ID: 339270
Cookbook: browseurl.jbs
Time: 19:23:36
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

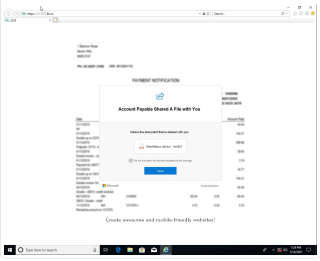
Analysis Report https://217023.8b.io/

Overview

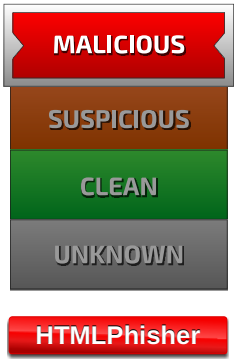
General Information

Sample URL:	http://https://217023.8b.io/
Analysis ID:	339270

Most interesting Screenshot:



Detection

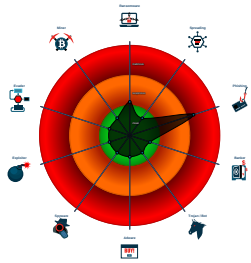


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Yara detected HtmlPhish_10
- HTML body contains low number of …
- HTML title does not match URL
- Suspicious form URL found

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5936 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4744 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5936 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

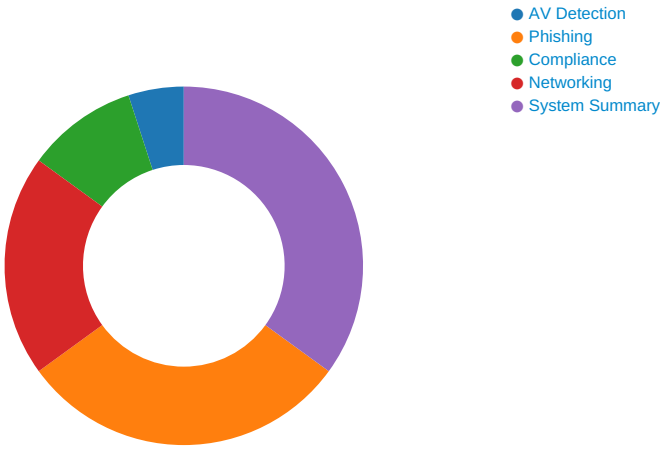
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\mfile[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

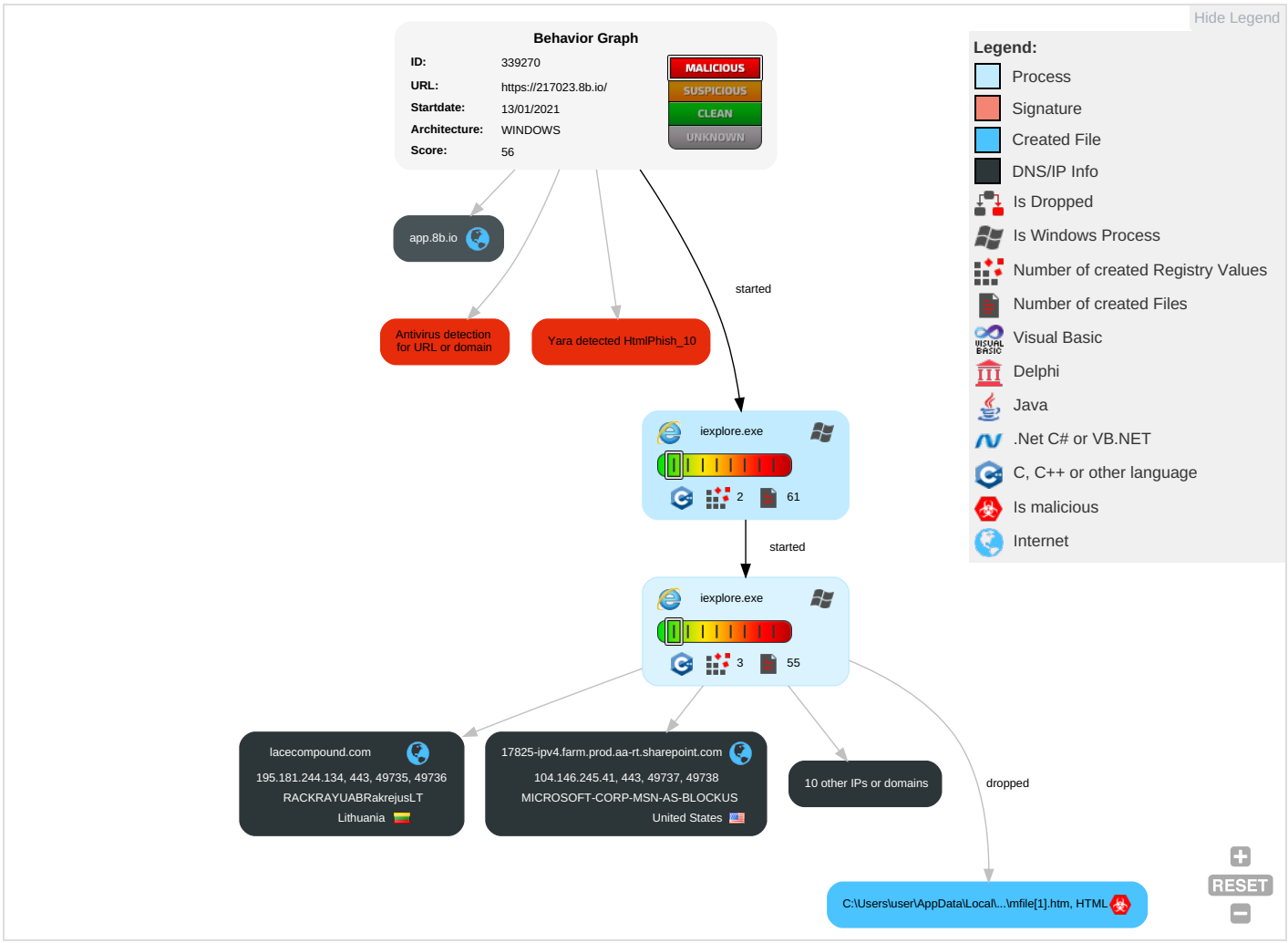
Phishing:

