ID: 339355
Cookbook: browseurl.jbs
Time: 21:33:40
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

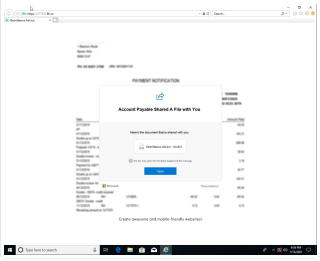
Analysis Report https://217251.8b.io/

Overview

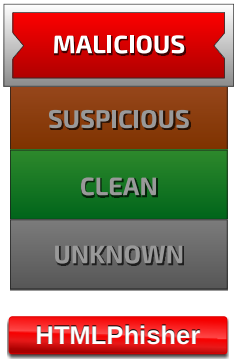
General Information

Sample URL:	http://https://217251.8b.io/
Analysis ID:	339355

Most interesting Screenshot:



Detection

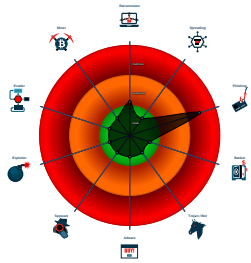


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Yara detected HtmlPhish_6
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 3448 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 1872 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3448 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

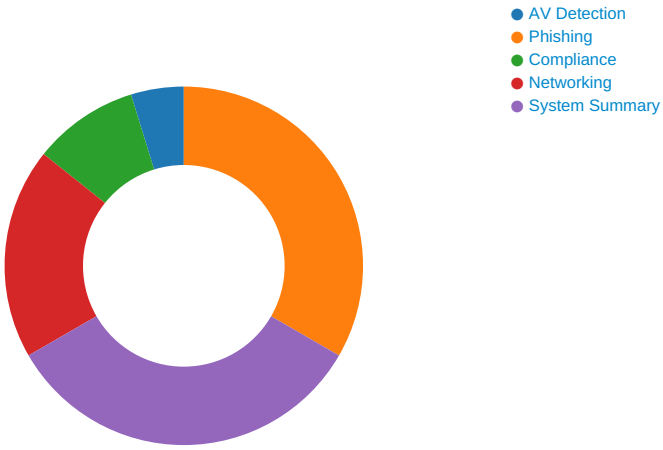
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\s[1].htm	JoeSecurity_HtmlPhish_6	Yara detected HtmlPhish_6	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_6

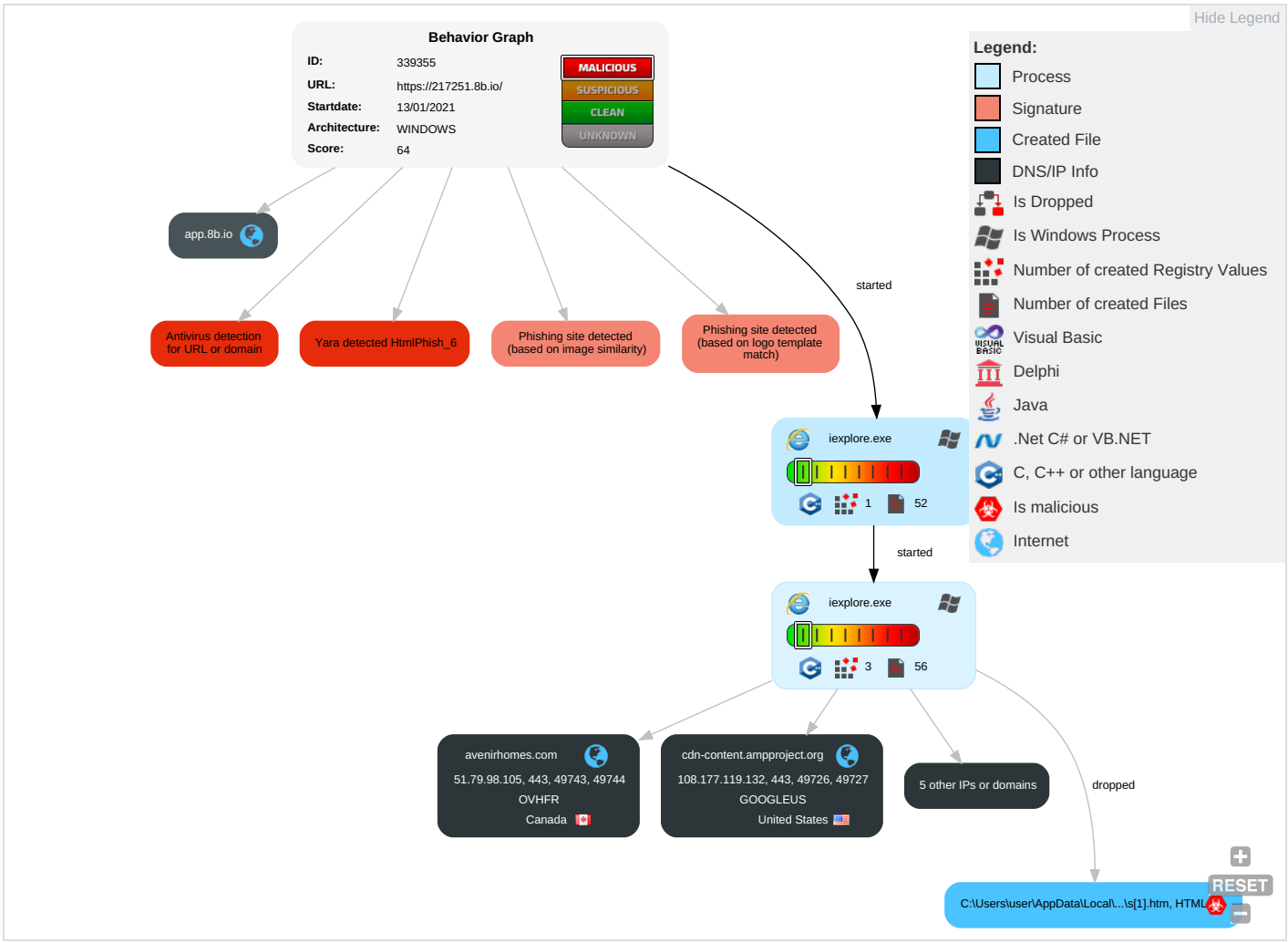
Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	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

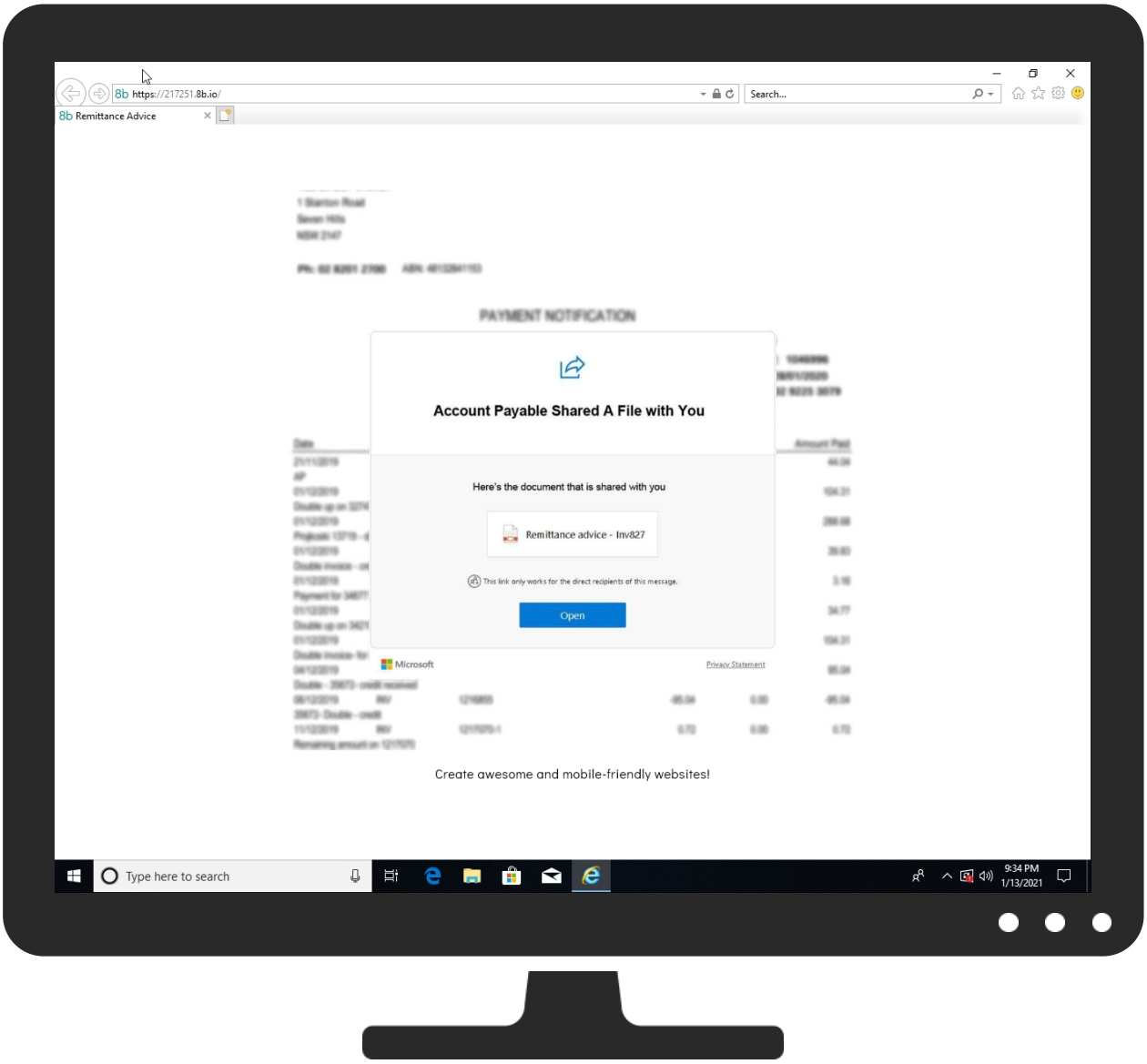
Behavior Graph



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://217251.8b.io/	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://avenirhomes.com/Paymentadvice/new/s/?signin=d41d8cd98f00b204e9800998ecf8427e&auth=c8fa2f9b74a88a59da9f7a1011b291d5be2837acfe48d4a938453ee0e10ca1e981936170	100%	SlashNext	Fake Login Page type: Phishing & Social usering	
http://https://217251.8b.io/Root	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://app.8b.io/app/themes/webamp/projects/company/assets/images/logo.pngn	0%	Avira URL Cloud	safe	
http://https://r.8b.io/217251/images/background5-h_kjvcr6x2.jpg	0%	Avira URL Cloud	safe	
http://https://avenirhomes.com/Paymentadvice/new/	0%	Avira URL Cloud	safe	
http://https://217251.8b.io/L	0%	Avira URL Cloud	safe	
http://https://log.amp.dev/?v=012012301722001&id=	0%	Avira URL Cloud	safe	
http://https://avenirhomes.coL	0%	Avira URL Cloud	safe	
http://https://app.8b.io/app/themes/webamp/projects/company/assets/images/logo.png	0%	Avira URL Cloud	safe	
http://https://mths.be/cssescape	0%	Avira URL Cloud	safe	
http://https://avenirhomes.com/favicon.icoJ=	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://amp.dev/documentation/guides-and-tutorials/develop/style_and_layout/control_layout	0%	Avira URL Cloud	safe	
http://https://avenirhomes.com/Paymentadvice/new	0%	Avira URL Cloud	safe	
http://https://avenirhomes.co	0%	Avira URL Cloud	safe	
http://https://avenirhomes.com/Paymentadvice/new/s/?signin=d41d8cd98f00b204e9800998ecf8427e&auth=c8fa2f9b74	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		unknown
avenirhomes.com	51.79.98.105	true	false		unknown
r.8b.io	104.24.105.39	true	false		unknown
proxy-8b-io-1762796164.us-east-1.elb.amazonaws.com	52.7.227.232	true	false		high
cdn-content.ampproject.org	108.177.119.132	true	false		high
cdn.ampproject.org	unknown	unknown	false		high
217251.8b.io	unknown	unknown	false		unknown

Contacted URLs

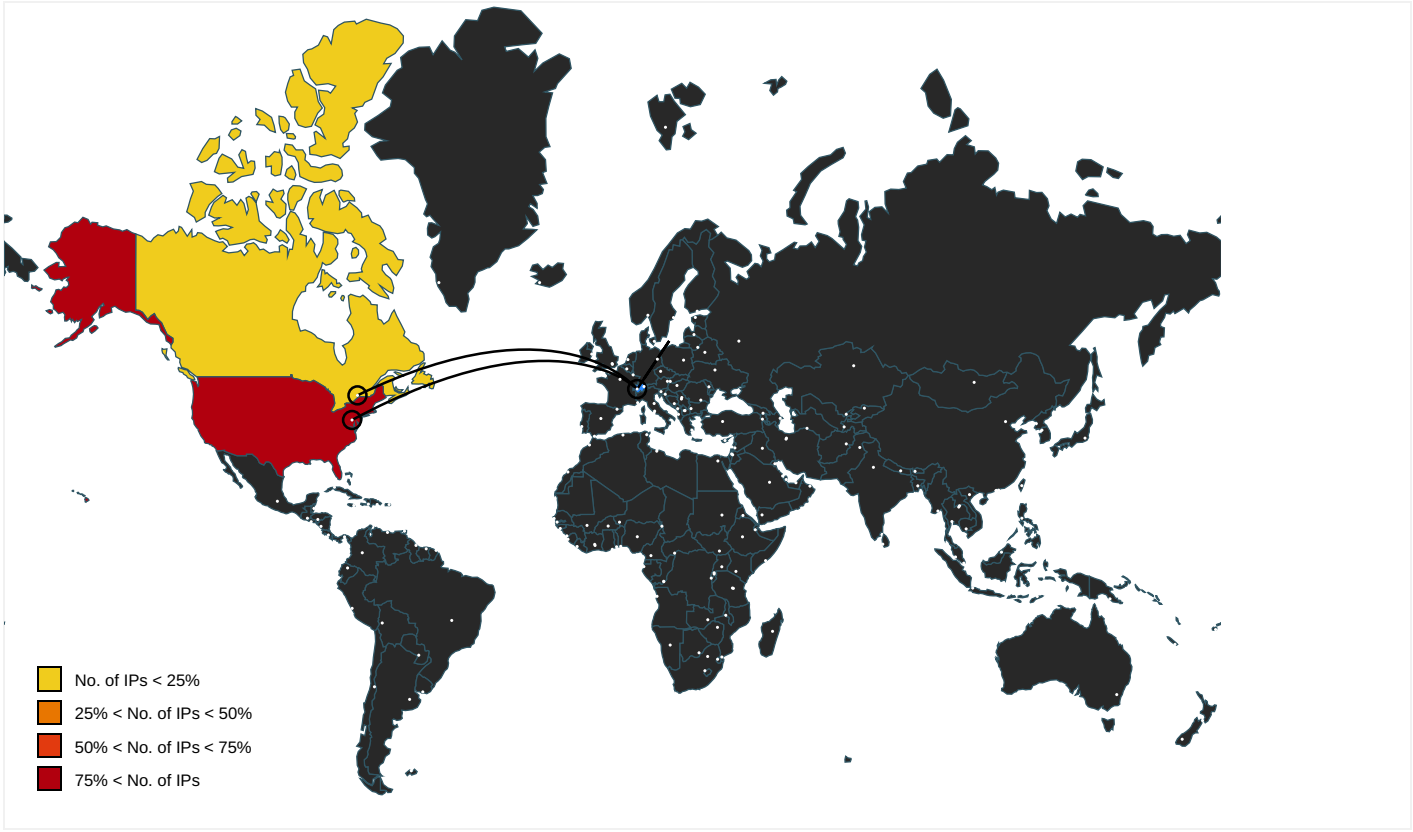
Name	Malicious	Antivirus Detection	Reputation
http://https://217251.8b.io/	true		unknown
http://https://avenirhomes.com/Paymentadvice/new/s/?signin=d41d8cd98f00b204e9800998ecf8427e&auth=c8fa2f9b74a88a59da9f7a1011b291d5be2837acfe48d4a938453ee0e10ca1e981936170	true	• SlashNext: Fake Login Page type: Phishing & Social usering	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://217251.8b.io/Root	{2D1690D1-562A-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://app.8b.io/app/themes/webamp/projects/company/assets/images/logo.pngn	imagestore.dat.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://r.8b.io/217251/images/background5-h_kjvcr6x2.jpg	T08OXF6I.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://avenirhomes.com/Paymentadvice/new/	new[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.ampproject.org/v0/amp-analytics-0.1.js	T08OXF6I.htm.3.dr	false		high
http://https://217251.8b.io/	{2D1690D1-562A-11EB-90E5-ECF4BB2D2496}.dat.1.dr, T08OXF6I.htm.3.dr	false		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://217251.8b.io/L	{2D1690D1-562A-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.ampproject.org/v0.js	T08OXF6I.htm.3.dr	false		high
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

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://avenirhomes.coL	{2D1690D1-562A-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://app.8b.io/app/themes/webamp/projects/company/assets/images/logo.png	T08OXF6I.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://mths.be/cssescape	amp-intersection-observer-polyfill-0.1[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://avenirhomes.com/favicon.icoJ=	imagestore.dat.3.dr	false	• Avira URL Cloud: safe	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	T08OXF6I.htm.3.dr	false	• 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://avenirhomes.com/Paymentadvice/new	T08OXF6I.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://avenirhomes.co	{2D1690D1-562A-11EB-90E5-ECF4BB2D2496}.dat.1.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://avenirhomes.com/Paymentadvice/new/s/?signin=d41d8cd98f00b204e9800998ecf8427e&auth=c8fa2f9b74	{2D1690D1-562A-11EB-90E5-ECF4BB2D2496}.dat.1.dr, ~DF50AF0D1DD5FFBE3A.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.ampproject.org/v0/amp-mustache-0.2.js	T08OXF6I.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
51.79.98.105	unknown	Canada		16276	OVHFR	false
52.7.227.232	unknown	United States		14618	AMAZON-AESUS	false
104.24.105.39	unknown	United States		13335	CLOUDFLARENETUS	false
104.24.104.39	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339355
Start date:	13.01.2021
Start time:	21:33:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://217251.8b.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:	9
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:	mal64.phis.win@3/27@6/5
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://avenirh omes.com/Paymentadvice/new
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.64.90.137, 104.43.193.48, 88.221.62.148, 108.177.126.95, 108.177.127.94, 104.43.139.144, 168.61.161.212, 51.104.139.180, 92.122.213.194, 92.122.213.247, 152.199.19.161 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, skypedataprdcolwus17.cloudapp.net, fonts.googleapis.com, arc.msn.com.nsatc.net, fonts.gstatic.com, ie9comview.vo.msecnd.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtDeviceIoControlFile calls found. • VT rate limit hit for: https://217251.8b.io/

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\EQAWN5DV\217251.8b[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.{2D1690CF-562A-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8501290259312688
Encrypted:	false
SSDEEP:	96:rGfZ46ZvL2VU/9Wcqtc9AfcFCO1MzmTOgRz+fBCjlX:rUZDZD2a9WttBfMBMwfqfB8X
MD5:	14C44134B030F0A54A1190680CC621F4
SHA1:	BFA8AD58924B748BEE990E3A92A5442113016266
SHA-256:	B5EA2EFF7C4109421D32DB3A373FC3D3648E7B6D5F696DB9721269C492CACD04
SHA-512:	DF811CCF7BE92941F8AC675AE8A878E0C28453601EC724C26A27652B1FC77E523C1B3D889117D9D125216B0F182AEF651629339D8BAD3A8CBB5FD404448A6AB
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\{2D1690D1-562A-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{2D1690D1-562A-11EB-90E5-ECF4BB2D2496}.dat	
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	39590
Entropy (8bit):	2.0980482598366192
Encrypted:	false
SSDEEP:	192:rSZFQZ6skgFjR2bkWHMOYUm0/wRUlysDERklrFZdV3h4EK2X:rO60RghA/sOV3/kUxDok3Tf
MD5:	EB574A86D3EBC3ACCEBB363162953C9F
SHA1:	160CE136EECCAD56E2A7B03C413D899DBF8A6BF4
SHA-256:	749CC82D2AD9DC840BC0100C23343001BD4AC81A606861A566C1B5BCA83E8EC5
SHA-512:	4815E3CBCAF92C9D903B1315E63C9E56717A521BA0003A6C4BE93A8FC77401512CDD97026DB7854B3C7EDA5A5180AB05951A5C605A81A3DF3E5B47AA0B8EBBCA
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\{331FBFBE-562A-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.566324967135074
Encrypted:	false
SSDEEP:	48:IwQGcprVGwpaDG4pQ/GrapbSg/rGQpKKG7HpRT/sTGIpG:rUZ/Q16DBSg/FAlTT/4A
MD5:	BF015644447CC357DEF29771A202A72B
SHA1:	BC0A836805FEC671714FD8979A17770F31CE3DA5
SHA-256:	1C2BDCB99AB690D98EB2C83A245622B013057387E465E79160E5841884CF9912
SHA-512:	5B7EE61F150BDE708B7D7491B4E7F06F495B7E6A312090F9F340DDFBE6CA13BA430B1DDCE6F5387EFC1AD6182242063CDE6DDB7B75A0C00640B515819E65C50
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\wlm7n14\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	18144
Entropy (8bit):	7.937783572332254
Encrypted:	false
SSDEEP:	384:MnAOlQtPloTnMWbF2fQLQVTDtNY5jaMDHe9vwk5nOW5S2xJ4y:MnstPSN52frDHEjaCHe9vwkpeaJz
MD5:	F302CB1EB2BC37B9C3BB40C020BB7F96
SHA1:	B444387030E740579ADECA65623CE38600CCFD6C
SHA-256:	98670E1CF58F854443FA10633E7DA6C10B027FCD08E42E46907144BBC95EB17F
SHA-512:	B9BD566EC61542DE95E3FCB1FDFB863AA34640D6E16636B8127664C4A48BB511D2D8DC3DEE93EEE56E1AB1D62DCF2D48F8A850AC5F7ED6D3E24277C2CC7C171
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./.c.o.m.p.a.n.y./.a.s.s.e.t.s./.i.m.a.g.e.s./.l.o.g.o...p.n.g.n....PNG.....IHDR.....PLTE.....IDATx....r.@...c..6..L5%....Sm....zR.DGf.2#Y?..f..+...D".H$..D"....6..gm..b...@.....&.YG.e.N7.e.s.*...u.?-k..a/mt5..BV..r?.,....`...!.,...CU7..*.z.ef.!....^t..J\..E Y.p....."..S...V,...rw.K8....f.hOS..7.Uj~g..Mh.L...Y'|X...7.....\|..Z.....u.5%wS...f...J.....Yz..:..a3..b.aN.....: .f.Y1..`.,..j?.1...<dY.Pf.W...R0YS.....`{..?^..L*59.....\d^a#..l%..M..i`4M..b:.5...I$.&.^.....c.....Y.E.....V.aa..3..Ev..#W.9l...z..n.W.:..F.-....U..m.....g..u.w

