ID: 342953
Cookbook: browseurl.jbs
Time: 23:29:02
Date: 21/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

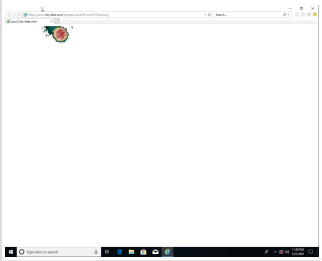
Analysis Report http://pics3.city-data.com/images/covid…

Overview

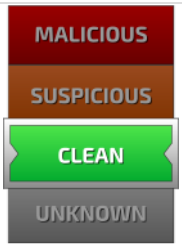
General Information

Sample URL:	http://pics3.city-data.com/images/covid19/covid-19-btn.png
Analysis ID:	342953

Most interesting Screenshot:



Detection

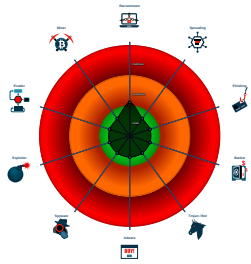


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 3732 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5708 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3732 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

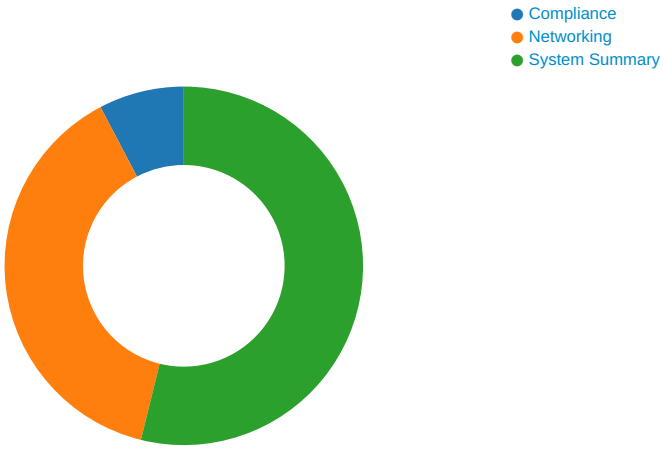
Yara Overview

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.

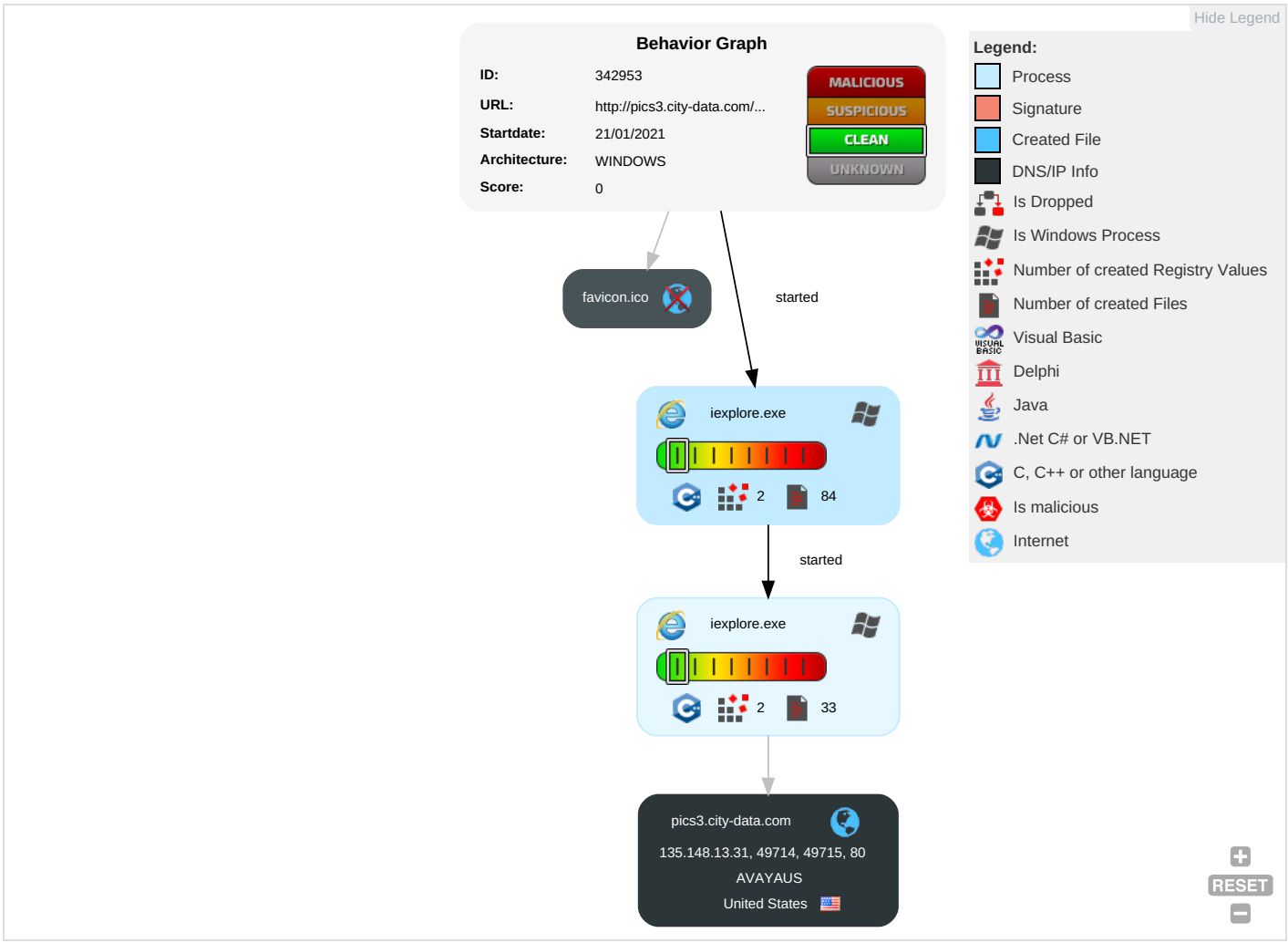
Compliance:

Uses new MSVCR Dlls

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

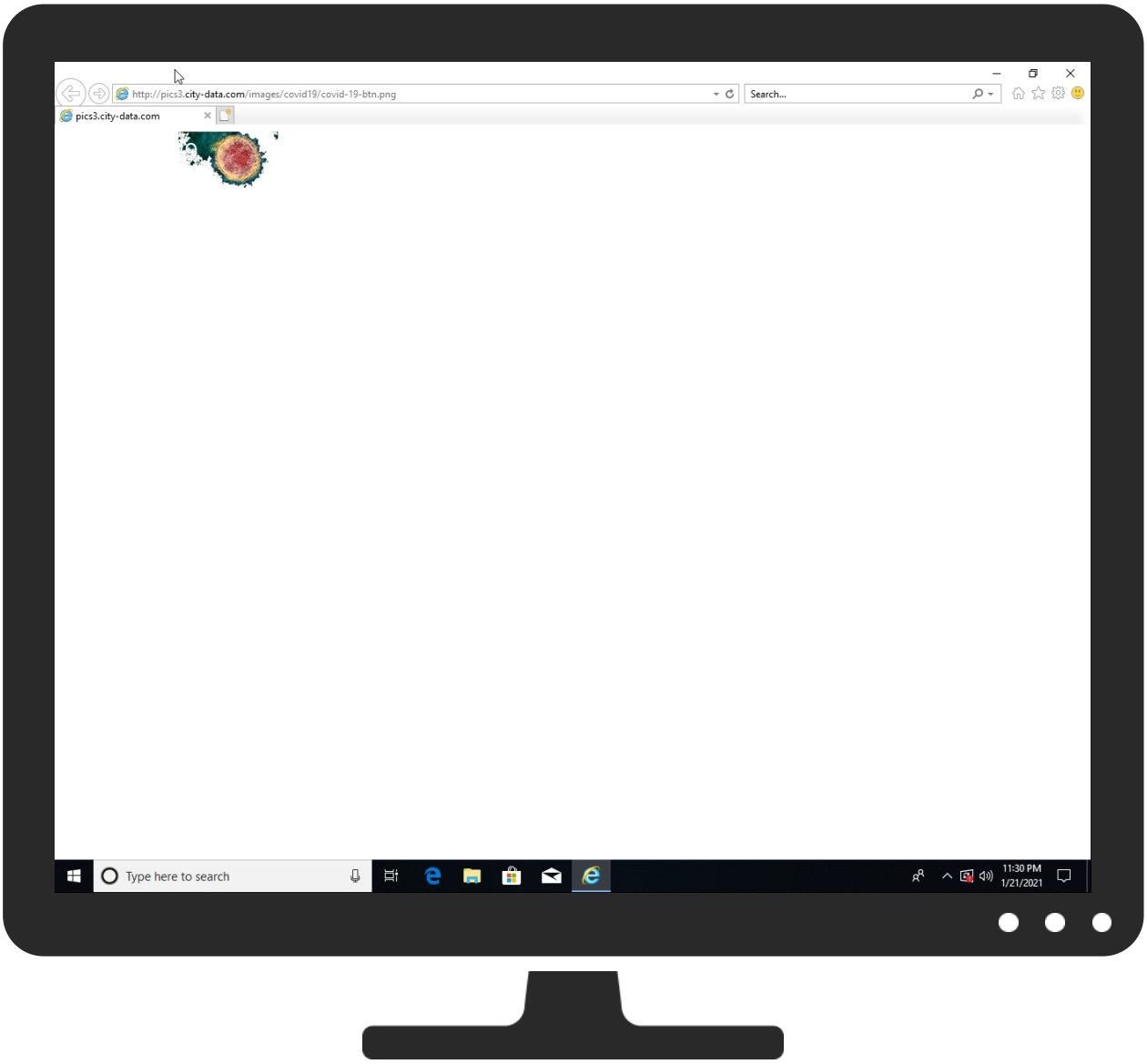
Behavior Graph



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://pics3.city-data.com/images/covid19/covid-19-btn.png	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	
http://www.wikipedia.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pics3.city-data.com	135.148.13.31	true	false		high
favicon.ico	unknown	unknown	false		unknown

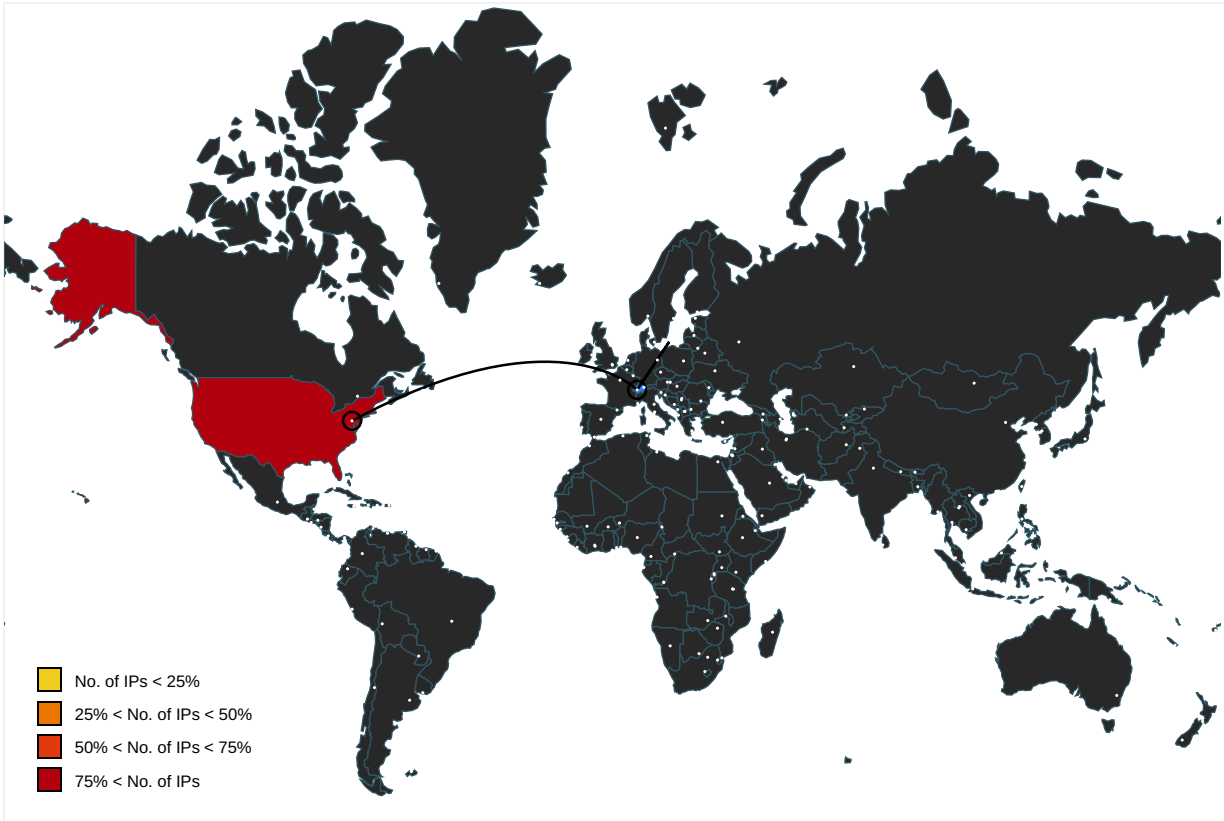
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://pics3.city-data.com/images/covid19/covid-19-btn.png	false		high
http://pics3.city-data.com/images/covid19/covid-19-btn.png	false		high
http://pics3.city-data.com/favicon.ico	false		high

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://pics3.city-data.com/images/covid19/covid-19-btn.pngRoot	{9B03AC28-5C83-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://www.amazon.com/	msapplication.xml.1.dr	false		high
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
135.148.13.31	unknown	United States		18676	AVAYAUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	342953
Start date:	21.01.2021
Start time:	23:29:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://pics3.city-data.com/images/covid19/covid-19-btn.png
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): BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 104.43.193.48, 88.221.62.148, 51.104.139.180, 104.79.90.110, 152.199.19.161, 92.122.213.247, 92.122.213.194, 2.20.142.209, 2.20.142.210, 20.54.26.129, 52.155.217.156 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, 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, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, go.microsoft.com, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, ie9comview.vo.msecnd.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.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.{9B03AC26-5C83-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.857700052177407
Encrypted:	false
SSDEEP:	96:ru/ZhZk2u9WSRtSlvfSchMSySxS87fSrcX:ru/ZhZk2u9WGtGvfhhMrEr7fGcX
MD5:	D1976603CB1B57B7DAB819B29814BD0E
SHA1:	63E3AD5D6CE459BEF43B1AF329C5E0FCFE86A29D
SHA-256:	4CEA51A47249F55D2AA45AF75488C2BE411831BEA4CAE4D27C8D129FFBD2C4B5
SHA-512:	91BB5D32FA41080DD8C643A1B5F38FDE3EA4E3A7718C9430E806DAFBA91A9F5E813F73E1EC2B7CC4EA45FE5AD1D431DDC1BB727CC46A16C9F921C0BA868B0E31
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\{9B03AC28-5C83-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24228
Entropy (8bit):	1.6439059462108963

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9B03AC28-5C83-11EB-90E4-ECF4BB862DED}.dat	
Encrypted:	false
SSDEEP:	48:IwIZGcpr9GwpaEZG4pQEhGrapbS2rGQpBTWGHHpc4sTGUp8dGzYpmIpYGopRujwl:rI/ZnQE76GBS2Fjp24kWjMiYXsg
MD5:	A010E6121846CAE04961058EBB007AE3
SHA1:	A077B3F68A905AD006960F63BCEF0F0CDEF08BAA
SHA-256:	6EA43DBEA7B26DF1119C47CA5B64F6E2FE452E1279E210EAFBF566E842BF2738
SHA-512:	B4897D0E5C1364A14728BF2F5B180AAE912C637D2DBB6C27879A0800F6EABA761A7B33500EC894013EE4144228D990C64E5A429DE2472AD638462C4488528193
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\{9B03AC29-5C83-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5635462148731956
Encrypted:	false
SSDEEP:	48:Iw9/ZGcprv6GwpawZG4pQYGrapbSJrGQpKMG7HpRqsTGIpG:r9//ZviQw76mBSJFAnTq4A
MD5:	E69BF6702E526B6CDED50937B08C2467
SHA1:	B18AB844CD5B54FC4DA5126CE06D9E491BC8FBEF
SHA-256:	15A35377257CDA64664977ADEBFF0E077718B676CE3F39BE680ED8B86363AE4A
SHA-512:	84A71EF5B7C64B4C59F152629CE5CC972C0EEA63298184429F29FB209DFD6E11014C1623485E97CF91D2995BF84CB0293A2A9A5B62A3E9AA8E4CE02744BEF89
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):	5.073253024958182
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEWy/nWimI002EtM3MHdNMNxOEWy/nWimI00ObVbkEtMb:2d6NxOUSZHKd6NxOUSZ76b
MD5:	881D3E332050B69ACFA059F3018C1A0F
SHA1:	DBBEDAF8659A15BDEB9A2A3E4115DFC72613050C
SHA-256:	282C534E4CEDD9C427343538E8FF96E21C141D8BD2D1D5793FE06C2B7F003282
SHA-512:	7E1BF54FFF8F578F35F3D7D700E6EC119440EDA81C01D8528C121A141D7B672A9FE7E6B3A969AD9F71ECEE4439220C2B7B084365EC43E8E6CED8C6CC598945 0
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x7056da66,0x01d6f090</date> accdate>0x7056da66,0x01d6f090</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>0x7056da66,0x01d6f090</date><accdate>0 x7056da66,0x01d6f090</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):	5.124523951090877
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kxkmnWimI002EtM3MHdNMNxe2kxr/nWimI00Obkak6EtMb:2d6Nxr8SZHKd6NxrYSZ7Aa7b
MD5:	E6A375F186EA5C7C572D198FA5D11130
SHA1:	9672617A2D0DADA665EAB2CB2BCC6A5B5AE81290
SHA-256:	44B22BFC75AA45752468692ADDB28C16EC66BCD38490AA6EF603236445F8AF03
SHA-512:	29317D96B4A79A726665AF56352FFC3DFD34A431B865C05904974557292FC74A213B7D92A0E994AB9245610B49D76A11E26FAB178C19A817124BD5B6DEE24F38

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x704fb36a,0x01d6f090</date><accdate>0x704fb36a,0x01d6f090</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>0x704fb36a,0x01d6f090</date><accdate>0x705215c6,0x01d6f090</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):	5.1094529698972
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLbLLnWimI002EtM3MHdNMNxvLbLLnWimI00ObmZEtMb:2d6Nxv3SZHKd6Nxv3SZ7mb
MD5:	521B94559CECE3BCB9075CCF1B9E13BA
SHA1:	0B1BC22FCFDB9647158AF048188251E4F96CDCD3
SHA-256:	312D45D76C8AF53994B3FF6D394812A1F45AABDE5801789A299FA49E655CCEFD
SHA-512:	2FE5024238B296EF8698D311CCEF911BD34FCD323CC0DFE3510AF4D118C402CA0CF9846D8F255C9E17859043326EBC10A473B391A21581981067C9739D46F3D5
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x70593ce2,0x01d6f090</date><accdate>0x70593ce2,0x01d6f090</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>0x70593ce2,0x01d6f090</date><accdate>0x70593ce2,0x01d6f090</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):	5.1107546654944205
Encrypted:	false
SSDEEP:	12:TMHdNMNxi3uTu/nWimI002EtM3MHdNMNxi3uTu/nWimI00Obd5EtMb:2d6NxkwoSZHKd6NxkwoSZ7Jjb
MD5:	F39793CBDE18173CB94C168C4CB1E8D9
SHA1:	EC89CA2734A9DA691D1AB9AB499E09BBE43EA2C6
SHA-256:	842DA461A543ABB5956795DE48BED2C47A6785C36A46FDAE01C9E4454DEE2777
SHA-512:	09110125C3F30ABFF05104DA7FD14B62A04BDD22C49CA95986C5FBE87AD417495CC8289A3A59484B797CA9E72FA55F9F7BED323BF5FCFDF0D8B4A4463991D98 8
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x7054780f,0x01d6f090</date><accdate>0x7054780f,0x01d6f090</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>0x7054780f,0x01d6f090</date><accdate>0x7054780f,0x01d6f090</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):	5.124166094743051
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwbLLnWimI002EtM3MHdNMNxhGwbLLnWimI00Ob8K075EtMb:2d6NxQ+SZHKd6NxQ+SZ7YKajb
MD5:	044933374F4A9EBFC2780F14A0E598AA
SHA1:	F0263435EECF3F2662AFCE1AEFF077C72D75E93F
SHA-256:	D5450E156825865878F4F592485AA08AC3EE7A1533A9CF4AE503F3A52BE7C32B
SHA-512:	CF6E92D76D5759938ED42ED47E7F3C6DBFFA1D3B5E47CB7FFA72FBD584178C05B84EEC4A77CAE937EEE115C3D4C44D7B85E21962A2AF5F9FC6A152AF7268EACF
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x70593ce2,0x01d6f090</date><accdate>0x70593ce2,0x01d6f090</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>0x70593ce2,0x01d6f090</date><accdate>0x70593ce2,0x01d6f090</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):	5.073894731407674
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nWy/nWimI002EtM3MHdNMNx0nWy/nWimI00ObxEtMb:2d6Nx05SZHKd6Nx05SZ7nb
MD5:	13C011EB30C1802BA262F9B8212E472C
SHA1:	DFFF7E4BF7F98430021EFD287DD16D45B92F5273
SHA-256:	C104471BCCCB51456C87D442E6B7E9DD10122AB4968D8DE4AF0AD64B88666146
SHA-512:	EFC80011A33D8E7D07040E5F25254C686E79BAF2DA1B9CCA2EFBA98DB502146CDD58E31EC2AF6B3FD175076F846B1B71085666FBF2A58AC251F8A1040FD4619
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x7056da66,0x01d6f090</date><accdate>0x7056da66,0x01d6f090</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>0x7056da66,0x01d6f090</date><accdate>0x7056da66,0x01d6f090</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):	5.113676726228879
Encrypted:	false
SSDEEP:	12:TMHdNMNxxWy/nWimI002EtM3MHdNMNxxWy/nWimI00Ob6Kq5EtMb:2d6NxjSZHKd6NxjSZ7ob
MD5:	80DBC1130FBA22DFB354C6C55E1FCB91
SHA1:	8D0DC57593705B34111031990F88FD1D6C5FF674
SHA-256:	9929D1A7574FA318D708C17574989F5887FFC0742982E511F1D62BB93524408F
SHA-512:	968F9BCFEB155D80DE488FF4736B795BC4FD36EAF55DA4C751DE46482C00643015F6DA45AD21F84A1B4D9401C67036F6EFDB1CE5009BB4D032767B1102E6C1F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x7056da66,0x01d6f090</date><accdate>0x7056da66,0x01d6f090</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>0x7056da66,0x01d6f090</date><accdate>0x7056da66,0x01d6f090</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):	5.114372086815224
Encrypted:	false
SSDEEP:	12:TMHdNMNxc3uTu/nWimI002EtM3MHdNMNxc3uTu/nWimI00ObVEtMb:2d6NxOwoSZHKd6NxOwoSZ7Db
MD5:	9D17F83639F14FFF0DF6BB6D97AF7B02
SHA1:	C83F9500F810417CE58ADC422EBED78D63C2AC97
SHA-256:	59DD88760C2F63652A6EF61A8057EB12AC65F53F5D16CAB91A7648AB9D60D0B9
SHA-512:	1FF35FFBD5401F5EE9F67EBC8DF33F87EFF6951478D8F19FDE255779838847D35E7B9E92B959DC0DEDB5C0CD0F524AC90B92089D7B519554663D39B3235CDB4
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x7054780f,0x01d6f090</date><accdate>0x7054780f,0x01d6f090</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>0x7054780f,0x01d6f090</date><accdate>0x7054780f,0x01d6f090</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):	5.096421622258924
Encrypted:	false
SSDEEP:	12:TMHdNMNxfn3uTu/nWimI002EtM3MHdNMNxfn3uTu/nWimI00Obe5EtMb:2d6NxPwoSZHKd6NxPwoSZ7ijb
MD5:	B5DBCD49B6A795357A2F862CD354D538
SHA1:	A33B73015C0F114A91790725B3AAFDCE63F60F57
SHA-256:	2EA8FE19B46CD10232E9E430C818F805EA5D5F60B8D37A95FE3E4EDAC4FE774A
SHA-512:	18FFDFD9531B296864C0AFF37D3594E4456AC05ADDB2D371CB746C4D4DAD5076FCE1831C7A59FD3FB78F964E4AC563BCA653A7E1993693AF6043A19E262B65 D
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x7054780f,0x01d6f090</date><a ccdate>0x7054780f,0x01d6f090</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>0x7054780f,0x01d6f090</date><accdate>0x7 054780f,0x01d6f090</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\covid-19-btn[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 268 x 80, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	22559
Entropy (8bit):	7.986669850540404
Encrypted:	false
SSDEEP:	384:YgOXEB3cm2fbSdCmK5ssJ+dz+FE01pwqDjjoTNFXmRAE17zhYDksNq/5:SEB8f2dCmK1WWXdmN9031HMU/5
MD5:	CCD6A0C5DABD6C707AB69170A20A62E4
SHA1:	7939D05E2697FB189EA212C2BF3388C2B0ED9EE6
SHA-256:	39085EC813E9E509AD1D618F8F8207FC4FB2F35BE2169324C1E6CAD9B2207E0D
SHA-512:	4ED1883E38AD9938835F66054C1C3330AE31940DC1303B65EADC6214FADC026C9306BC49562212C9B5D92AFBC5E36EFCCBC188735A62FA927B9FFAF238BB42 D
Malicious:	false
Reputation:	low
IE Cache URL:	http://pics3.city-data.com/images/covid19/covid-19-btn.png
Preview:	.PNG.....IHDR.....P.....K... .IDATx....eWY..[{<.p...uo...P.TR$!.& .4.....T\|.[..mm.n.....Z[.Q..O% J7..A.<....x.i.....T%..6.z..T..>...^...../1.R...w.....J...k;...H.....7....0c...~. p.T.q...2.O.z)....S.....Q..)H.!.....,.L..A..f.mF.....*.a...:..-..L.....Z...`.R...)...C.u\|j+..<.V.....b..a.h.....s8.Kx...e!.....#,-...."}....9..i.T.a'q.W4.o,...w..?0...6..5....t.....&z,M..!.....Th&a.H.,.. :!.....\|K..K.C..`..%....[4....l.P.G.....jh.`e..`h....4.....)$B.<.....W...aZ.q...=.X..../..V|B..g..X.B..-.$..hl...UC:M..o..Z... [@*P.....X..A.E.E.....%..G...x?..".gkh..-?....D.....YQ7F#>4@.. .....8!v..!...<Z<...w...j..W....i#.2F2....L.....8...i...6V.....C...}O.....BuO....h.....r..".....tL.g.=-..p.....h....R.n....U..j/.....|..=.r.;..w.K,...4.W....H..Xz?n..q...B....[..U.a..GV.Q..f.]8-d.Fd i)..".....2.P.I.....t/..0..D!K"n.4tZ-..T..1GG...'....a..f.L_.5..vHOJc #.L.k .7L&a...b..v.[....eX..X....A...lj..zn....).:A..a[._..9.*/.].....2..64....

C:\Users\user\AppData\Local\Temp\~DF050F801E709E9CD1.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34421
Entropy (8bit):	0.3617138013678112
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lw29lwG9l2l9l2o9l/lj:kBqoxKAuvScS+5XF0III7ujw1
MD5:	7AF1A328287784E47FB3FBC636260ABD
SHA1:	A8DBEBD3E4195DE0A63B18CFB982F230ABFFE7A8
SHA-256:	7CD159E180E76E1F7E088BC444C0A4A440096C4DD1D5BBA195DDEC5B2421D92B
SHA-512:	55A5F4DA7956D0499925A614152835311930BADB8ABF5FEEBD9E969B93F5E378B10003935F73B7F47CE1B3C0F13F97427EB0C7F01ACCD7553CCC8A06BA5F486
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF54FBC132C3E6AF67.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441

C:\Users\user\AppData\Local\Temp\~DF54FBC132C3E6AF67.TMP	
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\~DF95CCCC079EE04922.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47908442814096136
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loFF9lof9lWyuIH:kBqoIAeyuIH
MD5:	C7AC48C8FB92371BEB52A8E66BEE832F
SHA1:	23FDA014B85864A0BE2A2C11E696B95E31E49A74
SHA-256:	0FA964F40F230EF4E9473E6CB4BE78311378BF7F40CA0C23AC5D8A8819E65C0D
SHA-512:	D900B9F6DB88AAAC501698291B7D01E28DC6A80AA2D630283AE82AE8895BFE5F091FF2E46DBC919B4898482DE831F1B118ADB06D50675DBE91D9C6DD16C97C B
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: 62

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 23:29:50.865756989 CET	49714	80	192.168.2.3	135.148.13.31
Jan 21, 2021 23:29:50.866132975 CET	49715	80	192.168.2.3	135.148.13.31
Jan 21, 2021 23:29:50.999659061 CET	80	49715	135.148.13.31	192.168.2.3
Jan 21, 2021 23:29:50.999773979 CET	49715	80	192.168.2.3	135.148.13.31
Jan 21, 2021 23:29:51.002228022 CET	80	49714	135.148.13.31	192.168.2.3
Jan 21, 2021 23:29:51.002321959 CET	49714	80	192.168.2.3	135.148.13.31
Jan 21, 2021 23:29:51.002568007 CET	49715	80	192.168.2.3	135.148.13.31
Jan 21, 2021 23:29:51.135929108 CET	80	49715	135.148.13.31	192.168.2.3
Jan 21, 2021 23:29:51.136131048 CET	80	49715	135.148.13.31	192.168.2.3
Jan 21, 2021 23:29:51.136174917 CET	80	49715	135.148.13.31	192.168.2.3
Jan 21, 2021 23:29:51.136212111 CET	80	49715	135.148.13.31	192.168.2.3
Jan 21, 2021 23:29:51.136250019 CET	80	49715	135.148.13.31	192.168.2.3
Jan 21, 2021 23:29:51.136274099 CET	49715	80	192.168.2.3	135.148.13.31
Jan 21, 2021 23:29:51.136290073 CET	80	49715	135.148.13.31	192.168.2.3
Jan 21, 2021 23:29:51.136322975 CET	49715	80	192.168.2.3	135.148.13.31
Jan 21, 2021 23:29:51.136328936 CET	80	49715	135.148.13.31	192.168.2.3
Jan 21, 2021 23:29:51.136367083 CET	80	49715	135.148.13.31	192.168.2.3
Jan 21, 2021 23:29:51.136404037 CET	80	49715	135.148.13.31	192.168.2.3
Jan 21, 2021 23:29:51.136426926 CET	49715	80	192.168.2.3	135.148.13.31
Jan 21, 2021 23:29:51.136451006 CET	80	49715	135.148.13.31	192.168.2.3
Jan 21, 2021 23:29:51.136492968 CET	80	49715	135.148.13.31	192.168.2.3
Jan 21, 2021 23:29:51.136496067 CET	49715	80	192.168.2.3	135.148.13.31
Jan 21, 2021 23:29:51.136558056 CET	49715	80	192.168.2.3	135.148.13.31
Jan 21, 2021 23:29:51.136646986 CET	49715	80	192.168.2.3	135.148.13.31
Jan 21, 2021 23:29:51.269718885 CET	80	49715	135.148.13.31	192.168.2.3
Jan 21, 2021 23:29:51.269823074 CET	80	49715	135.148.13.31	192.168.2.3
Jan 21, 2021 23:29:51.269850969 CET	80	49715	135.148.13.31	192.168.2.3
Jan 21, 2021 23:29:51.269851923 CET	49715	80	192.168.2.3	135.148.13.31
Jan 21, 2021 23:29:51.269872904 CET	80	49715	135.148.13.31	192.168.2.3
Jan 21, 2021 23:29:51.269892931 CET	49715	80	192.168.2.3	135.148.13.31
Jan 21, 2021 23:29:51.269897938 CET	80	49715	135.148.13.31	192.168.2.3
Jan 21, 2021 23:29:51.269897938 CET	49715	80	192.168.2.3	135.148.13.31
Jan 21, 2021 23:29:51.269923925 CET	80	49715	135.148.13.31	192.168.2.3
Jan 21, 2021 23:29:51.269928932 CET	49715	80	192.168.2.3	135.148.13.31
Jan 21, 2021 23:29:51.269942999 CET	49715	80	192.168.2.3	135.148.13.31
Jan 21, 2021 23:29:51.269970894 CET	80	49715	135.148.13.31	192.168.2.3
Jan 21, 2021 23:29:51.270000935 CET	49715	80	192.168.2.3	135.148.13.31
Jan 21, 2021 23:29:51.270018101 CET	49715	80	192.168.2.3	135.148.13.31
Jan 21, 2021 23:29:51.270087957 CET	80	49715	135.148.13.31	192.168.2.3
Jan 21, 2021 23:29:51.270138979 CET	49715	80	192.168.2.3	135.148.13.31
Jan 21, 2021 23:29:51.369046926 CET	49715	80	192.168.2.3	135.148.13.31
Jan 21, 2021 23:29:51.503371000 CET	80	49715	135.148.13.31	192.168.2.3
Jan 21, 2021 23:29:51.503442049 CET	80	49715	135.148.13.31	192.168.2.3
Jan 21, 2021 23:29:51.503539085 CET	49715	80	192.168.2.3	135.148.13.31
Jan 21, 2021 23:30:01.501705885 CET	80	49715	135.148.13.31	192.168.2.3
Jan 21, 2021 23:30:01.501902103 CET	49715	80	192.168.2.3	135.148.13.31

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 23:29:44.260360956 CET	53	55984	8.8.8.8	192.168.2.3
Jan 21, 2021 23:29:45.521255016 CET	64185	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:29:45.569335938 CET	53	64185	8.8.8.8	192.168.2.3
Jan 21, 2021 23:29:46.958312035 CET	65110	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:29:47.006445885 CET	53	65110	8.8.8.8	192.168.2.3
Jan 21, 2021 23:29:48.066881895 CET	58361	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:29:48.125583887 CET	53	58361	8.8.8.8	192.168.2.3
Jan 21, 2021 23:29:49.014528990 CET	63492	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:29:49.073982000 CET	53	63492	8.8.8.8	192.168.2.3
Jan 21, 2021 23:29:49.765376091 CET	60831	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:29:49.826018095 CET	53	60831	8.8.8.8	192.168.2.3
Jan 21, 2021 23:29:50.101902962 CET	60100	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 23:29:50.152740002 CET	53	60100	8.8.8.8	192.168.2.3
Jan 21, 2021 23:29:50.790333033 CET	53195	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:29:50.848503113 CET	53	53195	8.8.8.8	192.168.2.3
Jan 21, 2021 23:29:51.056045055 CET	50141	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:29:51.107076883 CET	53	50141	8.8.8.8	192.168.2.3
Jan 21, 2021 23:29:52.158948898 CET	53023	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:29:52.206834078 CET	53	53023	8.8.8.8	192.168.2.3
Jan 21, 2021 23:29:53.530324936 CET	49563	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:29:53.578241110 CET	53	49563	8.8.8.8	192.168.2.3
Jan 21, 2021 23:29:54.525585890 CET	51352	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:29:54.573590040 CET	53	51352	8.8.8.8	192.168.2.3
Jan 21, 2021 23:29:56.252304077 CET	59349	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:29:56.300259113 CET	53	59349	8.8.8.8	192.168.2.3
Jan 21, 2021 23:29:57.698481083 CET	57084	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:29:57.746495962 CET	53	57084	8.8.8.8	192.168.2.3
Jan 21, 2021 23:29:58.880774975 CET	58823	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:29:58.928664923 CET	53	58823	8.8.8.8	192.168.2.3
Jan 21, 2021 23:30:07.235977888 CET	57568	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:30:07.294986010 CET	53	57568	8.8.8.8	192.168.2.3
Jan 21, 2021 23:30:11.129782915 CET	50540	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:30:11.189188004 CET	53	50540	8.8.8.8	192.168.2.3
Jan 21, 2021 23:30:19.207493067 CET	54366	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:30:19.275684118 CET	53	54366	8.8.8.8	192.168.2.3
Jan 21, 2021 23:30:19.766457081 CET	53034	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:30:19.825227976 CET	53	53034	8.8.8.8	192.168.2.3
Jan 21, 2021 23:30:20.438301086 CET	57762	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:30:20.494856119 CET	53	57762	8.8.8.8	192.168.2.3
Jan 21, 2021 23:30:20.765713930 CET	53034	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:30:20.813807011 CET	53	53034	8.8.8.8	192.168.2.3
Jan 21, 2021 23:30:21.451255083 CET	57762	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:30:21.507584095 CET	53	57762	8.8.8.8	192.168.2.3
Jan 21, 2021 23:30:21.817424059 CET	53034	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:30:21.865520000 CET	53	53034	8.8.8.8	192.168.2.3
Jan 21, 2021 23:30:22.562743902 CET	57762	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:30:22.619543076 CET	53	57762	8.8.8.8	192.168.2.3
Jan 21, 2021 23:30:23.826857090 CET	53034	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:30:23.883507013 CET	53	53034	8.8.8.8	192.168.2.3
Jan 21, 2021 23:30:24.645796061 CET	57762	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:30:24.702472925 CET	53	57762	8.8.8.8	192.168.2.3
Jan 21, 2021 23:30:26.039372921 CET	55435	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:30:26.102130890 CET	53	55435	8.8.8.8	192.168.2.3
Jan 21, 2021 23:30:27.842703104 CET	53034	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:30:27.899240971 CET	53	53034	8.8.8.8	192.168.2.3
Jan 21, 2021 23:30:28.654577017 CET	57762	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:30:28.710727930 CET	53	57762	8.8.8.8	192.168.2.3
Jan 21, 2021 23:30:33.891154051 CET	50713	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:30:33.942935944 CET	53	50713	8.8.8.8	192.168.2.3
Jan 21, 2021 23:30:34.534245968 CET	56132	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:30:34.609544039 CET	53	56132	8.8.8.8	192.168.2.3
Jan 21, 2021 23:30:35.175333023 CET	58987	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:30:35.263621092 CET	53	58987	8.8.8.8	192.168.2.3
Jan 21, 2021 23:30:35.693535089 CET	56579	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:30:35.760566950 CET	53	56579	8.8.8.8	192.168.2.3
Jan 21, 2021 23:30:36.244709015 CET	60633	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:30:36.301527023 CET	53	60633	8.8.8.8	192.168.2.3
Jan 21, 2021 23:30:36.709357023 CET	61292	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:30:36.765584946 CET	53	61292	8.8.8.8	192.168.2.3
Jan 21, 2021 23:30:37.146029949 CET	63619	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:30:37.204185963 CET	53	63619	8.8.8.8	192.168.2.3
Jan 21, 2021 23:30:37.645880938 CET	64938	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:30:37.702153921 CET	53	64938	8.8.8.8	192.168.2.3
Jan 21, 2021 23:30:38.141988039 CET	61946	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:30:38.201226950 CET	53	61946	8.8.8.8	192.168.2.3
Jan 21, 2021 23:30:38.745074034 CET	64910	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 23:30:38.801328897 CET	53	64910	8.8.8.8	192.168.2.3
Jan 21, 2021 23:30:39.421215057 CET	52123	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:30:39.480643988 CET	53	52123	8.8.8.8	192.168.2.3
Jan 21, 2021 23:30:39.844429016 CET	56130	53	192.168.2.3	8.8.8.8
Jan 21, 2021 23:30:39.903721094 CET	53	56130	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 21, 2021 23:29:50.790333033 CET	192.168.2.3	8.8.8.8	0x15eb	Standard query (0)	pics3.city-data.com	A (IP address)	IN (0x0001)
Jan 21, 2021 23:30:07.235977888 CET	192.168.2.3	8.8.8.8	0xf040	Standard query (0)	favicon.ico	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 21, 2021 23:29:50.848503113 CET	8.8.8.8	192.168.2.3	0x15eb	No error (0)	pics3.city-data.com		135.148.13.31	A (IP address)	IN (0x0001)
Jan 21, 2021 23:30:07.294986010 CET	8.8.8.8	192.168.2.3	0xf040	Name error (3)	favicon.ico	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- pics3.city-data.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49715	135.148.13.31	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2021 23:29:51.002568007 CET	78	OUT	GET /images/covid19/covid-19-btn.png 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: pics3.city-data.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2021 23:29:51.136131048 CET	80	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 21 Jan 2021 22:29:51 GMT Content-Type: image/png Content-Length: 22559 Connection: keep-alive Last-Modified: Mon, 19 Oct 2020 17:41:49 GMT ETag: "581f-5b209a102fdc7" X-Content-Type-Options: nosniff X-Frame-Options: sameorigin Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Allow-Headers: DNT,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Range Access-Control-Expose-Headers: Content-Length,Content-Range Expires: Wed, 21 Apr 2021 22:29:51 GMT Cache-Control: max-age=7776000 X-Server: cdn1 X-Proxy-Cache: HIT Accept-Ranges: bytes Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 0c 00 00 00 50 08 06 00 00 00 ec b7 4b ab 00 00 20 00 49 44 41 54 78 9c ec bd 09 b8 65 57 59 e7 fd 5b 7b 3c f3 70 cf 1d ea 8e 75 6f dd 9a 93 ca 50 95 54 52 24 21 90 26 20 82 34 08 01 b1 1d 18 54 7c d4 b6 5b 1c a0 6d 6d db 6e ba 85 a6 a5 f1 fb 5a 5b a0 51 f0 d3 4f 25 20 4a 37 a2 10 41 c8 3c d5 94 9a e7 ba f3 78 e6 69 8f ab 9f b5 cf b9 95 9b 54 25 04 82 36 c4 7a 9f e7 54 dd bb f7 3e fb ec b3 ef 5e ff f5 0e ff f7 bf 04 2f 31 93 52 be d4 be d2 77 bd 89 ad 03 ff 4a f8 ee ef a0 6b 3b 88 a7 0e 48 b7 f5 17 02 f9 37 b2 dd fa b4 30 63 12 82 16 7e d8 20 70 93 54 db 71 b2 a9 d3 32 9b 4f 88 7a 29 83 95 08 b0 53 c8 d0 83 c2 08 a2 51 81 95 29 48 e5 21 d5 03 f1 14 08 1d 2c 1b 4c 1b dd b6 41 d3 f1 97 66 a3 6d 46 b6 a0 fe e8 f8 f5 2a ea 61 96 ba 06 cd 3a 08 0d 2d 99 c2 4c a5 b1 e3 16 ed 5a 13 b7 e5 60 a6 52 8c 8c a4 29 97 1d 0c 43 c3 75 7c 6a 2b 15 08 3c c2 56 03 bb d0 8b d4 0c 62 b6 8e 61 c7 68 ae 14 c1 0f 88 a7 73 38 ab 4b 78 8d 16 9a 65 21 eb ab 08 c3 c2 e8 1f 23 2c 2d 10 ac cc 82 e7 22 7d 07 cd b2 d1 12 39 bc 85 69 f4 54 0e 61 27 71 16 57 34 bb 6f 2c ab a7 ec 77 fb e5 95 3f 30 0d 03 dd 36 09 da 35 02 af 86 f4 74 8c d4 00 81 1f 10 1a 26 7a 2c 4d d0 2e 21 ac 10 e4 d3 c3 54 68 26 61 bb 48 d8 2c 12 18 3a 21 92 cb 06 b1 b8 7c 4b f7 ff 4b 83 43 84 d1 60 89 ee 25 9a d1 d9 a5 9b 5b 34 dd 0a 85 9d 6c 8a 50 be 47 b8 ed fb 84 d0 b6 6a 68 7f 60 65 fb bf 60 68 e6 0f 18 ff 34 1f f1 ab f6 9d b5 e0 1a 29 24 42 88 3c 9e f3 1b 84 e1 57 08 83 01 61 5a 87 71 9a 9b f1 3d 83 58 bc 0f dd 98 a3 2f 7f 07 56 7c 42 e8 d6 67 a3 e7 58 01 42 a6 0f 2d 96 24 f4 bd 68 6c 88 f1 eb a1 55 43 3a 4d 84 da 6f aa 01 5a 8e 1e ee 20 5b 40 2a 50 f1 dd 08 14 ec 98 81 e7 06 58 f9 02 41 bb 45 d0 a8 45 ef 11 9a 88 00 c6 f7 25 86 e7 47 13 c9 e0 78 3f e5 c5 22 0b 67 6b 68 f1 04 2d 3f c4 f7 03 8c 44 0c bf ee 81 d3 c0 59 51 37 46 23 3e 34 40 b3 d4 20 95 88 91 ef cb b3 bc ea e2 38 21 76 be 0f 21 03 bc e2 3c 5a 3c 8b a5 06 77 df 10 8d 6a 05 e9 57 08 bd 80 d0 69 23 82 32 46 32 0d a1 c4 08 4c Data Ascii: PNGIHDRPK IDATxeWY[{<puoPTR$!& 4T\|[mmnZ[QO% J7A<xiT%6zT>^/1RwJk;H70c~ pTq2Oz)SQ)H!,LAfmF *a:-LZ`R)Cu\|j+<Vbahs8Kxe!#,-"}9iTa'qW4o,w?065t&z,M.!Th&aH,:!\|KKC`%[4lPGjh`e`h4)$B<WaZq=X/V|BgXB-$hlUC:MoZ [@*PXAEE%Gx?"gkh-?DYQ7F#>4@ 8!v!<Z<wjWi#2F2L
Jan 21, 2021 23:29:51.369046926 CET	104	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: pics3.city-data.com Connection: Keep-Alive
Jan 21, 2021 23:29:51.503442049 CET	109	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 21 Jan 2021 22:29:51 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 02 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Code Manipulations

Statistics

Behavior

● iexplore.exe
● iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 3732 Parent PID: 792

General

Start time:	23:29:48
Start date:	21/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff613fa0000
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: 5708 Parent PID: 3732

General

Start time:	23:29:48
Start date:	21/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3732 CREDAT:17410 /prefetch:2
Imagebase:	0x190000
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