ID: 358569
Cookbook: browseurl.jbs
Time: 21:07:48
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

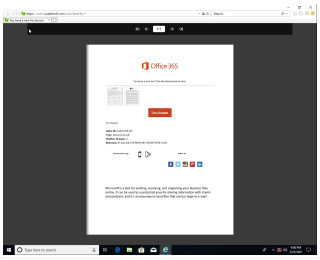
Analysis Report https://online.pubhtml5.com/whlz/taka/

Overview

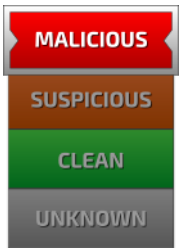
General Information

Sample URL:	http://https://online.pubhtml5.com/whlz/taka/
Analysis ID:	358569
Infos:	

Most interesting Screenshot:



Detection

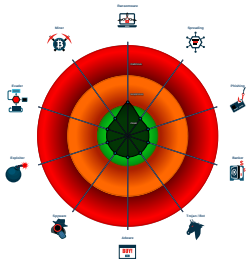


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6560 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6632 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6560 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

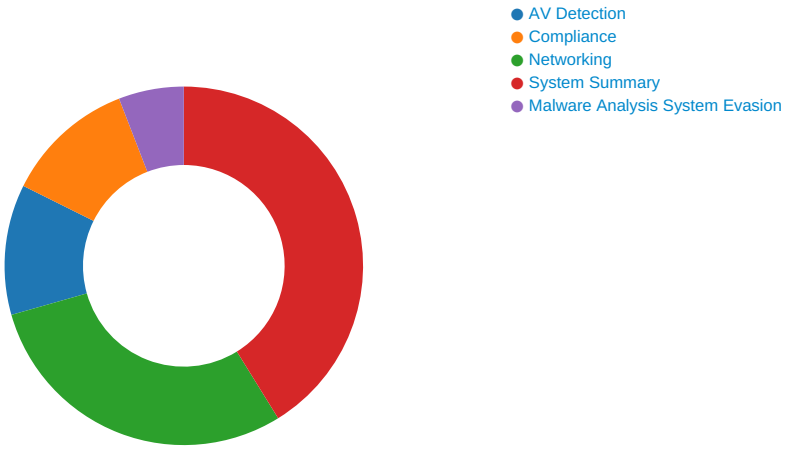
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Compliance:

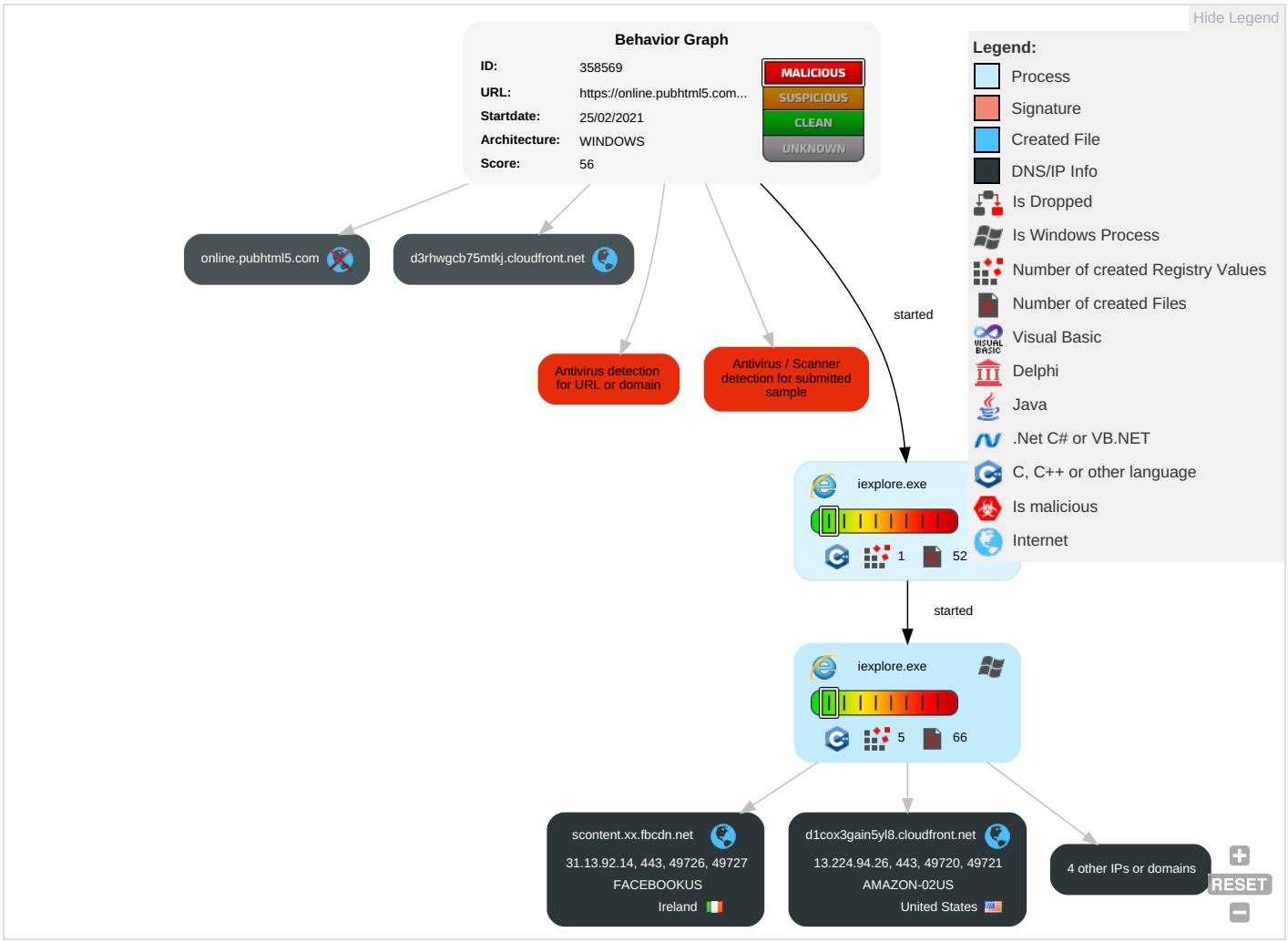
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impac
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software 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	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lockc
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data

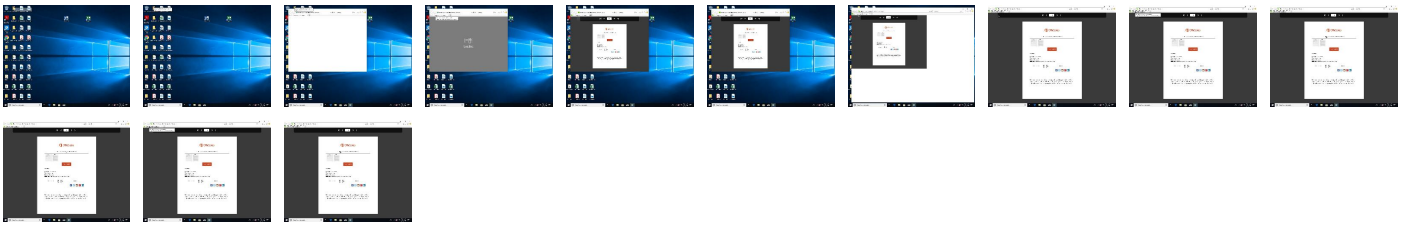
Behavior Graph

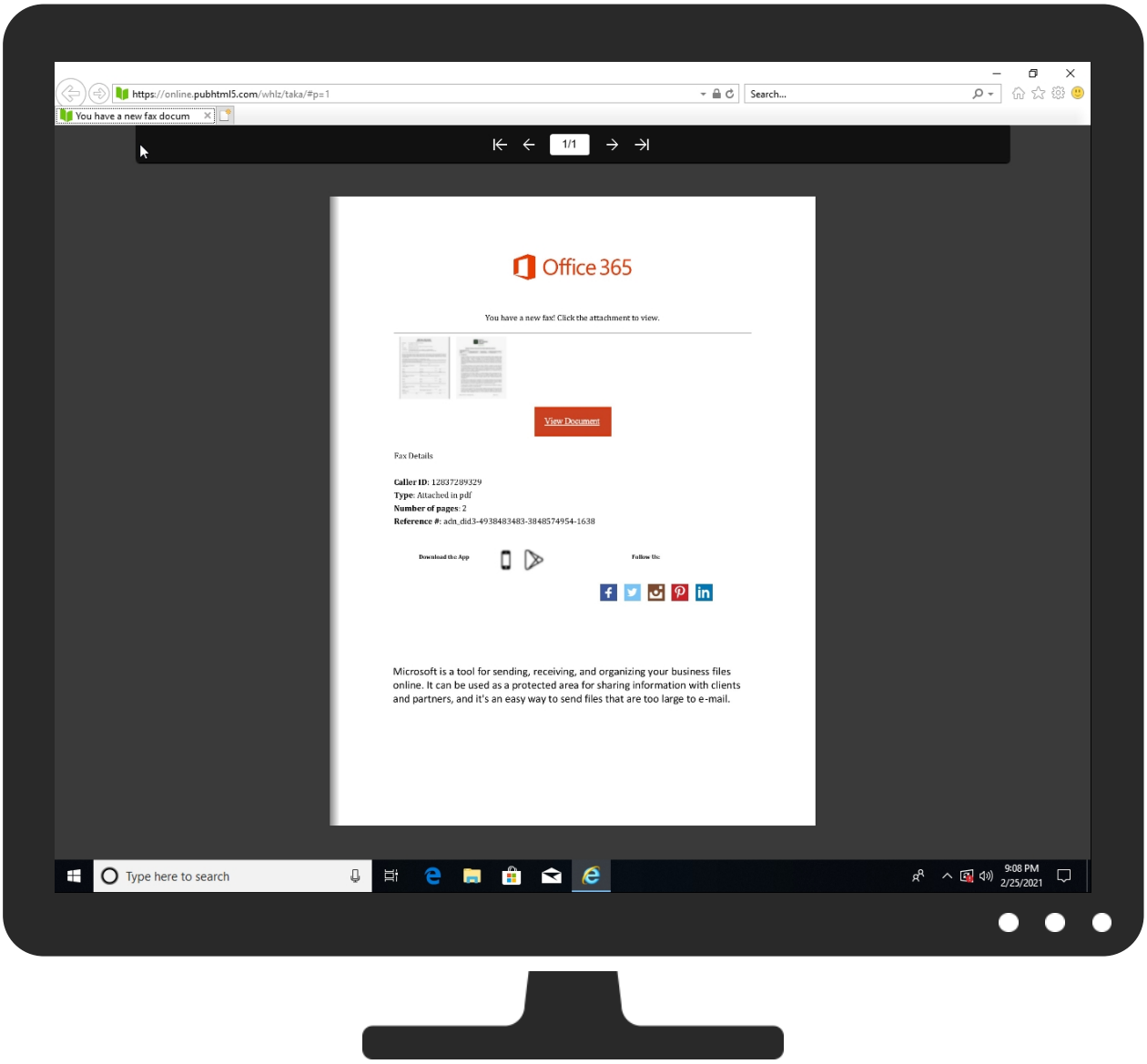


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://online.pubhtml5.com/whlz/taka/	0%	Virustotal		Browse
http://https://online.pubhtml5.com/whlz/taka/	0%	Avira URL Cloud	safe	
http://https://online.pubhtml5.com/whlz/taka/	100%	SlashNext	Fake Login Page type: Phishing & Social usering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
http://https://online.pubhtml5.com/whlz/taka/#p=1	100%	SlashNext	Fake Login Page type: Phishing & Social usering	
http://https://www.internalfb.com/intern/invariant/	0%	URL Reputation	safe	
http://https://www.internalfb.com/intern/invariant/	0%	URL Reputation	safe	
http://https://www.internalfb.com/intern/invariant/	0%	URL Reputation	safe	
http://https://www.internalfb.com/intern/invariant/	0%	URL Reputation	safe	
http://https://curepumpiones.com/foldersss	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
scontent.xx.fbcdn.net	31.13.92.14	true	false		high
d3rhwgcb75mtkj.cloudfront.net	13.227.156.43	true	false		high
d1cox3gain5yl8.cloudfront.net	13.224.94.26	true	false		high
connect.facebook.net	unknown	unknown	false		high
static.pubhtml5.com	unknown	unknown	false		high
online.pubhtml5.com	unknown	unknown	false		high