Yara detected HtmlPhish_10

Mitre Att&ck Matrix

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

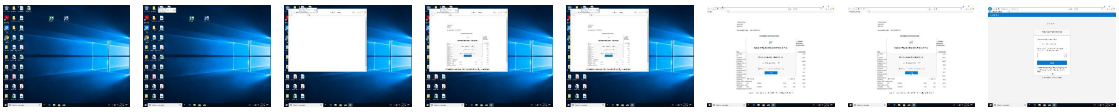
Behavior Graph

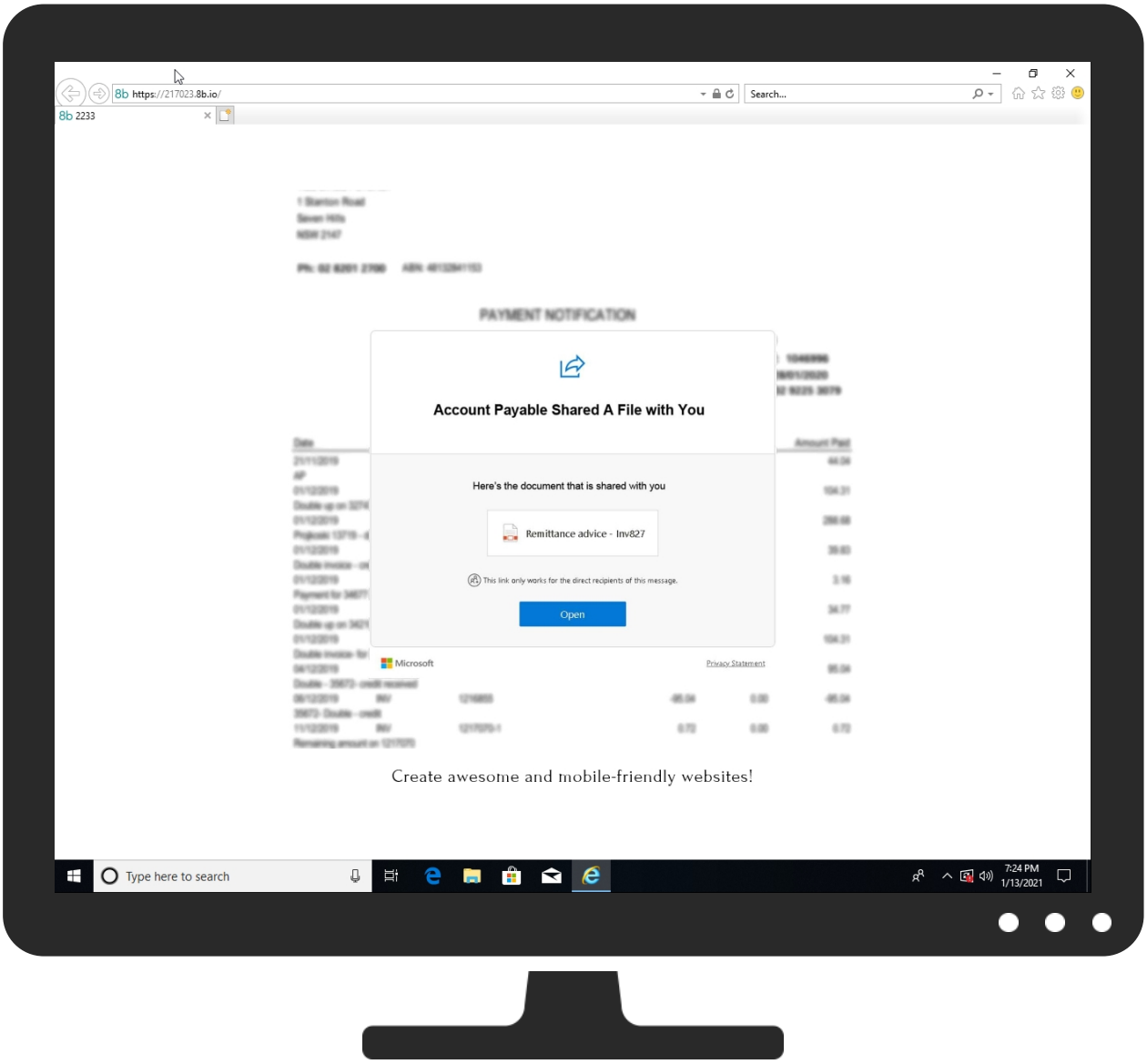


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://217023.8b.io/	0%	Virustotal		Browse
http://https://217023.8b.io/	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
app.8b.io	0%	Virustotal		Browse
lacecompound.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
http://https://lacecompound.com/sm/mfile/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://lacecompound.com/sm/mfile/.Sharing	0%	Avira URL Cloud	safe	
http://https://lacecompound.com/sm/mfile	0%	Avira URL Cloud	safe	
http://https://r.8b.io/217023/images/background5-h_kjukqdlq.jpg	0%	Avira URL Cloud	safe	
http://https://lacecompound.com/sm/mfile/L	0%	Avira URL Cloud	safe	
http://https://log.amp.dev/?v=012012301722001&id=	0%	Avira URL Cloud	safe	
http://https://app.8b.io/app/themes/webamp/projects/writer/assets/images/logo1.png	0%	Avira URL Cloud	safe	
http://https://mths.be/cssescape	0%	Avira URL Cloud	safe	
http://https://us-central1-amp-error-reporting.cloudfunctions.net/r	0%	Avira URL Cloud	safe	
http://https://8b.com	0%	Avira URL Cloud	safe	
http://https://lacecompound.com/sm/mfile/Root	0%	Avira URL Cloud	safe	
http://https://amp.dev/documentation/guides-and-tutorials/develop/style_and_layout/control_layout	0%	Avira URL Cloud	safe	
http://https://vikinggenetics-my.sharepoint.com/personal/datho_vikinggenetics_com_au/_layouts/15/images/pdf	0%	Avira URL Cloud	safe	
http://https://lacecompound.c	0%	Avira URL Cloud	safe	
http://https://217023.8b.io/Root	0%	Avira URL Cloud	safe	
http://https://us-central1-amp-error-reporting.cloudfunctions.net/r-beta	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
app.8b.io	104.24.104.39	true	false	• 0%, Virustotal, Browse	unknown
lacecompound.com	195.181.244.134	true	false	• 0%, Virustotal, Browse	unknown
r.8b.io	104.24.104.39	true	false		unknown
proxy-8b-io-1762796164.us-east-1.elb.amazonaws.com	52.201.120.251	true	false		high
cdn-content.ampproject.org	108.177.119.132	true	false		high
17825-ipv4.farm.prod.aa-rt.sharepoint.com	104.146.245.41	true	false		unknown
vikinggenetics-my.sharepoint.com	unknown	unknown	false		unknown
cdn.ampproject.org	unknown	unknown	false		high
217023.8b.io	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://lacecompound.com/sm/mfile/	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://217023.8b.io/	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://lacecompound.com/sm/mfile/.Sharing	~DFE679E51CD7555755.TMP.2.dr	true	• Avira URL Cloud: safe	unknown
http://https://lacecompound.com/sm/mfile	03OIYGP2.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://3p.ampproject.net	amp-mustache-0.2[1].js.3.dr, amp-analytics-0.1[1].js.3.dr, v0[1].js.3.dr	false		high
http://https://cdn.ampproject.org/v0/amp-analytics-0.1.js	03OIYGP2.htm.3.dr	false		high
http://https://r.8b.io/217023/images/background5-h_kjukqdlq.jpg	03OIYGP2.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/ampproject/amphtml/blob/master/spec/amp-iframe-origin-policy.md	amp-analytics-0.1[1].js.3.dr	false		high
http://https://cdn.ampproject.org/v0.js	03OIYGP2.htm.3.dr	false		high
http://https://lacecompound.com/sm/mfile/L	~DFE679E51CD7555755.TMP.2.dr	true	• Avira URL Cloud: safe	unknown
http://https://cdn.ampproject.org	amp-mustache-0.2[1].js.3.dr, amp-analytics-0.1[1].js.3.dr, v0[1].js.3.dr	false		high
http://https://log.amp.dev/?v=012012301722001&id=	v0[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://app.8b.io/app/themes/webamp/projects/writer/assets/images/logo1.png	imagestore.dat.3.dr, 03OIYGP2.htm.3.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://mths.be/cssescape	amp-intersection-observer-polyfill-0.1[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://lacecompound.com/sm/mfile/	~DFE679E51CD7555755.TMP.2.dr, mfile[1].htm.3.dr	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://us-central1-amp-error-reporting.cloudfunctions.net/r	amp-mustache-0.2[1].js.3.dr, amp-analytics-0.1[1].js.3.dr, v0[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://8b.com	03OIYGP2.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://lacecompound.com/sm/mfile/Root	{FDCDEC83-5617-11EB-90E4-ECF4BB862DED}.dat.2.dr	true	• Avira URL Cloud: safe	unknown
http://https://amp.dev/documentation/guides-and-tutorials/develop/style_and_layout/control_layout	v0[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://vikinggenetics-my.sharepoint.com/personal/datho_vikinggenetics_com_au/_layouts/15/images/pdf	mfile[1].htm0.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://lacecompound.c	{FDCDEC83-5617-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://github.com/janl/mustache.js	amp-mustache-0.2[1].js.3.dr	false		high
http://https://217023.8b.io/	~DFE679E51CD7555755.TMP.2.dr, 03OIYGP2.htm.3.dr	false		unknown
http://https://spoprod-a.akamaihd.net	mfile[1].htm0.3.dr	false		high
http://https://217023.8b.io/Root	{FDCDEC83-5617-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.ampproject.org/v0/amp-mustache-0.2.js	03OIYGP2.htm.3.dr	false		high
http://https://us-central1-amp-error-reporting.cloudfunctions.net/r-beta	amp-mustache-0.2[1].js.3.dr, amp-analytics-0.1[1].js.3.dr, v0[1].js.3.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.177.119.132	unknown	United States		15169	GOOGLEUS	false
104.146.245.41	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
195.181.244.134	unknown	Lithuania		62282	RACKRAYUABRakrejusLT	false
52.201.120.251	unknown	United States		14618	AMAZON-AESUS	false
104.24.104.39	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339270
Start date:	13.01.2021
Start time:	19:23:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://217023.8b.io/
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:	8
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.phis.win@3/24@7/5
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://lacecompound.com/sm/mfile
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 40.88.32.150, 88.221.62.148, 108.177.126.95, 172.217.18.99, 51.104.144.132, 152.199.19.161 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, fonts.googleapis.com, arc.msn.com.nsatc.net, fonts.gstatic.com, ie9comview.vo.msecnd.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus15.cloudapp.net, skypedataprdcoleus17.cloudapp.net, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, watson.telemetry.microsoft.com, 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\ABBRNDE4\217023.8b[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Reputation:	low
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{FDCDEC81-5617-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8574615924401467
Encrypted:	false
SSDEEP:	192:ryfZM6Z5L2J9WICtI8FfIrLSAMd66o6EilXfgL/wX:ryBMm5CJUI6IElGdo0tJ
MD5:	E1483F92CBD19F9CC2777AE7E5FE1798
SHA1:	90AED2F22ACCAB5EB2C03D3E22FDBFEA95D343C6
SHA-256:	C0A5B0091BC5004DAB98CCACFC46298E33FB7A0360D54A9623946AC516F1CACA
SHA-512:	7812494341EF922E3E010FEAB6D96D7BF48C2BC45AF5EC20986620E89F77F9BA93DBF755716288016148C1FA267550C45EBA48AAF8C63C7A4BAE9F0C9955E1B4
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\{FDCDEC83-5617-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	39846
Entropy (8bit):	2.1427299689112695
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{FDCDEC83-5617-11EB-90E4-ECF4BB862DED}.dat	
SSDEEP:	192:rvZ0QM6ak4FjZ2ckWcMYYUcoKSBF7sSQ3XQmt/ZuhOJtX:rR9Xz4hoIZYVNtBp/8XQmD9T
MD5:	3C4FC29ABB91412C377B142AC59717BE
SHA1:	724340377CEC44469EBBDCCC1226CFECC1D68952
SHA-256:	BFF41ECE984219C1B9783F4327048E9F3EDAB841D2D842A2DC83CD6CDF5A0C11
SHA-512:	0F0A5F434E92FCA74E1E4491F9A574FF6EABC2764AA0A1097DF9A638027134B083F20BF55937783A21B9420DE1FA5B943824B0D13246190FE595E3BD6D22D0A1
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\{FDCDEC84-5617-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5664794169532632
Encrypted:	false
SSDEEP:	48:IwFGcprMGwpaNG4pQd7GrapbSgjrGQpKe3G7HpRsxsTGIpG:rbZkQv6dvBSoFAhTsx4A
MD5:	14C4560B0360F6517B849356394616D6
SHA1:	9C3E28690213B6B44EFA8C4CA0420F9B0F9EE043
SHA-256:	9C1C8ADC93FDD5A5830853D9B49808DC3A69C4F1C92369A24295CEF8B40EE7B3
SHA-512:	611191CE0F34B2C5808A639E2A7A04292F485C74ABC3486C38435028326B84FEC10AACA02FE259E8CC11ABFF399810BF3E20FB96FA817A4211CD883067C78DC
Malicious:	false
Reputation:	low
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):	1988
Entropy (8bit):	7.504810719771759
Encrypted:	false
SSDEEP:	48:Q5Vv64FrnMpqLQ8Ai8eL6mSRHIFcJlNK28vgNEPD:MA8LMpqaiRL6fIFcb6BPD
MD5:	1B1E2BE5F03705BAC9041461A5BCCA1C
SHA1:	D5E62F27049F8DB43055C6ECC03FEB0A97591909
SHA-256:	B9A393A64D636E247FD2F6BCE55C45845B4DA5C31FD90581F41BEE24F708433B
SHA-512:	0A5FBC739FCEAE616C923356CCFFCB3E3DEB86BC9A83E2E8F847E9F063C131084FDCBA6CCF9787065E1F8AD3E3B2C7453807BB82F613AA0118E833E9D19A90BB
Malicious:	false
Reputation:	low
Preview:	K.h.t.t.p.s.:././.a.p.p...8.b...i.o./.a.p.p./.t.h.e.m.e.s./.w.e.b.a.m.p./.p.r.o.j.e.c.t.s./.w.r.i.t.e.r./.a.s.s.e.t.s./.i.m.a.g.e.s./.l.o.g.o.1...p.n.g.....PNG.....IHDR.....PLTE.....tRNS.+:...R..5.$.gy.B...K].....o....b..1.F..~e>1....IDATx..i..0....<PqA...kw.....B2...>._....IH&.....7?p..p..;c.<.`.z....q.@kv.. 2.^...z.....O.:m...9>....".z...&.....l...k.R..|.....t(...1..E.ZWg3./fR.W..X.....3.#.,;.Z.....b.....TL..9.c-.'.h.b../.k-\..Q..j..\1...w.u..(.....j..'...h._;.q....#.t...V.6Fo...F..w}j.#.y..O.._=...Z...y{J.....B..i...@.x.V.q.....;L...bJp.".k.....c[.AO.*+..eZD-.(..iH.o.wA..V0.fv..j...j...5n.....2.xT?..3>....6E+../....k...O....m..i...n. .JKi.:.,....36...[....y.....);6n.....uS..k.....p...0...)....HeY.{.d...&...Y.....VXK..x...h.2....@.`.-L2.. ..D...J..t..4.&.N..;.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\amp-analytics-0.1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	98815
Entropy (8bit):	5.426219391512523
Encrypted:	false
SSDEEP:	1536:dCnsjVr6tmjE93elQIB+A1kfYGh8wPBDOKa:dd4u3B++oOwPBDOH
MD5:	3C7A16E30FEF30EFB221DDD3944B7F21
SHA1:	A458DBE35B4261C967EEA284B5D174335A001619
SHA-256:	F95305FFA81A843FD855D10212D8A52D308679931B107E1869239F0DFAB49EB9
SHA-512:	FFEB60D593FC3D724925377AE50689EEAA78514D78D99DB060C5EFD2F7FD41BE2B43E5E813D25EFCA4086B61B43D201CD39471758A45031A4635E7DC2A13F19
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\amp-analytics-0.1[1].js	
Reputation:	low
IE Cache URL:	http://https://cdn.ampproject.org/v0/amp-analytics-0.1.js
Preview:	(self.AMP=self.AMP||[]).push({n:"amp-analytics",v:"2012301722001",f:(function(AMP,_){.'use strict';var l,aa="function"==typeof Object.create?Object.create:function(a){function b(){}b.prototype=a;return new b};function ba(a){for(var b=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global],c=0;c<b.length;++c){var d=b[c];if(d&&d.Math==Math)return d}return function(){throw Error("Cannot find global object");}()}var ca=ba(this);"function"===typeof Symbol&&Symbol("x");var da;.if("function"==typeof Object.setPrototypeOf)da=Object.setPrototypeOf;else{var ea;a:{var fa={a:!0},ha={};try{ha.__proto__=fa;ea=ha.a;break a}catch(a){}ea=!1}da=ea?function(a,b){a.__proto__=b;if(a.__proto__!==b)throw new TypeError(a+" is not extensible");return a}:null}var ia=da;.function p(a,b){a.prototype=aa(b.prototype);a.prototype.constructor=a;if(ia)ia(a,b);else for(var c in b)if("prototype"!=c)if(Object.defineProperties){var d=Object.ge

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\background5-h_kjukqdlq[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 1446x1410, frames 3
Category:	downloaded
Size (bytes):	104013
Entropy (8bit):	7.533819949957715
Encrypted:	false
SSDEEP:	1536:AjCKmdJ+C1i7a4m3s5ciTiqtTW1VetP0TD4JXqzVFGr/4ifx61:A670OpiPHW1gQUMz2rQil
MD5:	CD21AD096013ABD227DA90B82BFE0C3A
SHA1:	878FC3D0ABAD817D6CD5BCD81F943EB2745C820F
SHA-256:	2763F69A231E96638E749DFC9E7BBD1CA01E2664C33853BA06D4A3BBE0916FB4
SHA-512:	487115EDD004FB092C9B33F9F6EA815C21E0BEC6EBB51F314BEC8FCCC12D525D8E5B0560824E96967C301194DE38E515651698654D9A069B0F48434ABE5BDCA3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://r.8b.io/217023/images/background5-h_kjukqdlq.jpg
Preview:	......JFIF.....C.....C.....".....g.....!1..Qaq... "2AR.....UV...36BST....#5bt..CFWrs...$4%8Du....de(9v.....)Ecf.....:.....!QSa.1AT.....5q"2BR.3bs..r.....?..S..<I.%..3...c.79.....N..k.,.. ....0.t..RJ..G+..x.....S....~.K....X.....=.Y..F..."..lQ3NI..e\.n..q.G....F..i*x5=..<7F..BY^..r.q...d..v.KZ.....5....Y;.=.....kTr..Z.h.~.cr&...f...:a.$.X._.....L.s.i...)&@ZSa.X..J{....N.(X.. [....\.q..52DP>.....i.dL.I,k..U..&h...2a.9..Z..5.....^..r.Vx.....C.q.S.....q...c.`C...5..4..e.>.i$..}..3J1...n..Z.....j=Z..".E<_.....p.....@..... .....\.ku.y..-...cl.+z..F...1..9+..h.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\pdf[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	6830
Entropy (8bit):	7.849424154989951
Encrypted:	false
SSDEEP:	192:n6ND9AxRGozwHD0Ksf+GQUAU6Z0WoYGoKUcsgYRU:6xWRXwHmtfYGLUYIU
MD5:	F1E3F187F7C23FA8D1555004F3800356
SHA1:	E71E52A142E754399AE39EF38584789B66E9EA00
SHA-256:	DB307FCEF7F95139689007D7A623B340EC21282BD421C4E4B2BA09078F230545
SHA-512:	BD568B1C92D7C3B586E2EA7E9C47B08FD1171FF6615FA4F670F12950DC62315B58E6BB5336F50B111FF42B27558398DFF9715054A8E44F0A8B9CD1541F0BC07D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://vikinggenetics-my.sharepoint.com/personal/datho_vikinggenetics_com_au/_layouts/15/images/pdf.png
Preview:	.PNG.....IHDR.....\r.f... cHRM..z&.....u0...`..:....p..Q<....bKGD.....7IDATx..K....j.[....{..&....V6....np3...-.. $.qF..0.a....a6y.....&D.g.#.....;..aC..q.5.k.... n..SU.T...Oj.[..w.....:.....Nz....P.0.,.....b`..X.....`10.,.....b`..X.....U.@...?...Dfs..S....".....y.I.'q.s...^.9.....u.~qnn.....p.....?\u..Pz..&.>.E....)O....zzz.?.. k.q#...;0..`Y...jaA.....S.\HF...#"...".dY:.O./..@.C).....f.I...<..;o.9..0... ..B.....I..&`.4...|..1..9z...o.E...P..h...R..P.q...l....1....8....$..v.....q.q.j6.4555Vw.g..=:TJ.....v\.6.%.).H(...._'. ._.>.f...s].&.....j.U]..?2..-..rs....U.....7T0._.p..<.....*.4.".|S...C....L@=...Q..(,.^.S...`?@...f...1x.....w.6.~....F.....7....{.\....z..B.....d..;.....F.&.... 3\.T.....q..Fcq...9|.&....A.....<... .....{..L 3,. ..1a...!(.`- .F.ASK&px..<p...D...d....*W~g].....h.j.0.Y.....d...4dK. .F...`.Y`j..\.7SQ{_.f.AS.....\....S..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\v0[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	260053
Entropy (8bit):	5.369323142824894
Encrypted:	false
SSDEEP:	3072:1d1NMZo12NdZgOX2w/FU52Rw+o6y0OyCa:D1NMZoYNdNGw/FU5IeA
MD5:	76044E118D79DCF4046348A96A1ADF29
SHA1:	B290E62F428143D4E730E89EEAB96E7A9D0240C7
SHA-256:	4DDFCE71F7DB4C847F4410C9C4093D4182098D9A87646F6BE35AC9E65ADA543B
SHA-512:	EE62BB3330B64D944F522E5513CC08979661FF702FFCD02AE35795B9889D57973966190E735074BA2FB36A7572ACA5495BF0F70C36738BE8793E313B9FBEDCA1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\v0[1].js	
IE Cache URL:	http://https://cdn.ampproject.org/v0.js
Preview:	self.AMP_CONFIG={"v":"012012301722001","type":"production","allow-doc-opt-in":["amp-next-page","analytics-chunks-inabox"],"allow-url-opt-in":["pump-early-frame"],"canary":0,"a4aProfilingRate":0.01,"adsense-ad-size-optimization":0.1,"amp-accordion-display-locking":1,"amp-action-macro":1,"amp-story-responsive-units":1,"amp-story-v1":1,"chunked-amp":1,"doubleclickSraExp":0.01,"doubleclickSraReportExcludedBlock":0.1,"expand-json-targeting":1,"fix-inconsistent-responsive-height-selection":0,"flexAdSlots":0.05,"intersect-resources":0,"ios-fixed-no-transfer":0,"pump-early-frame":1,"adsense-ptt-exp":0.1,"doubleclick-ptt-exp":0.1,"fie-resources":0.1,"visibility-trigger-improvements":1};/*AMP_CONFIG*/var global=self;self.AMP=self.AMP||[];try{(function(_){.'use strict';var g,aa="function"==typeof Object.create?Object.create:function(a){function b(){}b.prototype=a;return new b};function ca(a){for(var b=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\amp-loader-0.1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	14986
Entropy (8bit):	5.442055514702969
Encrypted:	false
SSDEEP:	384:mSba5F4U5A4WR2vj5F4U5A4WR2vFinnHX+l:mD5F4U5A4WR2vj5F4U5A4WR2vEG
MD5:	F5256BD9CACED5B54BFF3ED3E7AD9D6B
SHA1:	4EA0EF3D3EE0A6A2CCFC324CB986A8C09C2FC824
SHA-256:	EA23401A3895913CEA6ED0EA456373C9081C4A116594B2306A994F15470BF34F
SHA-512:	9C232D49CECAA2396F4BAFFF0EDC637409AB78E041EEEB2D57E925621F7729CF53D679C1CCD1158246E33278EC75A26061B15412A878E8CDCE591027577870A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.ampproject.org/rtv/012012301722001/v0/amp-loader-0.1.js
Preview:	(self.AMP=self.AMP||[]).push({n:"amp-loader",v:"2012301722001",f:(function(AMP,_){.'use strict';var g=self.AMP_CONFIG||{},k=("string"==typeof g.cdnProxyRegex?new RegExp(g.cdnProxyRegex):g.cdnProxyRegex)||/^https:\/\/([a-zA-Z0-9_-]+\.)?cdn\.ampproject\.org$/;function l(a){if(self.document&&self.document.head&&(!self.location||!k.test(self.location.origin))){var b=self.document.head.querySelector('meta[name="'+a+'"]');b&&b.getAttribute("content")}}g.cdnUrl||l("runtime-host");g.geoApiUrl||l("amp-geo-api");self.__AMP_LOG=self.__AMP_LOG||{user:null,dev:null,userForEmbed:null};function m(a){a=a.__AMP_TOP||(a.__AMP_TOP=a);var b=a.__AMP_SERVICES;b||(b=a.__AMP_SERVICES={});a=b.extensions;a.obj||(a.obj=new a.ctor(a.context),a.ctor=null,a.context=null,a.resolve&&a.resolve(a.obj));return a.obj};/*. https://mths.be/cssescape v1.5.1 by @mathias | MIT license */.var n;function p(a){a=a.ownerDocument||a;n&&n.ownerDocument===a||(n=a.createElement("div"));return q}function q(a){var b=n;b.innerHTML=a[0];

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	175
Entropy (8bit):	5.047535944462214
Encrypted:	false
SSDEEP:	3:0SYWFFWlIYCd4dSRI5XwDKLRIHDfFRWdFTfqzrZqcduTiGKOnkUYARNin:0IFFqdS+56ZRWHTizlpduTimJNin
MD5:	3A015FB2F44F9C2C0885F8B4F087B782
SHA1:	50D21ACD13DA2E6A233FE53F1058D9E35CDAE0DB
SHA-256:	7E23D171A94F7EBF386AD6E544368FFA22EC113B724E5916003F943F6B041A14
SHA-512:	36B6585DD500EB535F198900CB2ECC354DE468E5F67C0B1697E149885EC0468AB3A6877901D41119EBBCFFB31AD7D78F7BC660EF70ABBBF9A84ABD78B941AACA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Neucha:400
Preview:	@font-face {. font-family: 'Neucha';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/neucha/v12/q5uGsou0JOdh94bfvQlr.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\css[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	172
Entropy (8bit):	5.057077814309068
Encrypted:	false
SSDEEP:	3:0SYWFFWlIYCPX7sRI5XwDKLRIHDfFRWdFTfqzrZqcdcAJlCTOq7LSuMUYARNin:0IFFg+56ZRWHTizlpdcrCaYLSuNin
MD5:	C8F8B59F84161FE076FC915857FFD06F
SHA1:	B9C8C8492C55999F1188F66911935B3D0B38409F
SHA-256:	50A15F59ECB3FEBE2F62BA9DD4A12B93F7AB7E113D23A098E599F9041D1ADDFD
SHA-512:	BD7848DC190B7200E4D3D7BCFCE10D3A4E5E0DE587288DF2531A7D4183756B6C156543A1B82A609A677910DED237DFF32F95B244414AA14FA9DE86870F6F4EE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Forum:400

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\css[2].css	
Preview:	@font-face {. font-family: 'Forum';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/forum/v11/6aey4Ky-Vb8Ew8IROpQ.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\mfile[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	22197
Entropy (8bit):	5.833061488368081
Encrypted:	false
SSDEEP:	384:PReesgg2CtFgHdEXZDRbcOZrVorDYsCarDWWWlGhcTQmqLXJRquD2gqBzBO0:PHsgg2G6HdEXZDRSg8cchcxO0
MD5:	47D6CCFC553E918E0FC748756267866F
SHA1:	84EB468749227A656FA8BF1C9AD6CC601C01F19F
SHA-256:	CE3D11FC2297995D19C211B046134A7CFC3081CC5C4C5B5791562236D93D9B46
SHA-512:	D85ABFE968628CED336C4446CD890F10632952403AD950D446DB4F9947C0497523930B884152B6F23E89AD07EF2F919F435F4B2E58954E5E30B9243529DC99BD
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\mfile[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://lacecompound.com/sm/mfile/
Preview:	..<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">..<html xmlns:o="urn:schemas-microsoft-com:office:office" lang="en-us" dir="ltr">..<head><meta name="GENERATOR" content="Microsoft SharePoint" /><meta http-equiv="Content-Type" content="text/html; charset=utf-8" /><meta http-equiv="Expires" content="0" /><meta name="Robots" content="NOHTMLINDEX" /><meta charset="UTF-8" /><meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1" /><meta http-equiv="X-UA-Compatible" content="IE=edge" /><link id="favicon" rel="shortcut icon" href="images/favicon.ico?rev=45" type="image/vnd.microsoft.icon" /><title>...Sharing Link Validation..</title>...<style type="text/css" media="screen, print, projection">....html{line-height:1.15;-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}body{margin:0}article,aside,footer,header,nav,section{display:block}h1{font-size:2em;margin:.67em 0}figcaption,figure,main{display:bl

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\amp-intersection-observer-polyfill-0.1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	12475
Entropy (8bit):	5.36778912603774
Encrypted:	false
SSDEEP:	192:AYRscGnKsnR8pncgHO8NN4BUcXalO/G8iQGRXOBM/Z5+p1ycO+HbXjyhXuV99QyJ:AYoAJHLwFipRCdFbye+h39j6
MD5:	9F81383065E00538C374286DFDA095C3
SHA1:	52A1A7CC4414862E71A92684FFB65774D778F081
SHA-256:	22611BBA3A501FEFB8F4BA7749809BD532AE504FB752DAD1D5A6C10AD861FAFD
SHA-512:	4535AB538871854EC6B504F0E3AEFA6007921FACBA831648542B31D59A514A71F6DEDF86967A5CFD1C7A77B3A0E8F1744DAFEC287D4E1CDFA8988EFB47C5E0A9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.ampproject.org/rtv/012012301722001/v0/amp-intersection-observer-polyfill-0.1.js
Preview:	(self.AMP=self.AMP||[]).push({n:"amp-intersection-observer-polyfill",v:"2012301722001",f:(function(AMP,_){.'use strict';function B(c){for(var f=["object"==typeof globalThis&&globalThis,c,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global],e=0;e<f.length;++e){var k=f[e];if(k&&k.Math==Math)return}(function(){throw Error("Cannot find global object");})()}B(this);.function F(){(function(){function c(a){try{return a.defaultView&&a.defaultView.frameElement||null}catch(b){return null}}function f(a){this.time=a.time;this.target=a.target;this.rootBounds=E(a.rootBounds);this.boundingClientRect=E(a.boundingClientRect);this.intersectionRect=E(a.intersectionRect||z());this.isIntersecting=!!a.intersectionRect;var b=this.boundingClientRect,d=b.width*b.height,g=this.intersectionRect,h=g.width*g.height;this.intersectionRatio=d?Number((h/d).toFixed(4)):this.isIntersecting?.1:0}function e(a,b){b=b||{};if("function"!=typeof a)throw Error("callback must be a functio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\amp-mustache-0.2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	36278
Entropy (8bit):	5.511282334881756
Encrypted:	false
SSDEEP:	768:XPBgluaZE0cYUS6KIv72SMkPH3hsUekoDJBzYXYNW+e05l:UdZEL2ksUeLq6ttl
MD5:	8B41DA4B6B319D3F8E9F1E3DAE1CA8A9
SHA1:	8639EF63F16BBD2BC53D59083E734CE07AAAEB0B
SHA-256:	18980A3ABB4D681235F6C00E44BE13D6DB484681B1361AF1999066485C78FDFF
SHA-512:	9FDBC4AE128C0312BB5E7E87004A0D53DCE7B8B88CB2D0C87B43DED44C122981274154316FE049EF536E589655E930E8A6DAF02ABC18927A86BB65D8F070B385
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.ampproject.org/v0/amp-mustache-0.2.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\amp-mustache-0.2[1].js	
Preview:	(self.AMP=self.AMP||[]).push({n:"amp-mustache",v:"2012301722001",f:(function(AMP,_){.'use strict';var z;function aa(a){for(var b=["object"==typeof globalThis&&g lobalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global],c=0;c<b.length;++c){var d=b[c];if(d&&d.Math==Math)return} (function(){throw Error("Cannot find global object");})()}aa(this);"function"===typeof Symbol&&Symbol("x");var ca="function"==typeof Object.create?Object.create:functio n(a){function b(){}b.prototype=a;return new b},da;.if("function"==typeof Object.setPrototypeOf)da=Object.setPrototypeOf;else{var na;a:{var oa={a:!0},pa={};try{pa.__proto_ _=oa;na=pa.a;break a}catch(a){}na=!1}da=na?function(a,b){a.__proto__=b;if(a.__proto__!==b)throw new TypeError(a+" is not extensible");return a}:null}var qa=da;function va(a,b){var c=b=void 0===b?"":b;try{return decodeURIComponent(a)}catch(d){return c}};var wa=/(?:^[#?]?|&)([^=&]+)(?:=([^&]*))?/g;var J=self.AMP_CONFIG||{},xa=("st ring"==typ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\logo1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 150 x 150, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1800
Entropy (8bit):	7.684986795686894
Encrypted:	false
SSDEEP:	48:0rnMpqLQ8Ai8eL6mSRHIFcJlNK28vgNEPY:0LMpqaiRL6fIFcb6BPY
MD5:	7A171A1BC5BD4C43DF195ADFEADDEB3D
SHA1:	3C144DCED2C3BBD498777DC32ACC3679E470FC44
SHA-256:	A4DC520571540D3661034628E72005CC9C52E022C67526DC7BD20B7C12CBD615
SHA-512:	2C149208ED7884ED6C2EA7F3CA822817B20226F417CE0EC51CCD0A7BD039EEDE36D477AA934D671C2E249709533E81877BE0A2213CBBF774DCD1F4E6A14E91 D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://app.8b.io/app/themes/webamp/projects/writer/assets/images/logo1.png
Preview:	.PNG.....IHDR.....PLTE.....tRNS.+:...R..5.$.gy.B...K].....o....b.. 1.F..~e>1....IDATx..i..0....<PqA...kw.....B2...>._....IH&.....7?p..p..;c.<.`.z....q.@kv.. 2.^...z.....O.:m...9>....".z...&.....I...k.R..\|.....t(...1..E.ZWg3./fR.W..X.....3.#.,;.Z.....b... ..TL..9.c-.'.h.b../.k-\..Q..j..\1...w.u..(.....j..'.....h._;.q....#.t...V.6Fo...F..w}j.#.y..O.._=...Z...y{J.....B..i...@.x.V.q.....;L...bJp.".k.....c[.AO.*+..eZD-.(..iH.o.wA..V0.fv..j...j...5n.....2 .xT?..3>....6E+../....k...O....m..i...n. .JKi.:.,....36...[....y.....);6n.....uS..k.....p...0...)....HeY.{.d...&...Y.....VXK..x...h.2....@.`.-L2.. ..D...J..t..4.&.N..:,...UJ....%....;.....I.....swR...0..." {.._.s..^.ES.e.0.VM...Bt..2P]...*D/@$IGd-.....r...>Q+!.3VICGvY..z...C.B.Ml..'.U...?...*,....'^dz.Z."yx7!.0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\03OIYGP2.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	36338
Entropy (8bit):	5.157731420366808
Encrypted:	false
SSDEEP:	768:8y0DlkvJOdKkUGfkxXjwWSwOsZ4aGuejvgCijX:WDlCOdKk7IkWSwOsZ4a7ejvgT
MD5:	659A68F9335B456C05723AAC85236444
SHA1:	195AE093F4DCCB8B9E44286558C958ECF54B946A
SHA-256:	EC9E36F1DF4E04F42C3D0A1F1531D8B19DE55A35EFF85EC73CEE3D9A937AA733
SHA-512:	FA078D7D8AA29762AC71071849E856A55BA1C5CA835F0C5F97059080B362A649AB79AE6DE431977274E837BB0315AD40E21F77C82EA6833D2403F7C4A4A861CA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://217023.8b.io/
Preview:	<!DOCTYPE html>.<html amp>.<head>. Site made with 8b Website Builder v0.0.0.0, https://8b.com -->. <meta charset="UTF-8">. <meta http-equiv="X-UA-Compatib le" content="IE=edge">. <meta name="generator" content="8b v0.0.0.0, 8b.com">. <meta name="viewport" content="width=device-width, initial-scale=1, minimum-sca le=1">. <link rel="shortcut icon" href="https://app.8b.io/app/themes/webamp/projects/writer/assets/images/logo1.png" type="image/x-icon">. <meta name="description" content="">. <title>2233</title>. .<link rel="canonical" href="https://217023.8b.io/">. <style amp-boilerplate>body{-webkit-animation:-amp-start 8s steps(1,end) 0s 1 normal both;-moz-animation:-amp-start 8s steps(1,end) 0s 1 normal both;-ms-animation:-amp-start 8s steps(1,end) 0s 1 normal both;animation:-amp-start 8s steps(1,end) 0s 1 normal both}@-webkit-keyframes -amp-start{from{visibility:hidden}to{visibility:visible}}@-moz-keyframes -amp-start{from{visibility:hidden}to{visibility:visible}}@-ms-keyfram

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\6aey4Ky-Vb8Ew8IROpQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 30208, version 1.1
Category:	downloaded
Size (bytes):	30208
Entropy (8bit):	7.982638126084365
Encrypted:	false
SSDEEP:	768:YTZ6XBcgqEOWcLaKUD2LPdndYiTJ7r08x9mQh07Eo63/aMuP:YTZIB+EOG/O1l5r08xMQh07EBiP
MD5:	B1C4BE7C6BB01AB2125BEE6D723CD52E
SHA1:	F3006406A5E4B33C0248661B1201A3B23D0DE267
SHA-256:	A4A8AC69ACE5555AA9BF5AF6824B8D1AFDB0BFA404EE63103AC7AF09859634CD
SHA-512:	5FF9DB28D72598A3CB1A3CA76C16D48B2C93005030569EE78B1984D717B7FD6F91E0FD78621B4269682D126AA99C8DA4FC732DDF4940817A1E9F64FD3307439
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\6aey4Ky-Vb8Ew8IROpQ[1].woff	
IE Cache URL:	http://https://fonts.gstatic.com/s/forum/v11/6aey4Ky-Vb8Ew8IROpQ.woff
Preview:	wOFF.....v.....H.....GPOS.....!.....?.SOS/2.....Q...`....VDMX...../....h.prcmap...(.....R.E.Icvt .....(...(.h.1fpgm.....s.Y.7gasp.....glyf.....R.....\.Nhdmx..e....M.....f..head..n....3...6..'&hhea..o,.....$.R.Mhmtx..oL.....8m...loca..q0.....z.Mmaxp..r.... ... ....name..r....%....=.Stpost..t....K....:.={prep..ud.....qu..x.,..p]Q.E....mkX.m.m.6...A...`..p.A2Q.G..... ..8zv..8HA.q...=O...C3G..3g=.1W..''..]..... U....>...w._._.)P'....^.l.....$|V..VQK..i^...''.&i{.K.....5..>E..#.1..e.1...L..cV2.....:UW.o.f...Y...!....d.[..R...p....?....'.H..FC...&...BV.....!/..O..R."...e)Gy*P.JT...A-...4....Dg..~.d(...(&2...b.s..|...%,e....f.....'8.)Ns.....TPSI>RY.SEM5.J.uk.O.J_....e..f..d..m..l...P.1..yY..Y..Z.....2oM.V(.l,c..xA*..UD..Q@K..R.!..''!..VBX./..C...vb.....3...%t!.a.2B)..1B(...>....&.|y..<...{.....z.M.IEg7....o.j..O...njg.MP..Km..{[.m.m..X.>jc.Nm...6..l....)jC..R{..lj.-...vp.....v.Z7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\amp-auto-lightbox-0.1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	5069
Entropy (8bit):	5.4494399468635635
Encrypted:	false
SSDEEP:	96:9sZVrZkAwc4nrhUAj87jdjEJaDv3/p3+e6HXFLE58M:o7wc4nrq1jEKv3xr6HNE57
MD5:	7012ACC9D81E0AF71AC19EDFD85AAF87
SHA1:	56D9539EF3E0D57B978F52279142273A851D7FD7
SHA-256:	C9029AE9DCAF52BD278EBC3A87DE7340F47F3050780994EFCBBFF06A7FD62E6C
SHA-512:	DC4A56445E3FF16627B34CE9751CC23B775B0C71EEA9480A16C8C5E15391978E08E19E49987D5012A0DF0824173F7B539AB26DFACCA8271ECB127CE518AB86C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.ampproject.org/rtv/012012301722001/v0/amp-auto-lightbox-0.1.js
Preview:	(self.AMP=self.AMP||[]).push({n:"amp-auto-lightbox",v:"2012301722001",f:(function(AMP,_){.'use strict';function k(a){for(var b=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global],c=0;c<b.length;++c){var d=b[c];if(d&&d.Math==Math)return}(function(){throw Error("Cannot find global object");})()}k(this);"function"===typeof Symbol&&Symbol("x");var m;function n(){var a,b;this.promise=new Promise(function(c,d){a=c;b=d});this.resolve=a;this.reject=b};function p(a){return a?Array.prototype.slice.call(a):[]};var q=self.AMP_CONFIG||{},r=("string"==typeof q.cdnProxyRegex?new RegExp(q.cdnProxyRegex):q.cdnProxyRegex)||/^https:\/\/([a-zA-Z0-9_-]+\.)?cdn\.ampproject\.org$/;function t(a){if(self.document&&self.document.head&&(!self.location||r.test(self.location.origin))){var b=self.document.head.querySelector('meta[name="'+a+'"]');b&&b.getAttribute("content")}}q.cdnUrl||t("runtime-host");q.geoApiUrl||t("amp-geo-api")

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\mfile[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	242
Entropy (8bit):	5.0737173888397455
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwol6hEr6VX16hu9nP3GNKYMJfw+KqD:J0+ox0RJWWP3ezMRT
MD5:	B8664C5CB94E26F82CBA5DDD725810B8
SHA1:	C4BD14AF6073721229AEE0A7D0611F7EE3DE5027
SHA-256:	30089A819C8CD726BECD00C6088A23C250ACCDF0DB5282BC1516A0E0F83C2469
SHA-512:	FF9C5965B618A75322BE6274F606887B9AAB20BC50E451132F1D1A0E762D45A89661F3E3147C62F869B0B113BFDBEA80EDFDC65A2BDBEB90146CA2667B8D495D
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>301 Moved Permanently</title>.</head><body>. Moved Permanently . The document has moved here. .</body></html>.

C:\Users\user\AppData\Local\Temp\datBA90.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 2532, version 2.24904
Category:	dropped
Size (bytes):	2532
Entropy (8bit):	7.627755614174705
Encrypted:	false
SSDEEP:	48:WGMiY6eIlk7QuaqrjRh4pi6j4fN6+XRsnBBpr+bes:WRBLIIoQuHfRh4pi6sfPGnDFs
MD5:	10600F6B3D9C9BE2D2B2CE58D2C6508B
SHA1:	421CA4369738433E33348785FE776A0C839605D5
SHA-256:	29B7A9358ABDC68C51DB5A5AF4A4F4E2E041A67527ADEE2366B1F84F116FE9A5
SHA-512:	B6C04F3068EB7DAC8F782BDED0FE815B4FE5A9BECCF0B561D6CEAEAA7365919A39710B2D1AD58D252330476AA836629B3C62C84FABFA6DC4BCF1C8F055D66C1C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\datBA90.tmp	
Preview:	wOFF.....aH.....OS/2...D...H...`1Wp.cmap.....l...b..ocvt ..... ...*....fpgm.....Y...gasp.....glyf.....Whead.....2...6.tJ.hhea.....$....hmtx..... .....loca.....X.hmaxp...,..... .y..name...L.....Mpost...D..... .Q.}prep...X.....x...x.c`aog.....:....Q.B3_dHc..`e.bdb... .`@..`.....,9.\|...V...)00...C..x.c```f.`..F.....\|... ..... .\..K..n.,..g`@.I\|.8"vYl.....p...0.....x.c.b.e(`h`X.....x.....x.]..N.@..s$..'@:!.u*C....K$.%%...J.....n..b.....\|.s...\|v..G*)V.7.....!O.6eaL.yV.e.j..kN..M.h....Lm....-b....p.N.m. v.....U<..#...O.}.K..,V..&...^...L.c.x.....?ug..l9e..Ns.D....D...K.....m..A.M....a.....g.P..`....d.....x..R.K.1...$....g-.B.Vq..m..Z..T..@\t.E...7X...:.).c... ].{.Q.['...`.^...&....{y<..N. ....t...6..f....\.K1..Z}{.eA-..x.{....0P7p.....l.....E...r....EVQ.....Q_.4.A.Z..;...PGs.o..Eo...{t...a.P.~...b,Dz.}.OXdp."d4."C.X..&,u.g.....r.c..j

C:\Users\user\AppData\Local\Temp\~DF35D918A5D4402B2C.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.28883759889035865
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	BF5C20FE9AC2E37A2E98341C1C1B7CE8
SHA1:	4D05CA4074C665936792647919101E01DC83FDDB
SHA-256:	D2F5C6188CA81305EF7C440DA11470CB5542871AFEB6D7C6719E28A367536ADD
SHA-512:	42B370849E2871BA8EB96915013D3BD9545CEE8220C1E4237BCB5CA9606D876B8553E33A0E9CBBC9C00187FAC914A3111FEBC3751428E050B547C9A90AD17E2B
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFBBCE481DAF4343C1.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.48005770725532293
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loiF9loe9lWLvkPXKg2kvKgBgCv:kBqoIp/LvkPXd2kvdB5v
MD5:	11FE12E9FDFA76BBB3EDC1D5D0F1A28A
SHA1:	18F6BB28B66A0AB78426E01E88DA7060D2AF4705
SHA-256:	01ABBABDACBF5DA7281577FFF55EDBE081222C1C690D39D42B33EFDE61FF4AB9
SHA-512:	7B086E55DA29975819CABEE7571E8D32541C0AFDB08DC41996B4AB2B9CE8601B27D16C035BDB88CE22D43B8B3E713ADCC4181E6CA98AACD9380B494EDD956E20
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

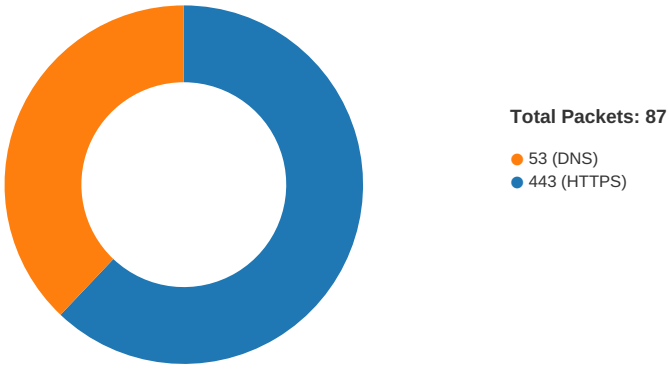
C:\Users\user\AppData\Local\Temp\~DFE679E51CD7555755.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	46819
Entropy (8bit):	0.9588807871049881
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+TtfW9VZFhL/hRNRHlQm2GQQa/pY5440XAZ7sh/:kBqoxKAuqR+TtfW9VZFhLhXQmt/Zuh
MD5:	EEF745AD9D071303ADB99A8C5A0F713E
SHA1:	8194571A317F70A7D03679F62816FF8315588364
SHA-256:	A52B60D46745CBA4B8C7FA9FC42760826DC948E6630D982F3633C8A433109220
SHA-512:	E691F75441224E976C4A8F7E1CFA51F3D315A72B82D3331BAF1C50203C72E654715DC570CAB7E5E37BB5C24EC4AE684A9CDB56BEE088AFC4660A913EA5EC47FA
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
Jan 13, 2021 19:24:23.685626984 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:23.685842991 CET	49713	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:23.812405109 CET	443	49713	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:23.812462091 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:23.812525988 CET	49713	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:23.812566042 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:23.818306923 CET	49713	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:23.818486929 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:23.944729090 CET	443	49713	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:23.944950104 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:23.945882082 CET	443	49713	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:23.945986986 CET	443	49713	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:23.946028948 CET	443	49713	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:23.946105957 CET	49713	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:23.946135998 CET	49713	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:23.946147919 CET	49713	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:23.946274042 CET	443	49713	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:23.946471930 CET	49713	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:23.946891069 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:23.946943998 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:23.946984053 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:23.947115898 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:23.947160006 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:23.947170019 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:23.947179079 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:23.947211981 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:23.980176926 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:23.980381966 CET	49713	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:23.986254930 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:23.986382008 CET	49713	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:23.986447096 CET	49712	443	192.168.2.3	52.201.120.251

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 19:24:24.107104063 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.107136965 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.107172966 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.107214928 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.107258081 CET	443	49713	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.107296944 CET	443	49713	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.107332945 CET	49713	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.107367039 CET	49713	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.108386993 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.109965086 CET	49713	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.112771988 CET	443	49713	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.112842083 CET	49713	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.112864017 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.112921953 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.155957937 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.156056881 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.156105042 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.156146049 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.156172037 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.156183004 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.156210899 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.156220913 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.156245947 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.156270027 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.156280994 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.156313896 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.156328917 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.156373978 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.234025002 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.234102011 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.234122038 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.234168053 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.234186888 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.234205008 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.234232903 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.234265089 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.239577055 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.239643097 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.239671946 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.239705086 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.276971102 CET	443	49713	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.283008099 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.283051968 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.283104897 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.283124924 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.283139944 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.283215046 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.283226013 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.283256054 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.283272982 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.283312082 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.283329010 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.283384085 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.283415079 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.283472061 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.283489943 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.283549070 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.283557892 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.283597946 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.283615112 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.283633947 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.283653975 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.283670902 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.283690929 CET	49712	443	192.168.2.3	52.201.120.251

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 19:24:24.283730984 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.283739090 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.283777952 CET	443	49712	52.201.120.251	192.168.2.3
Jan 13, 2021 19:24:24.283797026 CET	49712	443	192.168.2.3	52.201.120.251
Jan 13, 2021 19:24:24.283834934 CET	49712	443	192.168.2.3	52.201.120.251

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 19:24:18.647885084 CET	64185	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:18.696011066 CET	53	64185	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:19.854541063 CET	65110	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:19.902832985 CET	53	65110	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:20.678781986 CET	58361	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:20.727063894 CET	53	58361	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:21.513556957 CET	63492	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:21.572916031 CET	53	63492	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:22.515542984 CET	60831	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:22.575056076 CET	53	60831	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:22.775511980 CET	60100	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:22.826328039 CET	53	60100	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:23.611802101 CET	53195	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:23.666194916 CET	50141	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:23.675849915 CET	53	53195	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:23.716963053 CET	53	50141	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:24.335514069 CET	53023	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:24.392066956 CET	53	53023	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:24.480214119 CET	49563	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:24.536294937 CET	53	49563	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:24.735043049 CET	51352	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:24.782927036 CET	53	51352	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:26.004601955 CET	59349	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:26.061570883 CET	53	59349	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:26.072170019 CET	57084	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:26.136073112 CET	58823	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:26.171911001 CET	53	57084	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:26.183912039 CET	53	58823	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:26.914899111 CET	57568	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:26.962816954 CET	53	57568	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:27.706162930 CET	50540	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:27.756886959 CET	53	50540	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:28.519021034 CET	54366	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:28.568106890 CET	53	54366	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:29.359289885 CET	53034	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:29.407505989 CET	53	53034	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:30.656039000 CET	57762	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:30.703989983 CET	53	57762	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:31.572029114 CET	55435	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:31.620037079 CET	53	55435	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:32.481456995 CET	50713	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:32.532480955 CET	53	50713	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:39.897914886 CET	56132	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:39.957340002 CET	53	56132	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:42.142231941 CET	58987	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:42.508584023 CET	53	58987	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:44.262964964 CET	56579	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:44.383820057 CET	53	56579	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:47.609656096 CET	60633	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:47.657654047 CET	53	60633	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:52.509288073 CET	61292	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:52.557375908 CET	53	61292	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:53.172055006 CET	63619	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:53.228282928 CET	53	63619	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:53.513302088 CET	61292	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 19:24:53.569555998 CET	53	61292	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:54.185372114 CET	63619	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:54.241776943 CET	53	63619	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:54.528206110 CET	61292	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:54.584810019 CET	53	61292	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:55.197503090 CET	63619	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:55.245729923 CET	53	63619	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:56.543057919 CET	61292	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:56.591589928 CET	53	61292	8.8.8.8	192.168.2.3
Jan 13, 2021 19:24:57.213306904 CET	63619	53	192.168.2.3	8.8.8.8
Jan 13, 2021 19:24:57.261337996 CET	53	63619	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 19:24:23.611802101 CET	192.168.2.3	8.8.8.8	0x76b9	Standard query (0)	217023.8b.io	A (IP address)	IN (0x0001)
Jan 13, 2021 19:24:24.480214119 CET	192.168.2.3	8.8.8.8	0xe57c	Standard query (0)	cdn.ampproject.org	A (IP address)	IN (0x0001)
Jan 13, 2021 19:24:26.004601955 CET	192.168.2.3	8.8.8.8	0x961	Standard query (0)	app.8b.io	A (IP address)	IN (0x0001)
Jan 13, 2021 19:24:26.072170019 CET	192.168.2.3	8.8.8.8	0x230b	Standard query (0)	r.8b.io	A (IP address)	IN (0x0001)
Jan 13, 2021 19:24:39.897914886 CET	192.168.2.3	8.8.8.8	0xdbf3	Standard query (0)	app.8b.io	A (IP address)	IN (0x0001)
Jan 13, 2021 19:24:42.142231941 CET	192.168.2.3	8.8.8.8	0x65e9	Standard query (0)	lacecompound.com	A (IP address)	IN (0x0001)
Jan 13, 2021 19:24:44.262964964 CET	192.168.2.3	8.8.8.8	0x13c4	Standard query (0)	vikinggenetics-my.sharepoint.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 19:24:23.675849915 CET	8.8.8.8	192.168.2.3	0x76b9	No error (0)	217023.8b.io	proxy-8b-io-1762796164.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:24:23.675849915 CET	8.8.8.8	192.168.2.3	0x76b9	No error (0)	proxy-8b-io-1762796164.us-east-1.elb.amazonaws.com		52.201.120.251	A (IP address)	IN (0x0001)
Jan 13, 2021 19:24:23.675849915 CET	8.8.8.8	192.168.2.3	0x76b9	No error (0)	proxy-8b-io-1762796164.us-east-1.elb.amazonaws.com		52.7.227.232	A (IP address)	IN (0x0001)
Jan 13, 2021 19:24:24.536294937 CET	8.8.8.8	192.168.2.3	0xe57c	No error (0)	cdn.ampproject.org	cdn-content.ampproject.org		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:24:24.536294937 CET	8.8.8.8	192.168.2.3	0xe57c	No error (0)	cdn-content.ampproject.org		108.177.119.132	A (IP address)	IN (0x0001)
Jan 13, 2021 19:24:26.061570883 CET	8.8.8.8	192.168.2.3	0x961	No error (0)	app.8b.io		104.24.104.39	A (IP address)	IN (0x0001)
Jan 13, 2021 19:24:26.061570883 CET	8.8.8.8	192.168.2.3	0x961	No error (0)	app.8b.io		172.67.215.39	A (IP address)	IN (0x0001)
Jan 13, 2021 19:24:26.061570883 CET	8.8.8.8	192.168.2.3	0x961	No error (0)	app.8b.io		104.24.105.39	A (IP address)	IN (0x0001)
Jan 13, 2021 19:24:26.171911001 CET	8.8.8.8	192.168.2.3	0x230b	No error (0)	r.8b.io		104.24.104.39	A (IP address)	IN (0x0001)
Jan 13, 2021 19:24:26.171911001 CET	8.8.8.8	192.168.2.3	0x230b	No error (0)	r.8b.io		104.24.105.39	A (IP address)	IN (0x0001)
Jan 13, 2021 19:24:26.171911001 CET	8.8.8.8	192.168.2.3	0x230b	No error (0)	r.8b.io		172.67.215.39	A (IP address)	IN (0x0001)
Jan 13, 2021 19:24:39.957340002 CET	8.8.8.8	192.168.2.3	0xdbf3	No error (0)	app.8b.io		104.24.104.39	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 19:24:39.957340002 CET	8.8.8.8	192.168.2.3	0xdbf3	No error (0)	app.8b.io		172.67.215.39	A (IP address)	IN (0x0001)
Jan 13, 2021 19:24:39.957340002 CET	8.8.8.8	192.168.2.3	0xdbf3	No error (0)	app.8b.io		104.24.105.39	A (IP address)	IN (0x0001)
Jan 13, 2021 19:24:42.508584023 CET	8.8.8.8	192.168.2.3	0x65e9	No error (0)	lacecompound.com		195.181.244.134	A (IP address)	IN (0x0001)
Jan 13, 2021 19:24:44.383820057 CET	8.8.8.8	192.168.2.3	0x13c4	No error (0)	vikinggenetics-my.sharepoint.com	vikinggenetics.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:24:44.383820057 CET	8.8.8.8	192.168.2.3	0x13c4	No error (0)	vikinggenetics.sharepoint.com	614-ipv4e.clump.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:24:44.383820057 CET	8.8.8.8	192.168.2.3	0x13c4	No error (0)	614-ipv4e.clump.prod.aa-rt.sharepoint.com	17825-ipv4e.farm.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:24:44.383820057 CET	8.8.8.8	192.168.2.3	0x13c4	No error (0)	17825-ipv4e.farm.prod.aa-rt.sharepoint.com	17825-ipv4.farm.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 19:24:44.383820057 CET	8.8.8.8	192.168.2.3	0x13c4	No error (0)	17825-ipv4.farm.prod.aa-rt.sharepoint.com		104.146.245.41	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
Jan 13, 2021 19:24:23.946274042 CET	52.201.120.251	443	192.168.2.3	49713	CN=8b.io 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	Thu Jul 09 02:00:00 CEST 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	Mon Aug 09 14:00:00 CEST 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
Jan 13, 2021 19:24:23.947160006 CET	52.201.120.251	443	192.168.2.3	49712	CN=8b.io 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	Thu Jul 09 02:00:00 CEST 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	Mon Aug 09 14:00:00 CEST 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		
Jan 13, 2021 19:24:24.685760975 CET	108.177.119.132	443	192.168.2.3	49718	CN=misc-sni.google.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:44:18 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:44:17 CET 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jan 13, 2021 19:24:24.686079979 CET	108.177.119.132	443	192.168.2.3	49717	CN=misc-sni.google.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:44:18 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:44:17 CET 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jan 13, 2021 19:24:24.733676910 CET	108.177.119.132	443	192.168.2.3	49719	CN=misc-sni.google.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:44:18 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:44:17 CET 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 13, 2021 19:24:26.170821905 CET	104.24.104.39	443	192.168.2.3	49722	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 Jul 29 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Jul 29 14:00:00 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		
Jan 13, 2021 19:24:26.170895100 CET	104.24.104.39	443	192.168.2.3	49723	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 Jul 29 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Jul 29 14:00:00 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		
Jan 13, 2021 19:24:26.281090021 CET	104.24.104.39	443	192.168.2.3	49724	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 Jul 29 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Jul 29 14:00:00 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		
Jan 13, 2021 19:24:26.283150911 CET	104.24.104.39	443	192.168.2.3	49725	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 Jul 29 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Jul 29 14:00:00 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		
Jan 13, 2021 19:24:40.073023081 CET	104.24.104.39	443	192.168.2.3	49734	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 Jul 29 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Jul 29 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 13, 2021 19:24:42.656095982 CET	195.181.244.134	443	192.168.2.3	49735	CN=lacecompound.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sat Jan 09 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sat Apr 10 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jan 13, 2021 19:24:42.656172991 CET	195.181.244.134	443	192.168.2.3	49736	CN=lacecompound.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sat Jan 09 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sat Apr 10 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior

● iexplore.exe
● iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5936 Parent PID: 792

General

Start time:	19:24:21
Start date:	13/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff717c30000
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: 4744 Parent PID: 5936

General

Start time:	19:24:22
Start date:	13/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5936 CREDAT:17410 /prefetch:2
Imagebase:	0x120000
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

Disassembly