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\amp-auto-lightbox-0.1[1].js	
SSDEEP:	96:9sZVrZkAwc4nrhUAj87jdjEJaDv3/p3+e6HXFLE58M:o7wc4nrq1jEKv3xr6HNE57
MD5:	7012ACC9D81E0AF71AC19EDFD85AAF87
SHA1:	56D9539EF3E0D57B978F52279142273A851D7FD7
SHA-256:	C9029AE9DCAF52BD278EBC3A87DE7340F47F30507809 94EFCBBFF06A7FD62E6C
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\3Y2ADQKS\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:	9FDBC4AE128C0312BB5E7E87004A0D53DCE7B8B88CB2D0C87B43DED44C122981274154316FE049EF536E589655E930E8A6DAF02ABC18927A86BB65D8F070B3E5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.ampproject.org/v0/amp-mustache-0.2.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&&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");})()}aa(this);"function"===typeof Symbol&&Symbol("x");var ca="function"==typeof Object.create?Object.create:function(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=("string"==typ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 226 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	3331
Entropy (8bit):	7.927896166439245
Encrypted:	false
SSDEEP:	96:zHjOKn3csE3x5liVsCo4GcPIZpV6x5cge8oo9:zDOK3zE3x5TCwcP4LQNeq
MD5:	EF884BDEDEF280DF97A4C5604058D8DB
SHA1:	6F04244B51AD2409659E267D308B97E09CE9062B
SHA-256:	825DE044D5AC6442A094FF95099F9F67E9249A8110A2FBD57128285776632ADB
SHA-512:	A083381C53070B65B3B8A7A7293D5D2674D2F6EC69C0E19748823D3FDD6F527E8D3D31D311CCEF8E26FC531770F101CDAF95F23ECC990DB405B5EF48B0C91B2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://avenirhomes.com/Paymentadvice/new/s/files/logo.png
Preview:	.PNG.....IHDR.....0.....sRGB.....IDATx..=w....G.z..L.4fN.k\dS..._`.....r...~.F..e._.RZ.0.K.\..CB...1.{qq/..^|.G..o.....?....Or.....y~....]..V.a.mM...M.\k*H..@B`s.$"n...)!.@"b#4. !.9...7.u...hD ....T.....:EJ.4"..X.....<\|.pgkk+....>~.....pju1i"b.J.&!.!...=T....k..D7.....O.<.?}...../..(.`0..!.C..'.?..e..~.....l6...._.x1rmR...$|E...l.WKDH...f..... ...Y.0R....>...{...-..o.....,...E../....._....eM.Q....@Q...w sp5.9..l.W)...Pq... .]..B..).../M.G.g....].V...5$<.....Eb.9.....>LYAk.Z.k..b..]N%>}4a....4!S...t..d..<.8AH+.../r...._...!qt.:q..fR.:..KW..._...T...5..>.0!.hq.rbND\...XR.,2.uX..Q.b...wQ.....g..X...F...~.....ikZE...UA....V.I!..]..Mm..R.....~k.VC.n..V.*B#W...\..yI.3.....2.....6c....2J....,g..5O1.s.4V2.....f..K..Obf\....;.w...\|.F>F>6_z..P.dU<.wVV.....?.q.?&.....O.>....l.S.upp....59.C_.....fJ.M.={v,.....]Y_....n.?UF....v<.$..AD...p.....:$r =p...C.k.3....n.v..~.TGd!...l.W...s..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\new[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	250
Entropy (8bit):	5.061482374747449

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\new[1].htm	
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwol6hEr6VX16hu9nPFy7PV+KqD:J0+ox0RJWWPFIwT
MD5:	127557FE426256EE010F61BDB2B04637
SHA1:	9F849010DCC1B67447E6B3609082C759CB7A2049
SHA-256:	4E4E2E98483A46ACDD38B7741056665A7FD89422D0A84B2D36BBA277065565F8
SHA-512:	4DF297F5D372A3B9C0BD30C9F550A78F1C98FA837E90D0BC7B0ECDDF139DFFBC2D2F22AE6784AD68FB056C84667953F5150AC5BB3FAD732DAAA6BE01419A7D0
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\Microsoft\Windows\INetCache\IE\9QTQHWWN\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:	4535AB538871854EC6B504F0E3AEFA6007921FACBA831648542B31D59A514A71F6DEDF86967A5CFD1C7A77B3A0E8F1744DAFEC287D4E1CDFA8988EFB47C5E09
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\9QTQHWWN\background5-h_kjvcr6x2[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, 1024x1001, frames 3
Category:	downloaded
Size (bytes):	36790
Entropy (8bit):	7.283615433782065
Encrypted:	false
SSDEEP:	768:65v5g2jMNr69mWfNkNd5gicARaHLmAA6WVLTOzG:6J5g2krHWfSNgicARX7VPOzG
MD5:	B4364BE41A18979385721E50FCEDA570
SHA1:	641AE951CECD5C1E0A64C9BF7457A27E751CF5F2
SHA-256:	B2AB9B6B07F882C35815E25A2BA62C9DEDDFA5B1BEC18626D8754AA86BC9BA0C
SHA-512:	6265616325E5E26BDF6D6A789FF948E4F0C49E160A3EB07E4FFDF8C0F70536C8A3E90E49B91540C10E46E16E1E9C30A84B6961554AB418A8098558FAD355E21E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://r.8b.io/217251/images/background5-h_kjvcr6x2.jpg
Preview:	......JFIF.....C..... ....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....F.....!.1..AQ..Saqr....."2R....3Tb..#6Bs.$45C.7ct.....".....Q!R."1A2.....?..p..J*KsGJ-c.*.7....\r...X7.c. EV.....P..!....7.eV..F]h.....R.0..sh.....F\...../[..*q}.D.`..J1XH...)<6..j0...r..$iR.js.#Z-sF]X..5..G..W.Gq..h.*..Op5v.o,.P..%.D.A..y$3.....I,# .....EK.).(7.....M,.B..6.....Q..d.....,.,No..9..o.5..N.nb..Irl.]2..&.m..En..Wu.O,.7..K,.z|.."z}E.00.....rxl..t..nv[Y:r._.T...u...z....Y..SKi. #..E..W.....S.....$.L..R..I..*JO-....E....-.Kv.....W{|.M..K}EIe.-\".ZC.=....j7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	198
Entropy (8bit):	5.141302562856387
Encrypted:	false
SSDEEP:	3:0SYWFFWlIYCtj2G3FMRI5XwDKLRIHDfFRWdFTfqzrZqcd9GkdT3ENGlGUOmA13bt:0IFFni+56ZRWHTizlpdBIGh0AmuNin
MD5:	C87C1DEA05879100FDCD035896CD5186

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\css[1].css	
SHA1:	69D3FDBFD79ED542D35346F93A4D74F2E62EB97E
SHA-256:	87D7DE69590AD53F5749E32D2CD3DB331FB6A20F2E2E426C9E3F3D30A62DA407
SHA-512:	3BAA8F08660AC4F14E7F2DF33E7B6CAA553DDFAFEE279A9164B4F6372C1BBCDB80899567CEC065CF4ACD2675EB611092194B622D286C31589CBD202E53B21A8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Didact+Gothic&subset=cyrillic
Preview:	@font-face {. font-family: 'Didact Gothic';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/didactgothic/v14/ahcfv8qz1zt6hCC5G4F_P4ASlU-YoA.woff) format('woff');.}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\logo[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):	2158
Entropy (8bit):	7.661420652897611
Encrypted:	false
SSDEEP:	48:WVOkQtRUF3r8JpnTIR4H5yUqqgqVD1LEkIm33jNMNM:HkQtRu3rynTQ82qgqVD1LEkIAN+M
MD5:	322CF2389ECB328DF2E573945F40F58E
SHA1:	6FBE4C22EE928C3B7B28212B1086771E67D8F4A2
SHA-256:	16E155AB1ACBA70A9DD91D52B3238BC124D33023AD8C580CA8D9C8CE20BC8DAD
SHA-512:	FE1639DEF6FFAEF5479EB755603F9940F5567CEC65F96776AE3F44D0B5EEDAA41B64F52E303CB901207DF6572FF42F837F6FB7DB3F2C0B263DE41C7BDD5D580D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://app.8b.io/app/themes/webamp/projects/company/assets/images/logo.png
Preview:	.PNG.....IHDR.....PLTE......"....JtRNS.+:.....6..QB....z....U"...^&...if.....b....pMJ1....Fw.>4....Z...k....L.%?....IDATx....r.@...c..6..L5%....Sm....zR.DGf.2#Y?..f..+...D".H$..D"....6..gm..b...@.....&.YG.e.N7.e.s.*...u.?-k..a/mt5..BV...r?.,...`...!.,...CU7..*.z.ef.!....^t..J\..E Y.p....."..S...V,...rw.K8....f.hOS..7.Uj~g..Mh.L...Y'\|X...7.....\|..Z.....u.5%wS...f...J.....Yz..:..a3..b.aN.....: .f.Y1..`.,..j?.1...<dY.Pf.W...R0YS.....`{..?^..L*59.....\d^a#..l%..M..i`4M..b:.5...I$.&.^.....c.....Y.E.....V.aa..3..Ev..#W.9l...z..n.W.:..F.-....U..m.....g..u.w.xy..*..l..l...*...)d.....s&l..fY0c].U.*....._...`.[.I.....`WS.3..8..z..Z....1I..=8...x.r..r..v=..#.u.(V.,..V.8.....!...k.....c.....U.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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
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\G62TDH9B\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	188
Entropy (8bit):	5.119072399147113
Encrypted:	false
SSDEEP:	3:0SYWFFWlIYCiF15RI5XwDKLRIHDfFTo/TfqzrZqcdJ2dTi8EuRlGlL+9JYARNin:0IFFm15+56ZTo/Tizlpd0celdJNin
MD5:	4CFC4658F748E1FC67D2EA27F9B3692F
SHA1:	82C520D112F48E337E99DF00067BFAA75D0F9CA2
SHA-256:	ABC5A61E85F95E54C925FE9589099AD680912480E7C97052AF0496CBC6D111B8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\css[1].css	
SHA-512:	BFDDD6D4E0225EF444FD621B2CC20D022C02E30AB3E8AACA197E8F6304AA95E8C253815C6DC329646E5F39BBAF0B953A0667B296D15AB6BCECE788D1BFDC6 14B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Open+Sans:600
Preview:	@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 600;. src: url(https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UNirkOUuhv.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\footer-logo-min-150x141[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 150 x 141, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	15690
Entropy (8bit):	7.968566181279536
Encrypted:	false
SSDEEP:	384:OnMWbF2fQLQVTDtNY5jaMDHe9vwk5nOW5S2xJ4c:S52frDHEjaCHe9vwkpeaJZ
MD5:	05D66574B8DA470B54D565E9966A21EA
SHA1:	70D26FF8A98F9807250D0C189CC37293B11AD73B
SHA-256:	10611432F3F17898E840C201FD7A97FCD96847CE4103C8D46BB8651ED2071799
SHA-512:	B529FC7B447DA462619568A63AA922947901B4CB06549E78C1666E6C0060AE1A044D4AB30293840E9FBCEAE936DEB58373C47C0028D55E240A1BC5B39055191C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://avenirhomes.com/wp-content/uploads/2020/03/footer-logo-min-150x141.png
Preview:	.PNG.....IHDR.....U.....pHYs.....+.... .IDATx..yt../..[....B....$.E.NI.E.,....&.q.+...KO.;=...y.....3}:.|^....NZ...#...eY.im.(q.IQ"ER\...@.P....n".E.I...Ea.[..~u.w.....j..TU..u =. ...*).....0d.../....r.,w.f.S%.s.<...M.{.N%.....\...i...1.~=.(cd.S....{JYh.....w...\.....K,..[....a.....l...{.&.ec...J.&.....M..w.O.....3!.hT.....2.1.)B .....D*.M..!l.y.O..K./.../..U'.s.Xb.. .....(.W..?f..3.. `..|@.h.....F.`....[.k#.F..^....M..`..]P...6.....b.....c..`TjC.!.$Xm6.x.Z_[g.[....d.hb..\m. ...e...]..!.....,_...#.o.y3G.P{.m...W.j.^`....`.....`.....&.`OR. 9..s.&..B.$.`.....J ../.u_.+.i..<RT..[..X...q!k.{7...`..$.l:E=...m...9.I..p_... ...s.]ZYI.....C,..[!@0....D..(....j.;>z.K.4.o.....n...'6W:..2...D..J.....Q@.!.j...a.Hm.h.(...[J.7.....4.<.[q..U$...M.....*..+....S4M.). *c.8..R...U.)..<g0I.....K.I...5....?..dNN..qeI..F1....O4M.%.L..FM2r.".V...^.....P@. .c+.....]'.:.g.{.I.....-.#.3@.T".^S4....D.....,..Z..s/..6.X.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\s[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:	dropped
Size (bytes):	17394
Entropy (8bit):	3.324079896074607
Encrypted:	false
SSDEEP:	384:rKp84GZw7WZ1v5jBi1FnJICqWqjbTSIHaTPqsHkEiroLOweZnZq5fy6CJP:r+WfhjDUS
MD5:	474A9980C4D204E7D4B593832B226BEA
SHA1:	DBDB72D920A55C1AB76FDA122271C9986C8F9389
SHA-256:	163589FCFF3F5D67836D8DF3EC13D11E561E93C25B9679D3BA92B98F9D34EABF
SHA-512:	DFC58C88418F96A98009D0FF7BF626C5679A20BD63B0FE20C7B792D6EB95CD26C3206978DAB6DE70DA6CDDEAA612663C3972BAB5930DC84ADF1820F407A5EI 14
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_6, Description: Yara detected HtmlPhish_6, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\s[1].htm, Author: Joe Security
Reputation:	low
Preview:	..<script type="text/javascript">....document.write(unescape('%3c%6d%65%74%61%20%63%68%61%72%73%65%74%3d%22%55%54%46%2d%38%22%20%6 e%61%6d%65%3d%22%76%69%65%77%70%6f%72%74%22%20%63%6f%6e%74%65%6e%74%3d%22%77%69%64%74%68%3d%64%65%76%69%63%65% 2d%77%69%64%74%68%2c%20%69%6e%69%74%69%61%6c%2d%73%63%61%6c%65%3d%31%2e%30%2c%20%6d%61%78%69%6d%75%6d%2d%73%63 %61%6c%65%3d%31%2e%30%2c%20%6d%69%6e%69%6d%75%6d%2d%73%63%61%6c%65%3d%31%2e%30%2c%20%75%73%65%72%2d%73%63%61%6 c%61%62%6c%65%3d%6e%6f%22%3e%0d%0a%09%3c%74%69%74%6c%65%3e%56%61%6c%69%64%61%74%69%6f%6e%3c%2f%74%69%74%6c%65% 3e%0d%0a%09%3c%6c%69%6e%6b%20%72%65%6c%3d%22%73%74%79%6c%65%73%68%65%65%74%20%70%72%65%66%65%74%63%68%22%20%68 %72%65%66%3d%22%68%74%74%70%73%3a%2f%2f%66%6f%6e%74%73%2e%67%6f%6f%67%6c%65%61%70%69%73%2e%63%6f%6d%2f%63%73%7 3%3f%66%61%6d%69%6c%79%3d%4f%70%65%6e%2b%53%61%6e%73%3a%36%30%30%22%3e%0d%0a%09%3c%6c%69%6e%6b%20%72%65%6c%3d% 22%73%74%79%6c%65%73%68%65%65%74%22%20%68%72%65%66%3d%22%2e%2f%66%69%6c%65%73%2f%63%73%73%2e%63%73%7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\v0[1].js	
SHA-512:	EE62BB3330B64D944F522E5513CC08979661FF702FFCD02AE35795B9889D57973966190E735074BA2FB36A7572ACA5495BF0F70C36738BE8793E313B9FBEDCA1
Malicious:	false
Reputation:	low
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\OTUW0Q90\T08OXF6I.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	36364
Entropy (8bit):	5.1594430905615924
Encrypted:	false
SSDEEP:	768:EF0DlkvJOdKkUGfkxXjwWSwOsZ4aGtLuB9jlnija:BDlCOdKk7IkWSwOsZ4a0LuB9jl/
MD5:	492287B593524044D883ECE3826752B8
SHA1:	F7020794B1C553681450215632A0D2AB721B8893
SHA-256:	51AAF2449505F3EB946B835DCCC5704F2C7E694AF75F1BFCCBA6BA5F1D5FEFC1
SHA-512:	4C0FFF51FA7128AA68BB32D9FAF4C96A41A1099EE5F547B62B48AA055A1C9109B4D967BA779E1611B6B18C579BC623D0197419424043EF74176517A4FDEAE41A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://217251.8b.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-Compatible" 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-scale=1">. <link rel="shortcut icon" href="https://app.8b.io/app/themes/webamp/projects/company/assets/images/logo.png" type="image/x-icon">. <meta name="description" content="">. <title>Remittance Advice </title>. .<link rel="canonical" href="https://217251.8b.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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\ahcfv8qz1zt6hCC5G4F_P4ASlU-YoA[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 27548, version 1.1
Category:	downloaded
Size (bytes):	27548
Entropy (8bit):	7.981671835368044
Encrypted:	false
SSDEEP:	768:EBs3Uu5TgaaufAJJhUnF86+MmJw6kz/On/zD7S:TNBgnu4JJhUnWbMew7mnO
MD5:	C966ADD03B2623F6364DC54C08FFA17B
SHA1:	59BFF56121286E72E83B6B48BC817AFE497018BC
SHA-256:	9C3F598D4581DCD35FC68CE6F4A435AA64B56734FA8164AEFF4AB38F26935A64
SHA-512:	8EAC7918645C494AD4D581802AECE08037E228B46F967954721076B987184E1F8E621CC1F861D467355A574CDDDF2E8BA3B7B4D912056CF8127F635F3047AFC8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/didactgothic/v14/ahcfv8qz1zt6hCC5G4F_P4ASlU-YoA.woff
Preview:	wOFF.....k.....GDEF.....GGPOS.....Zd...GSUB.....2...l|b..OS/2.....O...`f..cmap...(...l...L.pp@cvt ...t...U.....SE.fpgm.....vd.|gasp.....glyf.....Kw....`.t.head..`...6...6..L.hhea..`.... ...$...phmtx..`.....z.s!.loca..c.....maxp..ft... ... ...!name..f.....-;D.post..g....u.....prep..j.....x.....s..$..$ . .....P.. .." ..{4.....@."yJ.e...^.....R..]z.g.C.#.>a.3.`.+.Q.e.{.~..g.~Up.....R.V...?E$.x..g...Lh]x....$Y...s..YU....v..6.m.m.c.m6.....c_.x.o.....9'...l.\...O...|.L...4...:6.i'|.L.m..`..1....}%..V..J..4V6..Ok....45.D....U.u]].|.>M...~...S....I.{.....fE...._Y.....(.|J.D....1....)..X..vr.8..N.wy.....-.m.J..N2.n...!$6.F...)...#.bd=j...#FE.\|..a..V.....]C....(h<.x.w.F5.d..l?...D..4kc...Nb.....x....e..nWf...r{udm`.G.....t<.q....6ob[..s..f..lg.&...8.....tE...v.8.....s.'4..0v!&!.@FN.2...d,....&2..l.fl.La*...f2...e've7vg..d...H..$N.,>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\amp-loader-0.1[1].js	
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\OTUW0Q90\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	15526
Entropy (8bit):	5.721275823828831
Encrypted:	false
SSDEEP:	384:Ox5T7PuUyxgg2Ctjo/kohz2YDDD1fSCRdVl37Sm9:OjT7GDxgg2GE/kohz2YDDD1fS8oh9
MD5:	63DF83784CADD3A339B776520600C21A
SHA1:	69BB829612F3E3CB2F521323945C9284A2B0DCDE
SHA-256:	2EE69AEF3AFB10B368BDE9FEA7E97CC75C030C890E3D2B8DC4AD19D498234DBF
SHA-512:	FC1C4F31A0817471D1D2CA8ADEA7F3C39B67B0EA688CC58EB4F6C68F5F6558E236B9D3D2D8BA95EE296CFBF3C0197CE54DFECADBCCCE1B7497542FEE2914 1D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://avenirhomes.com/Paymentadvice/new/s/files/css.css
Preview:	html {...line-height: 1.15;...-ms-text-size-adjust: 100%;...-webkit-text-size-adjust: 100%..}..body {...height: 100%;...margin: 0..}..article, aside, footer, header, nav, section { ...display: block..}..h1 {...font-size: 2em;...margin: .67em 0..}..figcaption, figure, main {...display: block..}..figure {...margin: 1em 40px..}..hr {...box-sizing: content-box;.. .height: 0;...overflow: visible..}..pre {...font-family: monospace, monospace;...font-size: 1em..}..a {...background-color: transparent;...-webkit-text-decoration-skip: objects..}. .abbr[title] {...border-bottom: none;...text-decoration: underline;...text-decoration: underline dotted..}..b, strong {...font-weight: inherit..}..b, strong {...font-weight: bolder ..}..code, kbd, samp {...font-family: monospace, monospace;...font-size: 1em..}..dfn {...font-style: italic..}..mark {...background-color: #ff0;...color: #000..}..small {...font-size: 80%..}..sub, sup {...font-size: 75%;...line-height: 0;...position: relative;...vertical-align: b

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\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://avenirhomes.com/Paymentadvice/new/s/files/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\Temp\datB730.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:WRBLIloQuHfRh4pi6sfPGnDFs
MD5:	10600F6B3D9C9BE2D2B2CE58D2C6508B
SHA1:	421CA4369738433E33348785FE776A0C839605D5
SHA-256:	29B7A9358ABDC68C51DB5A5AF4A4F4E2E041A67527ADEE2366B1F84F116FE9A5

C:\Users\user\AppData\Local\Temp\datB730.tmp	
SHA-512:	B6C04F3068EB7DAC8F782BDED0FE815B4FE5A9BECCF0B561D6CEAEAA7365919A39710B2D1AD58D252330476AA836629B3C62C84FABFA6DC4BCF1C8F055D66C1C
Malicious:	false
Reputation:	low
Preview:	wOFF.....aH.....OS/2...D...H...`1Wp.cmap.....l...b..ocvt ..... ...*....fpgm.....Y...gasp.....glyf.....Whead.....2...6.tJ.hhea.....$....hmtx.....loca.....X.hmaxp...,..... .y..name...L.....Mpost...D..... .Q.}prep...X.....x...x.c`aog.....:....Q.B3_dHc..`e.bdb... .`@..`.....,9.\|...V...)00...C..x.c```f.`..F.....\|... .....\..K..n.,..g`@.\|.8"vYl.....p...0.....x.c.b.e(`h`X.....x.....x.]..N.@..s$..'@:!.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.[7'...`.^...&....{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\~DF50AF0D1DD5FFBE3A.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	45823
Entropy (8bit):	0.713563471772699
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+V75orT/fKvoZLvTBZLv/ZLvdQSZLvtZLvbZLvoZLvX:kBqoxKAuqR+V75orT/yv4TzNdV3h4
MD5:	60F18F6D736E3D709884D9D13EDF9902
SHA1:	CC3B736FF05385DC58E5841F0AC26EA22C2ECB75
SHA-256:	5C42E04344A6B794AA5721398FD0D3C439F8EC2C813C0DA871538DF5DEF47373
SHA-512:	C12105217F70B29B046BAFF92ACCCE9DFCB29380C5FB3A96BD0232D070236389C46247AF9D09BCEF8A39A489E6452C81584F0E68E0AFB54852F05FA461661E04
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFAE0AF0D2B2A94533.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47685053801265154
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loE9loU9lWboILzUPhL:kBqoIv585
MD5:	EB1D53448018AD09191F7B52B90509FF
SHA1:	29BCE190CBB6286165874F450C64CBAB691591E0
SHA-256:	8F20443340C7A848ED8DEA72874C660DBA4736150661FAED36B7E0CA7D0156E1
SHA-512:	513C34449EABFB2A93F96983A1E44AF8699DE93EF5D8E1E046D4FAD6EF97D22610006FDF793A24B6F71A4B8DEE63BCC2D9598D35A4FA82B604F142BEBC48AEC9
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFCBDCB001D3AD68B8.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.37303732942765133
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAmnFh/2xa:kBqoxxJhHWSVSEabmnFh/Qa
MD5:	FA16C4106B7E29FCF2DA416C32EE014A
SHA1:	B789981D4DC489D510A3F3BA5D39E2E72AD74886
SHA-256:	48E0EB597856E76D8C275F76A06E2C7778985618CC7B13BECD59D3DCA416244B
SHA-512:	22CF6834F4A222B0794D47E66C1C51E5115CD5DBBAF768EFF59DC213A663125B0A5EA6CF611FAFD8662322AB140B4F7A07B30A4EB6C9452A60CD05EB2B36528D
Malicious:	false
Reputation:	low

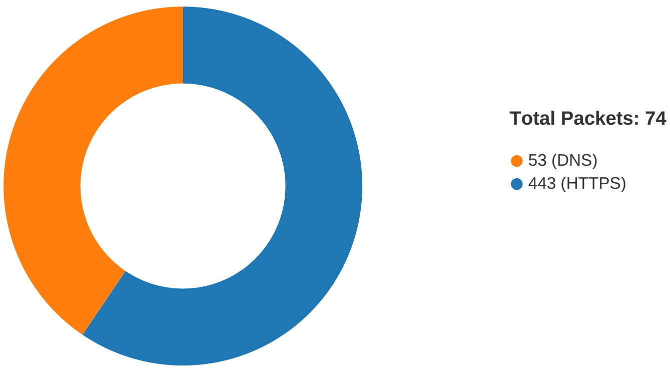
C:\Users\user\AppData\Local\Temp\~DFCBDCB001D3AD68B8.TMP	
Preview:	...............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

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 21:34:34.819166899 CET	49721	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:34.820281982 CET	49722	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:34.947046995 CET	443	49721	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:34.947227955 CET	49721	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:34.951668024 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:34.951865911 CET	49722	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:34.955068111 CET	49721	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:34.955121994 CET	49722	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.081232071 CET	443	49721	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.081260920 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.082283974 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.082310915 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.082325935 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.082341909 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.082425117 CET	49722	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.082464933 CET	49722	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.083362103 CET	443	49721	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.083388090 CET	443	49721	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.083405018 CET	443	49721	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.083424091 CET	443	49721	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.083488941 CET	49721	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.083559990 CET	49721	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.124385118 CET	49722	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.124588013 CET	49721	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.133130074 CET	49722	443	192.168.2.6	52.7.227.232

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:34:35.133289099 CET	49721	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.133375883 CET	49722	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.250860929 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.250891924 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.250987053 CET	49722	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.251079082 CET	443	49721	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.251096010 CET	443	49721	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.251151085 CET	49721	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.251214981 CET	49721	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.251862049 CET	49722	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.252495050 CET	49721	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.259356022 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.259387970 CET	443	49721	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.259473085 CET	49722	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.259738922 CET	49721	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.295156956 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.295191050 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.295202971 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.295219898 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.295237064 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.295257092 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.295339108 CET	49722	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.295392990 CET	49722	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.295437098 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.295490980 CET	49722	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.377099037 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.377125978 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.377144098 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.377160072 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.377213955 CET	49722	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.377268076 CET	49722	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.385601044 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.385632038 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.385714054 CET	49722	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.385746002 CET	49722	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.421379089 CET	443	49721	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.421420097 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.421437025 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.421453953 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.421472073 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.421489954 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.421506882 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.421539068 CET	49722	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.421602964 CET	49722	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.421910048 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.421931028 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.421947956 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.421964884 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.421972036 CET	49722	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.421986103 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.422003984 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.422022104 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.422035933 CET	49722	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.422039986 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.422089100 CET	49722	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.503308058 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.503335953 CET	443	49722	52.7.227.232	192.168.2.6
Jan 13, 2021 21:34:35.503489971 CET	49722	443	192.168.2.6	52.7.227.232
Jan 13, 2021 21:34:35.656692028 CET	49726	443	192.168.2.6	108.177.119.132
Jan 13, 2021 21:34:35.657243967 CET	49727	443	192.168.2.6	108.177.119.132
Jan 13, 2021 21:34:35.657435894 CET	49728	443	192.168.2.6	108.177.119.132
Jan 13, 2021 21:34:35.705080986 CET	443	49727	108.177.119.132	192.168.2.6
Jan 13, 2021 21:34:35.705154896 CET	443	49726	108.177.119.132	192.168.2.6
Jan 13, 2021 21:34:35.705226898 CET	49727	443	192.168.2.6	108.177.119.132

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:34:35.705265045 CET	49726	443	192.168.2.6	108.177.119.132
Jan 13, 2021 21:34:35.705324888 CET	443	49728	108.177.119.132	192.168.2.6
Jan 13, 2021 21:34:35.705400944 CET	49728	443	192.168.2.6	108.177.119.132
Jan 13, 2021 21:34:35.709696054 CET	49727	443	192.168.2.6	108.177.119.132
Jan 13, 2021 21:34:35.709975958 CET	49726	443	192.168.2.6	108.177.119.132
Jan 13, 2021 21:34:35.710243940 CET	49728	443	192.168.2.6	108.177.119.132
Jan 13, 2021 21:34:35.757920027 CET	443	49727	108.177.119.132	192.168.2.6
Jan 13, 2021 21:34:35.757962942 CET	443	49727	108.177.119.132	192.168.2.6
Jan 13, 2021 21:34:35.757977009 CET	443	49727	108.177.119.132	192.168.2.6
Jan 13, 2021 21:34:35.757989883 CET	443	49727	108.177.119.132	192.168.2.6
Jan 13, 2021 21:34:35.758007050 CET	443	49727	108.177.119.132	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:34:28.897046089 CET	60261	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:34:28.944883108 CET	53	60261	8.8.8.8	192.168.2.6
Jan 13, 2021 21:34:30.742163897 CET	56061	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:34:30.801484108 CET	53	56061	8.8.8.8	192.168.2.6
Jan 13, 2021 21:34:31.986736059 CET	58336	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:34:32.050944090 CET	53	58336	8.8.8.8	192.168.2.6
Jan 13, 2021 21:34:33.353482962 CET	53781	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:34:33.412729025 CET	53	53781	8.8.8.8	192.168.2.6
Jan 13, 2021 21:34:34.700258970 CET	54064	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:34:34.805576086 CET	53	54064	8.8.8.8	192.168.2.6
Jan 13, 2021 21:34:35.037133932 CET	52811	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:34:35.087826014 CET	53	52811	8.8.8.8	192.168.2.6
Jan 13, 2021 21:34:35.421118975 CET	55299	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:34:35.479854107 CET	53	55299	8.8.8.8	192.168.2.6
Jan 13, 2021 21:34:35.584480047 CET	63745	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:34:35.652131081 CET	53	63745	8.8.8.8	192.168.2.6
Jan 13, 2021 21:34:35.702671051 CET	50055	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:34:35.763896942 CET	53	50055	8.8.8.8	192.168.2.6
Jan 13, 2021 21:34:37.623502970 CET	61374	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:34:37.680561066 CET	50339	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:34:37.726142883 CET	53	61374	8.8.8.8	192.168.2.6
Jan 13, 2021 21:34:37.863241911 CET	53	50339	8.8.8.8	192.168.2.6
Jan 13, 2021 21:34:39.524734974 CET	63307	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:34:39.573853970 CET	53	63307	8.8.8.8	192.168.2.6
Jan 13, 2021 21:34:40.476066113 CET	49694	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:34:40.526669979 CET	53	49694	8.8.8.8	192.168.2.6
Jan 13, 2021 21:34:41.668816090 CET	54982	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:34:41.728396893 CET	53	54982	8.8.8.8	192.168.2.6
Jan 13, 2021 21:34:42.940119028 CET	50010	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:34:42.988774061 CET	53	50010	8.8.8.8	192.168.2.6
Jan 13, 2021 21:34:44.737037897 CET	63718	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:34:44.787642002 CET	53	63718	8.8.8.8	192.168.2.6
Jan 13, 2021 21:34:46.849057913 CET	62116	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:34:46.897053003 CET	53	62116	8.8.8.8	192.168.2.6
Jan 13, 2021 21:34:47.813404083 CET	63816	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:34:47.864233971 CET	53	63816	8.8.8.8	192.168.2.6
Jan 13, 2021 21:34:51.493727922 CET	55014	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:34:51.553679943 CET	53	55014	8.8.8.8	192.168.2.6
Jan 13, 2021 21:34:53.850383997 CET	62208	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:34:53.998867035 CET	53	62208	8.8.8.8	192.168.2.6
Jan 13, 2021 21:34:56.568605900 CET	57574	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:34:56.616635084 CET	53	57574	8.8.8.8	192.168.2.6
Jan 13, 2021 21:34:59.408788919 CET	51818	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:34:59.468884945 CET	53	51818	8.8.8.8	192.168.2.6
Jan 13, 2021 21:35:03.293885946 CET	56628	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:35:03.350502014 CET	53	56628	8.8.8.8	192.168.2.6
Jan 13, 2021 21:35:04.064822912 CET	60778	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:35:04.113656998 CET	53	60778	8.8.8.8	192.168.2.6
Jan 13, 2021 21:35:04.306579113 CET	56628	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:35:04.362656116 CET	53	56628	8.8.8.8	192.168.2.6
Jan 13, 2021 21:35:05.072304010 CET	60778	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:35:05.122724056 CET	53	60778	8.8.8.8	192.168.2.6
Jan 13, 2021 21:35:05.324374914 CET	56628	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:35:05.372225046 CET	53	56628	8.8.8.8	192.168.2.6
Jan 13, 2021 21:35:06.087867022 CET	60778	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:35:06.140758991 CET	53	60778	8.8.8.8	192.168.2.6
Jan 13, 2021 21:35:07.344172955 CET	56628	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:35:07.391995907 CET	53	56628	8.8.8.8	192.168.2.6
Jan 13, 2021 21:35:08.491204977 CET	60778	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:35:08.538923979 CET	53	60778	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 21:34:34.700258970 CET	192.168.2.6	8.8.8.8	0xa574	Standard query (0)	217251.8b.io	A (IP address)	IN (0x0001)
Jan 13, 2021 21:34:35.584480047 CET	192.168.2.6	8.8.8.8	0x711d	Standard query (0)	cdn.ampproject.org	A (IP address)	IN (0x0001)
Jan 13, 2021 21:34:37.623502970 CET	192.168.2.6	8.8.8.8	0x70d7	Standard query (0)	app.8b.io	A (IP address)	IN (0x0001)
Jan 13, 2021 21:34:37.680561066 CET	192.168.2.6	8.8.8.8	0x1593	Standard query (0)	r.8b.io	A (IP address)	IN (0x0001)
Jan 13, 2021 21:34:51.493727922 CET	192.168.2.6	8.8.8.8	0xbde6	Standard query (0)	app.8b.io	A (IP address)	IN (0x0001)
Jan 13, 2021 21:34:53.850383997 CET	192.168.2.6	8.8.8.8	0x25ac	Standard query (0)	avenirhomes.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 21:34:34.805576086 CET	8.8.8.8	192.168.2.6	0xa574	No error (0)	217251.8b.io	proxy-8b-io-1762796164.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:34:34.805576086 CET	8.8.8.8	192.168.2.6	0xa574	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 21:34:34.805576086 CET	8.8.8.8	192.168.2.6	0xa574	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 21:34:35.652131081 CET	8.8.8.8	192.168.2.6	0x711d	No error (0)	cdn.ampproject.org	cdn-content.ampproject.org		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:34:35.652131081 CET	8.8.8.8	192.168.2.6	0x711d	No error (0)	cdn-content.ampproject.org		108.177.119.132	A (IP address)	IN (0x0001)
Jan 13, 2021 21:34:37.726142883 CET	8.8.8.8	192.168.2.6	0x70d7	No error (0)	app.8b.io		104.24.104.39	A (IP address)	IN (0x0001)
Jan 13, 2021 21:34:37.726142883 CET	8.8.8.8	192.168.2.6	0x70d7	No error (0)	app.8b.io		104.24.105.39	A (IP address)	IN (0x0001)
Jan 13, 2021 21:34:37.726142883 CET	8.8.8.8	192.168.2.6	0x70d7	No error (0)	app.8b.io		172.67.215.39	A (IP address)	IN (0x0001)
Jan 13, 2021 21:34:37.863241911 CET	8.8.8.8	192.168.2.6	0x1593	No error (0)	r.8b.io		104.24.105.39	A (IP address)	IN (0x0001)
Jan 13, 2021 21:34:37.863241911 CET	8.8.8.8	192.168.2.6	0x1593	No error (0)	r.8b.io		104.24.104.39	A (IP address)	IN (0x0001)
Jan 13, 2021 21:34:37.863241911 CET	8.8.8.8	192.168.2.6	0x1593	No error (0)	r.8b.io		172.67.215.39	A (IP address)	IN (0x0001)
Jan 13, 2021 21:34:51.553679943 CET	8.8.8.8	192.168.2.6	0xbde6	No error (0)	app.8b.io		104.24.104.39	A (IP address)	IN (0x0001)
Jan 13, 2021 21:34:51.553679943 CET	8.8.8.8	192.168.2.6	0xbde6	No error (0)	app.8b.io		104.24.105.39	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 21:34:51.553679943 CET	8.8.8.8	192.168.2.6	0xbde6	No error (0)	app.8b.io		172.67.215.39	A (IP address)	IN (0x0001)
Jan 13, 2021 21:34:53.998867035 CET	8.8.8.8	192.168.2.6	0x25ac	No error (0)	avenirhomes.com		51.79.98.105	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 21:34:35.082341909 CET	52.7.227.232	443	192.168.2.6	49722	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 21:34:35.083424091 CET	52.7.227.232	443	192.168.2.6	49721	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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 21:34:35.758029938 CET	108.177.119.132	443	192.168.2.6	49727	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 21:34:35.758387089 CET	108.177.119.132	443	192.168.2.6	49726	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 21:34:35.758533955 CET	108.177.119.132	443	192.168.2.6	49728	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 21:34:37.869862080 CET	104.24.104.39	443	192.168.2.6	49731	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 21:34:37.873838902 CET	104.24.104.39	443	192.168.2.6	49732	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		

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 21:34:37.975450039 CET	104.24.105.39	443	192.168.2.6	49733	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 21:34:38.001187086 CET	104.24.105.39	443	192.168.2.6	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	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 21:34:51.667541027 CET	104.24.104.39	443	192.168.2.6	49742	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		
Jan 13, 2021 21:34:54.281721115 CET	51.79.98.105	443	192.168.2.6	49743	CN=*.avenirhomes.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.	Sun Nov 29 14:41:24 CET 2020 Thu Mar 17 17:40:46 CET 2016	Sat Feb 27 14:41:24 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		
Jan 13, 2021 21:34:54.285316944 CET	51.79.98.105	443	192.168.2.6	49744	CN=*.avenirhomes.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.	Sun Nov 29 14:41:24 CET 2020 Thu Mar 17 17:40:46 CET 2016	Sat Feb 27 14:41:24 CET 2021 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 3448 Parent PID: 792

General

Start time:	21:34:31
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:	0x7ff721e20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 1872 Parent PID: 3448

General

Start time:	21:34:32
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:3448 CREDAT:17410 /prefetch:2
Imagebase:	0x1090000
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