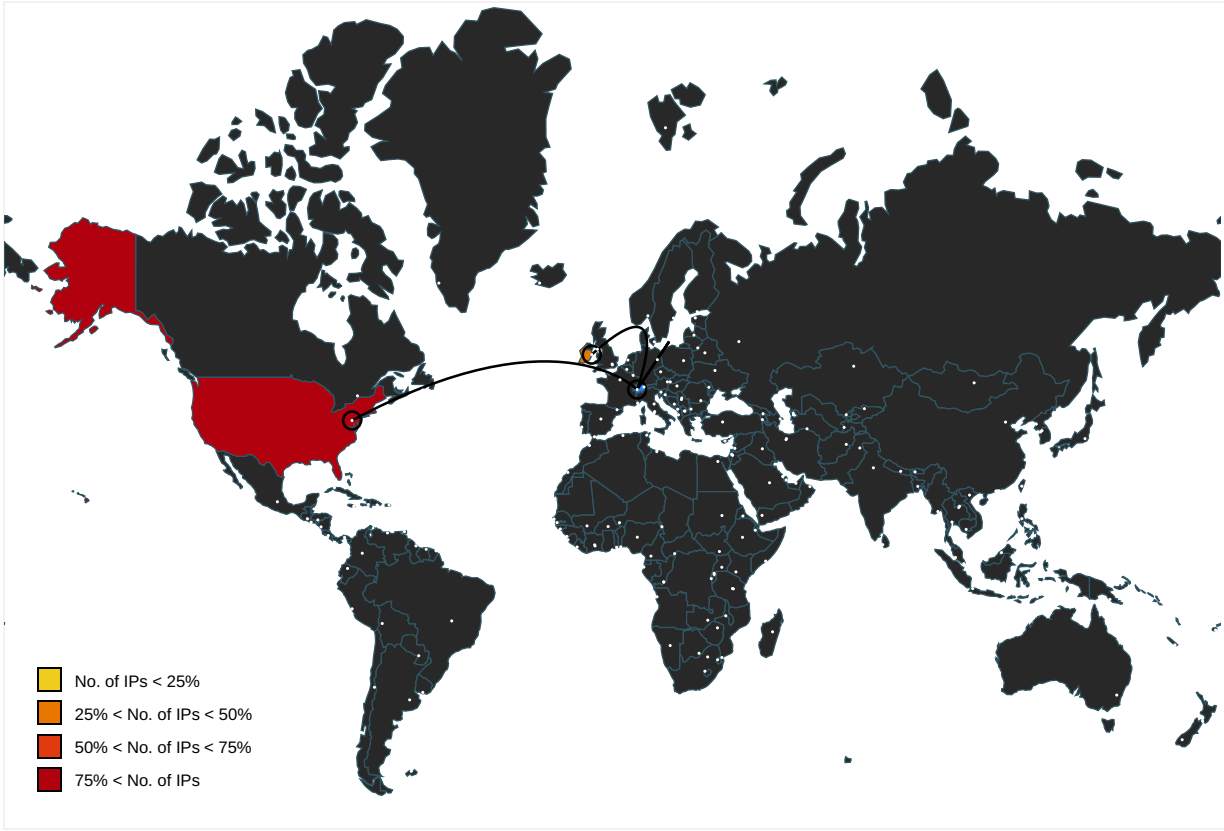
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://online.pubhtml5.com/whlz/taka/#p=1	false	• SlashNext: Fake Login Page type: Phishing & Social usering	high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://player.vimeo.com/api/player.js	main[1].js.3.dr	false		high
http://https://www.internalfb.com/intern/invariant/	sdk[2].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://online.pubhtml5.com/whlz/taka/files/shot.jpg	taka[1].htm.3.dr	false		high
http://www.paypal.com/cgi-bin/webscr?cmd=_cart&upload=1	main[1].js.3.dr	false		high
http://www.paypal.com/cgi-bin/webscr?cmd=_xclick&business=	main[1].js.3.dr	false		high
http://https://online.pubhtml5.com/favicon.ico~	imagestore.dat.3.dr	false		high
http://https://online.pubhtml5.com/whlz/taka/#p=1Root	{ACE24E76-77F0-11EB-90E5-ECF4BB2D2496}.dat.2.dr	false		high
http://https://online.pubhtml5.com/whlz/taka/Root	{ACE24E76-77F0-11EB-90E5-ECF4BB2D2496}.dat.2.dr	false		high
http://https://hm.baidu.com/hm.js?	main[1].js.3.dr	false		high
http://https://curepumpiones.com/foldersss	config[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://twitter.com/intent/tweet?url=	main[1].js.3.dr	false		high
http://www.fliphtml5.com	main[1].js.3.dr	false		high
http://www.linkedin.com/shareArticle?url=	main[1].js.3.dr	false		high
http://reddit.com/submit?url=	main[1].js.3.dr	false		high
http://https://online.pubhtml5.com/whlz/taka/#p=1	~DFEBD97EC9ADA788CD.TMP.2.dr	false	• SlashNext: Fake Login Page type: Phishing & Social usering	high
http://https://mail.qq.com/	main[1].js.3.dr	false		high
http://https://online.pubhtml5.com/whlz/taka/	~DFEBD97EC9ADA788CD.TMP.2.dr, online.pubhtml5[1].xml.3.dr, taka[1].htm.3.dr	false		high
http://digg.com/submit?url=	main[1].js.3.dr	false		high
http://www.addthis.com/bookmark.php?v=300&url=	main[1].js.3.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
31.13.92.14	unknown	Ireland		32934	FACEBOOKUS	false
13.227.156.43	unknown	United States		16509	AMAZON-02US	false
13.224.94.26	unknown	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358569
Start date:	25.02.2021
Start time:	21:07:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://online.pubhtml5.com/whlz/taka/
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:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.win@3/33@4/3

Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.147.198.201, 40.88.32.150, 23.54.113.53, 52.255.188.83, 88.221.62.148, 168.61.161.212, 51.11.168.160, 152.199.19.161, 52.155.217.156, 51.103.5.186, 2.20.142.210, 2.20.142.209, 20.54.26.129, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, go.microsoft.com, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, ie9comview.vo.msecnd.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, vip2-par02p.wns.notify.trafficmanager.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\EQAWN5DV\online.pubhtml5[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	129
Entropy (8bit):	4.806050179476776
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwsNjIjDIrJNsRn7qfqHlJR3lETVVHhOqSQVaFKb:JFK1rUFhjeDINNIQqHlJR3SZVHYQVakb
MD5:	622CD5ADB0D2607CCB4F9B566A86B7A8
SHA1:	5C3037D812FC94D3544626AF40763114CFEE0BE7
SHA-256:	5CA6557660ED80D99D25124C49D8051FCAA37A10BE34D5118815B89ADBF3E246
SHA-512:	02DDFA3398FF940C8067332D2C72AE3CDBD271207E87D8DD6A648B59831FAC9588632833A0A59FB24ACCAA58E4D1A37371268B159C59180411875182EA64DD7
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="https://online.pubhtml5.com/whlz/taka/" value="true" ltime="1914219600" htime="30870525" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{ACE24E74-77F0-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8543149973074429
Encrypted:	false
SSDEEP:	96:rUZXZy2UWOftO3AfOhqm1MMLOToWCoRoW2+foW6q7lX:rUZXZy2UW6tFfKRMZTDfSMX
MD5:	F76B6CAA408834EE77391DE276EC944A
SHA1:	52D2128A8D575227564EE75D837824C9D1B1456D
SHA-256:	9A3A3DEDBADD1BA70C2309961FF0260E8A0F23088E5B58E4E539F406A577F975
SHA-512:	CF77907142EF0CF91D36FA722F3500022A946DE0FCABA14196AE4941BD60AF0BA7D8DB944825F3CBCAC67C8ED7609ABB10A360F48D6DB8CF58A7A574F7AED3 80
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\{ACE24E76-77F0-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29564
Entropy (8bit):	1.8154806938765757
Encrypted:	false
SSDEEP:	192:r2ZpQS6gkMj52ZS+zZ+EK+8C8qQi8qa6kIZnA3ph:ryO9t+IMYii8O8+gH
MD5:	25A3A50BFAC2D41EC4C167E5CA5E4503
SHA1:	DFEA281BCC039B08C3F17CCE77EF23B46B68F6FE
SHA-256:	DA1BA672B409B3420B345FEBF47B32A61BDB3031BE93F0C7C99C8F6022ECFA72
SHA-512:	DDC222607D0D2AAC1826C63161C93B20A818C5FB93C661DC29CDF1B8E30420506718D3DC0A2E10455A2918E35981E5B1BADF9401D47AF443E48EF0C37AF749
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{ACE24E76-77F0-11EB-90E5-ECF4BB2D2496}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B38574C4-77F0-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5634284355165722
Encrypted:	false
SSDEEP:	48:IwhGcprEGwpaJG4pQpGrapbShGQpKsG7HpRCTGIpG:rXZ8QL6JBSbAHTWA
MD5:	C73A83D71F86F39FA9F710FC84FF2E59
SHA1:	7FB0250CB7D6BDF125A23643BE74771A30EC9EFC
SHA-256:	AE70E708A5DDE79773A45D7F924C781DEABCF2CEB5CA9C7D6F2893641F1F221C
SHA-512:	9DAE79DDA236D0AD1CA0946CCD93B21CF3CECB27512F45D620F116041FB4BDE68BCC5314B2B2B24473604410747A2608A6C7F4388B21C28D7EFBA9B62B8EE[94
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:	dropped
Size (bytes):	1266
Entropy (8bit):	3.172987674819497
Encrypted:	false
SSDEEP:	12:c3UnRGRplOXq8Xx0WRRRRRRRRRRRRRRR0WBHuOhRG2/:c3UnRaOUZE
MD5:	1E4C2560AC8BEA75472A8696F46A7D88
SHA1:	842169E4CB271839465AA69092245760C625B31A
SHA-256:	8128BE87BA1BC45D02D5210911C808BBDF629F8CC2D324F916C7E2202026980A
SHA-512:	9C0A1DB458C97FD0B4A57AB4DBED9240B7846B5BC75558397DB0A9982FB1B8FCCC141B89386054095F1F0A70DCAA24DB744DFBCAF292D55D4D3B7F863DFB3 DA
Malicious:	false
Reputation:	low
Preview:	'.h.t.t.p.s.:././.o.n.l.i.n.e...p.u.b.h.t.m.l.5...c.o.m./.f.a.v.i.c.o.n...i.c.o.~............... .h.......(....... ....k.......k...k...k?..k... k.......k...k...k...k...ko..k?..k...................kO..k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k..... ..k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k... k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k. ..k...k...k...k...........ko..k...k...k...k...k.......k...k...k...k...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\LoadingJS[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	21103
Entropy (8bit):	5.651609213689301
Encrypted:	false
SSDEEP:	384:K8J4Ympj/r2x9bgbEWDgUYPOLA0Aid4iMURLiPLiyRJl2+eWBt4+mcERCmOO1Wjw:J4npj/r2x9bgbEWDgUYPOLA0ddVMUwWl
MD5:	DE89531BDC0CC81C596E591CF703D593
SHA1:	3078C95408C5655A07CDCC9392D8D617DD8178EF
SHA-256:	DD167992A899A3286E656E86EBF1672A348E96E21E40EA669ADBE16079275676
SHA-512:	72438C65EB3C819DB1F99EF263AB9EF77738894308F6829133B0103ABDA0AE6FAFC62524D450031AAE265829DEA53D7C834DA0C625B6D05EF41ABFC4E9A568F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.pubhtml5.com/book/js/LoadingJS.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\LoadingJS[1].js	
Preview:	document.write("<style>"+.."@keyframes loadingAnimate{from {-webkit-transform: rotateY(0deg) scale(0.8);-o-transform: rotateY(0deg) scale(0.8);-ms-transform: ro tateY(0deg) scale(0.8);-moz-transform: rotateY(0deg) scale(0.8);transform: rotateY(0deg) scale(0.8);}to {-webkit-transform: rotateY(-180deg) scale(0.8);-o-transform: rota teY(-180deg) scale(0.8);-ms-transform: rotateY(-180deg) scale(0.8);-moz-transform: rotateY(-180deg) scale(0.8);transform: rotateY(-180deg) scale(0.8);}}"+.."@-webkit- keyframes loadingAnimate{from {-webkit-transform: rotateY(0deg) scale(0.8);-o-transform: rotateY(0deg) scale(0.8);-ms-transform: rotateY(0deg) scale(0.8);-moz-trans form: rotateY(0deg) scale(0.8);transform: rotateY(0deg) scale(0.8);}to {-webkit-transform: rotateY(-180deg) scale(0.8);-o-transform: rotateY(-180deg) scale(0.8);-ms-trans form: rotateY(-180deg) scale(0.8);-moz-transform: rotateY(-180deg) scale(0.8);transform: rotateY(-180deg) scale(0.8);}}"+..".loadingRun{-webkit-animation : load ingAnimate

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\hiSlider2.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	49738
Entropy (8bit):	5.087261989614924
Encrypted:	false
SSDEEP:	384:Ll7sawj6SHNout93qMmfqQpFrNqAKIfUx1sNU64xZjSRW5bN+BlfjfsNlwgnFeyo:L5AmuoCdUNqAKIcx1sm6+jSUNklfT
MD5:	21A677B5046027915D5D176115EE35ED
SHA1:	4B2142E2930BF43618DC0979FBCE2B02DBFE0012
SHA-256:	4A2410D9957AF385D10A11CB885A6E2E0B2A7E66BFACC0EE351B8FB94FB934A7
SHA-512:	18BCAFF85692E41CAEAA8C73EDE2724491CD2760F8DAB12B15756D7B93D424A8BB2AAE42509F7F2D897CAB84A9C3BB79650BC7AB830522BB9C5B7C717D6705 B8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.pubhtml5.com/book/css/hiSlider2.min.css
Preview:	/* !. * . * VERSION: 0.2.9. * DATE: 6/30/2016, 4:33:02 PM. * UPDATES AND DOCS AT: http://www.fliphtml5.com. * . * @license Copyright (c) 2012-2016 FlipHTML5 Sof tware Co., Ltd. All rights reserved.. * @author: Terence Z., Q.Y.B., support@fliphtml5.com.. *. */#leo-lightbox--audio,#leo-lightbox--msg #msg-left,.leo-app canvas,.leo-app img{-webkit-user-select:none;-webkit-user-drag:none}.leo-comp,.leo-comp--img>img,.leo-loading:before{position:absolute;top:0;left:0}.leo-center-wrapper,.leo-lightbox{text- align:center}.leo-app,.leo-app *{box-sizing:border-box;text-rendering:optimizeLegibility;-webkit-font-smoothing:antialiased}.leo-app canvas,.leo-app img{-ms-user-sel ect:none;user-select:none}.leo-app audio,.leo-app canvas,.leo-app video{display:inline-block;vertical-align:baseline}.leo-app audio:not([controls]){display:none;height:0} .leo-app a{background-color:transparent}.leo-app a:active,.leo-app a:hover{outline:0}.leo-app a img{border:0}.leo-app svg:not(:root){overflow:hidden}.leo-app bu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\jquery-1.9.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	93010
Entropy (8bit):	5.412891395382607
Encrypted:	false
SSDEEP:	1536:f5VEpk3rN84tqFmZcUZUutNTMLWqVvbwI6D95/u8uDUat8KXjZAh2Kaho4GG9PaP:xuk3x4qTMBTZAh2KahcoHGGnBpG8MIw
MD5:	AA987A5A07276484C5E4F7E18B16643C
SHA1:	B0ACF636B1AC1F3D4AF53A9BAFF19C987B87B082
SHA-256:	CEBFBBCBA46BEB5AD1C37AAF1B034652BDF1EAAA4E0BC67906B450A26AFF37EB
SHA-512:	1E8E7F8A6D5B62C44510077653451AD19A9EEAD7FD9DD400224F4454A1C633B41D4AB02C8BA76C96A67B30F8DA83834FB48B0709118F3223F5D1686CDDDA084
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.pubhtml5.com/book/js/jquery-1.9.1.min.js
Preview:	(function(r,n){function va(a){var b=a.length,d=c.type(a);return c.isWindow(a)?!1:1===a.nodeType&&b?!0:"array"===d||"function"!==d&&(0===b||"number"===typeof b&& 0<b&&b-1 in a)}function Qb(a){var b=Sa[a]={};c.each(a.match(O)||[],function(a,c){b[c]=!0});return b}function Ta(a,b,d,e){if(c.acceptData(a)){var f=c.expando,g="string"=== typeof b,h=a.nodeType,k=h?c.cache:a,l=h?a[f]:a[f]&&f;if(l&&k[l]&&(e||k[l].data)||!g||d!==n){l||(h?a[f]=l=G.pop()||c.guid++:l=f);k[l]||(k[l]={},h||(k[l].toJSON=c.noop));if("object"= ==.typeof b||"function"===typeof b)e?k[l]=c.extend(k[l],b):k[l].data=c.extend(k[l].data,b);a=k[l];e||(a.data||(a.data={}),a=a.data);d!==n&&(a[c.camelCase(b)]=d);g?(d=a[b] ,null==d&&(d=a[c.camelCase(b)])):d=a;return d}}function Ua(a,b,d){if(c.acceptData(a)){var e,f,g,h=a.nodeType,k=h?c.cache:a,l=h?a[c.expando]:c.expando;if(k[l]){if(b&& (g=d?k[l]:k[l].data)){c.isArray(b)?b=b.concat(c.map(b,c.camelCase)):b in g?b=[b]:(b=c.camelCase(b),b=b in g?[b]:b.split(" "));e=0;for(f=b.length;e<f;e++)d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\slideJS[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	12
Entropy (8bit):	3.584962500721156
Encrypted:	false
SSDEEP:	3:W2nn:xnn
MD5:	4A36E405711B42BE8F2FF61C241FD74B
SHA1:	DE8E09E66A801DB0E0E156FF9D5E18BBC92DFDCE
SHA-256:	DEB5AF9C897F2FFDCD6B1CD78AF78C2CE5EAFD8180161BF4EAC21C0E1B5CEB85
SHA-512:	8E3F672C94F743E78EF38E821206639EF3FF718470658EB2BD7264D06EB706347FA4AC230DA6D9F1916F8EFF818D98180B61B2782271A63E658EC41E90B399BA
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\slideJS[1].js	
IE Cache URL:	http://https://online.pubhtml5.com/whlz/taka/slide_javascript/slideJS.js?1614279113
Preview:	sliderJS=[];

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	276785
Entropy (8bit):	5.872634788926816
Encrypted:	false
SSDEEP:	6144:tgNIWRNIWiNIWj2iANNiAaYGe8M8Z8C83GpYf2IP74eUAuGbvG3DnqHfE4xr:tpYGAGpYf2IP74eUAuGbvG3DnqHfE4xr
MD5:	E7F5E2FABDB186B072D9E5F4D65F1C79
SHA1:	707C2F5ED7E396F81BC1E5E82F2548A0A5B1BCCC
SHA-256:	EEF5FC59B321B8434B5EC529C9635ACB94519A93607CEFD61E8CFF3F4D6770C3
SHA-512:	92D0F636470C4610772676616F233E6F49EE5D434AE82A2DDD6472C1717B173C119AD508C7F2FACE4279B427408E567F8C6A8DE88E2DC3AB3BEF593FB4B6D6A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.pubhtml5.com/book/template/Handy/style/style.css
Preview:	./* CSS Document */./* version 2020101601 */.* {. -webkit-box-sizing: content-box;. -moz-box-sizing: content-box;. box-sizing: content-box;.}.*:before, *:after {. -webkit-box-sizing: content-box;. -moz-box-sizing: content-box;. box-sizing: content-box;.}.select{. -webkit-box-sizing: border-box;. -moz-box-sizing: border-box;. box-sizing: border-box;.}..html{width:100%;height:100%;left:0;top:0;margin:0;padding:0;position:fixed;}.body{position:fixed;overflow:hidden!important;width:100%;height:100%;margin:0;padding:0!important;-ms-transform:translate(0);border:0;left:0;top:0;-webkit-user-select:none;-moz-user-select:none;-ms-user-select:none;user-select:none;}..tmpContainer{position:fixed;width:100%;height:100%;bottom: 0;top:0;left:0;display:block;z-index:-1;}..bookContainer{position:absolute;width:100%;height:100%;z-index:2;top:0;left:0;display:block;overflow:hidden;}./*//book object*/.img{-webkit-user-drag:none;}.p{margin:0;padding:0;}.input{outline:none;}.textarea{outline:non

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\template[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	downloaded
Size (bytes):	30092
Entropy (8bit):	5.103114163243284
Encrypted:	false
SSDEEP:	384:u5Rtencx6qy/3HBlWkQlur9holvtmet9jVaiiDs:u5RFHyfHBUf84lvtPjVIDs
MD5:	36B4526F5F8360E810DDAF92C253A4FB
SHA1:	132E33B5DF904A706829E59479D5668D938D4666
SHA-256:	0325B42381FC26804D51851B959C101FE9C6497C2EEF8C998987169D771198A1
SHA-512:	579102FDAEFE2F534FBFB99BF385995494137D42C5DBC3AD53385E99BD9F5CCBF4502073555977D13F5E6F71AB353943279D8C250C7BEEAF8180DF6FD7D7A17
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.pubhtml5.com/book/template/Handy/style/template.css
Preview:	.p{padding:0;margin:0;}.input{font-family:Calibri;}.textarea{font-family:Calibri;}..form_title{margin-left:0;}..form_title .favicon{. vertical-align: middle;. margin-right: 5px;. margin-top:-2px;width: 22px;. height: 22px;}. .form_title span{vertical-align: middle;}. .rightToLeft .form_title .favicon{margin-right:0;margin-left:5px;}..close{right:8px;left:auto;}..rightToLeft .form_title{margin-left:0;margin-right:0;}..rightToLeft .close{left:8px;right:auto;}...about_form{text-align:left;vertical-align:middle;line-height:20px;width:415px;background:#000000;border-radius:5px;padding:5px;color:#ffffff;font-size:12px;font-family:Calibri;position:absolute;}..about_form .form_title{font-size:15px;line-height:25px;}..about_form .close{top:7px;position:absolute;cursor:pointer;}..about_form .about_content{position:relative;background-color:rgba(255,255,255,0.2);width:381px;padding:17px 17px 10px 17px;}..about_form .content2{position:relative;height:105px;}..about_form .content1{position:re

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 1391x1800, frames 3
Category:	downloaded
Size (bytes):	142908
Entropy (8bit):	7.378423383704879
Encrypted:	false
SSDEEP:	1536:28OeICDcpb12lWG8G79x4Mz5bbfxm7O2C6sVoM9DoCML8rvlsl+kByvmAbfDfYnq:bQCDcuHF4HCdH9DxXII3BCmAbf8q
MD5:	971300FFA963B7E07B93289BED455F4A
SHA1:	BFF26144876AA318179691770C65233A3469F051
SHA-256:	196F12418A0484DC586ADA2C9F2826C65FD1F3CDE906F552E8DFBAC1268D4934
SHA-512:	477DA8B93C4C267E01643CC3ABA34DD0A03304F7D4B2E8A2CF5FBD535597D6F177978B67C7CE8B67C735E4C761E059A97B909A90BE3362BF5DC25013045F2C6B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://online.pubhtml5.com/whlz/taka/files/large/1.jpg?1614279112

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\1[1].jpg	
Preview:	......JFIF.....,.,.....C..C..o.."..}........!1A..Qa."q. 2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?..S..(...(...(...(...(...(...(...(...(...(...(... (... (...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\book_config[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	561
Entropy (8bit):	4.550786763919387
Encrypted:	false
SSDEEP:	12:Co88Aylc6P3hu9dlCqLj2maFujgLYiu1i:CT0lZUlumqPY10
MD5:	5C67AF2060C51257560D3377522665D9
SHA1:	50D56EE2E25AB9FAF9E952073FA506D147C4C550
SHA-256:	48557360A5FF4110F06565A93CBD4DF3F9B3F4F26EF04E75F08AB383C3865FC6
SHA-512:	355E699A773E2C28091D002FBD0444DC85DC0967C1B93432A862DB4B62C82E8313B83BC25705AF446D7872A6AB1CA9F6F111077BD5F1F8B68E702DC4F340526
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://online.pubhtml5.com/whlz/taka/files/search/book_config.js?1614279113
Preview:	.var textForPages = ["You have a new fax! Click the attachment to view. Fax Details Follow Us: Caller ID: 12837289329 Type: Attached in pdf Number of pages: 2 Reference #: adn_did3-4938483483-3848574954-1638 Download the App Microsoft is a tool for sending, receiving, and organizing y our business files online. It can be used as a protected area for sharing information with clients and partners, and it's an easy way to send files that are too large to e-mail."]; var positionForPages = [];

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\getuserinfo[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	33
Entropy (8bit):	4.0895524525606675
Encrypted:	false
SSDEEP:	3:qdTFX6sae:qdBX6sae
MD5:	A16DF71C7B85D91039864F1113705B63
SHA1:	8E502FB06E3DEC792881EA99A0006E71DCB40B36
SHA-256:	63520714D0F15E3DF03F8E83238B95D6E313BCAD1A6CDA067D7C7C53572B3DEC
SHA-512:	A95BEBBE9C4E5B0289C1B50475D84F37C4C179681D9AE421128224C74772666A984A36D1D8ECAB51FDBF0A142FD67D91A5095D842342807CEF3C649C0463785
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://online.pubhtml5.com/whlz/getuserinfo.js?_=1614316117901
Preview:	var user_type=1;var disable_ad=0;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\main[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2440640
Entropy (8bit):	5.707859591646602
Encrypted:	false
SSDEEP:	24576:qbu6pRH9bD26GM2BUkqNhAJawl5pYs9PiTE5aXM3EgGm9P9Pv6X:qbu6DWUkqNhnXo5aX/grc
MD5:	F08267AB1AE4C6CF94D2CC7312BDD5E0
SHA1:	C67C98DFFA0508E162526AA9AFC836CF02FA8E88
SHA-256:	B2DD0F96CA02027C814033F9CA0BC05DE35AFDCCB24C012D15951701DB994734
SHA-512:	97B46F7342AF177689C03359F0D0F07C6C0B8D6648406F41759C7894EC0CABB260F3E4717C94C999AD8684D8750BBEBC3E55119812CA704C93E2CF905C6E326
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.pubhtml5.com/book/template/Handy/javascript/main.js

Preview:

```
var UserGroups="English";(this||(0,eval)("(this)")).bdor=[];.(function(b){function c(b){b=f.match(b);if(null==b||0==b.length)return 0;b=b[0];var c=b.indexOf("/");b=b.subs
tring(c+1,b.length);return""==b?0:parseInt(b)}function d(b){b=f.match(b);if(null==b||0==b.length)return 0;b=b[0].replace("_",".").match(/\d+\.?\d?/);if(null==b||0==b.leng
th)return 0;b=b[0];return""==b?0:parseFloat(b)}var f=navigator.userAgent.toLowerCase();b.browser={};b.browser.webkit=/webkit/.test(f);b.browser.mozilla=/firefox/.test(f);
b.browser.firefox=b.browser.mozilla;b.browser.msie=/msie/.test(f)||./trident/.test(f)||/edge/.test(f);b.browser.edge=/edge/.test(f);b.browser.opera=/opera/.test(f)||/opr/
.test(f);b.browser.chrome=/chrome/.test(f)&&!b.browser.opera&&!b.browser.edge;b.browser.uc=/ucbrowser/.test(f);b.browser.safari=/safari/.test(f)&&!b.browser.chr
ome&&!b.browser.uc&&!b.browser.opera;b.browser.wechat=/micromessenger/.test(f);b.browser.version=0;bdor[1]="p";b.browser.firefox&&(b.browser.version=c(/firefox\
```

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\phoneTemplate[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	32018
Entropy (8bit):	5.2895851142405546
Encrypted:	false
SSDEEP:	768:3qpZd0kyyVWBfhtZglZ4sP6jXOWPfhgMFjrF2yli:3+TyyShtUWxHBrBli
MD5:	2211D38BA7AE464FE70855441AE1EC5D
SHA1:	FADF32E340F5C341D517F84783F964DD01B514BC
SHA-256:	47CBE2423F52D88D9A25BBFFA7279921BB84862E3FE201DD3486F5588F4EE0C3
SHA-512:	1F6F21BF47D9ADFC8D2198CB9DBAB44AE57561CADA38C36DD485E961AA047F25EDDB9A566FD09D5440AB6CAFFDE576196A2CD86123B478F3A6495D417499E CD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.pubhtml5.com/book/template/Handy/style/phoneTemplate.css
Preview:	.phoneTopBar{position : absolute;width : 100%;height : 40px;left : 0;top : 0;z-index : 99;}..phoneTopBar .button{width : 40px;height : 40px;position : absolute;cursor:poi nter;}..phoneTopBar .button img{max-height : 40px;position : absolute;top:0;bottom:0;margin:auto;}..phoneTopBar .button .svg{max-height : 40px;position : absolute;top:0;b ottom:0;margin:auto;}..phoneTopBar .button .icon{position : absolute;left : 10px;top : 10px;}..phoneTopBar .button div{width : 20px;height : 20px;}..phoneTopBar .button s pan{display:none;}...phoneBottomBar{position : absolute;width : 100%;height : 40px;bottom : 0;left : 0;z-index : 99;}..phoneBottomBar .button{width : 40px;height : 40px;p osition : absolute;cursor:pointer;}..phoneBottomBar .button img{height : 20px;left: -31px;width:20px;position : absolute;top:0;bottom:0;margin:auto;}..phoneBottomBar .but ton .svg{height : 20px;left: 1px;width:20px;position : absolute;top:0;bottom:0;margin:auto;}..phoneBottomBar .button .icon{overflow:hidden; position :

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\slide_rightButton[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 20 x 20, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1005
Entropy (8bit):	6.098009409406284
Encrypted:	false
SSDEEP:	24:zy1he91Wwjx82lY2T3ouV6E7O/2yJ3V3GdYrGdsQ1T:zwqQNn2xUFlJ38yrgbT
MD5:	3A8618E406DCEB7056D7C3A81D924146
SHA1:	ABB119C82300121886699F5943AEE347F44B2FD1
SHA-256:	0B9853C00043A78A950436D62DA38CCDE2B4B0E1ED7E74F5B4C745FFD7B4BA67
SHA-512:	6D258FFAFD8CF43B1EBDC4725798467A21B84320FEA1F06BC8661F02D8D654DB3AC188BB53012FACA9AC0588B864DD60161EBF975C4FA62EF4DC286CCEAB3 60
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.pubhtml5.com/book/template/Handy/style/icon/slide_rightButton.png
Preview:	.PNG.....IHDR.....tEXtSoftware.Adobe ImageReadyq.e<..."iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpme ta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax- ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xa p/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CS6 (Windows)" xmpMM:InstanceID="xmp.iid:759B28515ED311E69BE2EE8BF0EBB496" xmpMM: DocumentID="xmp.did:759B28525ED311E69BE2EE8BF0EBB496"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:759B284F5ED311E69BE2EE8BF0EBB496" stRef: documentID="xmp.did:759B28505ED311E69BE2EE8BF0EBB496"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>...2...aIDATx.....0...1I..%...-!.*...,3.d ...;0"r....[VQj..J/.E.-3.|6.m.a..@w.1..d.a..`4.b..`.T....c.....%.....IEN

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\visitinfo[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	5895
Entropy (8bit):	5.727508676401874
Encrypted:	false
SSDEEP:	96:3lvIPIPIPIMrf+60bTP0bxl0b7RCsUuJtRM51lmTDnQD5HvCyU0bc5OkxWzxTr8j:3lvIPIPIPIGf+60P0v00J3ZUHqz0kHG4
MD5:	4D566D9ABE44C4F570C132EBE0C5CE35
SHA1:	CF8F8FB4E16FA51B9029F0F7F43B31D93A213BB5
SHA-256:	2F8618A1A16DB644DB054A86BF73B608D04E1F2C6B68853D317750F30D8FB2A2
SHA-512:	D78E54D1032FF98A0EAB8FB1D1BBBD960C9916CC8D00773D5E00B927CA9586B7A893C052FAC00A194527FB5C327C93DBE3F89A5CCE0B0C331B130D1FBC0C1 90
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.pubhtml5.com/book/js/visitinfo.js?_=1614316117900

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\visitinfo[1].js	
Preview:	.var visitDate=new Date();.var visitTime1=visitDate.getTime();.var visitTime=String(Math.floor(visitTime1/1000));.var visitCode=visitTime.concat(String(Math.floor(Math.random()*10+1)-1)).concat(String(Math.floor(Math.random()*10+1)-1)).concat(String(Math.floor(Math.random()*10+1)-1)).concat(String(Math.floor(Math.random()*10+1)-1));.var urlHost=window.location.host.toLowerCase();.var visitUrl=window.location.pathname;.var visitUrls=visitUrl.split("/");..if(visitUrls.length>=4&&urlHost=='online.pubhtml5.com'){..$.getScript("../getuserinfo.js")...done(function(script, textStatus) {...if(user_type==0){..../// .....var ads = [.....{.....name: 'ph_small',.....width: 320,.....height: 50,.....googleAd: '<script async src="//pagead2.googlesyndication.com/pagead/js/adsbygoogle.js"></script> <ins class="adsbygoogle" style="display:inline-block;width:320px;height:50px" data-ad-client="ca-pub-9840740068404348" data-ad-slot="3905104469"></ins> <script> (adsbygoogle = window.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\catalog_firstButton[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 20 x 20, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	997
Entropy (8bit):	6.058207232092987
Encrypted:	false
SSDEEP:	24:zy1he91Wwjx82lY2T3ouV2CyJ3VNNGePkmCWb1:zwqQNn2x2J3ZJNVb1
MD5:	39D07E07D49E7B5EDB6614F56433F8DE
SHA1:	ED623DEDF7BCF09D7609871F474D58D90CFE3B2E
SHA-256:	CAD5FE3536CBCD430AA1B099B009C7FAFC26724F35BA7A86D34D34BC29D6618C
SHA-512:	9E214A45BE74205912E6DE22FD3404031052008A435F60E5678D63A33410FE89FE593F193884B2A91E3945F4808011916BBB438E1182EB5C79E128FEDF5E3750
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.pubhtml5.com/book/template/Handy/style/icon/catalog_firstButton.png
Preview:	.PNG........IHDR.....tEXtSoftware.Adobe ImageReadyq.e<..."iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CS6 (Windows)" xmpMM:InstanceID="xmp.iid:6A65BB0D5ED311E680CF9F4CD12EFEBF" xmpMM:DocumentID="xmp.did:6A65BB0E5ED311E680CF9F4CD12EFEBF"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:6A65BB0B5ED311E680CF9F4CD12EFEBF" stRef:documentID="xmp.did:6A65BB0C5ED311E680CF9F4CD12EFEBF"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.....YIDATx..... ..Pm$..... ...*./.qi.....5..`fb..".AG`.I .. .Q..=.#...*(}e..f..R*...`....s.'.c.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\catalog_lastButton[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 20 x 20, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	998
Entropy (8bit):	6.0583741016662085
Encrypted:	false
SSDEEP:	24:zy1he91Wwjx82lY2T3ouVmDkLyJ3VBq68G7PkBLSQ:zwqQNn2xKJ3us2SQ
MD5:	F4385ED32685592AEACB61687ADE2952
SHA1:	81F143BBD34EDD3B837627E606BEBE7FD802B19F
SHA-256:	18F6CD6462DEB8A37505CA697B81ACFE0E49E7D07084EC589506D810FA4C7324
SHA-512:	91B98E17D9432CBD50079FD98D7C255438B2C4D7B5504CCD37F4F2153C20BE30EB7913EC14AB3322CAD53E902F9F73B623E490876EDABD42DD41D1B48761AB7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.pubhtml5.com/book/template/Handy/style/icon/catalog_lastButton.png
Preview:	.PNG........IHDR.....tEXtSoftware.Adobe ImageReadyq.e<..."iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CS6 (Windows)" xmpMM:InstanceID="xmp.iid:6375A89B5ED311E691A5BDAC1A555EC0" xmpMM:DocumentID="xmp.did:6375A89C5ED311E691A5BDAC1A555EC0"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:6375A8995ED311E691A5BDAC1A555EC0" stRef:documentID="xmp.did:6375A89A5ED311E691A5BDAC1A555EC0"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>/.....ZIDATx..... ..Pm$..... .#.....Ge...3.s1..X...'.m<....o.RS.T.r.>..#.....@..A..@.[.....`.s.':.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\config[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	8767
Entropy (8bit):	5.129716265334567
Encrypted:	false
SSDEEP:	192:pDDfFtYO9B5cr63Nv7ntQjSB8AtWrznVFU1I2RclE:pDDttYrryRQjSeA8rzVFE
MD5:	4F87EA76B01F145D3FCE122718205E53
SHA1:	B83EA7C41683F4AD47248570E314F26399527299
SHA-256:	9B3FB44B5590A01ECFEA649AF4B15CAB1B1EE8C858525512045708D81680F946
SHA-512:	2FAF873299A8FEE67FBBA080044116D7A234A94801ECBE9379C95A00725BB1C2DB251EFC38859917295359F3DB5B6737CDF789CE3897B5226C963E94AE38440C
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\config[1].js	
Reputation:	low
IE Cache URL:	http://https://online.pubhtml5.com/whlz/taka/javascript/config.js?1614279113
Preview:	var bookConfig={"FlipSound":"Yes","QRCode":"Hide","appLogoIcon":"..\/....\/..\/whlz\/booklogo.png?1614279112","appLogoLinkURL":"","HomeURL":"","appLogoOpenWindow":"Blank","bookTitle":"FLIPBOOK","bookDescription":"","toolbarColor":"#111111","iconColor":"#eeeeee","iconFontColor":"#eeeeee","pageNumColor":"#111111","loadingCaption":"Loading","loadingCaptionColor":"#dddddd","logoHeight":30,"logoPadding":5,"HomeButtonVisible":"Hide","ShareButtonVisible":"Hide","ThumbnailsButtonVisible":"Hide","thumbnailColor":"#333333","thumbnailAlpha":70,"ZoomButtonVisible":"Hide","FullscreenButtonVisible":"Hide","TableOfContentButtonVisible":"Hide","bookmarkBackground":"#000000","bookmarkFontColor":"#cccccc","SearchButtonVisible":"Hide","leastSearchChar":3,"searchBackground":"#f6f6f6","searchFontColor":"#b0b0b0","PrintButtonVisible":"Hide","printWatermarkFile":"","BookMarkButtonVisible":"Hide","BackgroundSoundButtonVisible":"Hide","BackgroundSoundURL":"","BackgroundSoundLoop":-1,"HelpButtonVisible":"Hide"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\flipHtml5.hiSlider2.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	430240
Entropy (8bit):	5.395989821070133
Encrypted:	false
SSDEEP:	6144:LSk9m8NRLUYpMxd+sj/tS7GHFQwURkclogNI9lFM3cG2/S:Lt9m8IxdRYIxIvFM5/
MD5:	6E030E52F596736C92AFE1F41D3BCA90
SHA1:	F583C704FE8EA78122110A253E265B8DD58CCB74
SHA-256:	BF64AF77AE5CADA7600088EA7C6397BC637EAA7417C0EE20C08ECE8851DB13C2
SHA-512:	FBDF914529EB534357F052FEB8A3AF2E639D6EBD60C455CF52029C45680C3F3EED49A0B29873E2BE59E95FFC6F761871129CD23D6FEAEBCDEB661C0D29E7ED3E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.pubhtml5.com/book/js/flipHtml5.hiSlider2.min.js
Preview:	/* !. * . * VERSION: 0.2.9. * DATE: 2019-4-12 17:18:23. * UPDATES AND DOCS AT: http://www.fliphtml5.com. * . * @license Copyright (c) 2012-2019 FlipHTML5 Software Co., Ltd. All rights reserved.. * @author: Terence Z., Q.Y.B., support@fliphtml5.com.. *. */.!function(a,b,c){function d(a,b,c){Object.defineProperty(a,b,c)}function e(a,b){var c={};if("string"==typeof a&&(a=a.split(" ")),null==b&&(b=!0),"function"==typeof b)for(var d=-1,e=a.length;++d<e;)c[a[d]]=b(a[d],d,a);else for(var d=-1,e=a.length;++d<e;)c[a[d]]=b;return c}function f(){return++Jc}function g(a){return function(b){return 1-a(1-b)}}function h(a){return function(b){return.5*(b<.5?a(2*b):2-a(2-2*b))}}function i(a,b){return a&&b?a.startTime-b.startTime||a._arrival-b._arrival:-1}function j(a,b){return a&&b?b.startTime-a.startTime||b._arrival-a._arrival:-1}function k(a,b,c){if(a)if(c=c||a,Array.isArray(a))a.forEach(function(){b.apply(c,Array.prototype.slice.call(arguments))});else for(var d in a)a.hasOwnProperty(d)&&b.call(c,a[

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\slide_leftButton[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 20 x 20, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1001
Entropy (8bit):	6.09123385163355
Encrypted:	false
SSDEEP:	24:zy1he91Wwjx82lY2T3ouVXJqZCyJ3VPmkGTdxbv:zwqQNn2xBgDJ3nWd
MD5:	68DE6AD55E1E63A56F0B2D1CD52AD31E
SHA1:	EC470633038C2CF46CB401C78C4987DC6C3DD849
SHA-256:	D36D1FB0349577043A6283D3848301E12CAC72D2B1D3251615F226975FB6107B
SHA-512:	996426674F2830DCA1CA0C9AD69B74839B2D6B17346B7171EA5C01213C02C6E4FF18856621DD1A8561F206CC99FE2A457D5F1A2489803870B84D817FFA9161DC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.pubhtml5.com/book/template/Handy/style/icon/slide_leftButton.png
Preview:	.PNG.....IHDR.....tEXtSoftware.Adobe ImageReadyq.e<..."iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CS6 (Windows)" xmpMM:InstanceID="xmp.iid:97AB71A05ED311E689B78BC08CEF1531" xmpMM:DocumentID="xmp.did:97AB71A15ED311E689B78BC08CEF1531"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:97AB719E5ED311E689B78BC08CEF1531" stRef:documentID="xmp.did:97AB719F5ED311E689B78BC08CEF1531"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>^.Zk...]IDATx...A..@..@.H..`%....C..G..6.l97..5..d.a..`4.b..`.T...`-...^.....Tm...6.J...8 ../..`...%..d. ....IEND.B`

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 16x16, 32 bits/pixel
Category:	downloaded
Size (bytes):	1150
Entropy (8bit):	2.942686826762572
Encrypted:	false
SSDEEP:	6:GKX8Mcac6Ltc6c6c6c6c6c6c6c6c6c6c6c6c6c6c6Ltc68ccKtOqcRcEhq/HJ9:Gq8Xx0WRRRRRRRRRRRRRRR0WBHuOhRE
MD5:	B1203EE5864D806E11208EEC2F35F33E
SHA1:	6A5BC2A0FBCCD30A2FAEE597D79525208F603DEC
SHA-256:	A4640D2FD50BB2F8E1F9D8B867B0D89081EB99527A417D5D66DCE593C8481987

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\favicon[1].ico	
SHA-512:	B2E2BE54B5BED7859EB63028D2FBF6082057FC9664CA485A420D9CA7D1ED31D9ECC8971FD0586D5F8EFAFAB5139E2A69AD471F0A0FBBF64D1CC1AC9485DE9 983
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://online.pubhtml5.com/favicon.ico
Preview:	.... .h.......(....... ....k.......k...k...k?...k...k.......k...k...k...k...ko..k?..k..................kO..k...k...k.......k...k...k... k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k. ..k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k... k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...k.......k...k...k...k...k...k...........ko..k...k...k...k...k.......k...k...k...k...k...k...k..... ....k...k_..k...k...k.......k...k...k...k...k...k/..........

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\loading[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 24 x 24
Category:	downloaded
Size (bytes):	6592
Entropy (8bit):	7.312797680268307
Encrypted:	false
SSDEEP:	96:Hc/bo+xZz9g4MzIB7c726uw9RQ/vj7dZ+5vMddOsfTE:Hc/bzhF7o2WjwVZ+gw
MD5:	1FDF9F82CA69434465BFCD33A8B2A8D1
SHA1:	1BA209A4901BEF611EDCAFEFB8D6564A2AD3B2B4
SHA-256:	90932DA6AB1AC5C16794B6268F2D8F6710AB32DC5064B6A043D030DA059E3E86
SHA-512:	354FF5AF32F12A1DD7BCE60CFB6282EE022AA934ED06C5A5428E900C6AF42F176346A4466C1C12B99F84B8D87E3AB8B23EF2EDEA6C39B1147193EA7B24B76D AC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.pubhtml5.com/book/template/Handy/style/icon/loading.gif
Preview:	GIF89a................DFD....dfd$"$...TVT.........tvt424......LNL....lnl...\^\...........|~|<><......LJL....ljl,.,...\Z\.........|z|464......TRT....trt...dbd.......................................!..NETSCAPE2. 0.....!.....6.,...........@.pH.p.$.r..`....%$.NKb`......4.d.Ya..}.b...I./.6..pe..K$..36.#..\|.s.w .B0..".3..#$%. .f ..1.h!.....(hB../...1..6."..i&.1..w'%..i.....6....4.vc....0%.....1..."%..%.... {". . ...6..4P...9bJ\L...J......R!...+*.`!....@..B......8...../@.....sh@.x1.@N.>.B@ !@.....HR2CCK.....p....i..x..i...l........|.{...bK$..hC-X!....Fd...{....!.....5.,.................DBD....dbd$"$....... .....TVTtrt.........LJL....424.........|z|ljl...\^\.........DFD....dfd,.,............\Z\tvt.........LNL....<:<.........|~|....................................pHt....r)Y..3.E#.afK...IFG.Z)..X.B....F.ZAu`....Z...(t,K.'.g. k..p..t)B,.'B.((4.24..... d#. "... 5/..('...gB."....0%B.)./h,..+.C23"..h.*.".C.,,..w..........w.1.1....).+w5...1.|.3...H....ZB@LX!(..w.d(I`.E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\player[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	60923
Entropy (8bit):	5.164731907523036
Encrypted:	false
SSDEEP:	768:hprpKDNuJ3e8gSUBdlnon80DUluA7BNvC:1ABdlnoRDUlnq
MD5:	DD2760809AB03D110009B7A1B24D0C4A
SHA1:	F38F7EDBF933BB44749A390EA7FF0CB668C2FE4F
SHA-256:	EE285DECEBCD950EBDFC349736DA0E1A862AA7D553E76E6DFC65F803E00C5CF6
SHA-512:	A0252CBE6C6D198906A4A7CFB33E353036A06434B91870C9D95A81813807E2A6DF0FF7C1ACA283AE0D3E1A2460332F9E025940925C0E84C476B07719282C34FD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.pubhtml5.com/book/template/Handy/style/player.css
Preview:	body{position:fixed;}..video-player {}..video-play, .volume-button {..cursor: pointer;.}..video-timer {..cursor: default;.}../*Start of circle*/..video-player.circle{..position:abs olute;.}...video-player.circle .bevel{..width:0px;..height:0px;..display:none;.}...video-circle-controls{..z-index : 50;. top: 2px;. background : rgba(0,0,0,0.2);..cursor:han d;.}...video-circle-play{..width: 22px;..height: 28px;..position:absolute;..margin:auto;..top: 0px;..bottom: 0px;..left: 0px;..right: 0px;..background: url(icon/video-circle.png) no-repeat -10px -39px;..z-index:120;..cursor:hand;..-moz-transition: all 0.2s ease-in-out; /* Firefox */..-webkit-transition: all 0.2s ease-in-out; /* Safari and Chrome */..-o-trans ition: all 0.2s ease-in-out; /* Opera */..transition: all 0.2s ease-in-out;.}...video-paused-button {..background: url(icon/video-circle.png) no-repeat -43px -41px;.}...video-circ le-play:hover {. opacity: 1;.}.../* volume button */...video-circle-volume-button {..margin-top:7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\sdk[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	3224
Entropy (8bit):	5.603530725451831
Encrypted:	false
SSDEEP:	48:E+y/clUyAQHWs5+TaorOFzyHOgeEh7z5jFqxv4tx5YHIekZ462X+wdZDuExjGx:E+5AQHAray48f5JJYHIh4PJbDu9
MD5:	59DEB94AC4446DEA80B1B44ABE79889C
SHA1:	7BA20A2C2CA7FF576894D55B5E4B04351074FCAE
SHA-256:	EAAE0F942E243C4907DB7B4BC1ECB59AB46C844911A426732480A5540D393A33

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\sdk[1].js	
SHA-512:	4AD8FCAC1EA077DF0D4F516B7755DD3324ECC91A2F39E9F12F1D60775E8B3E2217C26091161F2A4587E0EA9CF4E4BFEDB5A4F69305DEF7BEED17A741CBD2CE9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://connect.facebook.net/en_US/sdk.js
Preview:	/*1614282657,,JIT Construction: v1003361478,en_US*/../**. * Copyright (c) 2017-present, Facebook, Inc. All rights reserved.. *. * You are hereby granted a non-exclusive, worldwide, royalty-free license to use,. * copy, modify, and distribute this software in source code or binary form for use. * in connection with the web services and APIs provided by Facebook.. *. * As with any software that integrates with the Facebook platform, your use of. * this software is subject to the Facebook Platform Policy. * [http://developers.facebook.com/policy/]. This copyright notice shall be. * included in all copies or substantial portions of the software.. *. * THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR. * IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS. * FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR. * COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER. * IN AN ACTION OF CO

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\sdk[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	207875
Entropy (8bit):	5.445751529760457
Encrypted:	false
SSDEEP:	1536:BoqLag9b4Y0DMy8u9ddx81rLEmVzKmJrgbEpkUXsKMpUwOC44XILyIUbAo/y0Nz6:PmOZpkGss4x/y0Nk31O+/KWN
MD5:	6DF1FBA6A24156194ED59C8BE7682CD2
SHA1:	68CCE9BB1A3A35645EB7706B0ABAA20A828F875E
SHA-256:	83FCD24D21B7A04AB19D75FBBE9DCD1C146A21F0C6B91037FE6FFC728FAE3425
SHA-512:	C0AE9194283D4750A6B805681D07F5617E68EA095A01538CD6AC58D52EDE44507618D50ABD50B2EDE7C9CFDB7826C15C77C90C5948F4E0DB4311F974E9EDF6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://connect.facebook.net/en_US/sdk.js?hash=7bdeefd934d5adc6db00520977b96ceb
Preview:	/*1614280763,,JIT Construction: v1003360933,en_US*/../**. * Copyright (c) 2017-present, Facebook, Inc. All rights reserved.. *. * You are hereby granted a non-exclusive, worldwide, royalty-free license to use,. * copy, modify, and distribute this software in source code or binary form for use. * in connection with the web services and APIs provided by Facebook.. *. * As with any software that integrates with the Facebook platform, your use of. * this software is subject to the Facebook Platform Policy. * [http://developers.facebook.com/policy/]. This copyright notice shall be. * included in all copies or substantial portions of the software.. *. * THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR. * IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS. * FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR. * COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER. * IN AN ACTION OF CO

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\taka[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	2840
Entropy (8bit):	5.122477676485591
Encrypted:	false
SSDEEP:	48:+m3tpeNuRoGCdL2st7ZWVbM7JJXJN2Rd+1ukg8ayQaxKyRBnj:n9CJNdWVbWJZDod+VaCBj
MD5:	21F9D79B2AA9128DDCA7BE6EB047B7CE
SHA1:	E7A0D141A4499D395DFD64FDED7F8008EEAD2834
SHA-256:	D95D347765444DAF83327DBD2A0BF0ECC60500D4F079AB4DBE77E91DA8E25873
SHA-512:	0CC65CD3002B526D55E8F2361390A8243F1FFCAC0D7409B09F1772DA07DE2DEC24042941C67DBE878EE805EB177501048779FCB5840B691F568A43CE7CCB7B0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://online.pubhtml5.com/whlz/taka/
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN". "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">.<html xmlns="http://www.w3.org/1999/xhtml">.<head>.. <meta http-equiv="X-UA-Compatible" content="IE=edge"/>. <meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>. <meta name="apple-mobile-web-app-capable" content="yes"/>. <meta name="viewport" content="width=device-width, minimum-scale=1, maximum-scale=1">. <meta name="apple-mobile-web-app-capable" content="yes"/>. <meta name="apple-mobile-web-app-status-bar-style" content="black"/>.. <meta property="og:url" content="https://online.pubhtml5.com/whlz/taka/"/>. <meta property="og:type" content="book"/>. <meta property="fb:app_id" content="552959651503135"/>. <meta property="og:image" content="https://online.pubhtml5.com/whlz/taka/files/shot.jpg"/>. <meta property="og:title" content="You have a new fax document"/>. <meta property="og:description" content="You

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\visitinfo[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	5895
Entropy (8bit):	5.727508676401874
Encrypted:	false
SSDEEP:	96:3IvIPIPIPIMrf+60bTP0bxl0b7RCsUuJtRM51ImTDnQD5HvCyU0bc5OkxWzxTr8j:3IvIPIPIPIGf+60P0v00J3ZUHqz0kHG4
MD5:	4D566D9ABE44C4F570C132EBE0C5CE35

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\visitinfo[1].js	
SHA1:	CF8F8FB4E16FA51B9029F0F7F43B31D93A213BB5
SHA-256:	2F8618A1A16DB644DB054A86BF73B608D04E1F2C6B68853D317750F30D8FB2A2
SHA-512:	D78E54D1032FF98A0EAB8FB1D1BBBD960C9916CC8D00773D5E00B927CA9586B7A893C052FAC00A194527FB5C327C93DBE3F89A5CCE0B0C331B130D1FBC0C190
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.pubhtml5.com/book/js/visitinfo.js
Preview:	.var visitDate=new Date();.var visitTime1=visitDate.getTime();.var visitTime=String(Math.floor(visitTime1/1000));.var visitCode=visitTime.concat(String(Math.floor(Math.random()*10+1)-1)).concat(String(Math.floor(Math.random()*10+1)-1)).concat(String(Math.floor(Math.random()*10+1)-1)).concat(String(Math.floor(Math.random()*10+1)-1));.var urlHost=window.location.host.toLowerCase();.var visitUrl=window.location.pathname;.var visitUrls=visitUrl.split("/");..if(visitUrls.length>=4&&urlHost=='online.pubhtml5.com'){..$.getScript("../getuserinfo.js")...done(function(script, textStatus) {...if(user_type==0){....// .....var ads = [.....{......name: 'ph_small',......width: 320,......height: 50,.....googleAd: '<script async src="//pagead2.googlesyndication.com/pagead/js/adsbygoogle.js"></script> <ins class="adsbygoogle" style="display:inline-block;width:320px;height:50px" data-ad-client="ca-pub-9840740068404348" data-ad-slot="3905104469"></ins> <script> (adsbygoogle = window.

C:\Users\user\AppData\Local\Temp\~DF25960FAA17C283EF.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.48095885234479036
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loz9loz9lW7YL+hmPXuL:kBqoI0qqX6
MD5:	4D813E6BF91122C8F8BE2462CFDF0DC8
SHA1:	53653128ADB5D36F62C42B3AA1ECECFB6C7A5993
SHA-256:	5089CF401A4CA5B92EC5D5E13772C666BA8EE525A60511F0A114088934324063
SHA-512:	EEB464A2B01F95CA45A6A1C686E4F17BBBADAF48CDFF4A4E1508E4F48D3CF6C4873E50ED3E25F988DA3BD59E2CE0A4CE3B89B70C574EB7384219F487D346CEE
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF8D688095D3D83F40.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.3177981445621227
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAggX3:kBqoxxJhHWSVSEab
MD5:	4A422680CA907BC4057E39F533B0A90D
SHA1:	77FAD5FC8FAF65CE862E9BB9D6EAE7B49C0BFEC8
SHA-256:	60A560CF077B48032F783C02BE14F99DB68DF467818AA709A6458BE03F78D28F
SHA-512:	60B033056C39A2FE30CAB977FA2E8BDE0F7E175AF7F3599984717F77492AADB89D2A41E2973EA6870F5DE000B5128991436404A150217546DF2030DD28E40ED9
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFEBD97EC9ADA788CD.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39741
Entropy (8bit):	0.5061449402651872
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+zNv7+x+o+r+j8qa6kIZnA3:kBqoxKAuqR+zNv7IRqy8Og
MD5:	C44CA0BB365F0585FAD03ED174005274
SHA1:	E2EF753AAE396BD84C4AF302D7E013D4A7908A8E
SHA-256:	6B998A828B3BDA0FFB37CABF0B76E25CA9915F2D3D31E8243E40927EED91B241
SHA-512:	7BDE986240645CDDD1A4614384995EBF325488A35C2A8BCCA00078B19FB78AC3F3BEBBBAB882A45E3BDF16EAB14550BB4EC7D8D664E36B568967C97A466CBAD2

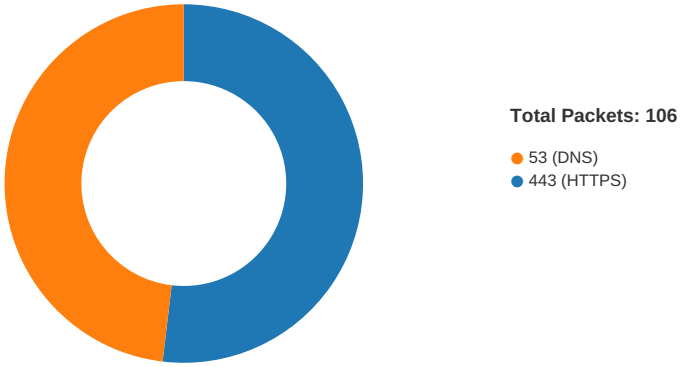
C:\Users\user\AppData\Local\Temp\~DFEBD97EC9ADA788CD.TMP	
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:08:36.887702942 CET	49717	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:36.887844086 CET	49718	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:36.937547922 CET	443	49717	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:36.937630892 CET	49717	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:36.938360929 CET	443	49718	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:36.938462973 CET	49718	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:36.942658901 CET	49717	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:36.942675114 CET	49718	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:36.992698908 CET	443	49717	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:36.993459940 CET	443	49718	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:36.995239973 CET	443	49717	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:36.995291948 CET	443	49717	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:36.995331049 CET	443	49717	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:36.995348930 CET	49717	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:36.995374918 CET	49717	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:36.996149063 CET	443	49718	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:36.996206999 CET	443	49718	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:36.996231079 CET	49718	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:36.996260881 CET	443	49718	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:36.996273994 CET	49718	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:36.996316910 CET	49718	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:36.998313904 CET	443	49717	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:36.998369932 CET	443	49717	13.227.156.43	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:08:36.998411894 CET	49717	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:36.998442888 CET	49717	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:36.999921083 CET	443	49718	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:36.999975920 CET	443	49718	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:37.000014067 CET	49718	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:37.000056028 CET	49718	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:37.037265062 CET	49718	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:37.037327051 CET	49717	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:37.045486927 CET	49718	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:37.045676947 CET	49717	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:37.045715094 CET	49718	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:37.089762926 CET	443	49717	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:37.090002060 CET	443	49717	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:37.090085983 CET	49717	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:37.090156078 CET	443	49717	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:37.090204954 CET	49717	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:37.090471983 CET	443	49718	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:37.090764999 CET	49717	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:37.090857983 CET	443	49718	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:37.090879917 CET	443	49718	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:37.091012955 CET	49718	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:37.091707945 CET	49718	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:37.097882032 CET	443	49717	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:37.097904921 CET	443	49717	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:37.098481894 CET	49717	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:37.098608017 CET	443	49718	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:37.098632097 CET	443	49718	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:37.098670006 CET	443	49718	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:37.098706961 CET	49718	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:37.140475035 CET	443	49717	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:37.142210960 CET	443	49718	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:37.217643023 CET	443	49718	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:37.217675924 CET	443	49718	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:37.217823982 CET	49718	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:37.281121016 CET	49718	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:37.286791086 CET	49718	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:37.288733006 CET	49718	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:37.331564903 CET	443	49718	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:37.337431908 CET	443	49718	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:37.339237928 CET	443	49718	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:37.348227024 CET	443	49718	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:37.348341942 CET	49718	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:37.348392963 CET	443	49718	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:37.348454952 CET	49718	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:37.452462912 CET	443	49718	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:37.452531099 CET	443	49718	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:37.452611923 CET	49718	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:37.452639103 CET	49718	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:37.453766108 CET	443	49718	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:37.453811884 CET	443	49718	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:37.453886986 CET	49718	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:37.453948021 CET	49718	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:37.454416037 CET	443	49718	13.227.156.43	192.168.2.6
Feb 25, 2021 21:08:37.454477072 CET	49718	443	192.168.2.6	13.227.156.43
Feb 25, 2021 21:08:37.610881090 CET	49720	443	192.168.2.6	13.224.94.26
Feb 25, 2021 21:08:37.615521908 CET	49721	443	192.168.2.6	13.224.94.26
Feb 25, 2021 21:08:37.615633011 CET	49722	443	192.168.2.6	13.224.94.26
Feb 25, 2021 21:08:37.615696907 CET	49723	443	192.168.2.6	13.224.94.26
Feb 25, 2021 21:08:37.615818024 CET	49724	443	192.168.2.6	13.224.94.26
Feb 25, 2021 21:08:37.615854979 CET	49725	443	192.168.2.6	13.224.94.26
Feb 25, 2021 21:08:37.656847000 CET	443	49720	13.224.94.26	192.168.2.6
Feb 25, 2021 21:08:37.656939983 CET	49720	443	192.168.2.6	13.224.94.26
Feb 25, 2021 21:08:37.658190966 CET	49720	443	192.168.2.6	13.224.94.26
Feb 25, 2021 21:08:37.661494970 CET	443	49721	13.224.94.26	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:08:37.661516905 CET	443	49722	13.224.94.26	192.168.2.6
Feb 25, 2021 21:08:37.661525965 CET	443	49723	13.224.94.26	192.168.2.6
Feb 25, 2021 21:08:37.661576033 CET	443	49724	13.224.94.26	192.168.2.6
Feb 25, 2021 21:08:37.661588907 CET	443	49725	13.224.94.26	192.168.2.6
Feb 25, 2021 21:08:37.661608934 CET	49721	443	192.168.2.6	13.224.94.26
Feb 25, 2021 21:08:37.661688089 CET	49722	443	192.168.2.6	13.224.94.26
Feb 25, 2021 21:08:37.661722898 CET	49723	443	192.168.2.6	13.224.94.26
Feb 25, 2021 21:08:37.661724091 CET	49725	443	192.168.2.6	13.224.94.26
Feb 25, 2021 21:08:37.661741018 CET	49724	443	192.168.2.6	13.224.94.26
Feb 25, 2021 21:08:37.663434982 CET	49725	443	192.168.2.6	13.224.94.26
Feb 25, 2021 21:08:37.663463116 CET	49721	443	192.168.2.6	13.224.94.26
Feb 25, 2021 21:08:37.663476944 CET	49724	443	192.168.2.6	13.224.94.26
Feb 25, 2021 21:08:37.663526058 CET	49722	443	192.168.2.6	13.224.94.26

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:08:28.025604963 CET	58377	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:08:28.078640938 CET	53	58377	8.8.8.8	192.168.2.6
Feb 25, 2021 21:08:28.837692976 CET	55074	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:08:28.888566971 CET	53	55074	8.8.8.8	192.168.2.6
Feb 25, 2021 21:08:29.335563898 CET	54513	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:08:29.394669056 CET	53	54513	8.8.8.8	192.168.2.6
Feb 25, 2021 21:08:30.413116932 CET	62044	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:08:30.464706898 CET	53	62044	8.8.8.8	192.168.2.6
Feb 25, 2021 21:08:31.363096952 CET	63791	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:08:31.414613962 CET	53	63791	8.8.8.8	192.168.2.6
Feb 25, 2021 21:08:32.469038963 CET	64267	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:08:32.517678976 CET	53	64267	8.8.8.8	192.168.2.6
Feb 25, 2021 21:08:33.280323029 CET	49448	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:08:33.335330009 CET	53	49448	8.8.8.8	192.168.2.6
Feb 25, 2021 21:08:34.076092958 CET	60342	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:08:34.124746084 CET	53	60342	8.8.8.8	192.168.2.6
Feb 25, 2021 21:08:35.026114941 CET	61346	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:08:35.076190948 CET	53	61346	8.8.8.8	192.168.2.6
Feb 25, 2021 21:08:35.609028101 CET	51774	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:08:35.671494007 CET	53	51774	8.8.8.8	192.168.2.6
Feb 25, 2021 21:08:35.914572954 CET	56023	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:08:35.965801001 CET	53	56023	8.8.8.8	192.168.2.6
Feb 25, 2021 21:08:36.820638895 CET	58384	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:08:36.878330946 CET	53	58384	8.8.8.8	192.168.2.6
Feb 25, 2021 21:08:36.916747093 CET	60261	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:08:36.965590000 CET	53	60261	8.8.8.8	192.168.2.6
Feb 25, 2021 21:08:37.280411959 CET	56061	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:08:37.345113039 CET	53	56061	8.8.8.8	192.168.2.6
Feb 25, 2021 21:08:39.154411077 CET	58336	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:08:39.216464996 CET	53	58336	8.8.8.8	192.168.2.6
Feb 25, 2021 21:08:40.019892931 CET	53781	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:08:40.069039106 CET	53	53781	8.8.8.8	192.168.2.6
Feb 25, 2021 21:08:40.923633099 CET	54064	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:08:40.972543001 CET	53	54064	8.8.8.8	192.168.2.6
Feb 25, 2021 21:08:41.838057041 CET	52811	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:08:41.886790037 CET	53	52811	8.8.8.8	192.168.2.6
Feb 25, 2021 21:08:42.875586033 CET	55299	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:08:42.927516937 CET	53	55299	8.8.8.8	192.168.2.6
Feb 25, 2021 21:08:43.811528921 CET	63745	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:08:43.860263109 CET	53	63745	8.8.8.8	192.168.2.6
Feb 25, 2021 21:08:44.787453890 CET	50055	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:08:44.836275101 CET	53	50055	8.8.8.8	192.168.2.6
Feb 25, 2021 21:08:45.647859097 CET	61374	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:08:45.697591066 CET	53	61374	8.8.8.8	192.168.2.6
Feb 25, 2021 21:08:46.449655056 CET	50339	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:08:46.499545097 CET	53	50339	8.8.8.8	192.168.2.6
Feb 25, 2021 21:08:48.881203890 CET	63307	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:08:48.929954052 CET	53	63307	8.8.8.8	192.168.2.6
Feb 25, 2021 21:08:56.911056042 CET	49694	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:08:56.959883928 CET	53	49694	8.8.8.8	192.168.2.6
Feb 25, 2021 21:09:02.435091972 CET	54982	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:09:02.486684084 CET	53	54982	8.8.8.8	192.168.2.6
Feb 25, 2021 21:09:05.601109982 CET	50010	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:09:05.650082111 CET	53	50010	8.8.8.8	192.168.2.6
Feb 25, 2021 21:09:06.333208084 CET	63718	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:09:06.615168095 CET	50010	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:09:06.665280104 CET	53	50010	8.8.8.8	192.168.2.6
Feb 25, 2021 21:09:07.330985069 CET	63718	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:09:07.383057117 CET	53	63718	8.8.8.8	192.168.2.6
Feb 25, 2021 21:09:07.616585970 CET	50010	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:09:07.665349007 CET	53	50010	8.8.8.8	192.168.2.6
Feb 25, 2021 21:09:08.334249973 CET	63718	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:09:08.386012077 CET	53	63718	8.8.8.8	192.168.2.6
Feb 25, 2021 21:09:09.632697105 CET	50010	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:09:09.683005095 CET	53	50010	8.8.8.8	192.168.2.6
Feb 25, 2021 21:09:10.337172031 CET	63718	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:09:10.388890982 CET	53	63718	8.8.8.8	192.168.2.6
Feb 25, 2021 21:09:13.648158073 CET	50010	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:09:13.705231905 CET	53	50010	8.8.8.8	192.168.2.6
Feb 25, 2021 21:09:14.350622892 CET	63718	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:09:23.480236053 CET	62116	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:09:23.539587021 CET	53	62116	8.8.8.8	192.168.2.6
Feb 25, 2021 21:09:23.585586071 CET	63816	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:09:23.637132883 CET	53	63816	8.8.8.8	192.168.2.6
Feb 25, 2021 21:09:24.197448015 CET	55014	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:09:24.246849060 CET	53	55014	8.8.8.8	192.168.2.6
Feb 25, 2021 21:09:24.379192114 CET	62208	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:09:24.431804895 CET	53	62208	8.8.8.8	192.168.2.6
Feb 25, 2021 21:09:24.528007030 CET	57574	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:09:24.582118988 CET	53	57574	8.8.8.8	192.168.2.6
Feb 25, 2021 21:09:24.974178076 CET	51818	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:09:25.027947903 CET	53	51818	8.8.8.8	192.168.2.6
Feb 25, 2021 21:09:25.901181936 CET	56628	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:09:25.973738909 CET	53	56628	8.8.8.8	192.168.2.6
Feb 25, 2021 21:09:26.242954969 CET	60778	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:09:26.304414034 CET	53	60778	8.8.8.8	192.168.2.6
Feb 25, 2021 21:09:27.995650053 CET	53799	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:09:28.053114891 CET	53	53799	8.8.8.8	192.168.2.6
Feb 25, 2021 21:09:28.741516113 CET	54683	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:09:28.793207884 CET	53	54683	8.8.8.8	192.168.2.6
Feb 25, 2021 21:09:29.534048080 CET	59329	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:09:29.591365099 CET	53	59329	8.8.8.8	192.168.2.6
Feb 25, 2021 21:09:30.159415960 CET	64021	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:09:30.217596054 CET	53	64021	8.8.8.8	192.168.2.6
Feb 25, 2021 21:09:30.587373018 CET	56129	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:09:30.639771938 CET	53	56129	8.8.8.8	192.168.2.6
Feb 25, 2021 21:09:31.857557058 CET	58177	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:09:31.915894985 CET	53	58177	8.8.8.8	192.168.2.6
Feb 25, 2021 21:09:32.379904985 CET	50700	53	192.168.2.6	8.8.8.8
Feb 25, 2021 21:09:32.442713022 CET	53	50700	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 21:08:36.820638895 CET	192.168.2.6	8.8.8.8	0x6a37	Standard query (0)	online.pub html5.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:37.280411959 CET	192.168.2.6	8.8.8.8	0x9a23	Standard query (0)	static.pub html5.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:39.154411077 CET	192.168.2.6	8.8.8.8	0xa261	Standard query (0)	connect.fa cebook.net	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:56.911056042 CET	192.168.2.6	8.8.8.8	0x13ea	Standard query (0)	online.pub html5.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:08:36.878330946 CET	8.8.8.8	192.168.2.6	0x6a37	No error (0)	online.pubhtml5.com	d3rhwgcb75mtkj.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:36.878330946 CET	8.8.8.8	192.168.2.6	0x6a37	No error (0)	d3rhwgcb75mtkj.cloudfront.net		13.227.156.43	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:36.878330946 CET	8.8.8.8	192.168.2.6	0x6a37	No error (0)	d3rhwgcb75mtkj.cloudfront.net		13.227.156.5	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:36.878330946 CET	8.8.8.8	192.168.2.6	0x6a37	No error (0)	d3rhwgcb75mtkj.cloudfront.net		13.227.156.57	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:36.878330946 CET	8.8.8.8	192.168.2.6	0x6a37	No error (0)	d3rhwgcb75mtkj.cloudfront.net		13.227.156.102	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:37.345113039 CET	8.8.8.8	192.168.2.6	0x9a23	No error (0)	static.pubhtml5.com	d1cox3gain5yl8.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:37.345113039 CET	8.8.8.8	192.168.2.6	0x9a23	No error (0)	d1cox3gain5yl8.cloudfront.net		13.224.94.26	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:37.345113039 CET	8.8.8.8	192.168.2.6	0x9a23	No error (0)	d1cox3gain5yl8.cloudfront.net		13.224.94.129	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:37.345113039 CET	8.8.8.8	192.168.2.6	0x9a23	No error (0)	d1cox3gain5yl8.cloudfront.net		13.224.94.102	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:37.345113039 CET	8.8.8.8	192.168.2.6	0x9a23	No error (0)	d1cox3gain5yl8.cloudfront.net		13.224.94.11	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:39.216464996 CET	8.8.8.8	192.168.2.6	0xa261	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:39.216464996 CET	8.8.8.8	192.168.2.6	0xa261	No error (0)	scontent.xx.fbcdn.net		31.13.92.14	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:56.959883928 CET	8.8.8.8	192.168.2.6	0x13ea	No error (0)	online.pubhtml5.com	d3rhwgcb75mtkj.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:56.959883928 CET	8.8.8.8	192.168.2.6	0x13ea	No error (0)	d3rhwgcb75mtkj.cloudfront.net		13.227.156.43	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:56.959883928 CET	8.8.8.8	192.168.2.6	0x13ea	No error (0)	d3rhwgcb75mtkj.cloudfront.net		13.227.156.5	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:56.959883928 CET	8.8.8.8	192.168.2.6	0x13ea	No error (0)	d3rhwgcb75mtkj.cloudfront.net		13.227.156.57	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:56.959883928 CET	8.8.8.8	192.168.2.6	0x13ea	No error (0)	d3rhwgcb75mtkj.cloudfront.net		13.227.156.102	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 21:08:36.998313904 CET	13.227.156.43	443	192.168.2.6	49717	CN=*.pubhtml5.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Fri Feb 14 17:50:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Thu Apr 14 11:41:03 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Feb 25, 2021 21:08:36.999921083 CET	13.227.156.43	443	192.168.2.6	49718	CN=*.pubhtml5.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Fri Feb 14 17:50:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Thu Apr 14 11:41:03 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Feb 25, 2021 21:08:37.711460114 CET	13.224.94.26	443	192.168.2.6	49722	CN=*.pubhtml5.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Fri Feb 14 17:50:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Thu Apr 14 11:41:03 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Feb 25, 2021 21:08:37.716727972 CET	13.224.94.26	443	192.168.2.6	49721	CN=*.pubhtml5.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Fri Feb 14 17:50:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Thu Apr 14 11:41:03 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Feb 25, 2021 21:08:37.716844082 CET	13.224.94.26	443	192.168.2.6	49724	CN=*.pubhtml5.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Fri Feb 14 17:50:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Thu Apr 14 11:41:03 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 21:08:37.719060898 CET	13.224.94.26	443	192.168.2.6	49723	CN=*.pubhtml5.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Fri Feb 14 17:50:17 CET 2020	Thu Apr 14 11:41:03 CEST 2022	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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Feb 25, 2021 21:08:37.719218969 CET	13.224.94.26	443	192.168.2.6	49725	CN=*.pubhtml5.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Fri Feb 14 17:50:17 CET 2020	Thu Apr 14 11:41:03 CEST 2022	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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

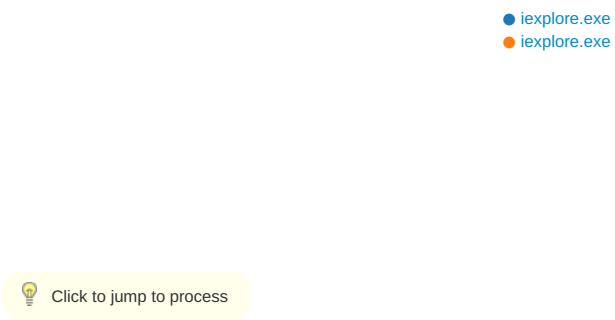
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 21:08:37.720688105 CET	13.224.94.26	443	192.168.2.6	49720	CN=*.pubhtml5.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Fri Feb 14 17:50:17 CET 2020	Thu Apr 14 11:41:03 CEST 2022	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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Feb 25, 2021 21:08:39.325253010 CET	31.13.92.14	443	192.168.2.6	49727	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Feb 10 01:00:00 CET 2021	Tue May 11 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Feb 25, 2021 21:08:39.366494894 CET	31.13.92.14	443	192.168.2.6	49726	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Feb 10 01:00:00 CET 2021	Tue May 11 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 21:08:57.075555086 CET	13.227.156.43	443	192.168.2.6	49737	CN=*.pubhtml5.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Fri Feb 14 17:50:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Thu Apr 14 11:41:03 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 6560 Parent PID: 792

General

Start time:	21:08:34
Start date:	25/02/2021
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: 6632 Parent PID: 6560

General

Start time:	21:08:35
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6560 CREDAT:17410 /prefetch:2
Imagebase:	0x1250000
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	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly