



ID: 339302
Cookbook: browseurl.jbs
Time: 20:36:59
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report http://unbouncepages.com/46598534393037243839343 37fl/
Overview 44
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Dropped Files 4
Sigma Overview 4
Signature Overview 4
AV Detection: 5
Phishing: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 9
Public 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 11
ASN 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 18
No static file info 18
Network Behavior 18
Snort IDS Alerts 18
Network Port Distribution 18
TCP Packets 19
UDP Packets 20
DNS Queries 21
DNS Answers 21
HTTP Request Dependency Graph 22
HTTP Packets 22
HTTPS Packets 26
Code Manipulations 27
Statistics 27

Behavior 27
System Behavior 27
Analysis Process: iexplore.exe PID: 5612 Parent PID: 792 27
General 27
File Activities 28
Registry Activities 28
Analysis Process: iexplore.exe PID: 476 Parent PID: 5612 28
General 28
File Activities 28
Registry Activities 28
Disassembly 29

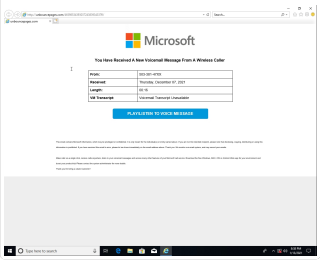
Analysis Report http://unbouncepages.com/4659853439…

Overview

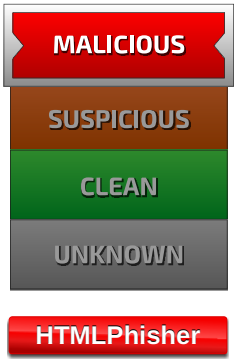
General Information

Sample URL:	http://unbouncepages.com/4659853439303724383934337fl/
Analysis ID:	339302

Most interesting Screenshot:



Detection

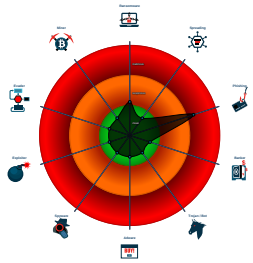


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected HtmlPhish_30

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5612 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 476 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5612 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

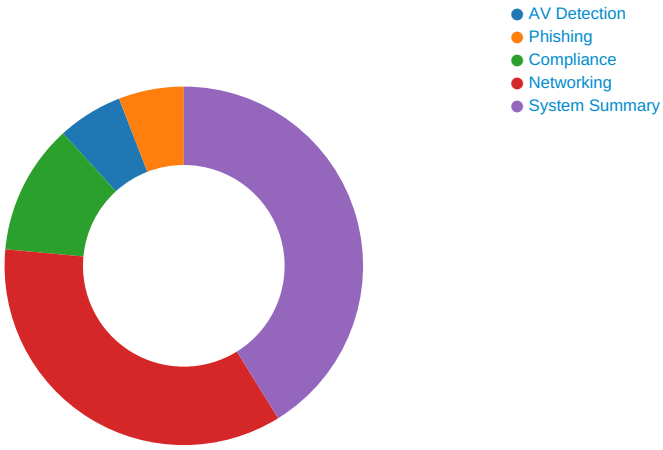
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\4659853439303724383934337fl[1].htm	JoeSecurity_HtmlPhish_30	Yara detected HtmlPhish_30	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:



Antivirus / Scanner detection for submitted sample

Phishing:

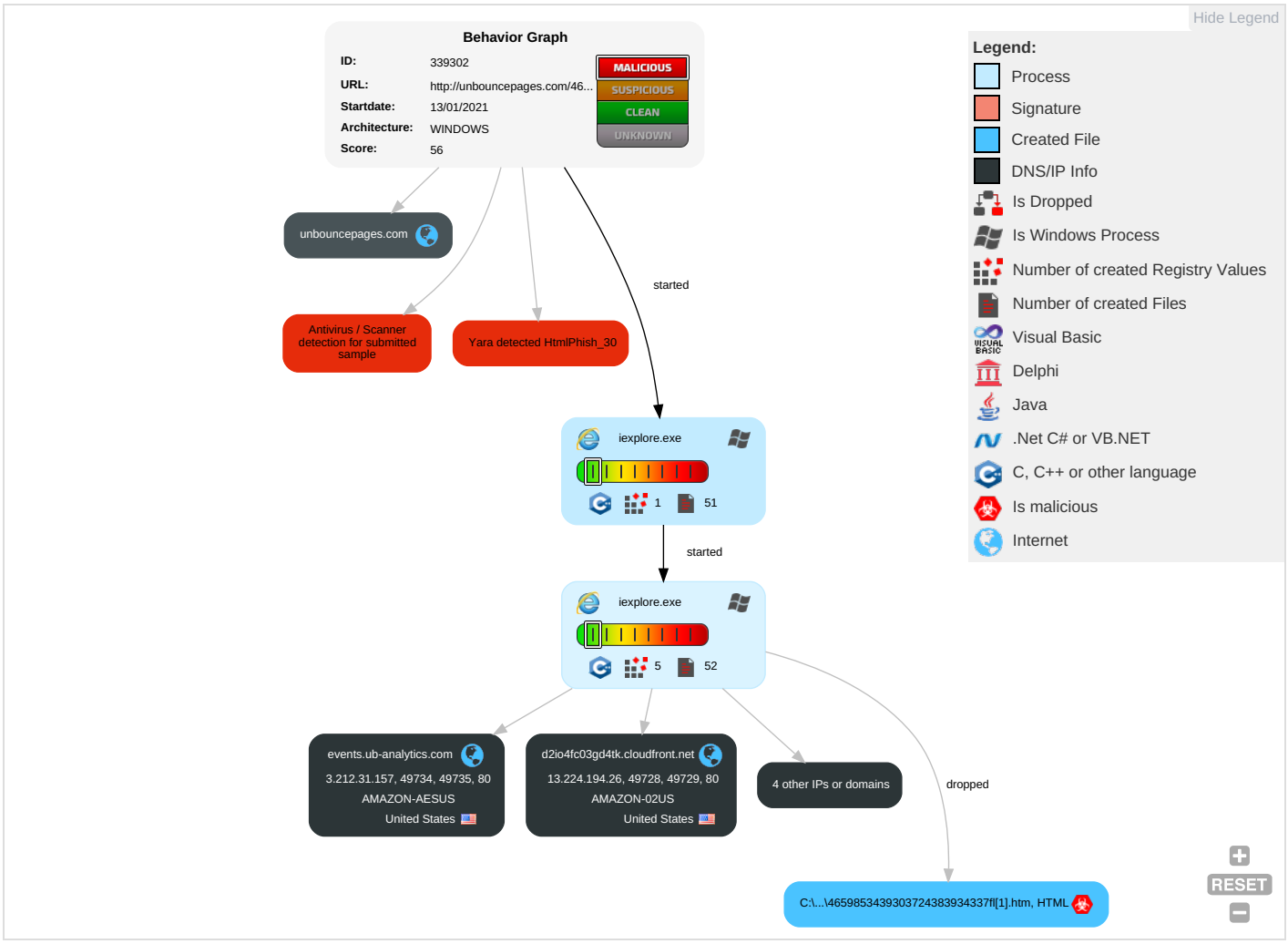


Yara detected HtmlPhish_30

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 4	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 3	SIM Card Swap		Carri Billin Fraud

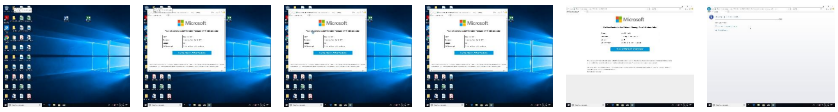
Behavior Graph

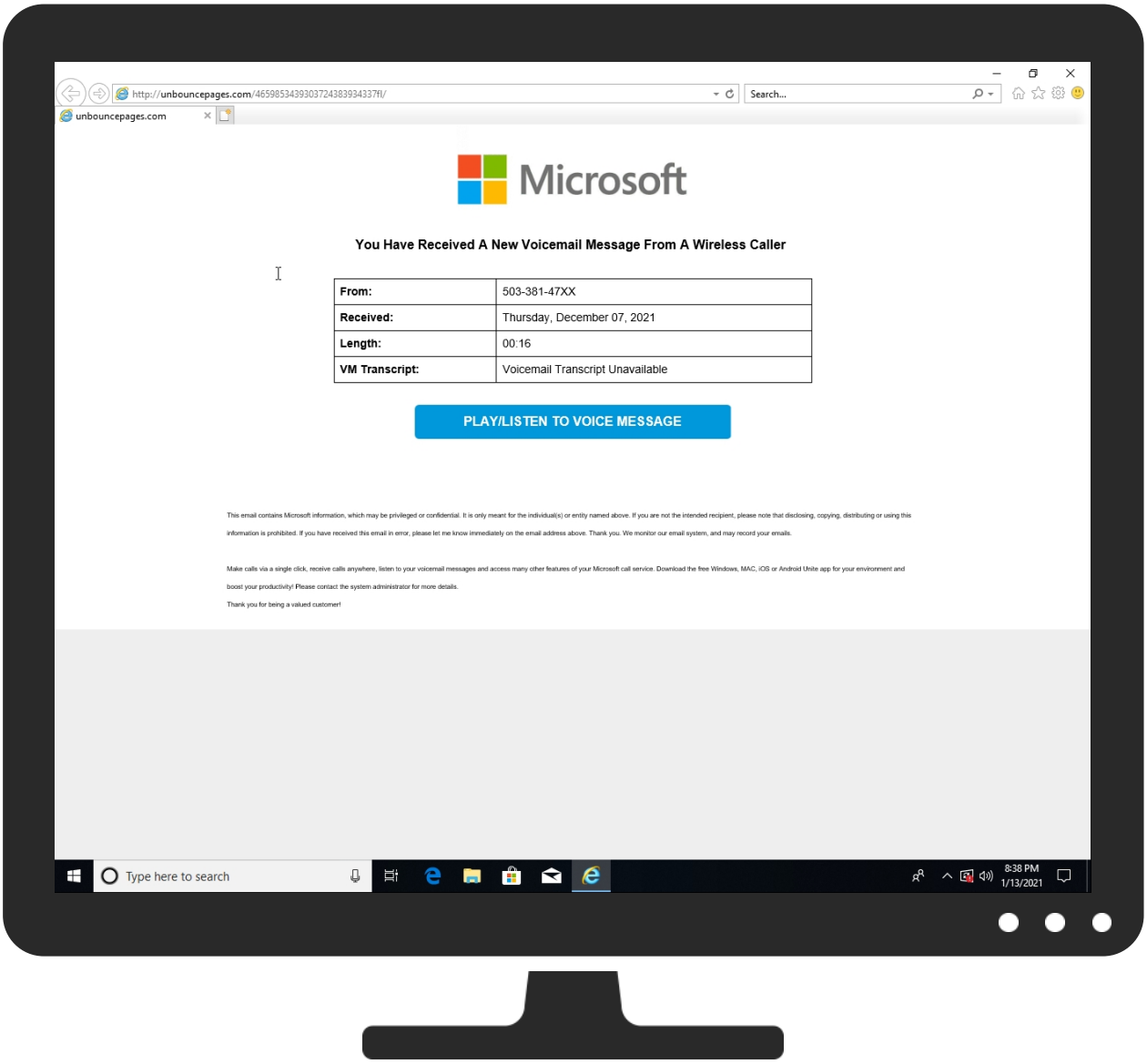


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://unbouncepages.com/46598534393037243839343 37fl/	0%	Avira URL Cloud	safe	
http://unbouncepages.com/46598534393037243839343 37fl/	100%	SlashNext	Fake Login Page type: Phishing & Social usering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://unbouncepages.c	0%	Avira URL Cloud	safe	

Copyright null 2021

Source	Detection	Scanner	Label	Link
http://events.ub-analytics.com/i?stm=1610599073847&e=pv&url=http%3A%2F%2Funbouncepages.com%2F46598534393037243839343337fl%2F&tv=js-2.14.0&tna=sp-ub&aid=landing_page&p=web&tz=America%2FLos_Angeles&lang=en-US&cs=utf-8&f_pdf=0&f_qt=0&f_realp=0&f_wma=0&f_dir=0&f_fla=1&f_java=1&f_gears=0&f_ag=0&res=1280x1024&cd=24&cookie=1&eid=2a64a8a9-e27f-48c4-a48a-7a2ffc5351b0&dtm=1610599073842&vp=784x554&ds=890x622&vid=1&sid=28f3e9e7-e98b-42c9-b3d2-0538bae3dee1&duid=2b34fd73-4516-40da-a1ed-d8d4fe0d734c&uid=84.17.52.741614371565357000&cx=eyJzY2hlbWEiOiJpZ2x1OmNvbS5zbm93cGxvd2FuYWx5dGljcy5zbm93cGxvdy9jb250ZXh0cy9qc29uc2NoZW1hLzEtMC0wIiwiZGF0YSI6W3sic2NoZW1hIjoianNfdHJhY2tlcl9jb250ZXh0X3YxLjEuanNvbiIsImRhdGEiOnsicGFnZUlkIjoiZWNiZDlkZGItNjBjNC00MmRhLThjMWItN2Q5NTVhMWM4Mjk1IiwidmFyaWFudElkIjoiYSIsImV2ZW50VHlwZSI6InZpc2l0IiwiZXZlbnRNZXRhZGF0YSI6W10sInJvdXRpbmdTdHJhdGVneSI6IndlaWdodGVkIn19XX0	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
d34qb8suadcc4g.cloudfront.net	13.225.80.63	true	false		high
unbouncepages.com	54.93.101.66	true	false		high
events.ub-analytics.com	3.212.31.157	true	false		unknown
d9hhrg4mnvzow.cloudfront.net	13.225.84.146	true	false		high
d2io4fc03gd4tk.cloudfront.net	13.224.194.26	true	false		high
builder-assets.unbounce.com	unknown	unknown	false		high

Contacted URLs

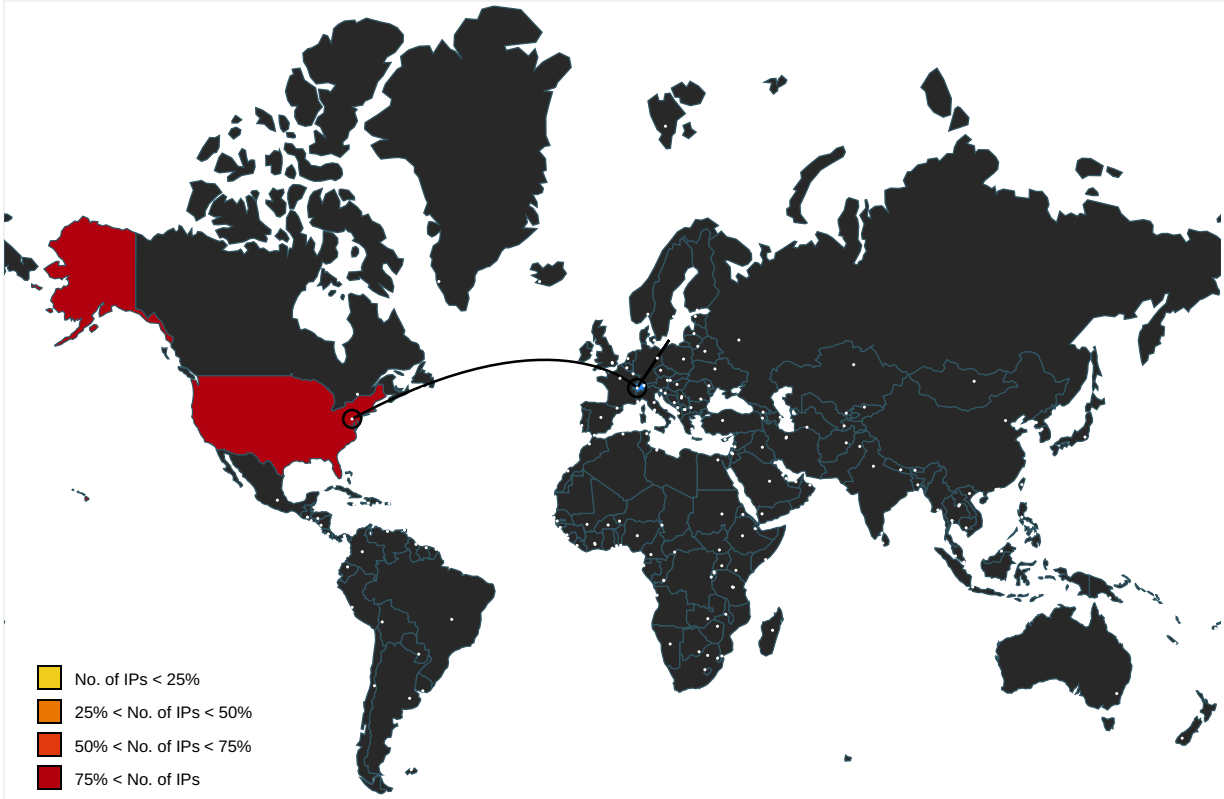
Name	Malicious	Antivirus Detection	Reputation
http://builder-assets.unbounce.com/published-js/main.bundle-5c6e41c.z.js	false		high
http://d9hhrg4mnvzow.cloudfront.net/unbouncepages.com/46598534393037243839343337fl/e8fc0c77-micro_107z040000000000000028.png	false		high
http://unbouncepages.com/46598534393037243839343337fl/clkn/https/artsana.limpcome.ml/email@thisisforu.com	false		high
http://events.ub-analytics.com/i?stm=1610599073847&e=pv&url=http%3A%2F%2Funbouncepages.com%2F46598534393037243839343337fl%2F&tv=js-2.14.0&tna=sp-ub&aid=landing_page&p=web&tz=America%2FLos_Angeles&lang=en-US&cs=utf-8&f_pdf=0&f_qt=0&f_realp=0&f_wma=0&f_dir=0&f_fla=1&f_java=1&f_gears=0&f_ag=0&res=1280x1024&cd=24&cookie=1&eid=2a64a8a9-e27f-48c4-a48a-7a2ffc5351b0&dtm=1610599073842&vp=784x554&ds=890x622&vid=1&sid=28f3e9e7-e98b-42c9-b3d2-0538bae3dee1&duid=2b34fd73-4516-40da-a1ed-d8d4fe0d734c&uid=84.17.52.741614371565357000&cx=eyJzY2hlbWEiOiJpZ2x1OmNvbS5zbm93cGxvd2FuYWx5dGljcy5zbm93cGxvdy9jb250ZXh0cy9qc29uc2NoZW1hLzEtMC0wIiwiZGF0YSI6W3sic2NoZW1hIjoianNfdHJhY2tlcl9jb250ZXh0X3YxLjEuanNvbiIsImRhdGEiOnsicGFnZUlkIjoiZWNiZDlkZGItNjBjNC00MmRhLThjMWItN2Q5NTVhMWM4Mjk1IiwidmFyaWFudElkIjoiYSIsImV2ZW50VHlwZSI6InZpc2l0IiwiZXZlbnRNZXRhZGF0YSI6W10sInJvdXRpbmdTdHJhdGVneSI6IndlaWdodGVkIn19XX0	false	• Avira URL Cloud: safe	unknown
http://unbouncepages.com/46598534393037243839343337fl/clkn/https/artsana.limpcome.ml/email@thisisforu.com	false		high
http://unbouncepages.com/46598534393037243839343337fl/	false		high
http://unbouncepages.com/46598534393037243839343337fl/	false		high
http://unbouncepages.com/favicon.ico	false		high
http://builder-assets.unbounce.com/published-css/main-7b78720.z.css	false		high
http://unbouncepages.com/46598534393037243839343337fl/favicon.ico	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://unbouncepages.com/46598534393037243839343 3Root	{425D55D0-5622-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false		high
http://https://github.com/snowplow/snowplow/wiki/javascript-tracker-setup	sp-2.14.0[1].js.2.dr	false		high
http://https://vimeo.com/api/oembed.json?url=	main.bundle-5c6e41c.z[1].js.2.dr	false		high
http://unbouncepages.c	{425D55D0-5622-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://unbouncepages.com/46598534393037243839343337fl/Root	{425D55D0-5622-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/snowplow/snowplow/wiki/javascript-tracker	sp-2.14.0[1].js.2.dr	false		high
http://unbouncepages.com/4659853439303724383934337om/4659853439303724383934337fl/c7fl/jhttp://unbounc	{425D55D0-5622-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false		high
http://unbouncepages.com/4659853439303724383934337fl/clkn/https/artsana.limpcome.ml/email	~DF5B31512BA0419CB8.TMP.1.dr	false		high
http://https://d34qb8suadcc4g.cloudfront.net/sp-2.14.0.js	ub[1].js.2.dr	false		high
http://https://d34qb8suadcc4g.cloudfront.net/ub.js?1605293159	4659853439303724383934337fl[1].htm.2.dr	false		high
http://unbouncepages.com/4659853439303724383934337fl/jhttp://unbouncepages.com/46598534393037243839343 37fl	~DF5B31512BA0419CB8.TMP.1.dr	false		high
http://unbouncepages.com/4659853439303724383934337om/4659853439303724383934337fl/Root	{425D55D0-5622-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.225.80.63	unknown	United States		16509	AMAZON-02US	false
13.225.84.146	unknown	United States		16509	AMAZON-02US	false
13.224.194.26	unknown	United States		16509	AMAZON-02US	false
54.93.101.66	unknown	United States		16509	AMAZON-02US	false
3.212.31.157	unknown	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339302
Start date:	13.01.2021
Start time:	20:36:59

Copyright null 2021

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://unbouncepages.com/46598534393037243839343 37fl/
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.phis.win@3/22@6/5
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: http://unbounce pages.com/46598534393037243839 34337fl/clkn/https/artsana.lim pcome.ml/email@thisisforu.com
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, 104.42.151.234, 88.221.62.148, 51.104.139.180, 92.122.213.194, 92.122.213.247, 152.199.19.161 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, ie9comview.vo.msecnd.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus17.cloudapp.net, 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, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net • VT rate limit hit for: http://unbouncepages.com/46598534393037243839 34337fl/

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\unbouncepages[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1817
Entropy (8bit):	5.686714674777268
Encrypted:	false
SSDEEP:	48:1vu42svu42bkEhhRrZw1/GPEHot+42svno2b/2svno2b/2F:F2K24+TZdb2mo2D2mo2D2F
MD5:	C7727B4C1394153B9A1AB08AA3B22454
SHA1:	1366097CA2DE2C178D9B26F648CE2CA15483B85A
SHA-256:	D2CEE795CDFA885E1C2D788E9BD7FB6BE585F1CBBD5F26A8D8AB289DDC7C1133
SHA-512:	F14D79E598C3E9DE765F26338FDA052FB50B99CC1EA20FC4D9EE77F34929CE413716533754A941A9875878D20398E46EC7B10CDBB88B03058A5C80E0FD28289(
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root></root><root><item name="snowplowOutQueue_ubSnowplow_sp-ub_get.expires" value="1673671073845" ltime="100089184" htime="30861871" /></root><root><item name="snowplowOutQueue_ubSnowplow_sp-ub_get.expires" value="1673671073845" ltime="100089184" htime="30861871" /><item name="snowplowOutQueue_ubSnowplow_sp-ub_get" value="["?e=pv&url=http%3A%2F%2Funbouncepages.com%2F46598534393037243839343 3fl%2F&tv=js-2.14.0&tna=sp-ub&aid=landing_page&p=web&tz=America%2FLos_Angeles&lang=en-US&cs=utf-8&f_pdf=0&f_qt=0&f_realp=0&f_wma=0&f_dir=0&f_fla=1&f_java=1&f_gears=0&f_ag=0&res=1280x1024&cd=24&cookie=1&eid=2a64a8a9-e27f-48c4-a48a-7a2ffc5351b0&dtm=1610599073842&vp=784x554&ds=890x622&vid=1&sid=28f3e9e7-e98b-42c9-b3d2-0538bae3dee1&duid=2b34fd73-4516-40da-a1ed-d8d4fe0d734c&uid=84.17.52.74161437156535700 0&cx=eyJzY2hlbWEiOiJpZ2x1OmNvbS5zbm93cGxvd2FuYWx5dGljcy5

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{425D55CE-5622-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8543089702921842
Encrypted:	false
SSDEEP:	96:rsZeZih2iba9WibxztibxCNAfibxCGgKG1MibxSeGwuTibxSAGHoRibxSAPGC+f7:rsZeZC2P9WKtQf3xMbsnfuMX
MD5:	D4D990FC3113ED555FD8C5AF8538AE60
SHA1:	E72C2C6FDA196FA22EA3104E1D7B540B558818D2
SHA-256:	2F24C0005FA0B5E19BBE0E93EB2ADBC038E6FF054AAE2835E82CA99C35D589FD
SHA-512:	6260C7AFB249BCA5B3CFC1DEC30DB5056D5FE9E281578F67A19D4B12097C270BE1EFC8407DDB11CC7BF85E6B041AE16E9C197F26B0C68BD8BCB2716025480 CD
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\{425D55D0-5622-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{425D55D0-5622-11EB-90E5-ECF4BB2D2496}.dat	
Size (bytes):	44582
Entropy (8bit):	2.0519134304601043
Encrypted:	false
SSDEEP:	192:rPZgQc6WkIFjB2skWdMpYjQIuyddIuIzSPWckIwgUPKdur:rx5nXIhwYupmFu6eiPk0Uide
MD5:	8B93CBFB56C023739D79D57256CC5D1D
SHA1:	58B7C4EE4AA37F4360A7B861CEE64575B029C269
SHA-256:	0648866D4BD560D940AA44994BA11E39C3BD11B2AD1E1481B58C3F9E9663C63D
SHA-512:	38A0FE6D381754657B4F94ADD69D8ADEA4DE671DA7C97FF63CDF1C9720D50BF9AA2C94C4D566239F246A10D294ED94D0861553E9CD5E8C697DF5463D35C0D 6
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\{425D55D1-5622-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.565599847593197
Encrypted:	false
SSDEEP:	48:IwGGcpr7Gwpa+G4pQOGrapbSqrGQpKcG7HpRHsTGIpG:raZVQ+6ABSqFA3TH4A
MD5:	7393331EBB81DA79E6BEC709CB69BFF0
SHA1:	A9239418B27C14A5FE6DCD656519933CFCE4BAA8
SHA-256:	ABE5CDF69365065B056BE2586410E71B33FCB7A3339A6842C17244A01FC472C2
SHA-512:	B17EE8BDF710B2F7A845CC347BDE31AFD02444B8D704EA5D2E12D98F826C85E2940093F4DCB35AF9A42A747ED369347DE5618BF52F604D58BA93B02C959FC9 F
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\background_gradient[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 1x800, frames 3
Category:	downloaded
Size (bytes):	453
Entropy (8bit):	5.019973044227213
Encrypted:	false
SSDEEP:	6:3llVuiPjlXJYhg5suRd8PImMo23C/kHrJ8yA/NIeYoWg78C/vTFvbKLAh3:V/XPYhiPRd8j7+9LoIrobtHTdbKi
MD5:	20F0110ED5E4E0D5384A496E4880139B
SHA1:	51F5FC61D8BF19100DF0F8AADAA57FCD9C086255
SHA-256:	1471693BE91E53C2640FE7BAEECBC624530B088444222D93F2815DFCE1865D5B
SHA-512:	5F52C117E346111D99D3B642926139178A80B9EC03147C00E27F07AAB47FE38E9319FE983444F3E0E36DEF1E86DD7C56C25E44B14EFDC3F13B45EDEDA064DB5 A
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/background_gradient.jpg
Preview:	......JFIF.....d.d.....Ducky.....P.....Adobe.d..... .....W..... .....Qa.....?.....%.....x.....s...Z.....j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.....p.....A.....BP..qD.(.....ntH.@.....h?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\httpErrorPagesScripts[1]	
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\i[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.0314906788435274
Encrypted:	false
SSDEEP:	3:CUnaaatwltxlHh/:f/
MD5:	FB02F374B8F73825415DB1BCCD4BD76D
SHA1:	B103AA629CACDD90B39538A7561DA7F8E49AD73F
SHA-256:	CAA849B179BEFA2645A8E2C474D2E82A76777A3305315ECE911013E8EE9A916C
SHA-512:	3BE8176915593E79BC280D08984A16C29C495BC53BE9B439276094B8DCD3764A3C72A046106A06B958E08E67451FE02743175C621A1FAA261FE7A9691CC77141
Malicious:	false
Reputation:	low
IE Cache URL:	http://events.ub-analytics.com/i?stm=1610599073847&e=pv&url=http%3A%2F%2Funbouncepages.com%2F46598534393037243839343 37fl%2F&tv=js-2.14.0&tna=sp-ub&aid=landing_page&p=web&tz=America%2FLos_Angeles&lang=en-US&cs=utf-8&f_pdf=0&f_qt=0&f_realp=0&f_wma=0&f_dir=0&f_fla=1&f_java=1&f_gears=0&f_ag=0&res=1280x1024&cd=24&cookie=1&eid=2a64a8a9-e27f-48c4-a48a-7a2ffc5351b0&dtm=1610599073842&vp=784x554&ds=890x622&vid=1&sid=28f3e9e7-e98b-42c9-b3d2-0538bae3dee1&duid=2b34fd73-4516-40da-a1ed-d8d4fe0d734c&uid=84.17.52.74161437 1565357000&cx=eyJzY2hlbWEiOiJpZ2x1OmNvbS5zbm93cGxvd2FuYWx5dGljcy5zbm93cGxvdy9jb250ZXh0cy9qc29uc2NoZW1hLzEtMC0wIiwiZGF0YSI6W3sic2NoZW1hIjoianNfdHJhY2tlcl9jb250ZXh0X3YxLjEuanNvbiIsImRhdGEiOnsicGFnZUlkIjoiZWNiZDlkZGItNjBjNC00MmRhLThjMWItN2Q5NTVhMWM4Mjk1IiwidmFyaWFudElkIjoiYSIsImV2ZW50VHlwZSI6InZpc2l0IiwiZXZlbnRNZXRhZGF0YSI6W10sInJvdXRpbmdTdHJhdGVneSI6IndlaWdodGVkIn19XX0
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\ub[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	5451
Entropy (8bit):	4.548234576392371
Encrypted:	false
SSDEEP:	96:dsJ51DjicoH95RX7DTcBhqPy9g3/2Tiz11+DxZC3rCY+Ck:dS51n3oH95RfcIEg3V1EDxErCZCk
MD5:	7B2EA18D249A8F17AC824B2379257636
SHA1:	0A8B2568FB67CAE8694411B5317D3AB7C673230F
SHA-256:	146713F310842933DC62D2BED7F0EAAF8A9CF3CDF72FD37610EF51E58378C8DC
SHA-512:	8DAEDF2066E1258B7C69EADE575A82051D1EE4FAF3F102EBB586381728F66D21864D13073ED385A10CDE1440EB71E996252A81A3AC49761ECC010E204A16DA6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d34qb8suadcc4g.cloudfront.net/ub.js?1605293159
Preview:	if (!window.ubSnowplow || !window.ubSnowplow.initialized) {. (function () {. // Load snowplow script (this is provided by snowplow). (function (p, l, o, w, i, n, g) {. if (!p[i]) {. p.UnbounceSnowplowNamespace = p.UnbounceSnowplowNamespace || [];. p.UnbounceSnowplowNamespace.push(i);. p[i] = function () {. (p[i].q = p[i].q || []).push(arguments);. };. p[i].q = p[i].q || [];. n = l.createElement(o);. g = l.getElementsByTagName(o)[0];. n.async = 1;. n.src = w;. g.parentNode.insertBefore(n, g);. }. })(. window,. document,. "script",. "https://d34qb8suadcc4g.cloudfront.net/sp-2.14.0.js",. "ubSnowplow".);. // Checks whether the current page is a "main" page. var isMainPage = (function () {. var usedAs = window.ub.page.usedAs;. return function () {. return usedAs === "main";. };. })();.. // Gets an attribute from the "main" page.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\down[1]	
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";....//used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\main-7b78720.z[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	15018
Entropy (8bit):	4.842804922382129
Encrypted:	false
SSDEEP:	96:xpvUp6pxpQp+Pp4Op4qpFp0DpppFpYp0sykBADv0xtalv08e6GjfZYyiVaJEX88y:7e/pYRYYc3lLezkcl6HaWsg5pOCjcQ
MD5:	CD2292597F3290F1644E4575EB2F106F
SHA1:	AAF356B422538222CAB2790E7BDB5975DBF63D3C
SHA-256:	7B787207F29FFD5672AB91B95F681B387B4D6433081CC8B47070F1D564827863
SHA-512:	F1E78B93BEC0A7829E732B8B3349F98E2EEEFA797EFEA89D20FFB700917C43805935CD284FF50204D4A24E183C4808344E9664095DCF9FD02D7E645B63F51E22
Malicious:	false
Reputation:	low
IE Cache URL:	http://builder-assets.unbounce.com/published-css/main-7b78720.z.css
Preview:	div.lp-pom-root .lp-pom-form-field.legacy{position:absolute;left:0;top:0;margin-bottom:12px}div.lp-pom-root .lp-pom-form-field.legacy label{position:absolute;left:0;top:0}div.lp-pom-root .lp-pom-form-field.legacy select{position:absolute;left:0;top:0;padding:0;margin:0;border:1px solid #666}div.lp-pom-root .lp-pom-form-field.legacy select option{padding:0.2em}div.lp-pom-root .lp-pom-form-field.legacy textarea,div.lp-pom-root .lp-pom-form-field.legacy input[type=text]{position:absolute;left:0;top:0;padding:0;margin:0;border:1px solid #666}div.lp-pom-root .lp-pom-form-field.legacy input[type=text]::-moz-focus-inner{padding:0;border:none}div.lp-pom-root .lp-pom-form-field.legacy select::-moz-focus-inner{padding:0;border:none}div.lp-pom-root .lp-pom-form-field.legacy .optionsList{position:absolute;left:0;top:0;right:0;padding:0;margin:0}div.lp-pom-root .lp-pom-form-field.legacy .option{position:relative;margin-bottom:6px}div.lp-pom-root .lp-pom-form-field.legacy .option input{position:abso

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\main.bundle-5c6e41c.z[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	106224
Entropy (8bit):	5.292379926793633
Encrypted:	false
SSDEEP:	1536:VpCaoSqc5xE/Efg2jWKc/IesSeCyvshBClNMJWdMCzz:ESuKNWKc/ImhBClDMiz
MD5:	0C115EAE8050F401FC7CE8093E0A1E43
SHA1:	4BFA6E206EC71F28A79BD5BF5046EE30FB62D882
SHA-256:	5C6E41CAB44D3FC8958DF6B852E4E728360A81D7A5FC3079B36E677CC07F8EDB

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\main.bundle-5c6e41c.z[1].js	
SHA-512:	FD4DB9DC157E266348CB9E83CF000BA7E8BE6698C73FC38031C076A624D76E297361C527E64E4FC59FCB86AB6C4E81219C3B2289E5917D8BD4DE51738EE317E 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://builder-assets.unbounce.com/published-js/main.bundle-5c6e41c.z.js
Preview:	!function(n){var o={};function r(e){if(o[e])return o[e].exports;var t=o[e]={i:e,l:!1,exports:{}};return n[e].call(t.exports,t,t.exports,r),t.l=!0,t.exports}r.m=n,r.c=o,r.d=function(e,t,n){r.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:n})},r.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},r.t=function(t,e){if(1&e&&(t=r(t)),8&e)return t;if(4&e&&"object"==typeof t&&t&&t.__esModule)return t;var n=Object.create(null);if(r.r(n),Object.defineProperty(n,"default",{enumerable:!0,value:t}),2&e&&"string"!=typeof t)for(var o in t)r.d(n,o,function(e){return t[e]}.bind(null,o));return n},r.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};return r.d(t,"a",t),t},r.o=function(e,t){return Object.prototype.hasOwnProperty.call(e,t)},r.p="",r(r.s=20)}([function(e,t,n){"use strict";Object.defineProperty(t,"__esModule",{value:!0});var o=n(1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\http_410[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4162
Entropy (8bit):	4.079892886688593
Encrypted:	false
SSDEEP:	48:upUP4V4V5BXvLSyq1a5TI7jn3GFa7KBuc1kpNc7KabOy:uwpeAKj36a75G7N
MD5:	FFCB90AD5A880C6E88DE7E211C7282C7
SHA1:	ED03E943DD09C79BA94BD4237CBF09F0BAC2B491
SHA-256:	BBB7E4F40606302DC3F9A4B22A6D9DB196DE9D47615DB81C1071EB21BF434707
SHA-512:	3A119BA698051752AFAA2E97AA342173C3821129B06D6DA0CEB5B929DC3EE79700C4FCD997F20D0DE3D0BC07B2367CA60440D9C6F7B23ADF8A083ECCEE6F4 6E
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/http_410.htm
Preview:	.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html>.... <head>.. <link rel="stylesheet" type="text/css" href="ErrorPageTemplate.css" >.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.... <title>HTTP 410 Gone</title>.. .. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.... </head>.... <body onLoad="javascript:expandCollapse('infoBlockID', true); initGoBack(); initMoreInfo('infoBlockID');">.... <table width="730" cellpadding="0" cellspacing="0" border="0">.... Error title -->.. <tr>.. <td id="infoIconAlign" width="60" align="left" valign="top" rowspan="2">.. <img src="info_48.png" id="infoIcon" alt="Info icon">.. </td>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC13 4
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/info_48.png
Preview:	.PNG.....IHDR.../...0.....#.....IDATx^...pUU..{....KB.....!....F.....jp.Q.....Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{.....[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po.....X..;.=.P...../...+...9./..s.....9..\|.....*.7v.`..V.....-^.$S[[[.....K..z.....3..3....5 ...0..''/n/.c...&.{.ht..?....A..l{.n...../....t.....N}..%.v...:.E..i....`....a.k.mg.LX..fcFU.fO-..YEfd.}...~.''.....}l$....^.re..'^X..*}.?.^U.G..... .30...X.....f[.l0.P`..KC...[..[..6....~..i..Q.|;x..T .....s.5...n+.0..;...H#.2..#.M..m[^3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..l[..a...N,,.h.....5...f*.y...}...BX{.G^...?.c.....s^..P.(..G...t.0.:.X.DCs.....]vf...py).....x..>-..Be.a...G...Y!...z...g.{....d.s.o.....%.x.....R.W.....Z.b,....!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a)..t..e.j.W.....C<.1.....c..l1w....]3%....tR;,..3..-.NW.5...t..H..h..D..b.....M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\sp-2.14.0[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	100488
Entropy (8bit):	5.421728623980021
Encrypted:	false
SSDEEP:	1536:Q52Q+J9sLaK1v011YR9QAFwAEeDkx5mwllKCf4DEvW:maa00CvADEvW
MD5:	576D9639026167DBD06E782DA275395F
SHA1:	80FE249778E307981557C0FA707CB8F4C5CB20E3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\sp-2.14.0[1].js	
SHA-256:	2E8292B18FC2ACC297E1AA6ACC6ABE05136604137E744BA1B49984DF330562BB
SHA-512:	4B792E4839AF2EFE7484C5C7BA08BFF9AE18AA6FD768A1C407DD5B309AE48924CAA43EBC0BA09CE6D3AB857159BFBB3677F7A1EB060C53E48A6131731E481867
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d34qb8suadcc4g.cloudfront.net/sp-2.14.0.js
Preview:	/*. * Snowplow - The world's most powerful web analytics platform. *. * @description JavaScript tracker for Snowplow. * @version 2.14.0. * @author Alex Dean, Simon Andersson, Anthon Pang, Fred Blundun, Joshua Beemster, Michael Hadam, Paul Boocock. * @copyright Anthon Pang, Snowplow Analytics Ltd. * @license Simplified BSD. *. * For technical documentation:. * https://github.com/snowplow/snowplow/wiki/javascript-tracker. *. * For the setup guide:. * https://github.com/snowplow/snowplow/wiki/javascript-tracker-setup. *. * Minimum supported browsers:. * - Firefox 27 . * - Chrome 32 . * - IE 9 . * - Safari 8 . */.."use strict";function ownKeys(t,e){var n=Object.keys(t);if(Object.getOwnPropertySymbols){var r=Object.getOwnPropertySymbols(t);e&&(r=r.filter(function(e){return Object.getOwnPropertyDescriptor(t,e).enumerable})),n.push.apply(n,r)}return n}function _objectSpread(t){for(var e=1;e<arguments.length;e++){var n=null!=arguments[e]?arguments[e]:{};e%2?ownKeys(n,!0).forEach

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\4659853439303724383934337fl[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	8329
Entropy (8bit):	5.392329476187314
Encrypted:	false
SSDEEP:	192:wDNOJN1GEVEPsypuE0o0WJN5Rajw3OpNQIHMMDzaVpVk:r68tWJNXaQObMMDei
MD5:	F753EDB4CAB9A924AEC0B26DBEF09994
SHA1:	F3BD33271D6CC671279DF40D06829C111BA73601
SHA-256:	129949A837C7782AD0D3AE1883CC4D3B902BEFF68B9BE1AE2713BC7909CCB71F
SHA-512:	C68E92989AC943013E51D24CD9DB700495BB0DC35DB1A879621B717E5A2DA1C394562DF80EF56CBEDF13E9FF26EA80D6E3869F94A2F844807267FB76D5B50CFA
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_30, Description: Yara detected HtmlPhish_30, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\4659853439303724383934337fl[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://unbouncepages.com/4659853439303724383934337fl/
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><META http-equiv="Content-Type" content="text/html; charset=UTF-8" >. ecbd9ddb-60c4-42da-8c1b-7d955a1c8295 a-->.. <title></title>. <meta name="keywords" content="">. <meta name="description" content="">.. .. .. <meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="lp-version" content="v6.23.9"><style title="page-styles" type="text/css" data-page-type="main_desktop">.body {. color:#000;.}.a {. color:#0000ff;. text-decoration:none;.}.#lp-pom-root {. display:block;. background:rgba(238,238,238,1);. border-style:none;. margin:auto;. padding-top:0px;. border-radius:0px;. min-width:890px;. height:622px;.}.#lp-pom-block-11 {. display:block;. background:rgba(255,255,255,1);. border-style:none;. margin-left:auto;. margin-right:auto;. margin-bottom:0px;. border-radius:0px;. width:100%;. height:0p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\ErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2168
Entropy (8bit):	5.207912016937144
Encrypted:	false
SSDEEP:	24:5+j5xU5k5N0ndgvoyeP0yyiyQCDr3nowMVworDtX3orKxWxDnCMA0da+hieyuSQK:5Q5K5k5pvFehWrrarrZIrHd3FIQfOS6
MD5:	F4FE1CB77E758E1BA56B8A8EC20417C5
SHA1:	F4EDA06901EDB98633A686B11D02F4925F827BF0
SHA-256:	8D018639281B33DA8EB3CE0B21D11E1D414E59024C3689F92BE8904EB5779B5F
SHA-512:	62514AB345B6648C5442200A8E9530DFB88A0355E262069E0A694289C39A4A1C06C6143E5961074BFAC219949102A416C09733F24E8468984B96843DC222B436
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/ErrorPageTemplate.css
Preview:	.body..{...font-family: "Segoe UI", "verdana", "arial";...background-image: url(background_gradient.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_gradient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...background-color: #F4F4F4;..}.. ..a..{...color: rgb(19,112,171);.font-size: 1em;...font-weight: normal;...text-decoration: none;...margin-left: 0px;...vertical-align: top;..}....a:link, a:visited..{...color: rgb(19,112,171);...text-decoration: none;...vertical-align: top;..}....a:hover..{...color: rgb(7,74,229);...text-decoration: underline;..}....p..{...font-size: 0.9em;..}.....h1 /* used for Title */..{...color: #4465A2;...font-size: 1.1em;...font-weight: normal;...vertical-align

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\bullet[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	447
Entropy (8bit):	7.304718288205936

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\bullet[1]	
Encrypted:	false
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKIv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/bullet.png
Preview:	.PNG.....IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.;j.;l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\e8fc0c77-micro_107z040000000000000028[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 318 x 159, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	2922
Entropy (8bit):	7.908366499459993
Encrypted:	false
SSDEEP:	48:sZ0TVBZYN4IgRqBGBDi1nYKx2GCdTjVNPVxd0NYQP/gMfF4bZMr+o3zPBQowCiRF:405B6qILU9UxxCdTjVvYNYbMfFjT3zcN
MD5:	6F896354F85C4EF6F8872B11027CFFF0
SHA1:	748CFA8CB5DA3F79DBC5F7009B9BF15D0E1DE00F
SHA-256:	9B3502A808899C20914A5BF1712FCFDFAC69DEA2F84757ADA5C475755355B867
SHA-512:	ABF74A55AAB7851E756D494A69788164A0EA71D8F80FF2EFD096FD2890F7C0F8C09D5D5ED3EE62BFDEF70C2917883C5E265B31355AC120FFBADC00C661A8C63
Malicious:	false
Reputation:	low
IE Cache URL:	http://d9hhrg4mnvzow.cloudfront.net/unbouncepages.com/46598534393037243839343 37fl/e8fc0c77-micro_107z040000000000000028.png
Preview:	.PNG.....IHDR...>.....W.E....BPLTE...kkk.....N"...rrr.....x.....yq...@.....IDATx..].b.:....WB@2...WW.ZB``..o.c..tQ.S.a`..6?..$2.H...@.2.L.2y.P...=..;.:..s .c....Q..8.z.C6~l...i.....7.....q....b@.WG/....$...6}?..2...2...!.~g..Sw.."....s...P..}.8d.N.{L ..'...T....?...e.x.*oK.j~.C".e1.+...&.^>.W}....C.....}.|.....x.....o..;...{S....VV.....W6}]...V. ...l.'....{-...}w.o.k.C.>.w.ox...J*.]..E.....?J}....].=+1.!.y....w.v'.!....K.$/S.p.A*..-...m..{..Q.5.}.....$<w.....j...._..f:...A....`_.....7>S}.H....Z8C....).... }..Z}..D.jB....b..../].Q-.}.X9.....]{f../ ^.....5..t.~.]`|..@tOm..+.W..}2....9.+...m..#.Z.....|...NO.A.q...."..K.[.....B,..(.Be.0...g..I.W..|I.....Xc.o..w.....F.P.QKZ:....u=..R.....0S.^/g{....}sq^4...._V]..YG..B9M.L:..F.4.. :..6.....]..Z.A.B..",..Y<.>}.<..}*..>.P.R]^.<.....1K.....es.....We.R\6....7Ld.Y..Ka..26.*!Z..FLF/..jp..="..(.$..\...m.XDf.v.s..?....0.m.....CO...3.....T.p.....-

C:\Users\user\AppData\Local\Temp\~DF5B31512BA0419CB8.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	48627
Entropy (8bit):	0.6240042327582911
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+xvdc/IKAfoUSIJ1C1QSIJ1rfuD1Oglbhl:kBqoxKAuqR+xvdc/Iut5ok
MD5:	4562FF202A4D777A49293C04A816C99F
SHA1:	04952D4D858889FA6087E1F8F76F9AEA6D7BA612
SHA-256:	65FBC6CB16E046B03B1BC5EF6D96F546DAAC15DB69169CA69E70FB3C394A2DD3
SHA-512:	F2E0A2A2C31D2F8D1DE1CAC6595B792B31F30578B533E4921728B9BA61773CAB069292352099B117B2C80BABC29ED1FDAF9E20C6CE7539B31832316A0D33635
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFA03ECB28CFFA1FC9.TMP	
SHA-512:	0AACF8ECF8B968C0D9B0FCCBE8E766EC640C56DD4DC205BBC71693209E566F07EF9A42D2CD76971C8D5522BBDDDFFD268265D80DC75D2E82C5CEC4E2C46 6D7
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFC0544526A9214E06.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

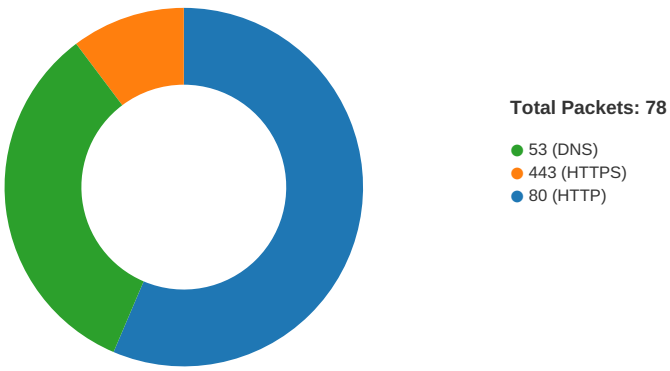
No static file info

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/21-20:37:54.617114	TCP	2925	INFO web bug 0x0 gif attempt	80	49734	3.212.31.157	192.168.2.6

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 20:37:53.542006016 CET	49726	80	192.168.2.6	54.93.101.66
Jan 13, 2021 20:37:53.542130947 CET	49727	80	192.168.2.6	54.93.101.66
Jan 13, 2021 20:37:53.583158016 CET	80	49726	54.93.101.66	192.168.2.6
Jan 13, 2021 20:37:53.583210945 CET	80	49727	54.93.101.66	192.168.2.6
Jan 13, 2021 20:37:53.583380938 CET	49726	80	192.168.2.6	54.93.101.66
Jan 13, 2021 20:37:53.583461046 CET	49727	80	192.168.2.6	54.93.101.66
Jan 13, 2021 20:37:53.585280895 CET	49726	80	192.168.2.6	54.93.101.66
Jan 13, 2021 20:37:53.632730007 CET	80	49726	54.93.101.66	192.168.2.6
Jan 13, 2021 20:37:53.632787943 CET	80	49726	54.93.101.66	192.168.2.6
Jan 13, 2021 20:37:53.632827997 CET	80	49726	54.93.101.66	192.168.2.6
Jan 13, 2021 20:37:53.632865906 CET	80	49726	54.93.101.66	192.168.2.6
Jan 13, 2021 20:37:53.632889032 CET	49726	80	192.168.2.6	54.93.101.66
Jan 13, 2021 20:37:53.632894039 CET	80	49726	54.93.101.66	192.168.2.6
Jan 13, 2021 20:37:53.632950068 CET	49726	80	192.168.2.6	54.93.101.66
Jan 13, 2021 20:37:53.633030891 CET	49726	80	192.168.2.6	54.93.101.66
Jan 13, 2021 20:37:53.639111996 CET	49726	80	192.168.2.6	54.93.101.66
Jan 13, 2021 20:37:53.679857016 CET	80	49726	54.93.101.66	192.168.2.6
Jan 13, 2021 20:37:53.755395889 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.755773067 CET	49729	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.762547016 CET	49730	443	192.168.2.6	13.225.80.63
Jan 13, 2021 20:37:53.762567997 CET	49731	443	192.168.2.6	13.225.80.63
Jan 13, 2021 20:37:53.795805931 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.795917034 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.796221018 CET	80	49729	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.796327114 CET	49729	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.797246933 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.797657967 CET	49729	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.802640915 CET	443	49730	13.225.80.63	192.168.2.6
Jan 13, 2021 20:37:53.802674055 CET	443	49731	13.225.80.63	192.168.2.6
Jan 13, 2021 20:37:53.802743912 CET	49730	443	192.168.2.6	13.225.80.63
Jan 13, 2021 20:37:53.802791119 CET	49731	443	192.168.2.6	13.225.80.63
Jan 13, 2021 20:37:53.807684898 CET	49731	443	192.168.2.6	13.225.80.63
Jan 13, 2021 20:37:53.807813883 CET	49730	443	192.168.2.6	13.225.80.63
Jan 13, 2021 20:37:53.837498903 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.837636948 CET	80	49729	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.838187933 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.838231087 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.838269949 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.838270903 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.838305950 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.838311911 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.838315964 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.838363886 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.838366032 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.838408947 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.838417053 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.838448048 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.838455915 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.838499069 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.838511944 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.838517904 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.838555098 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.838568926 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.838578939 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.838613033 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.838622093 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.838665009 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.839062929 CET	80	49729	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.839102030 CET	80	49729	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.839138985 CET	49729	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.839140892 CET	80	49729	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.839165926 CET	49729	80	192.168.2.6	13.224.194.26

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 20:37:53.839188099 CET	49729	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.839415073 CET	80	49729	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.839482069 CET	49729	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.839555025 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.839596033 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.839622974 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.839648008 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.840827942 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.840890884 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.840909958 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.840939045 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.841909885 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.841954947 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.841984987 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.842012882 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.843028069 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.843091011 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.843137980 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.843167067 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.844175100 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.844218969 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.844257116 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.844290018 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.845293045 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.845338106 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.845371008 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.845412970 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.846442938 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.846487045 CET	80	49728	13.224.194.26	192.168.2.6
Jan 13, 2021 20:37:53.846518040 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.846592903 CET	49728	80	192.168.2.6	13.224.194.26
Jan 13, 2021 20:37:53.847647905 CET	443	49731	13.225.80.63	192.168.2.6
Jan 13, 2021 20:37:53.848261118 CET	443	49730	13.225.80.63	192.168.2.6
Jan 13, 2021 20:37:53.848612070 CET	443	49730	13.225.80.63	192.168.2.6
Jan 13, 2021 20:37:53.848653078 CET	443	49730	13.225.80.63	192.168.2.6
Jan 13, 2021 20:37:53.848691940 CET	443	49730	13.225.80.63	192.168.2.6
Jan 13, 2021 20:37:53.848707914 CET	49730	443	192.168.2.6	13.225.80.63
Jan 13, 2021 20:37:53.848750114 CET	49730	443	192.168.2.6	13.225.80.63

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 20:37:47.249736071 CET	56061	53	192.168.2.6	8.8.8.8
Jan 13, 2021 20:37:47.370234013 CET	53	56061	8.8.8.8	192.168.2.6
Jan 13, 2021 20:37:48.143460989 CET	58336	53	192.168.2.6	8.8.8.8
Jan 13, 2021 20:37:48.194453001 CET	53	58336	8.8.8.8	192.168.2.6
Jan 13, 2021 20:37:48.986926079 CET	53781	53	192.168.2.6	8.8.8.8
Jan 13, 2021 20:37:49.042979956 CET	53	53781	8.8.8.8	192.168.2.6
Jan 13, 2021 20:37:49.879288912 CET	54064	53	192.168.2.6	8.8.8.8
Jan 13, 2021 20:37:49.929935932 CET	53	54064	8.8.8.8	192.168.2.6
Jan 13, 2021 20:37:50.794166088 CET	52811	53	192.168.2.6	8.8.8.8
Jan 13, 2021 20:37:50.844922066 CET	53	52811	8.8.8.8	192.168.2.6
Jan 13, 2021 20:37:51.914244890 CET	55299	53	192.168.2.6	8.8.8.8
Jan 13, 2021 20:37:51.964596987 CET	53	55299	8.8.8.8	192.168.2.6
Jan 13, 2021 20:37:52.296334982 CET	63745	53	192.168.2.6	8.8.8.8
Jan 13, 2021 20:37:52.355604887 CET	53	63745	8.8.8.8	192.168.2.6
Jan 13, 2021 20:37:53.363159895 CET	50055	53	192.168.2.6	8.8.8.8
Jan 13, 2021 20:37:53.411082983 CET	53	50055	8.8.8.8	192.168.2.6
Jan 13, 2021 20:37:53.476206064 CET	61374	53	192.168.2.6	8.8.8.8
Jan 13, 2021 20:37:53.527046919 CET	53	61374	8.8.8.8	192.168.2.6
Jan 13, 2021 20:37:53.692379951 CET	50339	53	192.168.2.6	8.8.8.8
Jan 13, 2021 20:37:53.702017069 CET	63307	53	192.168.2.6	8.8.8.8
Jan 13, 2021 20:37:53.751610994 CET	53	50339	8.8.8.8	192.168.2.6
Jan 13, 2021 20:37:53.760508060 CET	53	63307	8.8.8.8	192.168.2.6

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 20:37:53.989295006 CET	49694	53	192.168.2.6	8.8.8.8
Jan 13, 2021 20:37:54.051508904 CET	53	49694	8.8.8.8	192.168.2.6
Jan 13, 2021 20:37:54.309271097 CET	54982	53	192.168.2.6	8.8.8.8
Jan 13, 2021 20:37:54.357335091 CET	53	54982	8.8.8.8	192.168.2.6
Jan 13, 2021 20:37:54.481924057 CET	50010	53	192.168.2.6	8.8.8.8
Jan 13, 2021 20:37:54.529913902 CET	53	50010	8.8.8.8	192.168.2.6
Jan 13, 2021 20:37:55.760879040 CET	63718	53	192.168.2.6	8.8.8.8
Jan 13, 2021 20:37:55.811806917 CET	53	63718	8.8.8.8	192.168.2.6
Jan 13, 2021 20:38:10.391513109 CET	62116	53	192.168.2.6	8.8.8.8
Jan 13, 2021 20:38:10.448301077 CET	53	62116	8.8.8.8	192.168.2.6
Jan 13, 2021 20:38:16.157175064 CET	63816	53	192.168.2.6	8.8.8.8
Jan 13, 2021 20:38:16.208184004 CET	53	63816	8.8.8.8	192.168.2.6
Jan 13, 2021 20:38:21.651879072 CET	55014	53	192.168.2.6	8.8.8.8
Jan 13, 2021 20:38:21.712680101 CET	53	55014	8.8.8.8	192.168.2.6
Jan 13, 2021 20:38:22.314019918 CET	62208	53	192.168.2.6	8.8.8.8
Jan 13, 2021 20:38:22.364820004 CET	53	62208	8.8.8.8	192.168.2.6
Jan 13, 2021 20:38:23.047926903 CET	57574	53	192.168.2.6	8.8.8.8
Jan 13, 2021 20:38:23.095777988 CET	53	57574	8.8.8.8	192.168.2.6
Jan 13, 2021 20:38:23.323708057 CET	62208	53	192.168.2.6	8.8.8.8
Jan 13, 2021 20:38:23.382885933 CET	53	62208	8.8.8.8	192.168.2.6
Jan 13, 2021 20:38:24.038938999 CET	57574	53	192.168.2.6	8.8.8.8
Jan 13, 2021 20:38:24.087042093 CET	53	57574	8.8.8.8	192.168.2.6
Jan 13, 2021 20:38:24.335000038 CET	62208	53	192.168.2.6	8.8.8.8
Jan 13, 2021 20:38:24.394332886 CET	53	62208	8.8.8.8	192.168.2.6
Jan 13, 2021 20:38:25.053512096 CET	57574	53	192.168.2.6	8.8.8.8
Jan 13, 2021 20:38:25.101412058 CET	53	57574	8.8.8.8	192.168.2.6
Jan 13, 2021 20:38:26.350785017 CET	62208	53	192.168.2.6	8.8.8.8
Jan 13, 2021 20:38:26.401551008 CET	53	62208	8.8.8.8	192.168.2.6
Jan 13, 2021 20:38:27.085755110 CET	57574	53	192.168.2.6	8.8.8.8
Jan 13, 2021 20:38:27.133899927 CET	53	57574	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 20:37:53.476206064 CET	192.168.2.6	8.8.8.8	0x18ab	Standard query (0)	unbouncepages.com	A (IP address)	IN (0x0001)
Jan 13, 2021 20:37:53.692379951 CET	192.168.2.6	8.8.8.8	0xaeab	Standard query (0)	builder-assets.unbounce.com	A (IP address)	IN (0x0001)
Jan 13, 2021 20:37:53.702017069 CET	192.168.2.6	8.8.8.8	0x742a	Standard query (0)	d34qb8suadcc4g.cloudfront.net	A (IP address)	IN (0x0001)
Jan 13, 2021 20:37:53.989295006 CET	192.168.2.6	8.8.8.8	0x1cfd	Standard query (0)	d9hhrg4mnvzow.cloudfront.net	A (IP address)	IN (0x0001)
Jan 13, 2021 20:37:54.309271097 CET	192.168.2.6	8.8.8.8	0x3ca9	Standard query (0)	events.ub-analytics.com	A (IP address)	IN (0x0001)
Jan 13, 2021 20:38:10.391513109 CET	192.168.2.6	8.8.8.8	0x1a80	Standard query (0)	unbouncepages.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 20:37:53.527046919 CET	8.8.8.8	192.168.2.6	0x18ab	No error (0)	unbouncepages.com		54.93.101.66	A (IP address)	IN (0x0001)
Jan 13, 2021 20:37:53.527046919 CET	8.8.8.8	192.168.2.6	0x18ab	No error (0)	unbouncepages.com		18.196.95.178	A (IP address)	IN (0x0001)
Jan 13, 2021 20:37:53.751610994 CET	8.8.8.8	192.168.2.6	0xaeab	No error (0)	builder-assets.unbounce.com	d2io4fc03gd4tk.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 20:37:53.751610994 CET	8.8.8.8	192.168.2.6	0xaeab	No error (0)	d2io4fc03gd4tk.cloudfront.net		13.224.194.26	A (IP address)	IN (0x0001)
Jan 13, 2021 20:37:53.751610994 CET	8.8.8.8	192.168.2.6	0xaeab	No error (0)	d2io4fc03gd4tk.cloudfront.net		13.224.194.36	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 20:37:53.751610994 CET	8.8.8.8	192.168.2.6	0xaeab	No error (0)	d2io4fc03gd4tk.cloudfront.net		13.224.194.82	A (IP address)	IN (0x0001)
Jan 13, 2021 20:37:53.751610994 CET	8.8.8.8	192.168.2.6	0xaeab	No error (0)	d2io4fc03gd4tk.cloudfront.net		13.224.194.111	A (IP address)	IN (0x0001)
Jan 13, 2021 20:37:53.760508060 CET	8.8.8.8	192.168.2.6	0x742a	No error (0)	d34qb8suadcc4g.cloudfront.net		13.225.80.63	A (IP address)	IN (0x0001)
Jan 13, 2021 20:37:53.760508060 CET	8.8.8.8	192.168.2.6	0x742a	No error (0)	d34qb8suadcc4g.cloudfront.net		13.225.80.99	A (IP address)	IN (0x0001)
Jan 13, 2021 20:37:53.760508060 CET	8.8.8.8	192.168.2.6	0x742a	No error (0)	d34qb8suadcc4g.cloudfront.net		13.225.80.72	A (IP address)	IN (0x0001)
Jan 13, 2021 20:37:53.760508060 CET	8.8.8.8	192.168.2.6	0x742a	No error (0)	d34qb8suadcc4g.cloudfront.net		13.225.80.30	A (IP address)	IN (0x0001)
Jan 13, 2021 20:37:54.051508904 CET	8.8.8.8	192.168.2.6	0x1cfd	No error (0)	d9hhrg4mnvzow.cloudfront.net		13.225.84.146	A (IP address)	IN (0x0001)
Jan 13, 2021 20:37:54.051508904 CET	8.8.8.8	192.168.2.6	0x1cfd	No error (0)	d9hhrg4mnvzow.cloudfront.net		13.225.84.119	A (IP address)	IN (0x0001)
Jan 13, 2021 20:37:54.051508904 CET	8.8.8.8	192.168.2.6	0x1cfd	No error (0)	d9hhrg4mnvzow.cloudfront.net		13.225.84.77	A (IP address)	IN (0x0001)
Jan 13, 2021 20:37:54.051508904 CET	8.8.8.8	192.168.2.6	0x1cfd	No error (0)	d9hhrg4mnvzow.cloudfront.net		13.225.84.223	A (IP address)	IN (0x0001)
Jan 13, 2021 20:37:54.357335091 CET	8.8.8.8	192.168.2.6	0x3ca9	No error (0)	events.ub-analytics.com		3.212.31.157	A (IP address)	IN (0x0001)
Jan 13, 2021 20:37:54.357335091 CET	8.8.8.8	192.168.2.6	0x3ca9	No error (0)	events.ub-analytics.com		34.224.248.58	A (IP address)	IN (0x0001)
Jan 13, 2021 20:38:10.448301077 CET	8.8.8.8	192.168.2.6	0x1a80	No error (0)	unbouncepages.com		54.93.101.66	A (IP address)	IN (0x0001)
Jan 13, 2021 20:38:10.448301077 CET	8.8.8.8	192.168.2.6	0x1a80	No error (0)	unbouncepages.com		18.196.95.178	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- unbouncepages.com
  - builder-assets.unbounce.com
  - d9hhrg4mnvzow.cloudfront.net
  - events.ub-analytics.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49726	54.93.101.66	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 20:37:53.585280895 CET	91	OUT	GET /4659853439303724383934337fl/ HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: unbouncepages.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 20:37:53.632730007 CET	92	IN	HTTP/1.1 200 OK date: Wed, 13 Jan 2021 19:37:53 GMT content-type: text/html; charset=UTF-8 transfer-encoding: chunked p3p: CP="This is not a privacy policy." x-unbounce-pageid: ecbd9ddb-60c4-42da-8c1b-7d955a1c8295 etag: eaeedcd3b4d4aeb1f5b2455eb9db1220 content-location: http://unbouncepages.com/4659853439303724383934337fl/ x-unbounce-visitorid: 84.17.52.741614371565357000 last-modified: Thu, 07 Jan 2021 16:08:32 GMT x-unbounce-variant: a link: <http://unbouncepages.com/4659853439303724383934337fl/>; rel="canonical" set-cookie: ubpv=a%2Cecbd9ddb-60c4-42da-8c1b-7d955a1c8295; Max-Age=15897600; Expires=Fri, 16 Jul 2021 19:37:53 GMT; Path=/4659853439303724383934337fl/; SameSite=Lax set-cookie: ubrs=weighted; Path=/4659853439303724383934337fl/; SameSite=Lax set-cookie: ubvs=84.17.52.741614371565357000; Max-Age=15552000; Expires=Mon, 12 Jul 2021 19:37:53 GMT; Path=/; SameSite=Lax set-cookie: ubvt=84.17.52.741614371565357000; Max-Age=259200; Expires=Sat, 16 Jan 2021 19:37:53 GMT; Path=/; Domain=unbouncepages.com; SameSite=Lax content-encoding: gzip x-proxy-backend: page-server connection: close Data Raw: 42 42 41 0d 0a 1f 8b 08 00 00 00 00 00 00 d4 57 6d 6f db 36 10 fe 9e 5f c1 a9 18 b2 01 a6 de 65 4b 8a 6d 20 4b 53 ac 40 bb 15 ab 8b 75 18 86 81 12 69 9b 8b 24 6a 24 6d c7 2d f2 df 47 52 b2 2d d5 4e 93 66 58 81 05 48 22 9e ee 78 cf 73 3c dd f1 c6 df 3c ff f9 6a f6 db 9b 6b b0 94 65 01 de bc fb e1 d5 cb 2b 60 41 c7 f9 35 b8 72 9c e7 b3 e7 e0 fd 8f b3 d7 af 80 67 bb e0 ad e4 34 97 8e 73 fd 93 05 ac a5 94 75 ea 38 9b cd c6 de 04 36 e3 0b 67 f6 8b 73 ab 77 f1 b4 59 fb 08 85 b1 b1 b1 c4 d6 74 6c 7c dc 96 45 25 26 27 ec bd 24 49 1a 33 ad 4a 10 9e 8e 5f 5f cf 2e 81 d6 84 e4 ef 15 5d 4f ac 2b 56 49 52 49 38 db d6 c4 02 79 b3 9a 58 92 dc Data Ascii: BBAWmo6_eKm KS@ui$j$m-GR-NfXH"xs<<jke+`A5rg4su86gswYtl|E%&'$l3J__.]O+VIRI8yX

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49728	13.224.194.26	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 20:37:53.797246933 CET	102	OUT	GET /published-js/main.bundle-5c6e41c.z.js HTTP/1.1 Accept: application/javascript, */*;q=0.8 Referer: http://unbouncepages.com/4659853439303724383934337fl/ Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: builder-assets.unbounce.com Connection: Keep-Alive
Jan 13, 2021 20:37:53.838187933 CET	106	IN	HTTP/1.1 200 OK Content-Type: application/javascript Content-Length: 33645 Connection: keep-alive Date: Tue, 01 Dec 2020 03:28:57 GMT Last-Modified: Tue, 13 Oct 2020 18:07:24 GMT ETag: "8f54ee429acc92c4ec90173c4494c176" Cache-Control: max-age=31536000 Content-Encoding: gzip x-amz-version-id: 3Tf5CLt4Hplptlwy2gR6SrQuS3YM4exc Accept-Ranges: bytes Server: AmazonS3 X-Cache: Hit from cloudfront Via: 1.1 0e7eb16f335fe24acf3f13c5dee19c88.cloudfront.net (CloudFront) X-Amz-Cf-Pop: FRA2-C1 X-Amz-Cf-Id: SbSOzzWcEtAXkTJ6lo7cWfMQt4_napdAHSKgZmKT_S0HgXzgipi1oQ== Age: 3773337

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49729	13.224.194.26	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 20:37:53.797657967 CET	102	OUT	GET /published-css/main-7b78720.z.css HTTP/1.1 Accept: text/css, */* Referer: http://unbouncepages.com/4659853439303724383934337fl/ Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: builder-assets.unbounce.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 20:37:53.839062929 CET	121	IN	HTTP/1.1 200 OK Content-Type: text/css Content-Length: 2902 Connection: keep-alive Date: Sat, 02 Jan 2021 03:11:54 GMT Last-Modified: Wed, 09 Dec 2020 17:18:52 GMT ETag: "cd0dc5f3bbefd8a34b8e19c0a6dd75e5" Cache-Control: max-age=31536000 Content-Encoding: gzip x-amz-version-id: a2uJdoMSQ1AGBOFyETBT0EXZA0nFzQX9 Accept-Ranges: bytes Server: AmazonS3 X-Cache: Hit from cloudfront Via: 1.1 dde0b4b1e223fa23670e93078a04c116.cloudfront.net (CloudFront) X-Amz-Cf-Pop: FRA2-C1 X-Amz-Cf-Id: noVqioiU7us8iJrRXku1UgbbCrP28U5QIkyaT_X_j4038CLpldFFRg== Age: 1009560

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49733	13.225.84.146	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 20:37:54.100370884 CET	199	OUT	GET /unbouncepages.com/465985343930372438393433 7fl/e8fc0c77-micro_107z040000000000000028.png HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: http://unbouncepages.com/465985343930372438393433 7fl/ Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: d9hhrg4mnvzow.cloudfront.net Connection: Keep-Alive
Jan 13, 2021 20:37:54.166156054 CET	201	IN	HTTP/1.1 200 OK Content-Type: image/png Content-Length: 2922 Connection: keep-alive Date: Thu, 07 Jan 2021 16:56:34 GMT Last-Modified: Thu, 07 Jan 2021 16:08:32 GMT ETag: "6f896354f85c4ef6f8872b11027cfff0" Cache-Control: max-age=31557600 x-amz-version-id: LkoX25RIVrJNNXMafuDGkAUV.puNA2HE Accept-Ranges: bytes Server: AmazonS3 X-Cache: Hit from cloudfront Via: 1.1 eb1a8c1b1275e33a016e623478052111.cloudfront.net (CloudFront) X-Amz-Cf-Pop: FRA2-C2 X-Amz-Cf-Id: f2Sz2t1h4ghc57IRNGyqbObnddtWmaJMrDTPBi0DRcDpzom0EfZ1yQ== Age: 528080 Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 3e 00 00 00 9f 08 03 00 00 00 57 d1 45 fd 00 00 00 42 50 4c 54 45 ff ff ff 6b 6b 6b 85 85 85 f2 f2 f2 01 a3 ee f3 4e 22 80 ba 00 72 72 72 fa fc fb fe ba 03 9c 9c 9c d5 e8 ea dd d8 d5 ce cd bc bc bc bc b3 bd 9b ff ff ec f4 f2 ad 78 af 00 ed a1 89 f3 d7 79 71 c7 e5 e8 40 fe 80 00 00 0a e3 49 44 41 54 78 da ed 5d 89 62 a3 3a 12 a4 a5 dd a1 57 42 40 32 f3 fe ff 57 57 b7 5a 42 60 27 18 c7 6f dc 95 63 c6 e6 74 51 ea 53 90 61 60 9c 01 36 3f 8c 93 24 32 be 48 1d 93 f7 40 15 32 be 4c 18 32 79 8f 50 1c 13 f8 3d f2 90 c9 3b e5 3a 98 bd 73 ea 63 d7 cb ea fb 51 db c7 38 e5 7a 99 43 36 7e 6c fc fe ad 69 07 e3 1c 91 cc e2 37 f5 c7 96 ef fb e4 71 ca c6 16 f0 a5 62 40 c6 57 47 2f e3 0c 81 c8 24 9e f1 bb 0c 36 7d 3f 97 f3 32 1e 93 fa 32 be 9a a9 21 07 7e 67 ed 1d 53 77 c2 f1 22 8f df b3 91 0b 73 c7 f8 b1 50 8f eb 7d e7 38 64 f2 4e 86 7b 4c 20 ab ef 27 d4 c7 d4 9d 54 1f 97 ac 18 3f 17 b7 ec 65 c4 78 c7 2a 6f 4b df 6a 7e 1f 43 22 9a 65 31 f6 2b c0 e4 df 26 fe 5e 3e de 57 7d eb ef ff 1e 43 0f eb f2 f9 cb 7d 05 7c a6 df 9f e1 bd cf cf cf 8f f7 b5 99 78 8b be c9 d2 f7 eb 10 9f 6f ac be 3b e8 c3 bb e8 7b 53 b7 fd 08 fa 56 56 df be ed c3 e5 f3 57 36 7d 5d fa ac ee 56 ff cd f4 f5 6c df 27 db be ab e9 fb 7b 2d 1f 9e b5 7d 77 a9 6f fd 6b c9 43 87 3e 8b 77 a8 6f 78 eb c1 9b 4a 2a f8 5d f5 dd 45 1f fe c5 03 17 a5 dc ab c4 3f 4a 7d eb c3 ec c9 8b 5d 08 3d 2b 31 0a 21 16 79 a5 fa fa 92 77 ff 76 27 c0 21 1d 0d 18 ad 4b 18 24 2f 53 80 70 9f 41 2a 00 18 2d 00 e4 13 6d 9f d5 7b c2 8e ea 51 97 35 02 7d b3 bd c6 e6 95 c4 87 c3 24 3c 77 1e d7 aa af f9 d8 6a 14 a3 fd b6 5f ba 7f 66 3a 9d 16 cc 41 7f 8b bd cc 60 5f bc 10 7f 9a b0 37 3e 53 7d 83 48 e4 c0 d2 f5 5a 38 43 a1 cf 0d d8 29 bc 86 e9 85 d4 a7 20 7d 08 b8 5a 7d 8d b8 44 be 6a 42 f6 e8 93 82 aa cf 62 89 f4 99 d7 a1 2f 5d d1 51 2d d6 7d c8 58 39 96 f2 09 9e b7 d0 07 5d 7b 66 a0 a1 2f 5e e9 f8 ea 95 c4 e7 cd 8f 35 d5 2e 74 b6 7e d8 5d 60 7c 9e fa 40 74 4f 6d ac e8 2b 83 57 bf 0c 7d 32 9e 9f c6 08 39 0b 2b c5 8a be ab 6d df 0e 23 1a 5a fa bc fc 9c a5 7c 9d b1 1b 4e 4f c5 41 8b 71 c4 d4 e6 e5 22 cf 4b e9 5b b6 81 f1 d2 d0 e7 42 2c 1b b8 28 f3 42 65 d7 30 1e c8 d9 67 fa f0 49 9e 57 ec f8 7c 49 96 86 c0 e5 f5 e6 58 63 a4 6f de d2 77 b5 fa a2 ed 03 d5 0b 46 ec 50 f0 51 4b 5a 3a d3 da c6 0b 75 3d ef a1 ef 52 f5 c1 12 04 a6 1a fa d0 87 a3 30 53 fa 5e 2f 67 7b aa fa Data Ascii: PNGIHDR>WEBPLTEkkkN"rrrxyq@IDATx]b:WB@2WVZB`'octQSa`6?$2H@2L2yP=;:scQ8zC6~li7q b@WG/$6}?22!~gSw"sP}8dN{L 'T?ex*oKj~C"e1+&^>W}C}|xo;{SVVW6}]Vl'{-}wokC>woxJ*]E?J}]=+1!ywv'!K$/SpA*-m {Q5}$<wj_f:A`_7>S}HZ8C) }Z}DjBb/]Q-}X9]{f/^5.t~]`|@tOm+W}29+m#Z|NOAq"K[B,(Be0gIW|IXcowFPQKZ:u=R0S^/g{

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49727	54.93.101.66	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 20:37:54.390695095 CET	204	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: unbouncepages.com Connection: Keep-Alive Cookie: ubvs=84.17.52.741614371565357000; ubvt=84.17.52.741614371565357000
Jan 13, 2021 20:37:54.437995911 CET	204	IN	HTTP/1.1 404 Not Found date: Wed, 13 Jan 2021 19:37:54 GMT content-type: text/plain; charset=ISO-8859-1 transfer-encoding: chunked p3p: CP="This is not a privacy policy." content-encoding: gzip x-proxy-backend: page-server connection: close Data Raw: 34 39 0d 0a 1f 8b 08 00 00 00 00 00 00 0a c9 48 55 28 4a 2d 2c 4d 2d 2e 49 4d 51 08 0d f2 51 28 4f 2c 56 c8 cb 2f 51 48 cb 2f cd 4b 51 c8 cf 53 28 c9 c8 2c 56 28 4e 2d 2a 4b 2d d2 03 00 00 00 ff ff 03 00 d6 82 03 c0 2f 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 49HU(J-,M-.IMQQ(O,V/QH/KQS(,V(N-*K-/0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49734	3.212.31.157	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 20:37:54.488975048 CET	206	OUT	GET /i?stm=1610599073847&e=pv&url=http%3A%2F%2Funbouncepages.com%2F46598534393037243839343 37fl%2F&tv=js-2.14.0&tna=sp-ub&aid=landing_page&p=web&tz=America%2FLos_Angeles&lang=en-US&cs=utf-8&f _pdf=0&f_qt=0&f_realp=0&f_wma=0&f_dir=0&f_fla=1&f_java=1&f_gears=0&f_ag=0&res=1280x1024&cd=24&cookie =1&eid=2a64a8a9-e27f-48c4-a48a-7a2ffc5351b0&dtm=1610599073842&vp=784x554&ds=890x622&vid=1&sid=28f3e9e7- e98b-42c9-b3d2-0538bae3dee1&duid=2b34fd73-4516-40da-a1ed-d8d4fe0d734c&uid=84.17.52.74161437156535 7000&cx=eyJzY2hlbWEiOiJpZ2x1OmNvbS5zbm93cGxvd2FuYWx5dGljcy5zbm93cGxvdy9jb250ZXh0cy9qc29uc2 NoZW1hLzEtMC0wIiwiZGF0YSI6W3sic2NoZW1hIjoianNfdHJhY2tlcl9jb250ZXh0X3YxLjEuanNvbiIsImRhdGEiOnsicGFnZU lkIjoiZWNiZDlkZGItNjBjNC00MmRhLThjMWItN2Q5NTVhMWM4Mjk1IiwidmFyaWFudElkIjoiYSIsImV2ZW50VHlw ZSI6InZpc2l0IiwiZXZlbnRNZXRhZGF0YSI6W10sInJvdXRpbmdTdHJhdGVneSI6IndlaWdodGVkIn19XX0 HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: http://unbouncepages.com/46598534393037243839343 37fl/ Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: events.ub-analytics.com Connection: Keep-Alive
Jan 13, 2021 20:37:54.617114067 CET	207	IN	HTTP/1.1 200 OK Date: Wed, 13 Jan 2021 19:37:54 GMT Content-Type: image/gif Content-Length: 43 Connection: keep-alive P3P: policyref="/w3c/p3p.xml", CP="NOI DSP COR NID PSA OUR IND COM NAV STA" Access-Control-Allow-Origin: * Access-Control-Allow-Credentials: true Server: akka-http/10.0.9 Data Raw: 47 49 46 38 39 61 01 00 01 00 f0 00 00 ff ff ff 00 00 00 21 f9 04 01 00 00 00 00 2c 00 00 00 00 01 00 01 00 00 02 02 44 01 00 3b Data Ascii: GIF89a!,D;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49738	54.93.101.66	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 20:38:10.492245913 CET	233	OUT	GET /46598534393037243839343 37fl/favicon.ico HTTP/1.1 User-Agent: AutoIt Host: unbouncepages.com Cookie: ubpv=a%2Cecbd9ddb-60c4-42da-8c1b-7d955a1c8295; ubvt=84.17.52.741614371565357000; ubvs=84.17.52.741614371565357000
Jan 13, 2021 20:38:10.644714117 CET	234	IN	HTTP/1.1 404 Not Found date: Wed, 13 Jan 2021 19:38:10 GMT content-type: text/plain; charset=ISO-8859-1 content-length: 47 p3p: CP="This is not a privacy policy." x-proxy-backend: page-server connection: close Data Raw: 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e Data Ascii: The requested URL was not found on this server.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.6	49739	54.93.101.66	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 20:38:14.109415054 CET	235	OUT	GET /4659853439303724383934337fl/clkn/https/artsana.limpcome.ml/email@thisisforu.com HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: unbouncepages.com Connection: Keep-Alive Cookie: ubpv=a%2Cecbd9ddb-60c4-42da-8c1b-7d955a1c8295; ubrs=weighted; ubvs=84.17.52.741614371565357000; ubvt=84.17.52.741614371565357000
Jan 13, 2021 20:38:14.159493923 CET	235	IN	HTTP/1.1 410 Gone date: Wed, 13 Jan 2021 19:38:14 GMT content-type: text/plain; charset=ISO-8859-1 transfer-encoding: chunked p3p: CP="This is not a privacy policy." cache-control: no-cache, no-store, max-age=0 pragma: no-cache content-encoding: gzip x-proxy-backend: page-server connection: close Data Raw: 35 35 0d 0a 1f 8b 08 00 00 00 00 00 00 04 c1 41 0a 80 30 0c 04 c0 af ec cd 8b f8 1d cf 29 5d 31 18 9a 92 a6 4a 7f ef cc c9 2d 88 e1 11 6b 47 99 89 bc 09 d3 f6 60 f9 c4 e5 66 fe b1 42 7a a7 c4 40 3a 0a a1 ed 15 d3 7a fc 00 00 00 ff ff 03 00 00 9b 17 3d 3d 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 55A0)]1J-kG`fBz@:z==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	54.93.101.66	80	192.168.2.6	49740	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 20:38:24.149976015 CET	267	IN	HTTP/1.1 408 Request Time-out content-length: 110 cache-control: no-cache content-type: text/html connection: close Data Raw: 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 3c 68 31 3e 34 30 38 20 52 65 71 75 65 73 74 20 54 69 6d 65 2d 6f 75 74 3c 2f 68 31 3e 0a 59 6f 75 72 20 62 72 6f 77 73 65 72 20 64 69 64 6e 27 74 20 73 65 6e 64 20 61 20 63 6f 6d 70 6c 65 74 65 20 72 65 71 75 65 73 74 20 69 6e 20 74 69 6d 65 2e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <html><body> 408 Request Time-out Your browser didn't send a complete request in time.</body></html>

HTTPS Packets

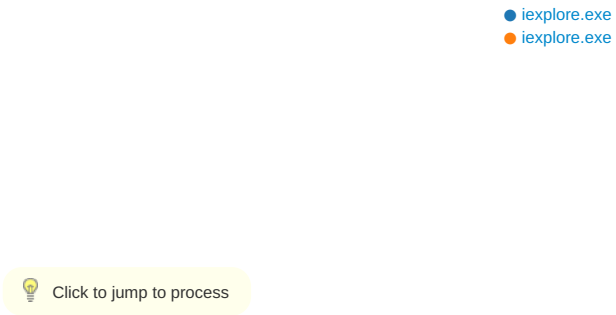
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 13, 2021 20:37:53.850569963 CET	13.225.80.63	443	192.168.2.6	49730	CN=*.cloudfront.net, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Tue May 26 02:00:00 CEST 2020	Wed Apr 21 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		

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 20:37:53.857095957 CET	13.225.80.63	443	192.168.2.6	49731	CN=*.cloudfront.net, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Tue May 26 02:00:00 CEST 2020 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Wed Apr 21 14:00:00 CEST 2021 Tue Aug 01 14:00:00 CEST 2028 Sun Nov 06 00:59:59 CET 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 5612 Parent PID: 792

General

Start time:	20:37:51
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: 476 Parent PID: 5612

General

Start time:	20:37:52
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:5612 CREDAT:17410 /prefetch:2
Imagebase:	0xb10000
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

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly