ID: 404278
Cookbook: browseurl.jbs
Time: 21:28:25
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

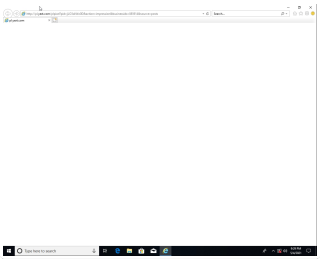
Analysis Report http://pl.yext.com/plpixel?pid=jLO3skW…

Overview

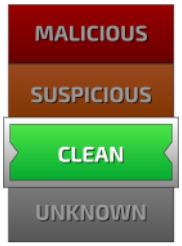
General Information

Sample URL:	http://pl.yext.com/plpixel?pid=jLO3skWo0D&action=impression&businessids=885914&source=posts
Analysis ID:	404278
Infos:	

Most interesting Screenshot:



Detection

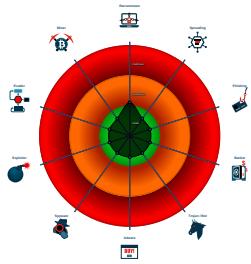


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5892 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5168 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5892 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

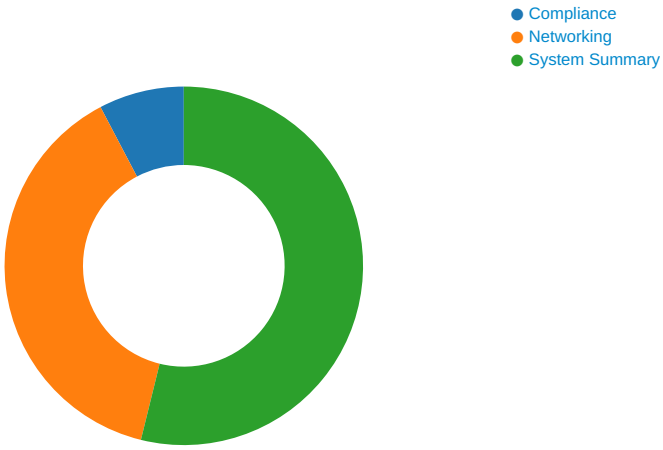
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



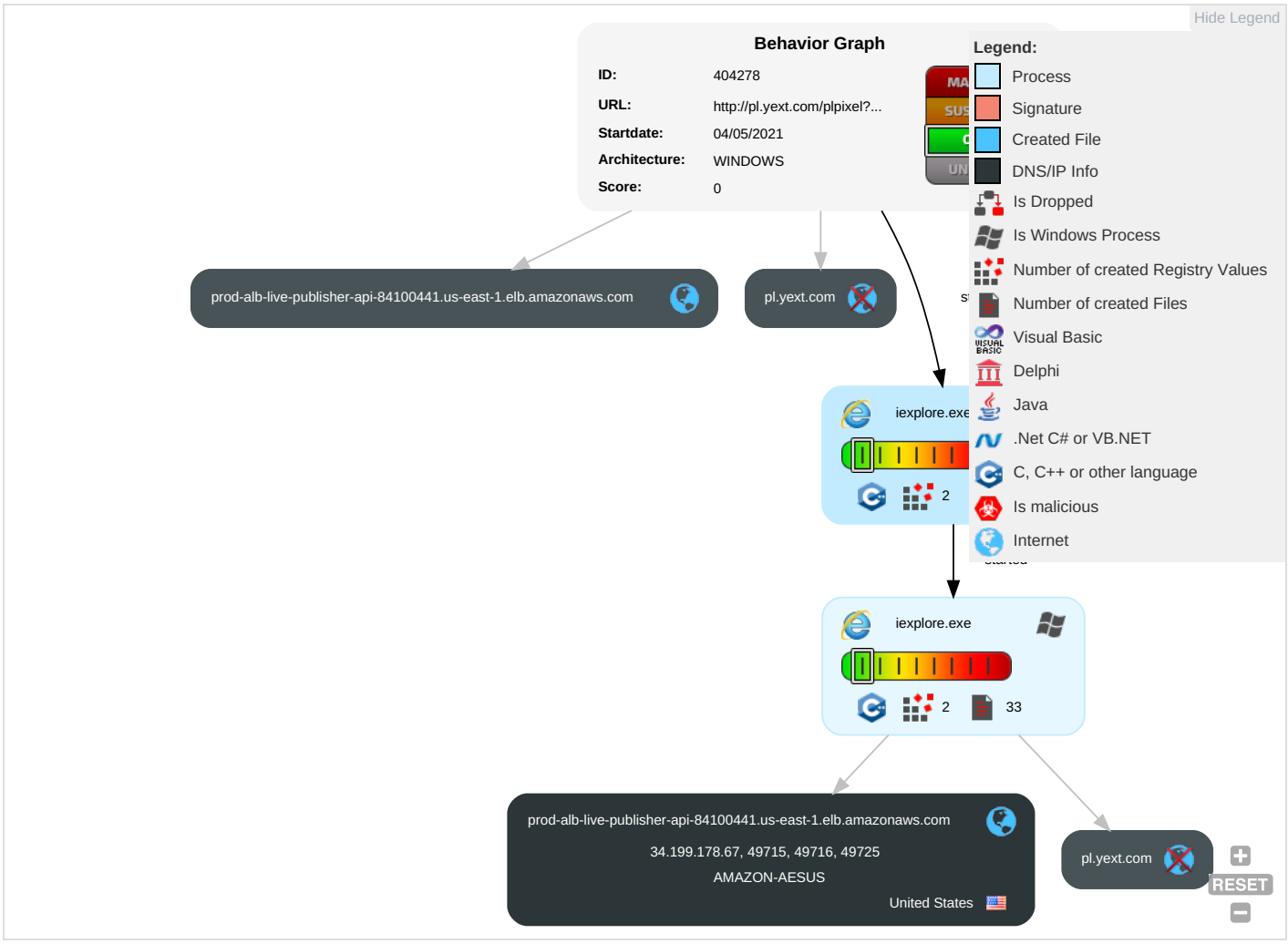
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

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	Non-Application Layer Protocol 3	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	Application Layer Protocol 3	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	Ingress Tool Transfer 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data

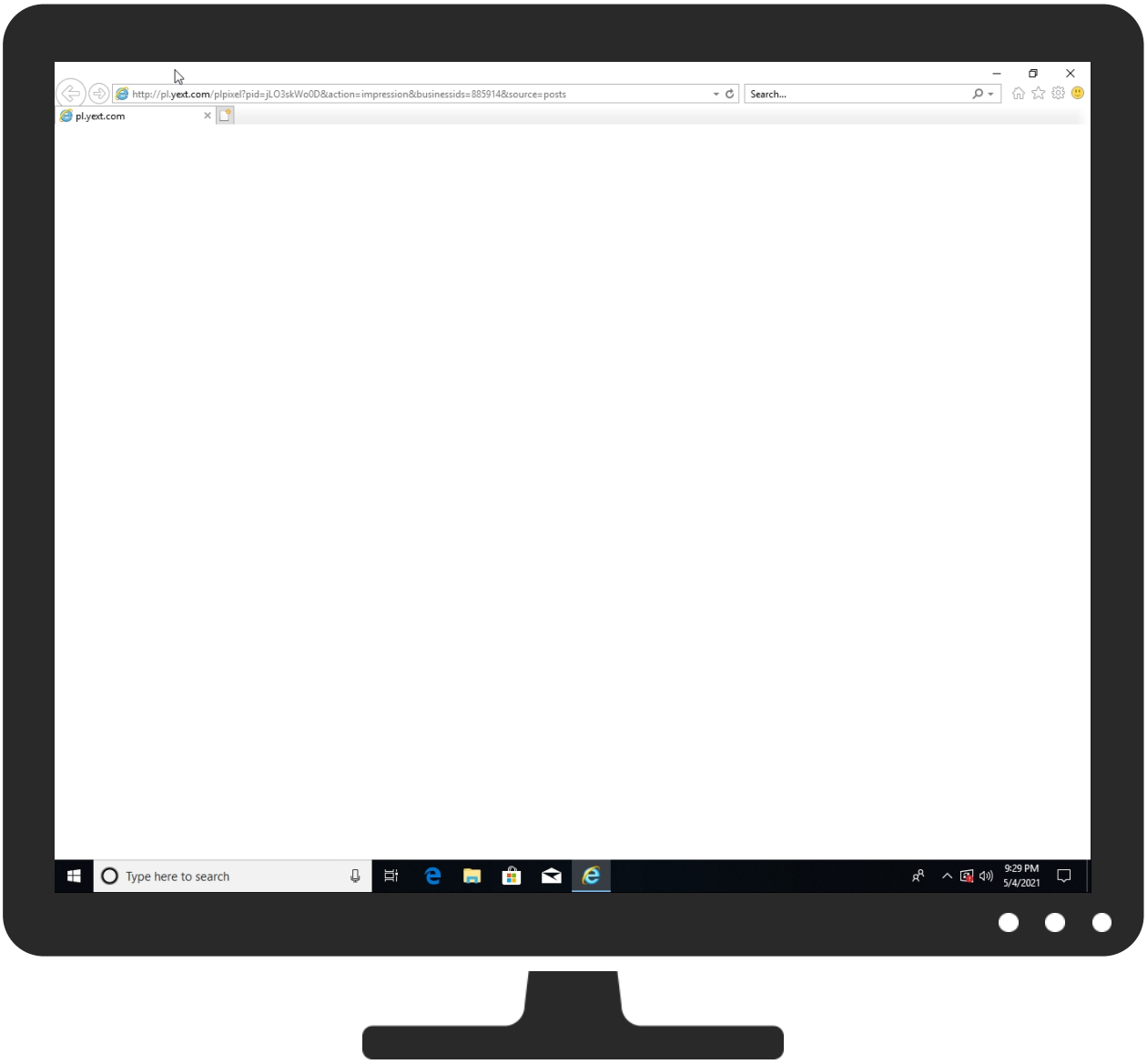
Behavior Graph



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://pl.yext.com/plpixel?pid=jLO3skWo0D&action=impression&businessids=885914&source=posts	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://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
prod-alb-live-publisher-api-84100441.us-east-1.elb.amazonaws.com	34.199.178.67	true	false		high
pl.yext.com	unknown	unknown	false		high

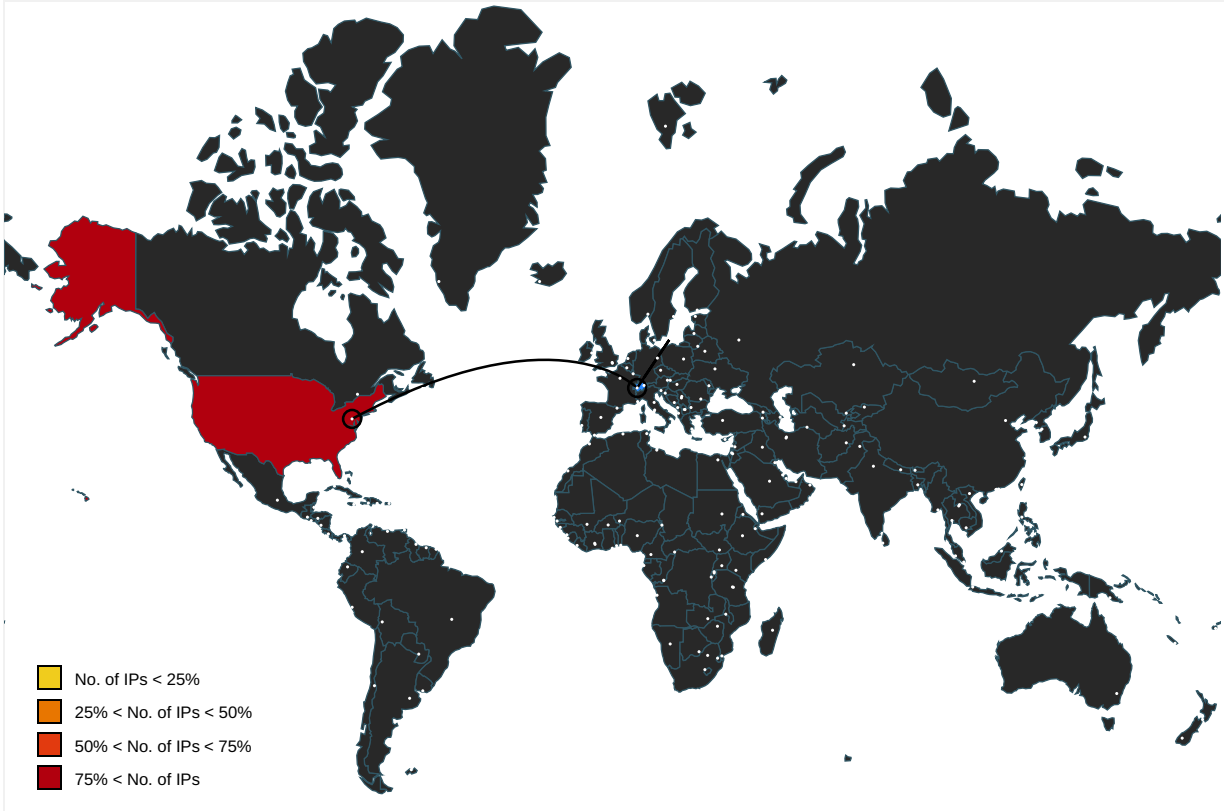
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://pl.yext.com/plpixel?pid=jLO3skWo0D&action=impression&businessids=885914&source=posts	false		high
http://pl.yext.com/plpixel?pid=jLO3skWo0D&action=impression&businessids=885914&source=posts	false		high
http://pl.yext.com/favicon.ico	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.wikipedia.com/	msapplication.xml6.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.com/	msapplication.xml.2.dr	false		high
http://pl.yext.com/plpixel?pid=jLO3skWo0D&action=impression&businessids=885914&source=postsRoot	{72C0D54A-AD5A-11EB-90E4-ECF4BB862DED}.dat.2.dr	false		high
http://www.nytimes.com/	msapplication.xml3.2.dr	false		high
http://www.live.com/	msapplication.xml2.2.dr	false		high
http://www.reddit.com/	msapplication.xml4.2.dr	false		high
http://www.twitter.com/	msapplication.xml5.2.dr	false		high
http://www.youtube.com/	msapplication.xml7.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.199.178.67	prod-alb-live-publisher-api-84100441.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404278
Start date:	04.05.2021
Start time:	21:28:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://pl.yext.com/plpixel?pid=jLO3skWo0D&action=impression&businessids=885914&source=posts
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@3/16@2/1
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 23.54.113.53, 52.255.188.83, 168.61.161.212, 88.221.62.148, 23.57.80.111, 152.199.19.161, 20.50.102.62, 93.184.221.240, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, go.microsoft.com, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, ie9comview.vo.msecnd.net, wu.ec.azureedge.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, cs9.wpc.v0cdn.net • VT rate limit hit for: http://pl.yext.com/plpixel?pid=jLO3skWo0D&action=impression&businessids=885914&source=posts

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{72C0D548-AD5A-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8557876183710507
Encrypted:	false
SSDEEP:	48:IwKGcprPGwpLMgG/ap8MzdZGIpcMzZGdoGvnZpvMzZGdNYGoGrqp9MzZGdNkJGoC:ruZ5ZV2WLWxLtxsfxHhMxSx1xufxjMX
MD5:	1ED371DFB16BC2124F32C890A1E68A90
SHA1:	2D0BBEAB694C375D0EEE1FF1F4186E7A02EB4B43
SHA-256:	623C11ACCD724D05FDAE62E5A9F6409931004A05CC5B80ABAF165CDF9D66780F
SHA-512:	6795916D662C3A82CE091F3A7AB0EBD517D52320378543C59C497047111B9941D42FDBBD6EE686ED77515FDDD96668CE12B994C4C2F6A91A33303D7E383B659
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\{72C0D54A-AD5A-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24292
Entropy (8bit):	1.6545629082717215
Encrypted:	false
SSDEEP:	48:IwzGcpruGwpaiG4pQCGrapbSbZGQpBKGHHpccaTGUp81WGzYpmfpOGopD1NJK8O3:rJZGQS6EBSbzjR2cqWcMR+XOCbg
MD5:	1B0DE80CB5B1195061E906E3E4438A94
SHA1:	F44B57113B441918CC4B0F6D4FB8EA34C8885754
SHA-256:	5643A109B5F0EFD707643A3FB5F01001F0A7361F5A9115DB1F4DAEE6BD726930
SHA-512:	31AD4E8DD75544E6506A89700C4732E32691E0113E6D00D841D2E09E8A96C04B3B22F3BA2B98D89FFF5C91AB721B07B1C7FC0AC9A56CFB550BF72D89A3BE20D
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\{72C0D54B-AD5A-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5621408844462001
Encrypted:	false
SSDEEP:	48:IwfGcpraGwpauG4pQSGrapbSj4ZGQpK5G7HpRVaTGIpG:r1ZCQO6UBSEzAYTVeA
MD5:	3F0B6BE270F975C086F1628B52BC9D7D
SHA1:	13CCA5F9C286B41741A1C18209DBC953DC8CBD34
SHA-256:	1DD7B326C0971D2FB8D19E91AF911B4856C30AB34F33890B03154244C0794CCD
SHA-512:	3B154AE160C07E3A3D0D562FB7AB5F1E53C2E80F99D195371D5DDE906C62983491403EDDB09881C8B6E12D5ADB29E0D321BCB5E3089B668F629F79FBBC84D8F
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Size (bytes):	656
Entropy (8bit):	5.118648628353623
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEwGelBGeknWimI002EtM3MHdNMNxOEwGelBGeknWimI00ObVbkEtMb:2d6NxOcGwBSZHKd6NxOcGwBSZ76b
MD5:	D82FE7F9BD07CC08794E479FB1076D7F
SHA1:	8C8ADA67241B69D0940EA98BF3FB19105C6246FD
SHA-256:	0575F1D9C83CAD3CB71D4FFB269B4CBCBAFF461D34E3E78379E402D8EEDF9870
SHA-512:	AF1E21052C14B66617FB2DFB35F5B0AAFCC3B492A3DBE587166FD08AD66623D6F74390DB667FD2658D564D4FD07688A2C00917F1C78C07580D26401B3CDDD6
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x48cb98a1,0x01d74167</date><accdate>0x48cb98a1,0x01d74167</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x48cb98a1,0x01d74167</date><accdate>0x48cb98a1,0x01d74167</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.143884337576146
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kwGXMsBGXMznWimI002EtM3MHdNMNxe2kwGXMsBGXMznWimI00ObkS:2d6Nxr8XMswXMzSZHKd6Nxr8XMswXMzo
MD5:	28BE69E2B0F5F0A40C5E3311A5A87E67
SHA1:	56AEADB0208C80256ACF4AC4FED7C4390708855E
SHA-256:	B7A5CE8FEF01ABDB0DB7B253CA8A3FF5F6892380D54D4FB61EDA8007B2EAD50B
SHA-512:	E4AD20FBA55856225581C475327BAF0AAA913DAEAB6654537E11A1ECA66C37A42561CB1C3369FC5D0E7DC809E2EAABDF5B9BF06F2BA73CC2285D14CF6CADA208
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x48c20f24,0x01d74167</date><accdate>0x48c20f24,0x01d74167</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x48c20f24,0x01d74167</date><accdate>0x48c20f24,0x01d74167</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.137573570248449
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLwGelBGeknWimI002EtM3MHdNMNxvLwGelBGeknWimI00ObmZEtMb:2d6NxvnGwBSZHKd6NxvnGwBSZ7mb
MD5:	12B2C6C1F3979F09AD0FE93AC66AC0C3
SHA1:	0F5123102A24C0E09446C7CB940ED60C62B3A7F5
SHA-256:	535E5AE74583F1F20F610F66496F0799CA029C7051B89D7C2F660E9229F24AF7
SHA-512:	C6FF5D2E80A4C68B5A6774A354E255B99C05B65BF07999539B9321AAAA0A52F40D9B0BE403AC2B28ECD10397391A8DCEC7C00C74C1E136DE3D4867EAC08A60EB
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x48cb98a1,0x01d74167</date><accdate>0x48cb98a1,0x01d74167</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x48cb98a1,0x01d74167</date><accdate>0x48cb98a1,0x01d74167</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.117019072538733
Encrypted:	false
SSDEEP:	12:TMHdNMNxiwGTysBGTyznWimI002EtM3MHdNMNxiwGTysBGTyznWimI00Obd5EtMb:2d6NxCOswOzSZHKd6NxCOswOzSZ7Jjb

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
MD5:	78475D7A1E8729689293BC962833B69C
SHA1:	84B9235D2196BACFD0B2B5DDBE882456ECB9325A
SHA-256:	1A14EB9A0ADAE82CA73236A485908FC750A999B90E132AD2AB2EDD675E58538E
SHA-512:	03DC8C0EFF54E18CBD4CC3E145D35587A8B546DDC46008FAC68763151A02498F3C635C42FB1101F767285DF903D9D487AE4307C066D045CB27C3D93CC14000
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x48c6d3c4,0x01d74167</date><acc date>0x48c6d3c4,0x01d74167</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x48c6d3c4,0x01d74167</date><accdate>0x48c6d 3c4,0x01d74167</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.1497491279024965
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwwGelBGeknWimI002EtM3MHdNMNxhGwwGelBGeknWimI00Ob8K075t:2d6NxQ4GwBSZHKd6NxQ4GwBSZ7YKajb
MD5:	00BD479719430A37CA605B00987D8452
SHA1:	234E04CFEF93A014912225A2766A38AAD0EF3D99
SHA-256:	4BBA6662F557011FE7421EBDB5B0C3B62C23D89C41740A1E75E3F9CAF5F68035
SHA-512:	A3CD36ECE4DEDB665AF3530766FF3D1A962E3AFED99E763BFB2E787989FC687BED301D221D979FD23676831AA03E5EE4ABF93A892C2F6BA1BF8D22F41712A2 E7
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x48cb98a1,0x01d74167</date>< accdate>0x48cb98a1,0x01d74167</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x48cb98a1,0x01d74167</date><accdate>0 x48cb98a1,0x01d74167</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.159062762750786
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nwGoBGnnWimI002EtM3MHdNMNx0nwGoBGnnWimI00ObxEtMb:2d6Nx0zownSZHKd6Nx0zownSZ7nb
MD5:	8E5A07D5BCFAD9E1C4E6E25CA5CBDC53
SHA1:	443DA826F62A021DE8488E8EA37C9D5F362E2FB2
SHA-256:	CA700B329A58B634BDF8018D72305A8E9E4FDC7B1763B204A191FD2A829DF600
SHA-512:	A207371794FEE00A3FEEB608BCF43B14E34A2A57567D430AACFA393C0B4E3D331B9F9B42151EB71E88900F9EEB6F1242C7027157C9A754982389FD914C81FE33
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x48c93629,0x01d74167</date><a ccdate>0x48c93629,0x01d74167</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x48c93629,0x01d74167</date><accdate>0x4 8c93629,0x01d74167</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.141588794701767
Encrypted:	false
SSDEEP:	12:TMHdNMNxxwGTysBGTyznWimI002EtM3MHdNMNxxwGTysBGTyznWimI00Ob6Kq5Es:2d6NxtOswOzSZHKd6NxtOswOzSZ7ob
MD5:	16BF3C34364FB45F69068119C930CEB3
SHA1:	22E355E13EC1BEDE8D0CE012A15D7CEE63531909
SHA-256:	720B12F5DA8BDC76EA646ED189070E0A5FFAD7B9EE13D159A8EAE0A6A31B1E1D
SHA-512:	B15495110B8521AE46FD08EE9A298D69CBF0AF869958B2F21E4DEF78E02D1F1C9963D06EBE86CAF385ED12789251E918CAF7FDB2415C41FCEA4778BB96ED383 5

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x48c6d3c4,0x01d74167</date><accdate>0x48c6d3c4,0x01d74167</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x48c6d3c4,0x01d74167</date><accdate>0x48c6d3c4,0x01d74167</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.118160027555834
Encrypted:	false
SSDEEP:	12:TMHdNMNxcwG6BG9nWimI002EtM3MHdNMNxcwG6BG9nWimI00ObVEtMb:2d6NxE6w9SZHKd6NxE6w9SZ7Db
MD5:	C300B8CA3862CB83F5223452BB6B079F
SHA1:	1B047375BB494788616CACD65DEE446A21C72687
SHA-256:	28CFAAB6C9CA2BEF39331C611ED82618531564288ADCF2B22762CB2BB190D0A7
SHA-512:	51A4FE9A208F77A01145E2FB750CB7D4E921F60987F9C3564E57811126B9988F21CD61E654015C50251CA808D550F1DA9D30187DE7164365476D0178663DB6C8
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x48c4717b,0x01d74167</date><accdate>0x48c4717b,0x01d74167</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x48c4717b,0x01d74167</date><accdate>0x48c4717b,0x01d74167</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.102533930646739
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnwG6BG9nWimI002EtM3MHdNMNxfnwG6BG9nWimI00Obe5EtMb:2d6Nx76w9SZHKd6Nx76w9SZ7ijb
MD5:	4AE0310E19397F5AAFFA69363E4D4618
SHA1:	42C90E5A3AE8AC653C7315CAC96E4CE4539B178F
SHA-256:	0D096B79A1D8F9B0770B6D1EF8D5161DFE08269AAA7746689F686EA291414C38
SHA-512:	C94DC9A4AD5F2CF63906F98E6D99D446853D89DD3ED8E75234A5812AA44039E4308BF62BD224DC78E4A2B8F4944A82B1E74CCD415644AFC283B4CEC9C299E98
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x48c4717b,0x01d74167</date><accdate>0x48c4717b,0x01d74167</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x48c4717b,0x01d74167</date><accdate>0x48c4717b,0x01d74167</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\plpixel[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):	3.2226627197680635
Encrypted:	false
SSDEEP:	3:CUMllRPQSkL1pse:Gl3QSk/se
MD5:	BA036C43037CFE89320D1EF7B64CD43F
SHA1:	88C72D3E26047EB1E45E5564A76427734F120EFE
SHA-256:	42CB846E07917F6731406E500F24AEB2E88C42CDA124EAA59E08C5331CAD8BCB
SHA-512:	AA80CCD27C05EB729F730B9D830B011650BCF12CBB25D19EDF29EFCF962C7465BB5685A5FF5D084356C6710C08E829D16B59E7A59A41767EB14744F326B6C12
Malicious:	false
Reputation:	low
IE Cache URL:	http://pl.yext.com/plpixel?pid=jLO3skWo0D&action=impression&businessids=885914&source=posts
Preview:	GIF89a.....!.....,.....L..;

C:\Users\user\AppData\Local\Temp\~DF45977A94477E6E61.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.48152912321792085
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loMDF9loMJ9lWMzZGdYlwrwZGywpGyw3lwfrwf2:kBqoIMSMMMzZGdYCkZGzpGz3Cfkf2
MD5:	61953B12B3A79A2FCFAAFDB1A6C31258
SHA1:	C46FA3B8E57FBAA50558AFE59A3B2D0911F163F4
SHA-256:	7D33F6EF38A37DCBA69A8E6080AE464F47BFF386BDB890A6B2D79E9CED42756D
SHA-512:	0D90ED879C5A367E565BFAD3A278E6CA4B1A18082EEA4B4C5DF2B3074D65F1E482411CAF45B22FDD91A93CF14071E1B824D1B6EB61ACAE75E2E33A8214DEF AC
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF8D99E155CE31F5C7.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.29696483110168154
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAP8w:kBqoxxJhHWSVSEabkw
MD5:	A1B57865A8E0AF72FE962D84ED804E30
SHA1:	E827528CB5006E8F1DA76030D4C83BFE5A539B4F
SHA-256:	E075C9C9E8E527F715BE1D63073CA741409D7CBB9B5FCF23045AFF0506085CDE
SHA-512:	05F345D023009FDE272D74D7E4C17B7DDC5DE2979136C7BC5A3CAE84018BA60FD234E18DE3584B357CBB86ECCA6A2EA578C7EF0E2433F384D6F8C7854EC9D 04
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF915A8B709283DF05.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34485
Entropy (8bit):	0.37309038912613673
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwd/9lwl9l2T9l2T9l/7:kBqoxKAuvScS+d4QKjfIfx1NJK8OyQ
MD5:	D61589A2604A131BC830A9CBB8D28F08
SHA1:	FCFF4CF771088386EE9B0F6FCF2F1F7EE855FB11
SHA-256:	8CC6467D588B7ADD0537F0DDE810EFB71B7C0A5D7D428606E445E113E8704266
SHA-512:	97E6992659897815147FC8068D29E591BD1BCCEFC3AFD0998726EE6A0A091C5524F1272B34CD66FAFC0530ABDF46ECC6B8DED2919455941EDABDEEC7ED23B 61
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

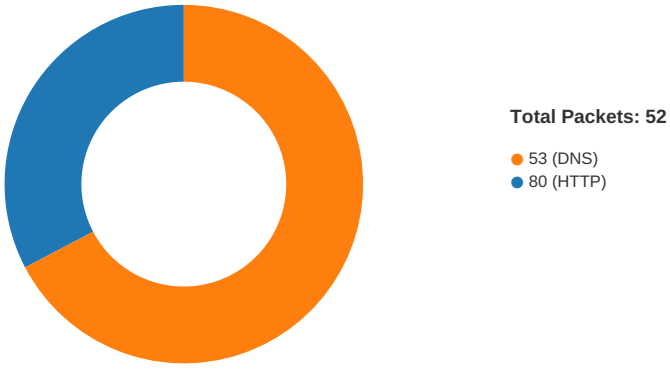
No static file info

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-21:29:18.636079	TCP	2925	INFO web bug 0x0 gif attempt	80	49715	34.199.178.67	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:29:18.366904020 CEST	49715	80	192.168.2.3	34.199.178.67
May 4, 2021 21:29:18.366935968 CEST	49716	80	192.168.2.3	34.199.178.67
May 4, 2021 21:29:18.499411106 CEST	80	49715	34.199.178.67	192.168.2.3
May 4, 2021 21:29:18.499516010 CEST	49715	80	192.168.2.3	34.199.178.67
May 4, 2021 21:29:18.499526024 CEST	80	49716	34.199.178.67	192.168.2.3
May 4, 2021 21:29:18.499584913 CEST	49716	80	192.168.2.3	34.199.178.67
May 4, 2021 21:29:18.500699043 CEST	49715	80	192.168.2.3	34.199.178.67
May 4, 2021 21:29:18.634727955 CEST	80	49715	34.199.178.67	192.168.2.3
May 4, 2021 21:29:18.636079073 CEST	80	49715	34.199.178.67	192.168.2.3
May 4, 2021 21:29:18.636198044 CEST	49715	80	192.168.2.3	34.199.178.67
May 4, 2021 21:29:19.124270916 CEST	49715	80	192.168.2.3	34.199.178.67
May 4, 2021 21:29:19.301080942 CEST	80	49715	34.199.178.67	192.168.2.3
May 4, 2021 21:29:19.428241014 CEST	80	49715	34.199.178.67	192.168.2.3
May 4, 2021 21:29:19.428262949 CEST	80	49715	34.199.178.67	192.168.2.3
May 4, 2021 21:29:19.428270102 CEST	80	49715	34.199.178.67	192.168.2.3
May 4, 2021 21:29:19.428378105 CEST	49715	80	192.168.2.3	34.199.178.67
May 4, 2021 21:29:19.428422928 CEST	49715	80	192.168.2.3	34.199.178.67
May 4, 2021 21:29:19.429438114 CEST	49715	80	192.168.2.3	34.199.178.67
May 4, 2021 21:29:19.429462910 CEST	49715	80	192.168.2.3	34.199.178.67
May 4, 2021 21:29:34.406034946 CEST	49725	80	192.168.2.3	34.199.178.67
May 4, 2021 21:29:34.538872004 CEST	80	49725	34.199.178.67	192.168.2.3
May 4, 2021 21:29:34.539088011 CEST	49725	80	192.168.2.3	34.199.178.67
May 4, 2021 21:29:34.539208889 CEST	49725	80	192.168.2.3	34.199.178.67
May 4, 2021 21:29:34.671900988 CEST	80	49725	34.199.178.67	192.168.2.3
May 4, 2021 21:29:34.777885914 CEST	80	49725	34.199.178.67	192.168.2.3
May 4, 2021 21:29:34.777914047 CEST	80	49725	34.199.178.67	192.168.2.3
May 4, 2021 21:29:34.777998924 CEST	49725	80	192.168.2.3	34.199.178.67
May 4, 2021 21:29:34.778213024 CEST	49725	80	192.168.2.3	34.199.178.67
May 4, 2021 21:29:34.778249979 CEST	49725	80	192.168.2.3	34.199.178.67

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:29:08.523149967 CEST	64938	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:08.577058077 CEST	53	64938	8.8.8.8	192.168.2.3
May 4, 2021 21:29:09.413702965 CEST	60152	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:09.444279909 CEST	57544	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:09.462547064 CEST	53	60152	8.8.8.8	192.168.2.3
May 4, 2021 21:29:09.505116940 CEST	53	57544	8.8.8.8	192.168.2.3
May 4, 2021 21:29:11.043932915 CEST	55984	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:11.092643023 CEST	53	55984	8.8.8.8	192.168.2.3
May 4, 2021 21:29:11.982235909 CEST	64185	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:12.042475939 CEST	53	64185	8.8.8.8	192.168.2.3
May 4, 2021 21:29:13.017007113 CEST	65110	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:13.067894936 CEST	53	65110	8.8.8.8	192.168.2.3
May 4, 2021 21:29:13.887789965 CEST	58361	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:13.936398029 CEST	53	58361	8.8.8.8	192.168.2.3
May 4, 2021 21:29:15.122016907 CEST	63492	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:15.171597958 CEST	53	63492	8.8.8.8	192.168.2.3
May 4, 2021 21:29:16.281929970 CEST	60831	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:16.333282948 CEST	53	60831	8.8.8.8	192.168.2.3
May 4, 2021 21:29:16.875655890 CEST	60100	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:16.937247992 CEST	53	60100	8.8.8.8	192.168.2.3
May 4, 2021 21:29:17.312208891 CEST	53195	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:17.360846996 CEST	53	53195	8.8.8.8	192.168.2.3
May 4, 2021 21:29:18.293873072 CEST	50141	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:18.357564926 CEST	53	50141	8.8.8.8	192.168.2.3
May 4, 2021 21:29:18.438671112 CEST	53023	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:18.487394094 CEST	53	53023	8.8.8.8	192.168.2.3
May 4, 2021 21:29:20.931278944 CEST	49563	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:20.982793093 CEST	53	49563	8.8.8.8	192.168.2.3
May 4, 2021 21:29:21.893368959 CEST	51352	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:21.944955111 CEST	53	51352	8.8.8.8	192.168.2.3
May 4, 2021 21:29:22.773684025 CEST	59349	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:22.824340105 CEST	53	59349	8.8.8.8	192.168.2.3
May 4, 2021 21:29:23.592231989 CEST	57084	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:23.642874956 CEST	53	57084	8.8.8.8	192.168.2.3
May 4, 2021 21:29:24.700480938 CEST	58823	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:24.757770061 CEST	53	58823	8.8.8.8	192.168.2.3
May 4, 2021 21:29:26.527374983 CEST	57568	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:26.576523066 CEST	53	57568	8.8.8.8	192.168.2.3
May 4, 2021 21:29:27.439093113 CEST	50540	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:27.487682104 CEST	53	50540	8.8.8.8	192.168.2.3
May 4, 2021 21:29:34.339936972 CEST	54366	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:34.402986050 CEST	53	54366	8.8.8.8	192.168.2.3
May 4, 2021 21:29:43.452084064 CEST	53034	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:43.526873112 CEST	53	53034	8.8.8.8	192.168.2.3
May 4, 2021 21:29:46.992909908 CEST	57762	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:47.052699089 CEST	53	57762	8.8.8.8	192.168.2.3
May 4, 2021 21:29:47.841223001 CEST	55435	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:47.890106916 CEST	53	55435	8.8.8.8	192.168.2.3
May 4, 2021 21:29:48.000380993 CEST	57762	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:48.051922083 CEST	53	57762	8.8.8.8	192.168.2.3
May 4, 2021 21:29:48.911113024 CEST	55435	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:48.960601091 CEST	53	55435	8.8.8.8	192.168.2.3
May 4, 2021 21:29:49.017256021 CEST	57762	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:49.071132898 CEST	53	57762	8.8.8.8	192.168.2.3
May 4, 2021 21:29:49.921761990 CEST	55435	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:49.970369101 CEST	53	55435	8.8.8.8	192.168.2.3
May 4, 2021 21:29:51.017884016 CEST	57762	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:51.069626093 CEST	53	57762	8.8.8.8	192.168.2.3
May 4, 2021 21:29:51.830125093 CEST	50713	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:51.880091906 CEST	53	50713	8.8.8.8	192.168.2.3
May 4, 2021 21:29:51.937573910 CEST	55435	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:51.990474939 CEST	53	55435	8.8.8.8	192.168.2.3
May 4, 2021 21:29:55.031830072 CEST	57762	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:55.085724115 CEST	53	57762	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:29:55.953501940 CEST	55435	53	192.168.2.3	8.8.8.8
May 4, 2021 21:29:56.002177954 CEST	53	55435	8.8.8.8	192.168.2.3
May 4, 2021 21:30:02.673202991 CEST	56132	53	192.168.2.3	8.8.8.8
May 4, 2021 21:30:02.735435009 CEST	53	56132	8.8.8.8	192.168.2.3
May 4, 2021 21:30:03.960730076 CEST	58987	53	192.168.2.3	8.8.8.8
May 4, 2021 21:30:04.021013021 CEST	53	58987	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 21:29:18.293873072 CEST	192.168.2.3	8.8.8.8	0xfa57	Standard query (0)	pl.yext.com	A (IP address)	IN (0x0001)
May 4, 2021 21:29:34.339936972 CEST	192.168.2.3	8.8.8.8	0xc11f	Standard query (0)	pl.yext.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 21:29:18.357564926 CEST	8.8.8.8	192.168.2.3	0xfa57	No error (0)	pl.yext.com	prod-alb-live-publisher-api-84100441.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:29:18.357564926 CEST	8.8.8.8	192.168.2.3	0xfa57	No error (0)	prod-alb-live-publisher-api-84100441.us-east-1.elb.amazonaws.com		34.199.178.67	A (IP address)	IN (0x0001)
May 4, 2021 21:29:18.357564926 CEST	8.8.8.8	192.168.2.3	0xfa57	No error (0)	prod-alb-live-publisher-api-84100441.us-east-1.elb.amazonaws.com		34.232.90.111	A (IP address)	IN (0x0001)
May 4, 2021 21:29:18.357564926 CEST	8.8.8.8	192.168.2.3	0xfa57	No error (0)	prod-alb-live-publisher-api-84100441.us-east-1.elb.amazonaws.com		34.232.174.249	A (IP address)	IN (0x0001)
May 4, 2021 21:29:34.402986050 CEST	8.8.8.8	192.168.2.3	0xc11f	No error (0)	pl.yext.com	prod-alb-live-publisher-api-84100441.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:29:34.402986050 CEST	8.8.8.8	192.168.2.3	0xc11f	No error (0)	prod-alb-live-publisher-api-84100441.us-east-1.elb.amazonaws.com		34.199.178.67	A (IP address)	IN (0x0001)
May 4, 2021 21:29:34.402986050 CEST	8.8.8.8	192.168.2.3	0xc11f	No error (0)	prod-alb-live-publisher-api-84100441.us-east-1.elb.amazonaws.com		34.232.90.111	A (IP address)	IN (0x0001)
May 4, 2021 21:29:34.402986050 CEST	8.8.8.8	192.168.2.3	0xc11f	No error (0)	prod-alb-live-publisher-api-84100441.us-east-1.elb.amazonaws.com		34.232.174.249	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- pl.yext.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49715	34.199.178.67	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 21:29:18.500699043 CEST	1124	OUT	GET /plpixel?pid=jLO3skWo0D&action=impression&businessids=885914&source=posts 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: pl.yext.com Connection: Keep-Alive
May 4, 2021 21:29:18.636079073 CEST	1125	IN	HTTP/1.1 200 OK Date: Tue, 04 May 2021 19:29:18 GMT Content-Type: image/gif Content-Length: 43 Connection: keep-alive Expires: Fri, 01 Jan 1990 00:00:00 GMT Pragma: no-cache Cache-control: no-cache, must-revalidate Data Raw: 47 49 46 38 39 61 01 00 01 00 80 01 00 00 00 00 ff ff ff 21 f9 04 01 0a 00 01 00 2c 00 00 00 00 01 00 01 00 00 02 02 4c 01 00 3b Data Ascii: GIF89a!,L;
May 4, 2021 21:29:19.124270916 CEST	1130	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: pl.yext.com Connection: Keep-Alive
May 4, 2021 21:29:19.428241014 CEST	1133	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 04 May 2021 19:29:19 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Server: nginx Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49725	34.199.178.67	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 21:29:34.539208889 CEST	1229	OUT	GET /favicon.ico HTTP/1.1 User-Agent: AutoIt Host: pl.yext.com
May 4, 2021 21:29:34.777885914 CEST	1229	IN	HTTP/1.1 503 Service Unavailable Date: Tue, 04 May 2021 19:29:34 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Server: nginx Cache-Control: no-cache Data Raw: 36 62 0d 0a 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 3c 68 31 3e 35 30 33 20 53 65 72 76 69 63 65 20 55 6e 61 76 61 69 6c 61 62 6c 65 3c 2f 68 31 3e 0a 4e 6f 20 73 65 72 76 65 72 20 69 73 20 61 76 61 69 6c 61 62 6c 65 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 69 73 20 72 65 71 75 65 73 74 2e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a 0d 0a Data Ascii: 6b<html><body> 503 Service Unavailable No server is available to handle this request.</body></html>

Code Manipulations

Statistics

Behavior

● iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5892 Parent PID: 792

General

Start time:	21:29:15
Start date:	04/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff71b9b0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 5168 Parent PID: 5892

General

Start time:	21:29:16
Start date:	04/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5892 CREDAT:17410 /prefetch:2
Imagebase:	0x11b0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly