ID: 338019
Cookbook: browseurl.jbs
Time: 14:31:03
Date: 11/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

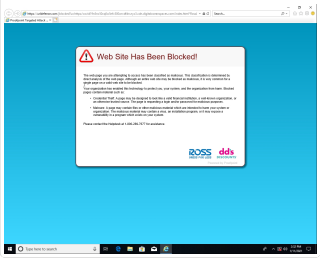
Analysis Report https://urldefense.com/jblocked?u=http…

Overview

General Information

Sample URL:	https://urldefense.com/jblocked?u=https:/covid19n5nc50cq0w5nfc500wrcdfdn.ny....com&c=rossstores_2_hosted&sig=xNz2wqSyfC7BuocSXhbPxEY94BKVH5LRt084W97v3_g=
Analysis ID:	338019

Most interesting Screenshot:



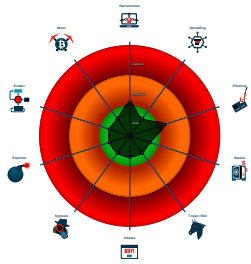
Detection

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

Signatures

URL contains potential PII (phishing…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 2432 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5436 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2432 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

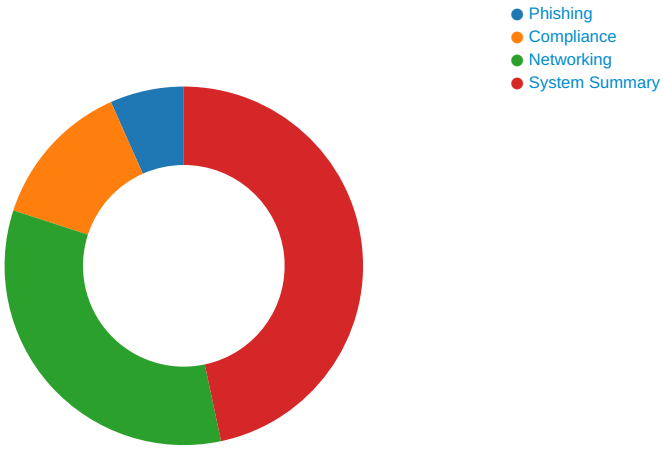
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



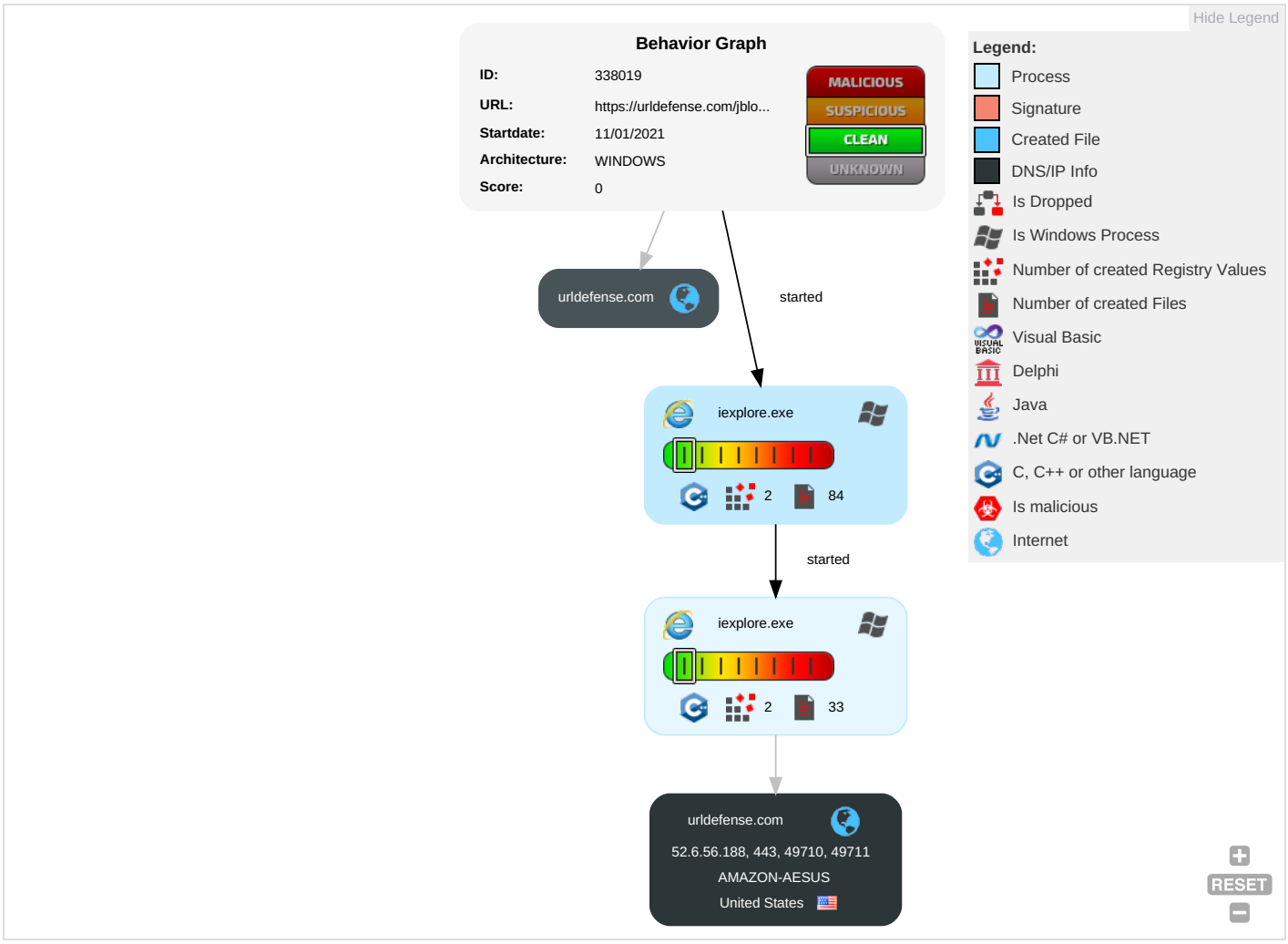
Click to jump to signature section

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	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partiti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lockc
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data

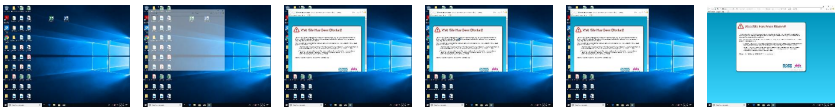
Behavior Graph

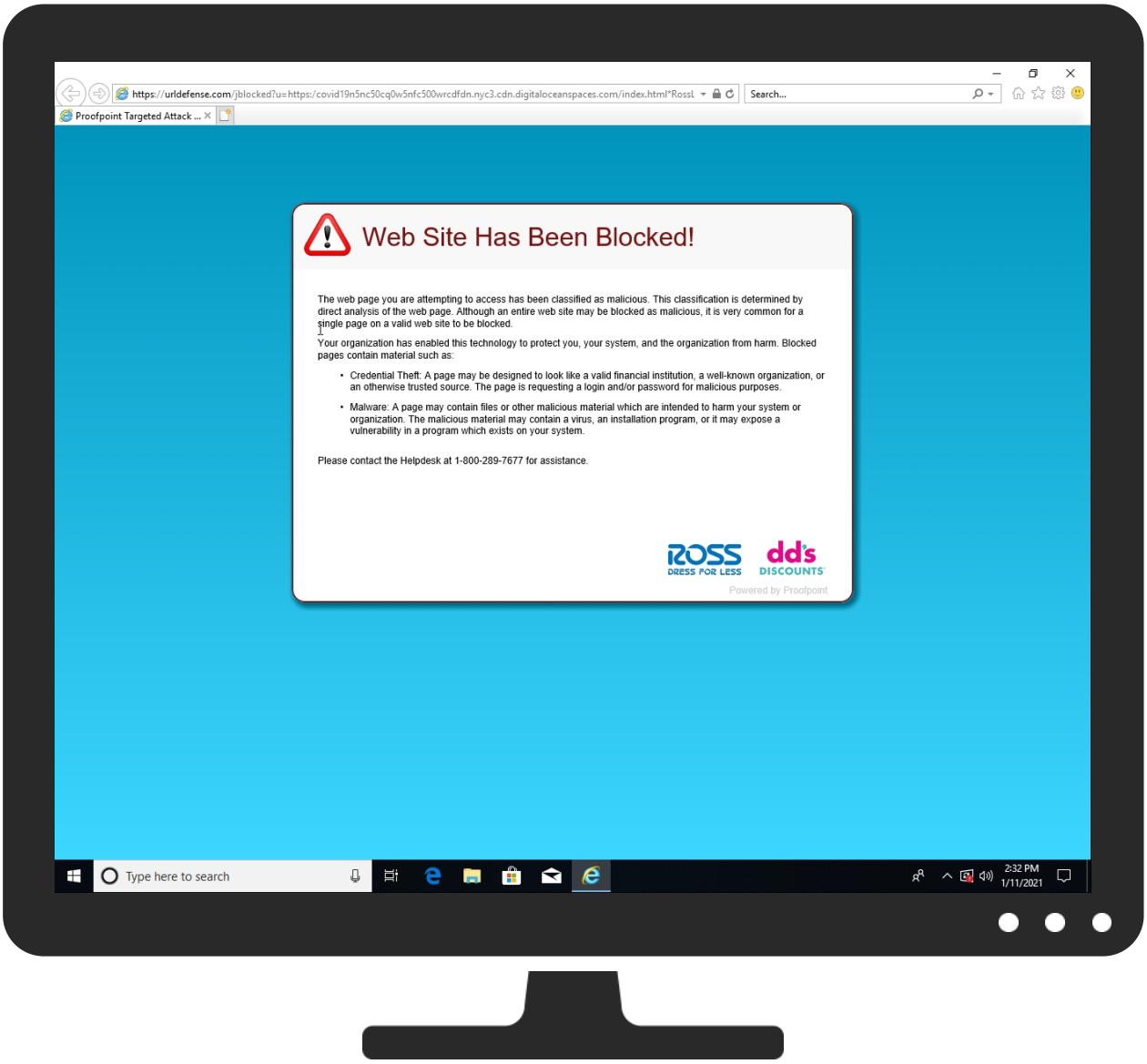


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://urldefense.com/jblocked?u=https:/covid19n5nc50cq0w5nfc500wrcdfdn.nyc3.cdn.digitaloceanspaces.com/index.html*RossLogistics.Procurement@ros.com&c=rossstores_2_hosted&sig=xNz2wqSyfC7BuocSXhbPxEY94BKVH5LRt084W97v3_g=	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
urldefense.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.wikipedia.com/	0%	URL Reputation	safe	

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	
http://https://urldefense.com/jblocked?u=https:/covid19n5nc50cq0w5nfc500wrcdfdn.nyc3.cdn.digitaloceanspaces	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
urldefense.com	52.6.56.188	true	false	• 0%, Virustotal, Browse	unknown

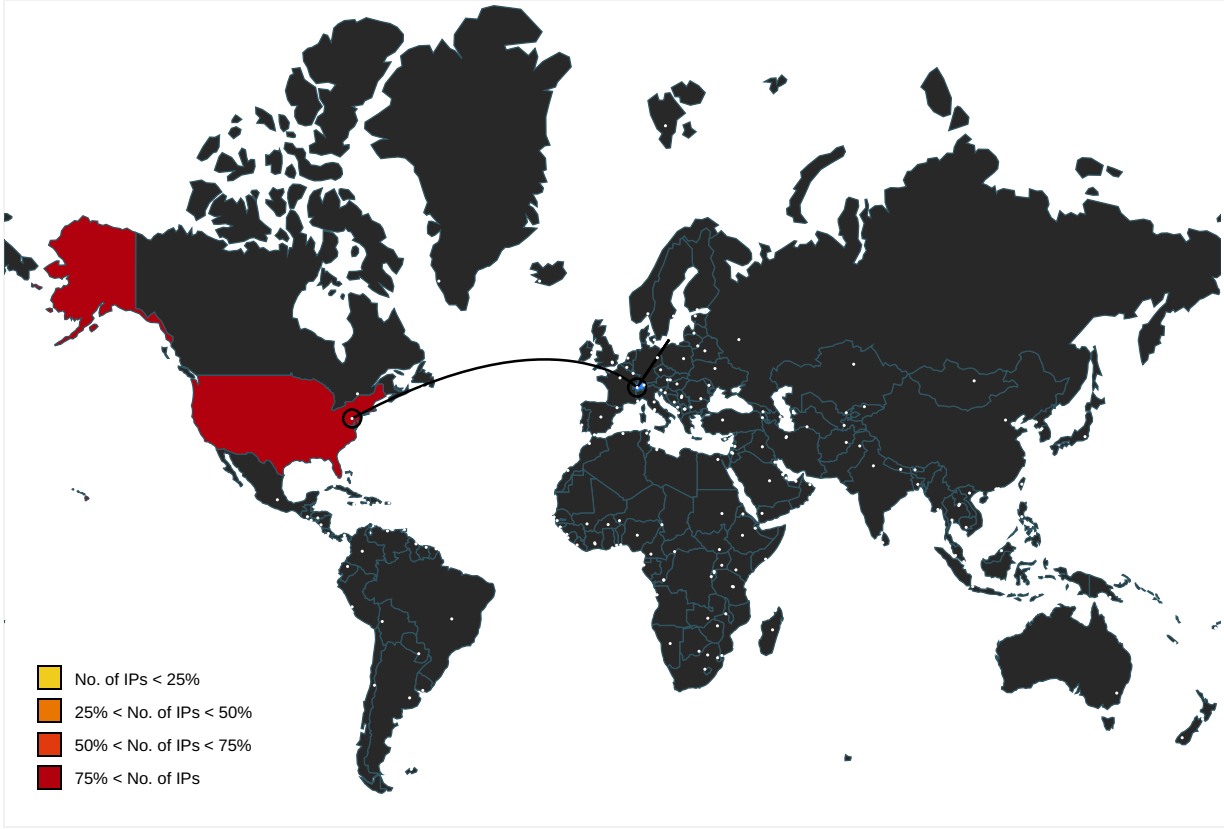
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://urldefense.com/jblocked?u=https:/covid19n5nc50cq0w5nfc500wrcdfdn.nyc3.cdn.digitaloceanspaces.com/index.html*RossLogistics.Procurement@ros.com&c=rossstores_2_hosted&sig=xNz2wqSyfC7BuocSXhbPxEY94BKVH5LRt084W97v3_g=	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.wikipedia.com/	msapplication.xml6.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.com/	msapplication.xml.1.dr	false		high
http://https://urldefense.com/jblocked?u=https:/covid19n5nc50cq0w5nfc500wrcdfdn.nyc3.cdn.digitaloceanspaces	{CC1C6D80-545C-11EB-90E4-ECF4BB862DED}.dat.1.dr, ~DF34F91D8FD1A165B0.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://www.nytimes.com/	msapplication.xml3.1.dr	false		high
http://www.live.com/	msapplication.xml2.1.dr	false		high
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://www.twitter.com/	msapplication.xml5.1.dr	false		high
http://www.youtube.com/	msapplication.xml7.1.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.6.56.188	unknown	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	338019
Start date:	11.01.2021
Start time:	14:31:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://urldefense.com/jblocked?u=https:/covid19n5nc50cq0w5nfc500wrcdfdn.nyc3.cdn.digitaloceanspaces.com/index.html*RossLogistics.Procurement@ros.com&c=rossstores_2_hosted&sig=xNz2wqSyfC7BuocSXhbPxEY94BKVH5LRt084W97v3_g=
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:	15
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@3/18@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): 88.221.62.148, 168.61.161.212, 104.43.193.48, 51.11.168.160, 152.199.19.161, 104.79.90.110, 92.122.213.247, 92.122.213.194, 93.184.221.240 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.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, go.microsoft.com, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.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, go.microsoft.com.edgekey.net, blobcollector.events.data.trafficmanager.net, cs9.wpc.v0cdn.net

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.{CC1C6D7E-545C-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8584740847802503
Encrypted:	false
SSDEEP:	96:rvZIZX2d9Wo/2to/tfo/XFMojMeoqoMbfoDssX:rvZIZX2d9WvtUfQFMqFVf/sX
MD5:	1E4D6190A2035F99B88BF5F44407733F
SHA1:	4F17D3E4F84DD0E706F031DC55520D20E6D5C104
SHA-256:	B9EC511A1FE931E97EFD8BCE065642D6A3DEB41EE1677BC85C87D119AEF98856
SHA-512:	242A60FBF8B5A9BACB88AC330AD07F73789AF097B7E50C89518ED92C1E5111739B957420289598021282FA207CF55A5D5B70388C51573742CF59B0E32FA786E9
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\{CC1C6D80-545C-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24552
Entropy (8bit):	1.7061104960196973
Encrypted:	false
SSDEEP:	48:IwPGcpriGwpaOG4pQGGrapbSMrGQpByGHHpc4sTGUp8ZGzYpmVkYGopADb0BW1JW:rFZKQu6IBSMFjJ24kW3MWYiccyGg
MD5:	A26DD4069BFD53C1DDEC6DB9172B35A2
SHA1:	A31863036F5F4BB57D642F99AEBA2811C98A6319
SHA-256:	7021435279C4081D296583C883EAFC7373DFDB59F8E5DD2FE53F384D97D13029
SHA-512:	A11262294FC12F7F30A93FDA51FD7C36816ABE4DDFA5672C4EB2309CA95A6E7B4AF5085EB68AA5FFE2FC2997DF7565BA39B2F51CAE2A4BA9130BC202229D0FAD
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\{CC1C6D81-545C-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5666895226732889
Encrypted:	false
SSDEEP:	48:IwpGcprPfGwpah0G4pQDmGrapbSQtrGQpKiG7HpRDtsTGIpG:rvZPpQhE6DoBSwFANTh4A
MD5:	52677FDB636B4D4C84C1C2D661DE43E3
SHA1:	CB8D58364129A1FABC369431EBA5A6216CEA3F52
SHA-256:	40F6B65E240E9121AD5DB320664DFCE37F97DB7882F278047F47DDFF0B958174
SHA-512:	B88921DA6766D5F2AA45305BD03F5A95605B7B53672FB10BEB8234E30E46A261F146D7CB3681F14B71A5062B5EA67C2062900B45A83D835B468FB2D73A92C3E5
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
Size (bytes):	656
Entropy (8bit):	5.1118812941794864

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEYF+FJnWimI002EtM3MHdNMNxOEYF+FJnWimI00ObVbkEtMb:2d6NxONF+FJSZHKd6NxONF+FJSZ76b
MD5:	11281647A72B5CA8EA807496D9A580C2
SHA1:	606F075FD814AAE51A712C594D76E6DCF0E3E506
SHA-256:	740D3C5DB5ED26E7AA90F9B0E925E95BA320B3DB42D0966DC8DAC027C16DD7B7
SHA-512:	161573BF74D181E682CC78CD2B20EE07F1EDCF5A20531D575DF17AEDAC0444F0ECE47E872E5AF9ACC757E41AC131DEC65B902C1C0AB5BFFB0CC8CD579C78DB7
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xa1877365,0x01d6e869</date><accdate>0xa1877365,0x01d6e869</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>0xa1877365,0x01d6e869</date><accdate>0xa1877365,0x01d6e869</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):	5.1259482888256
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kOX3+cUX3+cJnWimI002EtM3MHdNMNxe2kOX3+cUX3+cJnWimI00Ob:2d6Nxr/LULJSZHKd6Nxr/LULJSZ7Aa7b
MD5:	2750CD3C8590A1E6121E21EB2EAD0DE5
SHA1:	B0B51996624674D55B35547A364BD6A0463CB207
SHA-256:	E679796B7C5DFC55FEDD57545BE02DAACDAD30F13D868F0BD8CE443807BD7E4E
SHA-512:	C61AA495F75598E4F568F514A540449D06360C6412FFBA68AC5721265F669FCF2F268529444F729451F28B5B69F5FB5A6BC19BE4B7642648164AD2431E2FFD1E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xa1804c56,0x01d6e869</date><accdate>0xa1804c56,0x01d6e869</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>0xa1804c56,0x01d6e869</date><accdate>0xa1804c56,0x01d6e869</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):	5.130867571429364
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLYF+FJnWimI002EtM3MHdNMNxvLYF+FJnWimI00ObmZEtMb:2d6NxvUF+FJSZHKd6NxvUF+FJSZ7mb
MD5:	CD6B9B6BEA7A5C11B952ED78F8ED02BC
SHA1:	077A130BD8831712D33ECC0350DDE32B28293E6A
SHA-256:	4CB918EAF7A239587F36CB0BF01F25085AA3285D9E31C90F3347293CFD8AF517
SHA-512:	5A30BC9C455B1AEDC2AA3AEC6F298FA9DE55C57F8519228A9CCBE5D7193B1CEAA1B507E5063BE784A3E8BFA21B1150792BD315AE2E693FD64EC522E5407B5D3E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xa1877365,0x01d6e869</date><accdate>0xa1877365,0x01d6e869</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>0xa1877365,0x01d6e869</date><accdate>0xa1877365,0x01d6e869</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):	5.114902172709555
Encrypted:	false
SSDEEP:	12:TMHdNMNxiEuJnWimI002EtM3MHdNMNxiEuJnWimI00Obd5EtMb:2d6NxRuJSZHKd6NxRuJSZ7Jjb
MD5:	9FF98E8A06CB9CF4D4C39CD2B366AB3F

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
SHA1:	FB06169A2B9B86260CE4A526DBEA202F97530875
SHA-256:	98F2290A8386C8D8C84E09A1DE647162DFE543675ADF9B7A4E54680C1EBC3BA1
SHA-512:	2DFF15603E07EB0938590D782B30FF2F217BCF89ABFFA0129F5A10A534B1074C3F1FFD70A53C773EB4DA360497883B1428612080C0125C5068F1C9142F5B5589
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xa1851112,0x01d6e869</date><acc date>0xa1851112,0x01d6e869</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>0xa1851112,0x01d6e869</date><accdate>0xa1851 112,0x01d6e869</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):	5.144501318705123
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwQaGaJnWimI002EtM3MHdNMNxhGwQaGaJnWimI00Ob8K075EtMb:2d6NxQLaGaJSZHKd6NxQLaGaJSZ7YKa/
MD5:	FF7DD4A466B28B639B35CD077FBFDFD2
SHA1:	E9EE2BA733A916999E67B4D28BA98694C1A0213F
SHA-256:	BA3E83CB0F685C6157B29D02A6B4FA57397ACCA7974B342893015614DCA8B300
SHA-512:	B6CD3750B8A4EB0DF363C43F8061C93EFF0FFD81E1FD94003E0A03127E2F53CDAF93964C29B114EA3F44EED44D76571F54E233C6DCA97A64B42199760029844
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xa189d5b7,0x01d6e869</date>< accdate>0xa189d5b7,0x01d6e869</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>0xa189d5b7,0x01d6e869</date><accdate>0 xa189d5b7,0x01d6e869</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):	5.115132686386509
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nYF+FJnWimI002EtM3MHdNMNx0nYF+FJnWimI00ObxEtMb:2d6Nx0YF+FJSZHKd6Nx0YF+FJSZ7nb
MD5:	03E3095186FE9B4AF31B69FC1893A7BD
SHA1:	C535D2BFAB51027E69AFE5E61D97E375AC2C0EA7
SHA-256:	8E1F05538865C9E952074648F7C422203199F5F120D95B23ECEF7737F6997A5C
SHA-512:	50A16DCB144DFF7C546CB76167E653DC9B15D98B3F0386662B7DD5286F90A63A847B86F9B057BCCD86DEE7319B30373F4EF4EFF40235775311B4F04371B2F476
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xa1877365,0x01d6e869</date><a ccdate>0xa1877365,0x01d6e869</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>0xa1877365,0x01d6e869</date><accdate>0xa 1877365,0x01d6e869</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):	5.13950093770561
Encrypted:	false
SSDEEP:	12:TMHdNMNxxEuJnWimI002EtM3MHdNMNxxEuJnWimI00Ob6Kq5EtMb:2d6NxauJSZHKd6NxauJSZ7ob
MD5:	7E1DD3C6A22B33C7331C936C6ADE2C81
SHA1:	29243B5496003C7FF596C45255D9726B4DCC52B0
SHA-256:	5A54F8C9366878827BB455C448A5A4E2846D0F4C261926BB80F19817D4E0DDCB
SHA-512:	6EA8DBF2EC925DF46AD11AD1F7F1902EA65AD0F50316B9C83AB53021E370C21749ABC06DB723AA93FA0305DED68B52E58CE0A2244CE73286E000720FAADA1A 5A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xa1851112,0x01d6e869</date><accdate>0xa1851112,0x01d6e869</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>0xa1851112,0x01d6e869</date><accdate>0xa1851112,0x01d6e869</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):	5.093032147451174
Encrypted:	false
SSDEEP:	12:TMHdNMNxcecYcJnWimI002EtM3MHdNMNxcecYcJnWimI00ObVEtMb:2d6NxLcYcJSZHKd6NxLcYcJSZ7Db
MD5:	E0AF87F53A6D801D04798006D60C5FD0
SHA1:	274521BEAE60DE78E5A9BED59286782B84F93444
SHA-256:	71BFC7C396A9C7E98934CCF7B65D75FECFBB563D86C637D372DF2B38EEBF2396
SHA-512:	B6D4164BD00D885B4E2A34277B7596D78466C51A6B9E00A85DB54D26E3B8EDE02396F9AA87621B2650FADB297FC46127B57C402B7CFE8AC3C8D20E801407DC(D
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xa182aead,0x01d6e869</date><accdate>0xa182aead,0x01d6e869</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>0xa182aead,0x01d6e869</date><accdate>0xa182aead,0x01d6e869</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):	5.100531020678819
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnEuJnWimI002EtM3MHdNMNxfnEuJnWimI00Obe5EtMb:2d6NxcuJSZHKd6NxcuJSZ7ijb
MD5:	76A1A2E5CC7615593DEE431208CCE623
SHA1:	B5845C1D6DF2B37573D6E4A2A2D4D8D17411541C
SHA-256:	20EB1675842F7F7C6C378807837178AE2DC7A774C204E78A11CBBAAA209C6122
SHA-512:	697F49B1372BECD526EDCB6C16432E0A9A69D4B318A8E342774029F2A8507735081CC6EA559E7E771E84983A6FB70EA9F4179806BEEBC1D54113BA97B47E255A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xa1851112,0x01d6e869</date><accdate>0xa1851112,0x01d6e869</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>0xa1851112,0x01d6e869</date><accdate>0xa1851112,0x01d6e869</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\0W10PBUV\warning[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 64 x 64, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4803
Entropy (8bit):	7.945415885603797
Encrypted:	false
SSDEEP:	96:bXPZaTvJQ6JqwminbkmNmxvkX76/rNQPQm0iPLfROzIya:L8jJFJqOkzxvczL0UbRO5a
MD5:	B69B8937C432C824243F1FF03FE4A169
SHA1:	CFF98ABE81FE41B5A2FAF269CB0F6859B616ED51
SHA-256:	8A552613C9B52A23149A7CEFE7C15C321E62162AED70E9A736E6C96BBB07BC5F
SHA-512:	75943C9F3728E8A7BB98D5C108C5F5B7982C3C18C559353B818A4BCE1EED8CD408B868964B853BAC42A8F3BC662AE242C91D344D1D53EC4F1048C4FA59AB2DC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://urldefense.com/jasset/images/warning.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\warning[1].png	
Preview:	.PNG.....IHDR...@...@.....iq.....sRGB.....}IDATx..y..U..?..~U..Z.'.t..:...$$!....DV.....[D...t.:.2...#g.....D..A.....9s...,.$!!Io.[u-..{w..u7.tc....v..._u.z.{.....5...rX.._.....Z..._."..... ._...n....&v.....(a.Rj.....[.|./.....nR6wk..@:SQA<Q.~:.H...Z./...Jw"1.N.o.....37N....3R).g.R.:)q..P....K....e.....X....|.P..;._.p..}{>3..7....{U.....a4.%F...K&...Q...R..-_<o....]..... Cj..'6.....:_....!.....1N..".D.H..Q...L.\....t...o|[z.7./..=.WO..Z5..t..!.X..2.B.....q5..5...../...2|..s.y...o?..emF;R...MW.O.W....+.&...d.}.....x.A..a.a.>Z..g..t...{..m.....I..2.k<...Q.0..,\@ ../A....z.6\L.I.(..C..Q..j.d.(..1..o+..:...;:.WUVi,]N,o..(.B..khy.{q^.Q.....}...;.BJ%<[.S%.KRQ[..:.N.....-....kj.w.tu.*.iSD5@.E4.'..}.z....Y.8...5M.^....''!...).YS%.%...y.=..t.[.....LoCbq ,J..p...yT.x<.X.QT.V...u.O^.@G.%..z.j..>.m-.;....4..6~&...)."U.A...|.R@o*I..!Q.....JjW.!.La.%.....i.2.'..}....6...`..?.V....[TJ%T.J..18...NX. ....."..0...E...I)....<

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\d723658279cbbd35cfd26ed15f20032fe7106cc37e64f913fd3c854d50deb3f0[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 200 x 50, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	9819
Entropy (8bit):	7.973276769809071
Encrypted:	false
SSDEEP:	192:i2uAmvFSXlBx63s/KzNvbDxhthV6YdF/8Id3SrGq8hvFbyJFo:i2uAm8b/KzNv7tzR5+Xk
MD5:	19265450D040390E5A1E3F16D1CEAA4F
SHA1:	99B8E17D0F4BC38873EC35FF11E31267F14C989B
SHA-256:	D723658279CBBD35CFD26ED15F20032FE7106CC37E64F913FD3C854D50DEB3F0
SHA-512:	60F4F5B215BDEC29FF58D0A901E4800EDF8E7203A40DB755C4B81A75916D0702A98317F93CFB8F58A4926BDBD83B0A9E4C39675600A0BDC302F1EB85F3BFAEA E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://urldefense.com/jimg/d723658279cbbd35cfd26ed15f20032fe7106cc37e64f913fd3c854d50deb3f0
Preview:	.PNG.....IHDR.....2.....Q.....sRGB.....gAMA.....a.....pHYs...%...%.IR$.....bKGD.....tIME.....(.....%.IDATx^.}.`TU..7....H!.PB.....*.."6...v]PDd.....X@.E:.;.k..RH HH....{o...RXD..O..y.{.;.)..wG. P...Lxh.5.A..@.AjP.k.&.A....1....u..j..n.....0..}U.(_.g..L..v..F...LP..D.....Fj...%../'.....0..h...!.%.T..`F#..zx!.6Q.~.P.b....{S...a.V7=7.7`..5....h..ru.B.. .n.j.R..\.e.X..(..B. ...K..^?.Ss..).i.<Y.J...d.X..k..-...V...h.J.X...6..FU)ZE2..Hk...}i.....C,..!..a.....f.h..v.6..Xa.....&..Az..M..+..8&.....}}.x.k....P._1lL.>....'9.f*..8.>6X.p..l..G.D.QX..... U.p<5O.W..,S@..{....J..|6.....&f.._.....1-0.Y....E...B..t...ft.....r.g....s..I.SEP..z...5...E.k.J#.l.....U2x1..k..S.d"...|..5...6E.:...r...-8~:..c=..U.."....3"cjO.....5g.z5...)u.*D..[..)...7.)....n=.....'.V.z.....so04.T.d...QU..l.8.TJ.....fM.;..L..s...$...I7.(....&.K.....IW.n..<..&.4.....r. >0..U^U6..2..*2.....n.....,gY.T.l..=..Qz..T...&....3....0...22.....qc.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\common[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	2864
Entropy (8bit):	5.139585964425596
Encrypted:	false
SSDEEP:	48:K/maEciRyMzMoKVJV1VAVMVwVJVNVZVMVoVcVqNHAVJV1VAVMVwVUVPVn5csN9Y5:5wiRJgo7NHut5csTUFPVLTP
MD5:	2FEC9CA2BE9C015E692928EB54429CA1
SHA1:	EAD795B071563A70FB00600551DDF1C7B2E2D07D
SHA-256:	080218E94B8FBE62AB1CBA4465CD549A03737E69C25F4FC375DA5AD9DC58DC35
SHA-512:	FA7DDE474AE3E0CBFA42E93C7D6836F66610D288FF02E9739BD7C749EDC9811CC9D34AE3D770E4F044C8BDE9C7F3D76C16CE68D3417F384BABEB2B82A85B2 C29
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://urldefense.com/jasset/stylesheets/common.css
Preview:	html{..min-height:100%;..background:#0094bc;..background:-moz-linear-gradient(#0094bc, #3dd6ff);..background:-ms-linear-gradient(#0094bc, #3dd6ff 100%);..backgr ound:-webkit-gradient(linear, left top, left bottom, from(#0094bc), to(#3dd6ff));..background:-webkit-linear-gradient(#0094bc, #3dd6ff 100%);..background:-o-linear-gradie nt(#0094bc, #3dd6ff 100%);..filter:progid:DXImageTransform.Microsoft.gradient(startColorstr='$background-gradient-start', endColorstr='$background-gradient-end');..-ms-filter:"progid:DXImageTransform.Microsoft.gradient(startColorstr='$background-gradient-start', endColorstr='$background-gradient-end')";..background:linear-gradie nt(#0094bc, #3dd6ff 100%).}.body{..font-family:arial, verdana, helvetica;font-size:12px.}...warningbox{..-moz-box-shadow:3px 3px 10px 3px #006c89;..-webkit-box-shadow:3px 3px 10px 3px #006c89;..box-shadow:3px 3px 10px 3px #006c89;..-webkit-border-top-left-radius:16px;..-moz-border-top-left-radius:16px;..border-top-left-radius:16px;..-webk

C:\Users\user\AppData\Local\Temp\~DF34F91D8FD1A165B0.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34745
Entropy (8bit):	0.41728133544681467
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwb9lwb9l2t9l2t9l/V1:kBqoxKAuvScS+kCo5VIV+Db0BW1JCj4
MD5:	D1D1594C5048F4B7536FEB168B191AD3
SHA1:	1C17F87289DEA8C400D1BA8DEBE6E51D98ADA04B
SHA-256:	8D935524638B0932D388EB741856EF2E281F1D36F86A772B76B11BE0C4A24F8F
SHA-512:	B9C60F8FA1834B45BEBE0EE788159FE0BFC2C0B5927DD3B7EF695315D2D4E4311AFF7195FB8AAD5523DBA2FE3B2562395CF54A04C2C342FF18B4BF6A3BB1B2 AD
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DF34F91D8FD1A165B0.TMP	
Reputation:	low
Preview:	.............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF4C48F98879DBC71D.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...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFD8DDACF787FA4662.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47980575938516806
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo7F9loB9lWox/8h+M:kBqoIKUI/8h+M
MD5:	26FABBD1E2999F1F020594EF9C76805D
SHA1:	201693B062A4F86E524221FE7BEFE571408C39A3
SHA-256:	10E4851A051E9CA0BED74117C51DD6D8FB9259B0A5DC57B530A8717A3DC61501
SHA-512:	F78FD36BF012989EA6A356EE2A67DF22C5E413D53D352EAAA116514F15C508B980821C4866228ABC1BBB827331624515FA9842D3A4A9FC9C49B6659366F444C1
Malicious:	false
Reputation:	low
Preview:	.............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

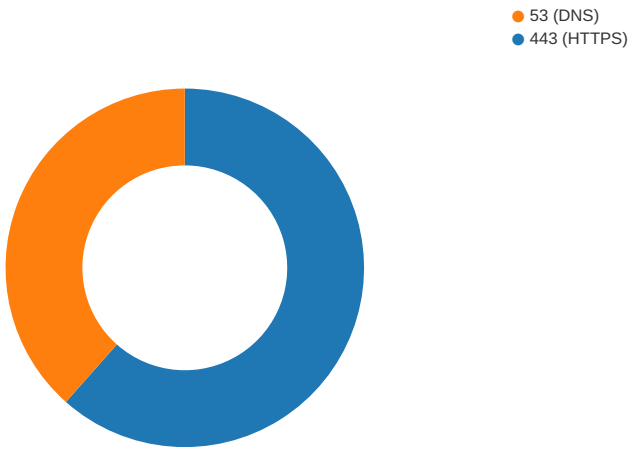
Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 65



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 14:31:52.616950989 CET	49711	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:52.617125988 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:52.743761063 CET	443	49711	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:52.743882895 CET	443	49710	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:52.744030952 CET	49711	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:52.744044065 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:52.754544973 CET	49711	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:52.754831076 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:52.880556107 CET	443	49711	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:52.880990028 CET	443	49710	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:52.883332014 CET	443	49711	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:52.883375883 CET	443	49711	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:52.883423090 CET	443	49711	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:52.883604050 CET	49711	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:52.883692026 CET	443	49710	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:52.883693933 CET	49711	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:52.883733988 CET	443	49710	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:52.883771896 CET	443	49710	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:52.883796930 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:52.883872986 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:52.923588037 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:52.923733950 CET	49711	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:52.930258989 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:52.930428982 CET	49711	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:52.930511951 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:53.051548004 CET	443	49710	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:53.051592112 CET	443	49710	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:53.051630974 CET	443	49711	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:53.051661968 CET	443	49711	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:53.051743984 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:53.051760912 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:53.052257061 CET	49711	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:53.052314043 CET	49711	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:53.052932978 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:53.053421974 CET	49711	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:53.056231022 CET	443	49711	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:53.056260109 CET	443	49710	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:53.056340933 CET	49711	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:53.056391954 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:53.057524920 CET	443	49710	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:53.057631016 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:53.107804060 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:53.107847929 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:53.218605995 CET	443	49710	52.6.56.188	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 14:31:53.218720913 CET	443	49711	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:53.237509966 CET	443	49710	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:53.238070011 CET	443	49710	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:53.238131046 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:53.239670038 CET	443	49710	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:53.239706039 CET	443	49710	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:53.239731073 CET	443	49710	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:53.239741087 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:53.239747047 CET	443	49710	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:53.239767075 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:53.239773035 CET	443	49710	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:53.239794970 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:53.239799023 CET	443	49710	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:53.239830971 CET	443	49710	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:53.239835024 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:53.239871025 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:53.239871025 CET	443	49710	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:53.239892960 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:53.239912987 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:53.286706924 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:53.413717985 CET	443	49710	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:53.413769960 CET	443	49710	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:53.413800955 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:53.413805962 CET	443	49710	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:53.413834095 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:53.413846970 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:53.413870096 CET	443	49710	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:53.413898945 CET	443	49710	52.6.56.188	192.168.2.3
Jan 11, 2021 14:31:53.413938999 CET	49710	443	192.168.2.3	52.6.56.188
Jan 11, 2021 14:31:53.413983107 CET	49710	443	192.168.2.3	52.6.56.188

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 14:31:51.514086008 CET	64185	53	192.168.2.3	8.8.8.8
Jan 11, 2021 14:31:51.572084904 CET	53	64185	8.8.8.8	192.168.2.3
Jan 11, 2021 14:31:52.539813042 CET	65110	53	192.168.2.3	8.8.8.8
Jan 11, 2021 14:31:52.596460104 CET	53	65110	8.8.8.8	192.168.2.3
Jan 11, 2021 14:32:00.276381969 CET	58361	53	192.168.2.3	8.8.8.8
Jan 11, 2021 14:32:00.324436903 CET	53	58361	8.8.8.8	192.168.2.3
Jan 11, 2021 14:32:01.233100891 CET	63492	53	192.168.2.3	8.8.8.8
Jan 11, 2021 14:32:01.283988953 CET	53	63492	8.8.8.8	192.168.2.3
Jan 11, 2021 14:32:02.192189932 CET	60831	53	192.168.2.3	8.8.8.8
Jan 11, 2021 14:32:02.242985010 CET	53	60831	8.8.8.8	192.168.2.3
Jan 11, 2021 14:32:03.200004101 CET	60100	53	192.168.2.3	8.8.8.8
Jan 11, 2021 14:32:03.259418964 CET	53	60100	8.8.8.8	192.168.2.3
Jan 11, 2021 14:32:04.224894047 CET	53195	53	192.168.2.3	8.8.8.8
Jan 11, 2021 14:32:04.272986889 CET	53	53195	8.8.8.8	192.168.2.3
Jan 11, 2021 14:32:10.418358088 CET	50141	53	192.168.2.3	8.8.8.8
Jan 11, 2021 14:32:10.469259024 CET	53	50141	8.8.8.8	192.168.2.3
Jan 11, 2021 14:32:10.620090961 CET	53023	53	192.168.2.3	8.8.8.8
Jan 11, 2021 14:32:10.668040037 CET	53	53023	8.8.8.8	192.168.2.3
Jan 11, 2021 14:32:11.589556932 CET	49563	53	192.168.2.3	8.8.8.8
Jan 11, 2021 14:32:11.637516975 CET	53	49563	8.8.8.8	192.168.2.3
Jan 11, 2021 14:32:12.597609043 CET	51352	53	192.168.2.3	8.8.8.8
Jan 11, 2021 14:32:12.646148920 CET	53	51352	8.8.8.8	192.168.2.3
Jan 11, 2021 14:32:21.525583029 CET	59349	53	192.168.2.3	8.8.8.8
Jan 11, 2021 14:32:21.573497057 CET	53	59349	8.8.8.8	192.168.2.3
Jan 11, 2021 14:32:21.703680038 CET	57084	53	192.168.2.3	8.8.8.8
Jan 11, 2021 14:32:21.764149904 CET	53	57084	8.8.8.8	192.168.2.3
Jan 11, 2021 14:32:22.210922956 CET	58823	53	192.168.2.3	8.8.8.8
Jan 11, 2021 14:32:22.259042978 CET	53	58823	8.8.8.8	192.168.2.3
Jan 11, 2021 14:32:22.540086031 CET	59349	53	192.168.2.3	8.8.8.8
Jan 11, 2021 14:32:22.588344097 CET	53	59349	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 14:32:23.227056980 CET	58823	53	192.168.2.3	8.8.8.8
Jan 11, 2021 14:32:23.275624037 CET	53	58823	8.8.8.8	192.168.2.3
Jan 11, 2021 14:32:23.554694891 CET	59349	53	192.168.2.3	8.8.8.8
Jan 11, 2021 14:32:23.602854013 CET	53	59349	8.8.8.8	192.168.2.3
Jan 11, 2021 14:32:24.242227077 CET	58823	53	192.168.2.3	8.8.8.8
Jan 11, 2021 14:32:24.290467024 CET	53	58823	8.8.8.8	192.168.2.3
Jan 11, 2021 14:32:25.962132931 CET	59349	53	192.168.2.3	8.8.8.8
Jan 11, 2021 14:32:26.018579006 CET	53	59349	8.8.8.8	192.168.2.3
Jan 11, 2021 14:32:27.199156046 CET	58823	53	192.168.2.3	8.8.8.8
Jan 11, 2021 14:32:27.247164965 CET	53	58823	8.8.8.8	192.168.2.3
Jan 11, 2021 14:32:29.977243900 CET	59349	53	192.168.2.3	8.8.8.8
Jan 11, 2021 14:32:30.070341110 CET	53	59349	8.8.8.8	192.168.2.3
Jan 11, 2021 14:32:30.795512915 CET	57568	53	192.168.2.3	8.8.8.8
Jan 11, 2021 14:32:30.853557110 CET	53	57568	8.8.8.8	192.168.2.3
Jan 11, 2021 14:32:31.211565018 CET	58823	53	192.168.2.3	8.8.8.8
Jan 11, 2021 14:32:31.259557962 CET	53	58823	8.8.8.8	192.168.2.3
Jan 11, 2021 14:32:32.906847954 CET	50540	53	192.168.2.3	8.8.8.8
Jan 11, 2021 14:32:32.957585096 CET	53	50540	8.8.8.8	192.168.2.3
Jan 11, 2021 14:32:37.054480076 CET	54366	53	192.168.2.3	8.8.8.8
Jan 11, 2021 14:32:37.102628946 CET	53	54366	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 11, 2021 14:31:52.539813042 CET	192.168.2.3	8.8.8.8	0x949c	Standard query (0)	urldefense.com	A (IP address)	IN (0x0001)
Jan 11, 2021 14:32:10.418358088 CET	192.168.2.3	8.8.8.8	0x8990	Standard query (0)	urldefense.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 11, 2021 14:31:52.596460104 CET	8.8.8.8	192.168.2.3	0x949c	No error (0)	urldefense.com		52.6.56.188	A (IP address)	IN (0x0001)
Jan 11, 2021 14:32:10.469259024 CET	8.8.8.8	192.168.2.3	0x8990	No error (0)	urldefense.com		52.71.28.102	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 11, 2021 14:31:52.883423090 CET	52.6.56.188	443	192.168.2.3	49711	CN=www.urldefense.com, OU=Ops, O="Proofpoint, Inc.", STREET=892 Ross Drive, L=Sunnyvale, ST=California, OID.2.5.4.17=94089, C=US CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Tue Nov 03 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018	Thu Nov 04 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031	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=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 11, 2021 14:31:52.883771896 CET	52.6.56.188	443	192.168.2.3	49710	CN=www.urldefense.com, OU=Ops, O="Proofpoint, Inc.", STREET=892 Ross Drive, L=Sunnyvale, ST=California, OID.2.5.4.17=94089, C=US CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Tue Nov 03 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018	Thu Nov 04 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031	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=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		

Code Manipulations

Statistics

Behavior

System Behavior

Analysis Process: iexplore.exe PID: 2432 Parent PID: 792

General

Start time:	14:31:50
Start date:	11/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7be0b0000
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: 5436 Parent PID: 2432

General

Start time:	14:31:51
Start date:	11/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2432 CREDAT:17410 /prefetch:2
Imagebase:	0xbf0000
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