start date:	15/10/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1876 CREDAT:17410 /prefetch:2
Imagebase:	0xda0000
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