ID: 323053
Cookbook: browseurl.jbs
Time: 09:17:49
Date: 26/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

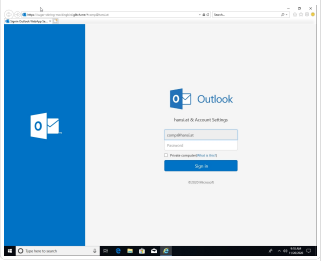
Analysis Report https://sugar-stirring-mockingbird.glitc…

Overview

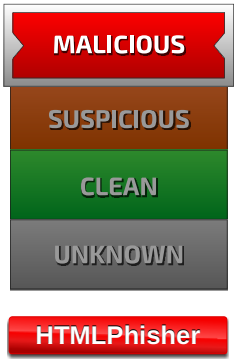
General Information

Sample URL:	http://https://sugar-stirring-mockingbird.glitch.me/#comp@hansi.at
Analysis ID:	323053

Most interesting Screenshot:



Detection

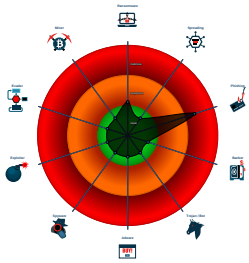


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected HtmlPhish_20
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- URL contains potential PII (phishing…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 68 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 2644 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:68 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

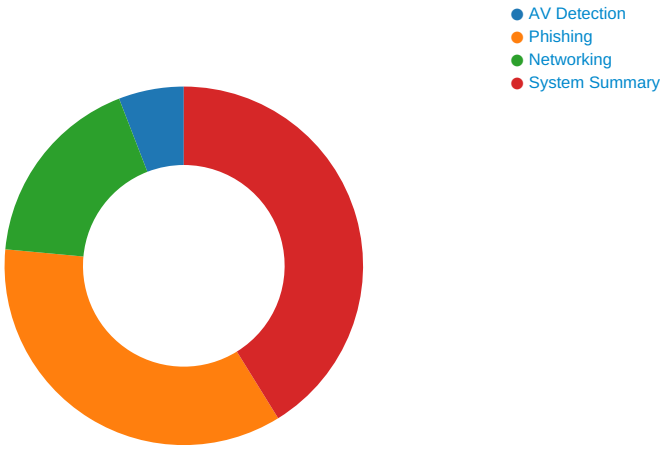
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\1RWIY0K9.htm	JoeSecurity_HtmlPhish_20	Yara detected HtmlPhish_20	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Phishing:

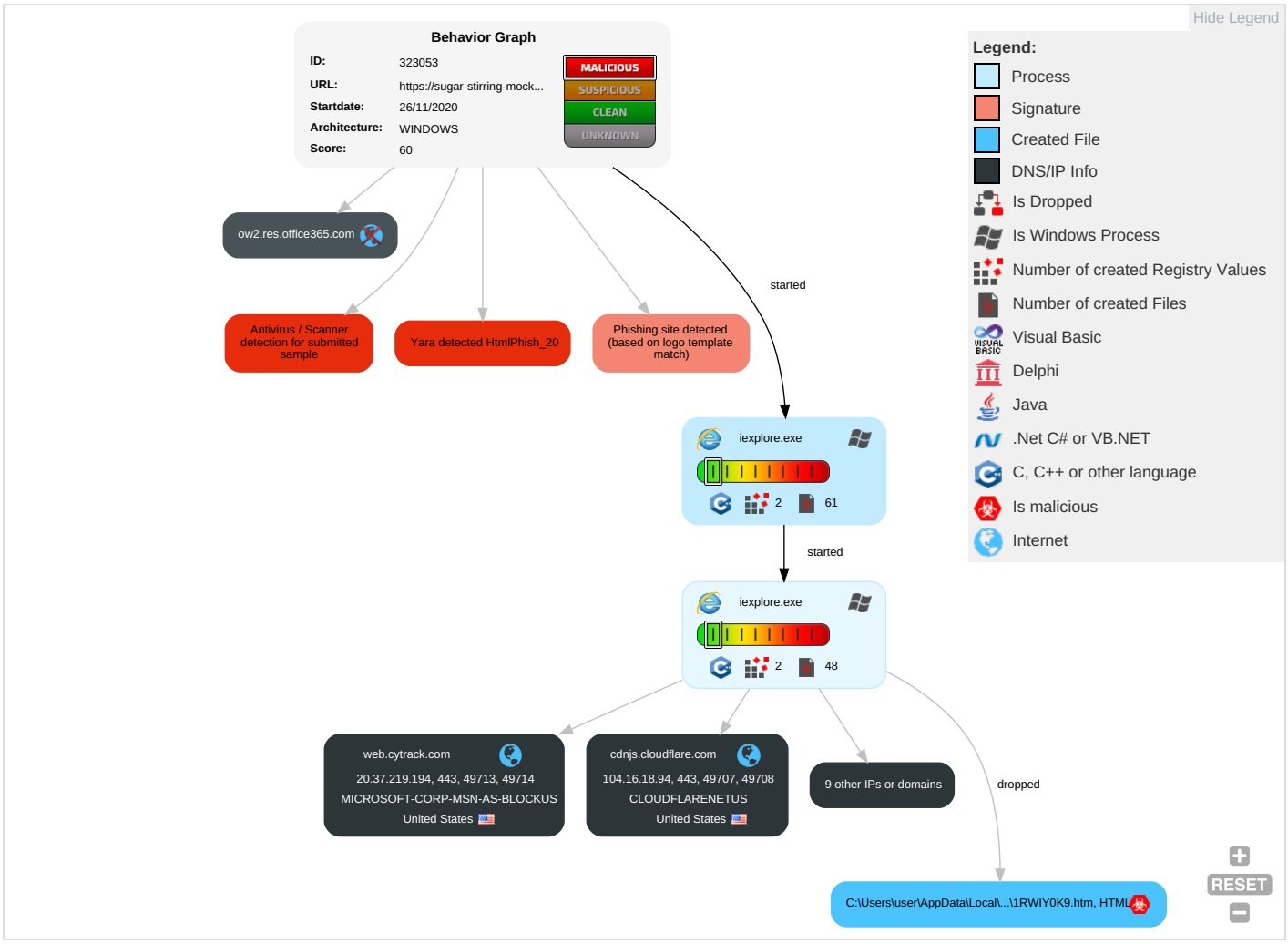
Yara detected HtmlPhish_20

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

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

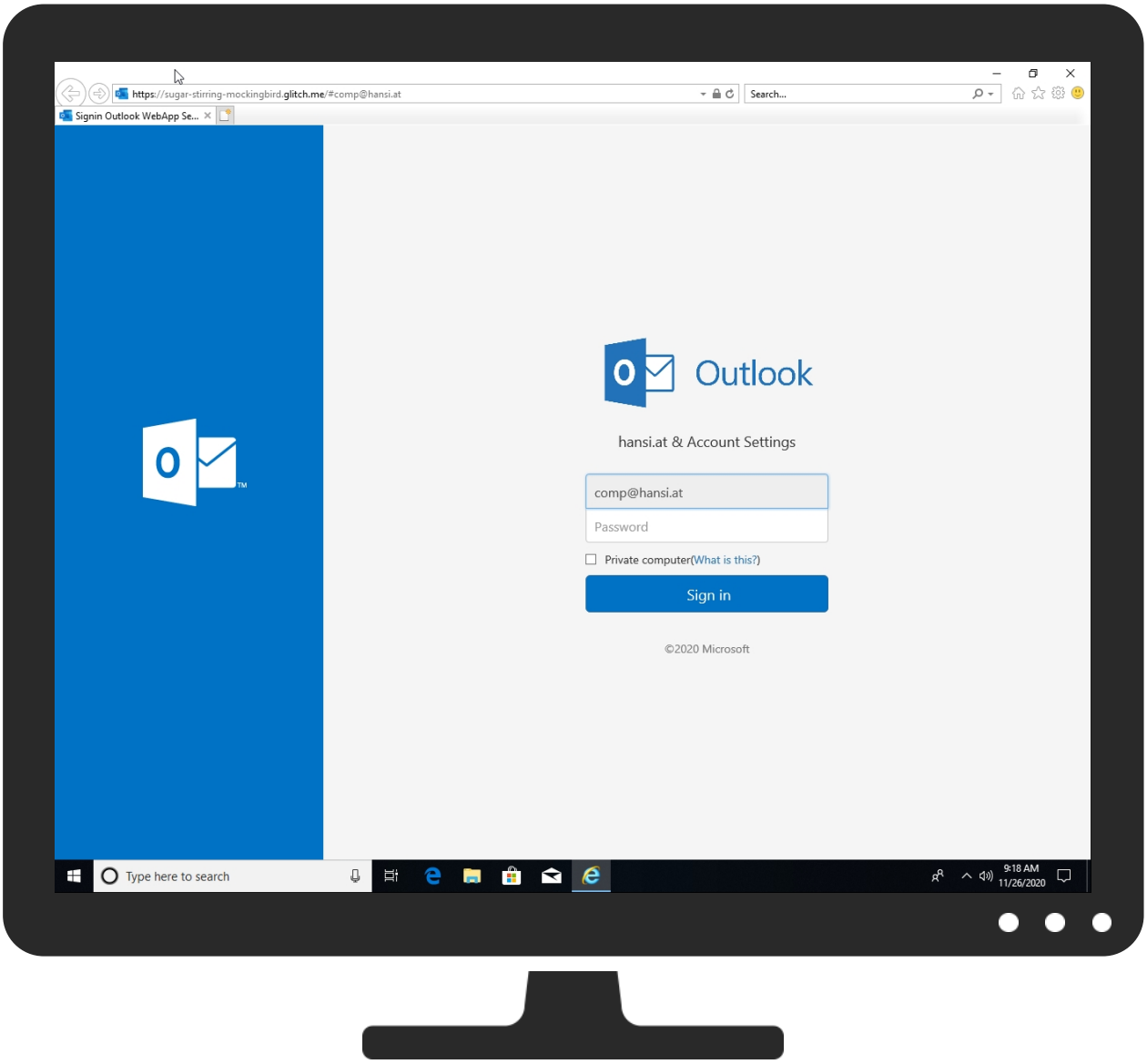
Behavior Graph



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://sugar-stirring-mockingbird.glitch.me/#comp@hansi.at	0%	Virustotal		Browse
http://https://sugar-stirring-mockingbird.glitch.me/#comp@hansi.at	0%	Avira URL Cloud	safe	
http://https://sugar-stirring-mockingbird.glitch.me/#comp@hansi.at	100%	UrlScan	phishing brand: outlook web access	Browse
http://https://sugar-stirring-mockingbird.glitch.me/#comp@hansi.at	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://https://autosoftug.com/wp-content/themes/satenet/inc/xz4/processor.php	0%	Avira URL Cloud	safe	
http://https://web.cytrack.com/wpv1/wp-content/uploads/microsoft-outlook-logo.jpg	0%	Virustotal		Browse
http://https://web.cytrack.com/wpv1/wp-content/uploads/microsoft-outlook-logo.jpg	0%	Avira URL Cloud	safe	
http://fontawesome.iohttp://fontawesome.iohttp://fontawesome.io/license/http://fontawesome.io/licens	0%	Avira URL Cloud	safe	
http://getbootstrap.com)	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
elb097307-934924932.us-east-1.elb.amazonaws.com	54.225.169.28	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
web.cytrack.com	20.37.219.194	true	false	• 0%, Virustotal, Browse	unknown
sugar-stirring-mockingbird.glitch.me	52.205.236.122	true	false		high
stackpath.bootstrapcdn.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
cdn.jsdelivr.net	unknown	unknown	false		high
maxcdn.bootstrapcdn.com	unknown	unknown	false		high
ow2.res.office365.com	unknown	unknown	false		high
api.ipify.org	unknown	unknown	false		high

Contacted URLs

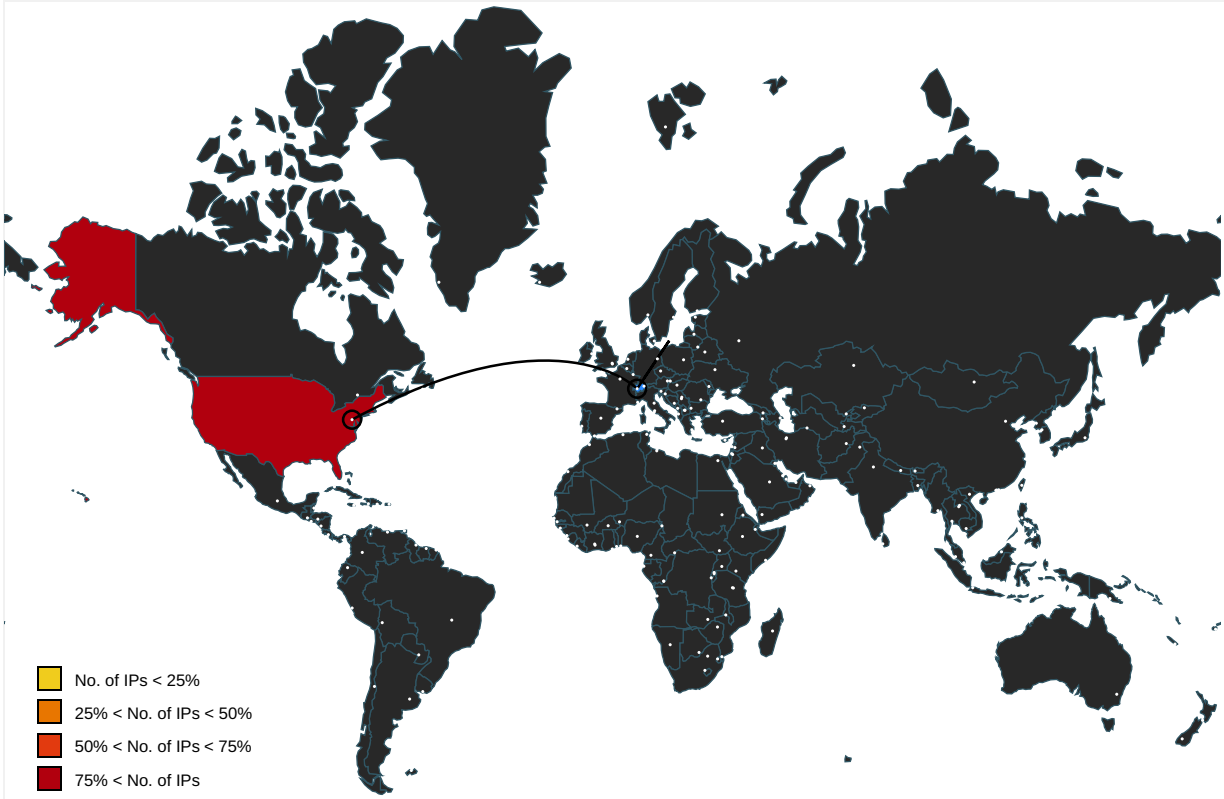
Name	Malicious	Antivirus Detection	Reputation
http://https://sugar-stirring-mockingbird.glitch.me/#comp@hansi.at	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://sugar-stirring-mockingbird.glitch.me/#comp	~DF7B847ADEC881B843.TMP.1.dr, {6D30CF7E-300B-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://fontawesome.io	fontawesome-webfont[1].eot.2.dr, font-awesome.min[1].css.2.dr	false		high
http://https://autosoftug.com/wp-content/themes/satenet/inc/xz4/processor.php	1RWIY0K9.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://code.jquery.com/jquery-migrate-3.1.0.min.js	1RWIY0K9.htm.2.dr	false		high
http://https://web.cytrack.com/wpv1/wp-content/uploads/microsoft-outlook-logo.jpg	1RWIY0K9.htm.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://fontawesome.iohttp://fontawesome.iohttp://fontawesome.io/license/http://fontawesome.io/licens	fontawesome-webfont[1].eot.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css	1RWIY0K9.htm.2.dr	false		high
http://https://stackpath.bootstrapcdn.com/bootstrap/4.1.0/js/bootstrap.min.js	1RWIY0K9.htm.2.dr	false		high
http://https://cdn.jsdelivr.net/npm/sweetalert2	1RWIY0K9.htm.2.dr	false		high
http://https://api.ipify.org?format=json	1RWIY0K9.htm.2.dr	false		high
http://https://ow2.res.office365.com/owalanding/2020.1.16.01/images/favicon.ico?v=4	imagestore.dat.2.dr, 1RWIY0K9.htm.2.dr	false		high
http://https://getbootstrap.com/)	bootstrap.min[1].js.2.dr	false		high
http://fontawesome.io/license	font-awesome.min[1].css.2.dr	false		high
http://fontawesome.io/license/	fontawesome-webfont[1].eot.2.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.0/umd/popper.min.js	1RWIY0K9.htm.2.dr	false		high
http://https://github.com/danieledesantis/jquery-browser-detection	1RWIY0K9.htm.2.dr	false		high
http://https://github.com/twbs/bootstrap/graphs/contributors)	bootstrap.min[1].js.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://stackpath.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css	1RWIY0K9.htm.2.dr	false		high
http://getbootstrap.com)	bootstrap.min[1].css.2.dr	false	• Avira URL Cloud: safe	low
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap.min[1].js.2.dr, bootstrap.min[1].css.2.dr	false		high
http://https://sugar-stirring-mockingbird.glitch.me/	~DF7B847ADEC881B843.TMP.1.dr	false		high
http://opensource.org/licenses/MIT).	popper.min[1].js.2.dr	false		high
http://https://code.jquery.com/jquery-3.3.1.min.js	1RWIY0K9.htm.2.dr	false		high
http://https://ow2.res.office365.com/owalanding/2020.1.16.01/images/favicon.ico?v=4~	imagestore.dat.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
20.37.219.194	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
54.225.169.28	unknown	United States		14618	AMAZON-AESUS	false
52.205.236.122	unknown	United States		14618	AMAZON-AESUS	false
104.16.18.94	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323053
Start date:	26.11.2020
Start time:	09:17:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 39s
Hypervisor based Inspection enabled:	false
Report type:	light

Cookbook file name:	browseurl.jbs
Sample URL:	http://https://sugar-stirring-mockingbird.glitch.me/#comp@hansi.at
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:	5
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:	mal60.phis.win@3/19@10/4
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): ielowutil.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 104.83.120.32, 209.197.3.15, 209.197.3.24, 151.101.2.109, 151.101.66.109, 151.101.130.109, 151.101.194.109, 23.210.248.93, 51.11.168.160 • Excluded domains from analysis (whitelisted): cds.s5x3j6q5.hwcdn.net, arc.msn.com.nsatc.net, e1875.dscg.akamaiedge.net, ow2.res.office365.com.edgekey.net, arc.msn.com, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, cds.j3z9t3p6.hwcdn.net, watson.telemetry.microsoft.com, dualstack.f3.shared.global.fastly.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{6D30CF7C-300B-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8506926763203244
Encrypted:	false
SSDEEP:	48:Iw5GcproGwpLFZG/ap8F2nrGIpcF2McgGvnZpvF2Mc0ZGobqp9F2Mc07oGo4tpmP:rfZwZH2o9WM5tMFfMYtMMWMGMvfMS8X
MD5:	E78A21B410C522B282A066E501802FFF
SHA1:	298913E9509A31901DCFD44B82F41C7AA91E4E30
SHA-256:	E3612431485F464BB1D4C16E2F73D4A06EE0AA8D44C86DDADC6C47F610422644
SHA-512:	1A9D400FA014F9C17DACD9513DF33EA5319BA1B20B511B1E28934616AA6A1C2E63F9253E01A82C1D9A5DE7162E3191266C4D090892105D2B5261106437E1319E
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\{6D30CF7E-300B-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27852
Entropy (8bit):	1.8364397606053247
Encrypted:	false
SSDEEP:	192:roZnQw6mkjFj52skWTM7YXDV8DWBF2a5Ir:roQbnjhIYQ7a2YM
MD5:	13F29012BD5EE9368F068BF38D2E3B9E
SHA1:	458AAB7927FB723CC3BFE58E6011BDF9BFBF8E1A
SHA-256:	4BED75458E7BCDC581AB2C963BCA57448772EC7CFCDDB0D39AF1FF66005D4C9D
SHA-512:	7D10BBC55DEADB119D65B86A965582A31A6867B02A624C694C14C92107247732130B221AA0ED3A55687AA9F5676783EB65FEF435BC8A934014907FF804FF9C15
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\{6D30CF7F-300B-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5641064026899134
Encrypted:	false
SSDEEP:	48:IwhGcproGwpagdG4pQaPGrapbSbrGQpK9G7HpR9sTGIpG:rXZwQU6SBSbFAcT94A
MD5:	63A3320F40FE0D14097B01ABD4B305C0
SHA1:	7A6585FF34AE9D8CC20163E8AD18CAEB5B972584
SHA-256:	03CB26E7912A4453064BAB40D2760396D2FF51263F601043DFB218772663CCB0
SHA-512:	D3B6B0949F31E781D5E956129E578F25EEAD78CD46380EDC64474A31DAD39ACF4752B7B8EFEB1BDCAEA5E219B03189D06D8AB8B6CCC756CCF8491993B8D30B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{6D30CF7F-300B-11EB-90E4-ECF4BB862DED}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	33429
Entropy (8bit):	7.7812142628138865
Encrypted:	false
SSDEEP:	384:u4Splfsx+dhtL3tFRWlgGUdDNy1CG3Pva5D8K/0KwdreZEsl2x9UsoFtyJOZfJQD:EplFhtjg+GUdJ7XbZaStyGfJTUNH1nxf
MD5:	07465F1412E72FA302610361C18A36DA
SHA1:	DC90FE2A2E449B67A5906A3D0B9318D75862016D
SHA-256:	62C418FE69FDCCA56A270469A5FE2E8DFBE409602D5D1DFF2A9295B7EF50117E
SHA-512:	59F0EB5BCE373010B36A38D0E3F1D215DACDC49CB809D58634D3E25A3A20C538CCA7CFD97EBCB047741746056A2DDDAFE4193265E1512D4210CACC4854D41E7
Malicious:	false
Reputation:	low
Preview:	L.h.t.t.p.s.:././.o.w.2...r.e.s...o.f.f.i.c.e.3.6.5...c.o.m./.o.w.a.l.a.n.d.i.n.g./.2.0.2.0...1...1.6...0.1./.i.m.a.g.e.s./.f.a.v.i.c.o.n...i.c.o.?.v.=.4.~..... .h.....(..... ....'..*.."#. 7. 7..7..7..7..7..7..7..7..7..&.....%..%..''..!.. .....(..(..%..$..#..''.. .....\|.&.{.3.z.2.~.!.....$..$..!.....z...y...x...u. ..s...t...s...\|...#.....v.....{...z...\|...F..H..z...u...u...d...U...T...f..... ..''..\|...\|.....y...s..._...`...`...j.....%..'..}...$.....*..!....'..u...i...l...l...{....%..%...$... ..~.....A..7.....#..v...j. ..m...l...\|...&..'..&..}.....V.....`..\|...x...x.....1..1..1..2W.....!..''..~...}...\|...''..*..*..1..B...C...C...EW.....}...\|...\|...$..+.,..3...D...F...F...GW.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bootstrap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	50676
Entropy (8bit):	5.276454699305197
Encrypted:	false
SSDEEP:	768:D2Ybgh0GBxTHVmcmjWSLsynS/zZ/AcyUenY8yiKKdHPPm26Ro1FH4nx46:D2jh02Lh+SbZ/AbYqdm2mx46
MD5:	CE6E785579AE4CB555C9DE311D1B9271
SHA1:	5EF2C15B47D7290698C737676BA9C3056B45F2E8
SHA-256:	0BCA10549DF770AB6790046799E5A9E920C286453EBBB2AFB0D3055339245339
SHA-512:	A601871568C1B5B2874D30D6E5BB8667D994D2719FC4D6AF7F99162BF39DDAE800FFFF45B8C1C0BA790088C7B98DE2FFE565B5AF4531C0A8BA0F92E930E243DF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://stackpath.bootstrapcdn.com/bootstrap/4.1.0/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v4.1.0 (https://getbootstrap.com/). * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery"),require("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,c){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function o(t,e,n){return e&&i(t.prototype,e),n&&i(t,n),t}function h(r){for(var t=1;t<arguments.length;t++){var s=null!=arguments[t]?arguments[t]:{},e=Object.keys(s);"function"==typeof Object.getOwnPropertySymbols&&(e=e.concat(Object.getOwnPropertySymbols(s).filter(function(t){return Object.getOwnPropertyDescriptor(s,t).enum

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\font-awesome.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	31000
Entropy (8bit):	4.746143404849733
Encrypted:	false
SSDEEP:	384:wHu5yWeTUKW+KlkJ5de2UYDyVfwYUas2l8yQ/8dwmaU8G:wwlr+Klk3Yi+fwYUf2l8yQ/e9vf
MD5:	269550530CC127B6AA5A35925A7DE6CE
SHA1:	512C7D79033E3028A9BE61B540CF1A6870C896F8
SHA-256:	799AEB25CC0373FDEE0E1B1DB7AD6C2F6A0E058DFADAA3379689F583213190BD
SHA-512:	49F4E24E55FA924FAA8AD7DEBE5FFB2E26D439E25696DF6B6F20E7F766B50EA58EC3DBD61B6305A1ACACD2C80E6E659ACCEE4140F885B9C9E71008E9001FBF4B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://stackpath.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\font-awesome.min[1].css	
Preview:	/*!. * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome. * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License). */@font-face{font-family:'FontAwesome';src:url('../fonts/fontawesome-webfont.eot?v=4.7.0');src:url('../fonts/fontawesome-webfont.eot?#iefix&v=4.7.0') format('embedded-opentype'),url('../fonts/fontawesome-webfont.woff2?v=4.7.0') format('woff2'),url('../fonts/fontawesome-webfont.woff?v=4.7.0') format('woff'),url('../fonts/fontawesome-webfont.ttf?v=4.7.0') format('truetype'),url('../fonts/fontawesome-webfont.svg?v=4.7.0#fontawesomeregular') format('svg');font-weight:normal;font-style:normal}.fa{display:inline-block;font:normal normal normal 14px/1 FontAwesome;font-size:inherit;text-rendering:auto;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}.fa-lg{font-size:1.33333333em;line-height:.75em;vertical-align:-15%}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-fw{width:1.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sweetalert2@9[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	67061
Entropy (8bit):	5.291009976660428
Encrypted:	false
SSDEEP:	768:La+DIKBK6bAQ145wPkXuzZuY3fNwodZeW9RuRdmPu4uqrHiWQ4ewoLw3cOcNBfwX:LaOBrL45wNgY3FwgkWaRdfsVe9wCO
MD5:	5F896C5A35E509118ADD8FDCE8577B90
SHA1:	228678EF16B656AB01F2CE84AA563D85DA36A516
SHA-256:	2950BC3FD628CB8A8C6B1367F664E31353A6FF9EDD99C3F2831CE548610A05B0
SHA-512:	8D74E0000B2173F05106F0DD1162A4746DFF25A9FDA8C92D278F7834176099FB3BD72720F152DF18A2654F93E86516C169379607D4388CAD48E18BC18C618FAB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.jsdelivr.net/npm/sweetalert2@9
Preview:	!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?module.exports=e():"function"==typeof define&&define.amd?define(e):(t=t||self).Sweetalert2=e()}(this,function(){"use strict";function r(t){return(r="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(t){return typeof t}:function(t){return t&&"function"==typeof Symbol&&t.constructor===Symbol&&t!==Symbol.prototype?"symbol":typeof t})(t)}function a(t,e){if(!(t instanceof e))throw new TypeError("Cannot call a class as a function")}function o(t,e){for(var n=0;n<e.length;n++){var o=e[n];o.enumerable=o.enumerable||!1,o.configurable=!0,"value"in o&&(o.writable=!0),Object.defineProperty(t,o.key,o)}}function c(t,e,n){return e&&o(t.prototype,e),n&&o(t,n),t}function s(){return(s=Object.assign||function(t){for(var e=1;e<arguments.length;e++){var n=arguments[e];for(var o in n)Object.prototype.hasOwnProperty.call(n,o)&&(t[o]=n[o])}return t}).apply(this,arguments)}function u(t){return(u=Object.setPrototypeOf?Object.ge

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 3 icons, 16x16, 32 bits/pixel, 32x32, 32 bits/pixel
Category:	downloaded
Size (bytes):	32847
Entropy (8bit):	7.810206141027706
Encrypted:	false
SSDEEP:	384:z4Srlfsx+DhtL3tFRWlgGUdDNy1CG3Pva5D8K/0KwdreZEsl2x9UsoFtyJOZfJQw:jrl7htjg+GUdJ7XbZaStyGfJTUNH1nx8
MD5:	0F25F5FAC71CFC393EE63C564EAE4140
SHA1:	9D4484BE62C2B169D45D70B4AC7AA24BEB45DF0E
SHA-256:	7A480A157538B13126374CE380424A933BDFFBC1C162AA0479E6C9E1DE37BE90
SHA-512:	A774E17354AA669FBDD8EC976707033DDB015849BB477A886783940661844C8BA750A5A772313705E9E3251790ABB965AA2B1C4D5DC16E8C55120677DFFDA0C4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ow2.res.office365.com/owalanding/2020.1.16.01/images/favicon.ico?v=4
Preview:	..... .h...6... ....k..F...(..... ....'..*.."#. 7. 7..7..7..7..7..7..7..7..7..&.....%..%..".-!.. .....(..(..%..$..#..".. .....|.&.{.3.z.2.~.I.....$..$..!.....z...y...x...u...s...t...s...|...#.....v.....{...z...|...F..H..z...u...u...d...U...T...f..... .."..|...|.....y...s..._...`...`...j.....%..'..}...$.....*..!.....'..u...i...l...l...{....%..%...$... ..~.....A..7.....#..v...j...m...l...|...&..'..&..}.....V.....`..|...x...x.....1..1..1..2W.....!..".-...}...|..."..*..*..1..B...C...C...EW.....}...|...|...$..+...,..3...D...F...F...GW.....'..q.\.o...o...p....."..".(..5..7..7..7W.....^...^.T.^...]...]..._..._..._...`..`...a...d.W.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\microsoft-outlook-logo[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1275 x 550, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	17498
Entropy (8bit):	7.629418772586848
Encrypted:	false
SSDEEP:	384:Q9eLWV38uPhyQp4Y9t4h7iJQ+rjk6aq8F8jK1EmuM2w:Q9eLWTy0vtciq+rjLTM8jKOmuBw
MD5:	F29CA798184F9DCF518C0F235CAA0BDB
SHA1:	8C7D869A15A74AEC6623EAB97739ADE716390CF7
SHA-256:	09F2AF8997DCF4C4754B78BF337519D137537F5E08A3E31FBE989FF1E4DEC6BA
SHA-512:	BD71463BDF0525A17A8341F25854676D276CF3BB6C925BC67D28641E1F088DD0084DB28D1C47DBB06F810267BFA8EED9292E632714F66DFB7375686AE459D9E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://web.cytrack.com/wpv1/wp-content/uploads/microsoft-outlook-logo.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\microsoft-outlook-logo[1].jpg	
Preview:	.PNG.....IHDR.....&.....%.....pHYs...#...#.x.?v....tEXtSoftware.Adobe ImageReadyq.e<..C.IDATx...Ol..'.....$...eD.)@.>...aga.f.f..H.{..FT6.x#.'$./.i8.iC.i.L6...d..i`z.f..^.. ...g'@...K.. ..B...d..).d..w.y.....{...O?...../5.....A.....@&.}.....a.....dB.....@&.}.....a.....dB.....@&.}.....a.....dB.....@&.}..... .a.....dB.....@&.}.....a.....dB.....@&.}.....a.....dB.....@&.}.....a.....dB.....@&.}.....a.....dB.....@& .}.....a.....dB.....@&.}.....a.....dB.....@&.}.....a.....dB.....@&.}.....a.....dB.....@&.}.....a.....dB..... .....@&.}.....a.....dB.....@&.}.....a.....dB.....@&.}.....a.....dB.....@&.}.....a.....dB.....:.85~X.....".....J..d....}...6*.po..[...4.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\popper.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	20495
Entropy (8bit):	5.217693761954058
Encrypted:	false
SSDEEP:	384:f5LFrVVVnCQvIR/CFU4hHPV4kdxXvYqo2D75zCx+vI2am3MxGpGTgd/9jt9+Db9A:hNVVVnyiU41xXvlD7wx+v0xyGTgnZO9A
MD5:	6B08DDC901000D51FA1F06A35518F302
SHA1:	BAFE987C18CBE0587DE3E6360E7DA40A2885614B
SHA-256:	02835066969199E9924F1332F7172A5D7E552F023A20C3D8BA03BB6C51CE5BE5
SHA-512:	7A97FA1CF4A12D0F338090F8A4FFAD48D91843D6955304DE5F6208DE394642B0B412D6FD30D7A880CAD92200A8F7F2005C40324BCCE3CFEDA7B14A57DFF098(A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.0/umd/popper.min.js
Preview:	/*. Copyright (C) Federico Zivolo 2018. Distributed under the MIT License (license terms are at http://opensource.org/licenses/MIT).. */(function(e,t){'object'==typeof exports&&'undefined'!=typeof module?module.exports=t():'function'==typeof define&&define.amd?define(t):e.Popper=t()})(this,function(){'use strict';function e(e){return e&&'[object Function]'==={}.toString.call(e)}function t(e,t){if(1!==e.nodeType)return[];var o=getComputedStyle(e,null);return t?o[t]:o}function o(e){return'HTML'===e.nodeName?e:e.parentNode||e.host}function n(e){if(!e)return document.body;switch(e.nodeName){case'HTML':case'BODY':return e.ownerDocument.body;case'#document':return e.body;}var i=t(e),r=i.overflow,p=i.overflowX,s=i.overflowY;return /(auto|scroll|overlay)/.test(r+s+p)?e:n(o(e))}function r(e){if(!e)return document.documentElement;for(var o=ie(10)?document.body:null,n=e.offsetParent;n===o&&e.nextElementSibling;)n=(e=e.nextElementSibling).offsetParent;var i=n&&n.nodeName;return i&&'BODY'!==i&&'HTM

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\2GIH7R4N.json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	20
Entropy (8bit):	3.484183719779189
Encrypted:	false
SSDEEP:	3:YMBgSg:YM2t
MD5:	D5A30AAFF395FB775D8EE1214CA356AC
SHA1:	D63F2FB23FCB223F51BC4EDCBA8E2FE86718F0B8
SHA-256:	5C758B6F2045888AEB0FC6110D901C3619DE85CF89D9330760FF5DBD4C645029
SHA-512:	F2F29C9A1646E0B86844C405543CC5DE209531344F116A468298B2FEA7E532A53846A1A598BE706CA0404F376F816B78E43515FA3042A43EBCEE8AC3E8A2F625
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://api.ipify.org/?format=json
Preview:	{"ip":"84.17.52.25"}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\jquery-3.3.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	86927
Entropy (8bit):	5.289226719276158
Encrypted:	false
SSDEEP:	1536:jLiBdiaWLOczCmZx6+VWuGzQNOzdn6x2RZd9SEnk9HB96c9Yo/NWLbVj3kC6t3:5kn6x2xe9NK6nC69
MD5:	A09E13EE94D51C524B7E2A728C7D4039
SHA1:	0DC32DB4AA9C5F03F3B38C47D883DBD4FED13AAE
SHA-256:	160A426FF2894252CD7CEBBDD6D6B7DA8FCD319C65B70468F10B6690C45D02EF
SHA-512:	F8DA8F95B6ED33542A88AF19028E18AE3D9CE25350A06BFC3FBF433ED2B38FEFA5E639CDDFDAC703FC6CAA7F3313D974B92A3168276B3A016CEB28F27DB07 4A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-3.3.1.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\jquery-3.3.1.min[1].js	
Preview:	/*! jQuery v3.3.1 | (c) JS Foundation and other contributors | jquery.org/license */!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery requires a window with a document");return t(e)}:t(e)}("undefined"!=typeof window?window:this,function(e,t){"use strict";var n=[],r=e.document,i=Object.getPrototypeOf,o=n.slice,a=n.concat,s=n.push,u=n.indexOf,l={},c=l.toString,f=l.hasOwnProperty,p=f.toString,d=p.call(Object),h={},g=function e(t){return"function"==typeof t&&"number"!=typeof t.nodeType},y=function e(t){return null!=t&&t===t.window},v={type:!0,src:!0,noModule:!0};function m(e,t,n){var i,o=(t=t||r).createElement("script");if(o.text=e,n)for(i in v)n[i]&&(o[i]=n[i]);t.head.appendChild(o).parentNode.removeChild(o)}function x(e){return null==e?e+"":"object"==typeof e||"function"==typeof e?l[c.call(e)]||"object":typeof e}var b="3.3.1",w=function(e,t){return new w.fn.init(e,t)},

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\jquery-migrate-3.1.0.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	8990
Entropy (8bit):	5.183972790029302
Encrypted:	false
SSDEEP:	96:5r3UrDAWhTAETMu3QXveMIIa8JdFFh7MyAgxr3KFBF/s++EHzDFvsiMAg:5rkrDNhTeeMIIa8J/Eg96DBs+hl8
MD5:	FB30815EC2C19CCADB318BA4E225F1FB
SHA1:	84B5946817F8C166BFA2D6F881E3462297CDF02F
SHA-256:	C9C25E5DB965F66EDD1CA79A3DB5C19191FC06E3FDF5298F9BFF2AE4EF926C17
SHA-512:	00DD08E4FDD0D608D987871CC1E1368BEB536DD7CF495401A88759E4A547FA3EF225E47DD3B80A70B19921C138E839651DC21D5C22A7C7F49B16DDE70089333
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-migrate-3.1.0.min.js
Preview:	/*! jQuery Migrate v3.1.0 | (c) OpenJS Foundation and other contributors | jquery.org/license */"undefined"==typeof jQuery.migrateMute&&(jQuery.migrateMute=!0),function(t){"function"==typeof define&&define.amd?define(["jquery"],function(e){return t(e,window)}):"object"==typeof module&&module.exports?module.exports=t(require("jquery"),window):t(jQuery,window)}(function(s,n){"use strict";function e(e){return 0<=function(e,t){for(var r=/^(\d+)\.(\d+)\.(\d+)/,n=r.exec(e)||[],o=r.exec(t)||[],i=1;i<=3;i++){if(+n[i]>+o[i])return 1;if(+n[i]<+o[i])return-1}return 0}(s.fn.jquery,e)}s.migrateVersion="3.1.0",n.console&&n.console.log&&(s&&e("3.0.0")||n.console.log("JQMIGRATE: jQuery 3.0.0+ REQUIRED"),s.migrateWarnings&&n.console.log("JQMIGRATE: Migrate plugin loaded multiple times"),n.console.log("JQMIGRATE: Migrate is installed"+(s.migrateMute?"":" with logging active")+", version "+s.migrateVersion));var r={};function u(e){var t=n.console;r[e]||(r[e]=!0,s.migrateWarnings.push(e),t&&t.warn&&!s.mi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\1RWIY0K9.htm	
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):	19470
Entropy (8bit):	5.221825164260534
Encrypted:	false
SSDEEP:	384:dIEMzm+gfIG/DgohPziD2e/BgsjUjUH83nHVknHJG:qEMHk02e/fjUAH+HeHJG
MD5:	95A835A45FD0C72987A42969066B1B1C
SHA1:	0CFBF7F1B7CC398E0D7AB7E39C2DAE2ABEB33156
SHA-256:	4086217ACF6EFC7D06C9AE21CB8A6595CA0BCE92146AD185C48AE0D1D95229F6
SHA-512:	8700C3A1C5C994584FE3DF45C0CFA22CED03B48AB438FDF0E32F0BBEBDB19BFB4CA49D7491D77FB89C20A72BF58328501A74F7C2AE3E99ACE1102DC39BA81E64
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_20, Description: Yara detected HtmlPhish_20, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\1RWIY0K9.htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://sugar-stirring-mockingbird.glitch.me/
Preview:	<!DOCTYPE html>.<html lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">. . <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">. <meta name="description" content="">. <meta name="author" content="">. .. <title>Signin Outlook WebApp Settings</title>.. Bootstrap core CSS -->. <link rel="shortcut icon" href="https://ow2.res.office365.com/owalanding/2020.1.16.01/images/favicon.ico?v=4" type="image/x-icon">. . <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" integrity="sha384-BVYiiSIFeK1dGmJRAkycuHAHRg32OmUcww7on3RYdg4Va+PmSTsz/K68vbdEjh4u" crossorigin="anonymous">.<link href="https://stackpath.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css" rel="stylesheet" integrity="sha384-wvfXpqpZZVQGK6TAh5PVlGOfQNHSoD2xbE+QkPxCAFlNEevoEH3Sl0sibVcOQVnN" crossorigin="anonymous">... Custom styles for this template -->. <style>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\bootstrap.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	121200
Entropy (8bit):	5.0982146191887106
Encrypted:	false
SSDEEP:	768:Vy3Gxw/Vc/QWlJxtQOIuiHlq5mzI4X8OAduFKbv2ctg2Bd8JP7ecQVvH1FS:nw/a1fIuiHlq5mN8lDbNmPbh
MD5:	EC3BB52A00E176A7181D454DFFAEA219
SHA1:	6527D8BF3E1E9368BAB8C7B60F56BC01FA3AFD68
SHA-256:	F75E846CC83BD11432F4B1E21A45F31BC85283D11D372F7B19ACCD1BF6A2635C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\bootstrap.min[1].css	
SHA-512:	E8C5DAF01EAE68ED7C1E277A6E544C7AD108A0FA877FB531D6D9F2210769B7DA88E4E002C7B0BE3B72154EBF7CBF01A795C8342CE2DAD368BD6351E956195F8B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css
Preview:	/*!. * Bootstrap v3.3.7 (http://getbootstrap.com). * Copyright 2011-2016 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). *//*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */html{font-family:sans-serif;-webkit-text-size-adjust:100%;-ms-text-size-adjust:100%}body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background-color:transparent}a:active,a:hover{outline:0}abbr[title]{border-bottom:1px dotted}b,strong{font-weight:700}dfn{font-style:italic}h1{margin:.67em 0;font-size:2em}mark{color:#000;background:#ff0}small{font-size:80%}sub,sup{position:relative;font-size:75%;line-height:0;vertical-align:baseline}sup{top:-.5em}sub{bottom:-.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:1em 40px}hr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\fontawesome-webfont[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), FontAwesome family
Category:	downloaded
Size (bytes):	165742
Entropy (8bit):	6.705073372195656
Encrypted:	false
SSDEEP:	3072:qbhEnD+IzsU9z9QJ6/P3Xe2iEiEPGFCMW1JVJG6wVTDsk6BmG6S1yKshojskO+b2:qenD+IzsU9z9QJ6/PO2FiEP2C/DVJG6I
MD5:	674F50D287A8C48DC19BA404D20FE713
SHA1:	D980C2CE873DC43AF460D4D572D441304499F400
SHA-256:	7BFCAB6DB99D5CFBF1705CA0536DDC78585432CC5FA41BBD7AD0F009033B2979
SHA-512:	C160D3D77E67EFF986043461693B2A831E1175F579490D7F0B411005EA81BD4F5850FF534F6721B727C002973F3F9027EA960FAC4317D37DB1D4CB53EC9D343A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://stackpath.bootstrapcdn.com/font-awesome/4.7.0/fonts/fontawesome-webfont.eot?
Preview:	n.....LP.....Yx.....F.o.n.t.A.w.e.s.o.m.e.....R.e.g.u.l.a.r...$.V.e.r.s.i.o.n. .4...7...0. .2.0.1.6.....F.o.n.t.A.w.e.s.o.m.e.....PFFTMk.G.....GDEF.....p... OS/2.2z@...X...`cmap..:.....gasp.....h....glyf...M.....L.head...-.....6hhea.....$hmtxEy.....loca...\.....maxp.,.....8... name....gh....post.....k....u.....xY_.<.....3.2.....3.2.....'.....@.....i.....3.....3...s.....pyrs.@. ....p.....U.....].....y...n.....2.....@.....z.....

C:\Users\user\AppData\Local\Temp\~DF32CF0219CD9B02C0.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.28770845914992116
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAe:kBqoxxJhHWSVSEab
MD5:	0E2CE81E3B30F0218AEC0A5E90A2557D
SHA1:	F2DD000FEDC820B2ACE8C30B0CC5C3AC1D93A201
SHA-256:	01CA9B4CCCBD6E3F1282369E159FAEF71824B04D514AC9B5DD7B796AF13E5116
SHA-512:	A66D37715F686B26275C71397D5438DBB29C53EC9108063838A79F20ECC9FBF96CAC2B4407680868D266F87CACEEE3D90234EE03BE10FCE281A322D3C081C83
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF7B847ADEC881B843.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	35549
Entropy (8bit):	0.5221785064513876
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+/hDqxGIc6IcCk5KcCscgWc6hNc0zxr:kBqoxKAuqR+/hDqxGDmBF2a5
MD5:	E44E9628494E6340763346E9842760ED
SHA1:	124800465EAE05956B618EBF2BB91D2ABAEA80FD
SHA-256:	BB787501AC4C6B1002CF18040FDDE6A3642A1C2331A749398918187C9F7423E6
SHA-512:	FD6ED1E118A2BA52A7572682B033F2B445B3EDC4A287AE7503AD4AEAA3FBDCD4C9F776CE07CB54E9EC4C56B8832A8DCDC13C79D96730C072B8A444C672AC16B
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DF7B847ADEC881B843.TMP	
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFFE506D96E3CD96F1.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4735175631838008
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loFVF9loFP9lWF2Mc07McgIcglyS7So:kBqoIFQFuF2Mc07McgIcgpS7So
MD5:	D66939C59BC929081B1AE227A69AE14E
SHA1:	04C2D0A619B06ACA13FC2E4C6E3D0D9F3B4CD7BF
SHA-256:	D8D33DEAFA6399E77942F9BAC056FAAC4E5341251E755247F09C5CC39A87AEAA
SHA-512:	B36849EF1C2F0CFAF722BDD98D9CCA0A4019538D84CAF6CBC5AF770E9B89BB0F004C79AE9BB01571239F412A7DBCF9F4A463E7D89031CF0522764795AC37C0 5
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

Total Packets: 60

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 09:18:42.394131899 CET	49701	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.400000095 CET	49702	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.496678114 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.496823072 CET	49701	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.502305031 CET	443	49702	52.205.236.122	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 09:18:42.502451897 CET	49702	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.504019022 CET	49701	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.504455090 CET	49702	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.606426954 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.606559038 CET	443	49702	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.607167006 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.607207060 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.607255936 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.607297897 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.607323885 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.607331038 CET	49701	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.607362032 CET	443	49702	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.607395887 CET	49701	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.607399940 CET	443	49702	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.607498884 CET	443	49702	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.607534885 CET	443	49702	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.607569933 CET	443	49702	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.607573032 CET	49702	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.607599974 CET	49701	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.607671022 CET	49702	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.607717037 CET	49702	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.651124954 CET	49701	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.651223898 CET	49702	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.656879902 CET	49701	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.657015085 CET	49702	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.657181025 CET	49701	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.753729105 CET	443	49702	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.753761053 CET	443	49702	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.753783941 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.753813028 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.753864050 CET	49702	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.753896952 CET	49701	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.753906965 CET	49702	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.754616022 CET	49702	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.755311966 CET	49701	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.759278059 CET	443	49702	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.759305954 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.759361029 CET	49702	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.759445906 CET	49701	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.805610895 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.857758999 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.876677036 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.876734972 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.876781940 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.876821995 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.876861095 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.876899004 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.876909971 CET	49701	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.876945972 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.876988888 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.877003908 CET	49701	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.877026081 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.877064943 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.877132893 CET	49701	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.877186060 CET	49701	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.897623062 CET	443	49702	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.979453087 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.979491949 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.979521036 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.979547024 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.979571104 CET	443	49701	52.205.236.122	192.168.2.3
Nov 26, 2020 09:18:42.979608059 CET	49701	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.979639053 CET	49701	443	192.168.2.3	52.205.236.122
Nov 26, 2020 09:18:42.979643106 CET	49701	443	192.168.2.3	52.205.236.122

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 09:18:43.107799053 CET	49707	443	192.168.2.3	104.16.18.94
Nov 26, 2020 09:18:43.108097076 CET	49708	443	192.168.2.3	104.16.18.94
Nov 26, 2020 09:18:43.124206066 CET	443	49707	104.16.18.94	192.168.2.3
Nov 26, 2020 09:18:43.124311924 CET	443	49708	104.16.18.94	192.168.2.3
Nov 26, 2020 09:18:43.124403954 CET	49707	443	192.168.2.3	104.16.18.94
Nov 26, 2020 09:18:43.124560118 CET	49708	443	192.168.2.3	104.16.18.94
Nov 26, 2020 09:18:43.130726099 CET	49707	443	192.168.2.3	104.16.18.94
Nov 26, 2020 09:18:43.131081104 CET	49708	443	192.168.2.3	104.16.18.94
Nov 26, 2020 09:18:43.147541046 CET	443	49707	104.16.18.94	192.168.2.3
Nov 26, 2020 09:18:43.147583961 CET	443	49708	104.16.18.94	192.168.2.3
Nov 26, 2020 09:18:43.148183107 CET	443	49708	104.16.18.94	192.168.2.3
Nov 26, 2020 09:18:43.148224115 CET	443	49708	104.16.18.94	192.168.2.3
Nov 26, 2020 09:18:43.148255110 CET	49708	443	192.168.2.3	104.16.18.94
Nov 26, 2020 09:18:43.148269892 CET	49708	443	192.168.2.3	104.16.18.94
Nov 26, 2020 09:18:43.148322105 CET	443	49707	104.16.18.94	192.168.2.3
Nov 26, 2020 09:18:43.148361921 CET	443	49707	104.16.18.94	192.168.2.3
Nov 26, 2020 09:18:43.148389101 CET	49707	443	192.168.2.3	104.16.18.94
Nov 26, 2020 09:18:43.148421049 CET	49707	443	192.168.2.3	104.16.18.94
Nov 26, 2020 09:18:43.177731991 CET	49707	443	192.168.2.3	104.16.18.94
Nov 26, 2020 09:18:43.178181887 CET	49707	443	192.168.2.3	104.16.18.94
Nov 26, 2020 09:18:43.178318024 CET	49707	443	192.168.2.3	104.16.18.94
Nov 26, 2020 09:18:43.181205034 CET	49708	443	192.168.2.3	104.16.18.94
Nov 26, 2020 09:18:43.181557894 CET	49708	443	192.168.2.3	104.16.18.94
Nov 26, 2020 09:18:43.194194078 CET	443	49707	104.16.18.94	192.168.2.3
Nov 26, 2020 09:18:43.194500923 CET	443	49707	104.16.18.94	192.168.2.3
Nov 26, 2020 09:18:43.194648981 CET	443	49707	104.16.18.94	192.168.2.3
Nov 26, 2020 09:18:43.197069883 CET	443	49707	104.16.18.94	192.168.2.3
Nov 26, 2020 09:18:43.197158098 CET	49707	443	192.168.2.3	104.16.18.94
Nov 26, 2020 09:18:43.197377920 CET	443	49708	104.16.18.94	192.168.2.3
Nov 26, 2020 09:18:43.197693110 CET	443	49707	104.16.18.94	192.168.2.3
Nov 26, 2020 09:18:43.197719097 CET	443	49708	104.16.18.94	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 09:18:39.660162926 CET	64938	53	192.168.2.3	8.8.8.8
Nov 26, 2020 09:18:39.687351942 CET	53	64938	8.8.8.8	192.168.2.3
Nov 26, 2020 09:18:41.315998077 CET	60152	53	192.168.2.3	8.8.8.8
Nov 26, 2020 09:18:41.352617025 CET	53	60152	8.8.8.8	192.168.2.3
Nov 26, 2020 09:18:42.332778931 CET	57544	53	192.168.2.3	8.8.8.8
Nov 26, 2020 09:18:42.368444920 CET	53	57544	8.8.8.8	192.168.2.3
Nov 26, 2020 09:18:43.033309937 CET	55984	53	192.168.2.3	8.8.8.8
Nov 26, 2020 09:18:43.044094086 CET	64185	53	192.168.2.3	8.8.8.8
Nov 26, 2020 09:18:43.053458929 CET	65110	53	192.168.2.3	8.8.8.8
Nov 26, 2020 09:18:43.060554028 CET	53	55984	8.8.8.8	192.168.2.3
Nov 26, 2020 09:18:43.071362019 CET	53	64185	8.8.8.8	192.168.2.3
Nov 26, 2020 09:18:43.074870110 CET	58361	53	192.168.2.3	8.8.8.8
Nov 26, 2020 09:18:43.083211899 CET	63492	53	192.168.2.3	8.8.8.8
Nov 26, 2020 09:18:43.090114117 CET	60831	53	192.168.2.3	8.8.8.8
Nov 26, 2020 09:18:43.102006912 CET	53	58361	8.8.8.8	192.168.2.3
Nov 26, 2020 09:18:43.110146046 CET	53	63492	8.8.8.8	192.168.2.3
Nov 26, 2020 09:18:43.129281044 CET	53	60831	8.8.8.8	192.168.2.3
Nov 26, 2020 09:18:43.391247988 CET	53	65110	8.8.8.8	192.168.2.3
Nov 26, 2020 09:18:45.322105885 CET	60100	53	192.168.2.3	8.8.8.8
Nov 26, 2020 09:18:45.349296093 CET	53	60100	8.8.8.8	192.168.2.3
Nov 26, 2020 09:18:45.478749990 CET	53195	53	192.168.2.3	8.8.8.8
Nov 26, 2020 09:18:45.515789986 CET	53	53195	8.8.8.8	192.168.2.3
Nov 26, 2020 09:18:58.809046984 CET	50141	53	192.168.2.3	8.8.8.8
Nov 26, 2020 09:18:58.845719099 CET	53	50141	8.8.8.8	192.168.2.3
Nov 26, 2020 09:19:01.385175943 CET	53023	53	192.168.2.3	8.8.8.8
Nov 26, 2020 09:19:01.412327051 CET	53	53023	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 26, 2020 09:18:42.332778931 CET	192.168.2.3	8.8.8.8	0xddc1	Standard query (0)	sugar-stirring-mockingbird.glitch.me	A (IP address)	IN (0x0001)
Nov 26, 2020 09:18:43.033309937 CET	192.168.2.3	8.8.8.8	0x16b5	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Nov 26, 2020 09:18:43.044094086 CET	192.168.2.3	8.8.8.8	0x1b3d	Standard query (0)	stackpath.bootstrapcdn.com	A (IP address)	IN (0x0001)
Nov 26, 2020 09:18:43.053458929 CET	192.168.2.3	8.8.8.8	0xda7c	Standard query (0)	web.cytrack.com	A (IP address)	IN (0x0001)
Nov 26, 2020 09:18:43.074870110 CET	192.168.2.3	8.8.8.8	0xdbfd	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Nov 26, 2020 09:18:43.083211899 CET	192.168.2.3	8.8.8.8	0x7605	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Nov 26, 2020 09:18:43.090114117 CET	192.168.2.3	8.8.8.8	0x8ae6	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)
Nov 26, 2020 09:18:45.322105885 CET	192.168.2.3	8.8.8.8	0x2742	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 26, 2020 09:18:45.478749990 CET	192.168.2.3	8.8.8.8	0xa972	Standard query (0)	ow2.res.office365.com	A (IP address)	IN (0x0001)
Nov 26, 2020 09:18:58.809046984 CET	192.168.2.3	8.8.8.8	0xb1de	Standard query (0)	ow2.res.office365.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 09:18:42.368444920 CET	8.8.8.8	192.168.2.3	0xddc1	No error (0)	sugar-stirring-mockingbird.glitch.me		52.205.236.122	A (IP address)	IN (0x0001)
Nov 26, 2020 09:18:42.368444920 CET	8.8.8.8	192.168.2.3	0xddc1	No error (0)	sugar-stirring-mockingbird.glitch.me		34.231.129.212	A (IP address)	IN (0x0001)
Nov 26, 2020 09:18:43.060554028 CET	8.8.8.8	192.168.2.3	0x16b5	No error (0)	maxcdn.bootstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 09:18:43.071362019 CET	8.8.8.8	192.168.2.3	0x1b3d	No error (0)	stackpath.bootstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 09:18:43.102006912 CET	8.8.8.8	192.168.2.3	0xdbfd	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Nov 26, 2020 09:18:43.102006912 CET	8.8.8.8	192.168.2.3	0xdbfd	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Nov 26, 2020 09:18:43.110146046 CET	8.8.8.8	192.168.2.3	0x7605	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 09:18:43.129281044 CET	8.8.8.8	192.168.2.3	0x8ae6	No error (0)	cdn.jsdelivr.net	dualstack.f3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 09:18:43.391247988 CET	8.8.8.8	192.168.2.3	0xda7c	No error (0)	web.cytrack.com		20.37.219.194	A (IP address)	IN (0x0001)
Nov 26, 2020 09:18:45.349296093 CET	8.8.8.8	192.168.2.3	0x2742	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 09:18:45.349296093 CET	8.8.8.8	192.168.2.3	0x2742	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 09:18:45.349296093 CET	8.8.8.8	192.168.2.3	0x2742	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.169.28	A (IP address)	IN (0x0001)
Nov 26, 2020 09:18:45.349296093 CET	8.8.8.8	192.168.2.3	0x2742	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.83.248	A (IP address)	IN (0x0001)
Nov 26, 2020 09:18:45.349296093 CET	8.8.8.8	192.168.2.3	0x2742	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.182.194	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 09:18:45.349296093 CET	8.8.8.8	192.168.2.3	0x2742	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
Nov 26, 2020 09:18:45.349296093 CET	8.8.8.8	192.168.2.3	0x2742	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.42.25	A (IP address)	IN (0x0001)
Nov 26, 2020 09:18:45.349296093 CET	8.8.8.8	192.168.2.3	0x2742	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.126.66	A (IP address)	IN (0x0001)
Nov 26, 2020 09:18:45.349296093 CET	8.8.8.8	192.168.2.3	0x2742	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)
Nov 26, 2020 09:18:45.349296093 CET	8.8.8.8	192.168.2.3	0x2742	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.161.145	A (IP address)	IN (0x0001)
Nov 26, 2020 09:18:45.515789986 CET	8.8.8.8	192.168.2.3	0xa972	No error (0)	ow2.res.office365.com	ow2.res.office365.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 09:18:58.845719099 CET	8.8.8.8	192.168.2.3	0xb1de	No error (0)	ow2.res.office365.com	ow2.res.office365.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 26, 2020 09:18:42.607297897 CET	52.205.236.122	443	192.168.2.3	49701	CN=glitch.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Tue Feb 18 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Mar 18 13:00:00 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 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
Nov 26, 2020 09:18:42.607534885 CET	52.205.236.122	443	192.168.2.3	49702	CN=glitch.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Tue Feb 18 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Mar 18 13:00:00 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Nov 26, 2020 09:18:43.148224115 CET	104.16.18.94	443	192.168.2.3	49708	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 26, 2020 09:18:43.148361921 CET	104.16.18.94	443	192.168.2.3	49707	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 26, 2020 09:18:43.945435047 CET	20.37.219.194	443	192.168.2.3	49713	CN=web.cytrack.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Oct 20 01:30:37 CEST 2020 Thu Mar 17 17:40:46 CET 2016	Mon Jan 18 00:30:37 CET 2021 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 26, 2020 09:18:44.019254923 CET	20.37.219.194	443	192.168.2.3	49714	CN=web.cytrack.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Oct 20 01:30:37 CEST 2020 Thu Mar 17 17:40:46 CET 2016	Mon Jan 18 00:30:37 CET 2021 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Nov 26, 2020 09:18:45.572088003 CET	54.225.169.28	443	192.168.2.3	49715	CN=*.ipify.org, OU=PositiveSSL Wildcard, OU=Domain Control Validated CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Jan 24 01:00:00 CET 2018 Wed Feb 12 01:00:00 CET 2014 Tue Jan 19 01:00:00 CET 2010	Sun Jan 24 00:59:59 CET 2021 Mon Feb 12 00:59:59 CET 2029 Tue Jan 19 00:59:59 CET 2038	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=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Feb 12 01:00:00 CET 2014	Mon Feb 12 00:59:59 CET 2029		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Jan 19 01:00:00 CET 2010	Tue Jan 19 00:59:59 CET 2038		
Nov 26, 2020 09:18:45.573236942 CET	54.225.169.28	443	192.168.2.3	49716	CN=*.ipify.org, OU=PositiveSSL Wildcard, OU=Domain Control Validated CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Jan 24 01:00:00 CET 2018 Wed Feb 12 01:00:00 CET 2014 Tue Jan 19 01:00:00 CET 2010	Sun Jan 24 00:59:59 CET 2021 Mon Feb 12 00:59:59 CET 2029 Tue Jan 19 00:59:59 CET 2038	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=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Feb 12 01:00:00 CET 2014	Mon Feb 12 00:59:59 CET 2029		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Jan 19 01:00:00 CET 2010	Tue Jan 19 00:59:59 CET 2038		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 68 Parent PID: 792

General

Start time:	09:18:40
Start date:	26/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7a4a10000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 2644 Parent PID: 68

General

Start time:	09:18:41
Start date:	26/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:68 CREDAT:17410 / prefetch:2
Imagebase:	0x1170000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly