ID: 323029
Sample Name:
#U260eVoiCeCALLER@ensono.com.htm
Cookbook: default.jbs
Time: 08:28:04
Date: 26/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

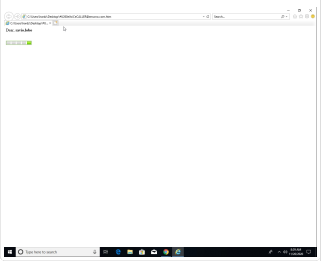
Analysis Report #U260eVoiCeCALLER@ensono.com.htm

Overview

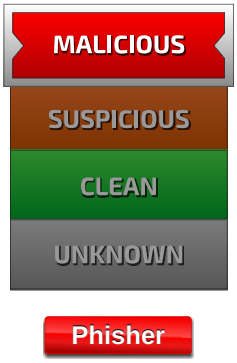
General Information

Sample Name:	#U260eVoiCeCALLER@ensono.com.htm
Analysis ID:	323029
MD5:	854acf666124399.
SHA1:	769e490db70e39..
SHA256:	9953401e31b3e8..

Most interesting Screenshot:



Detection

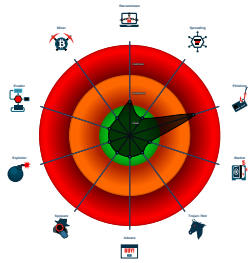


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Yara detected Phisher

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6048 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4812 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6048 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

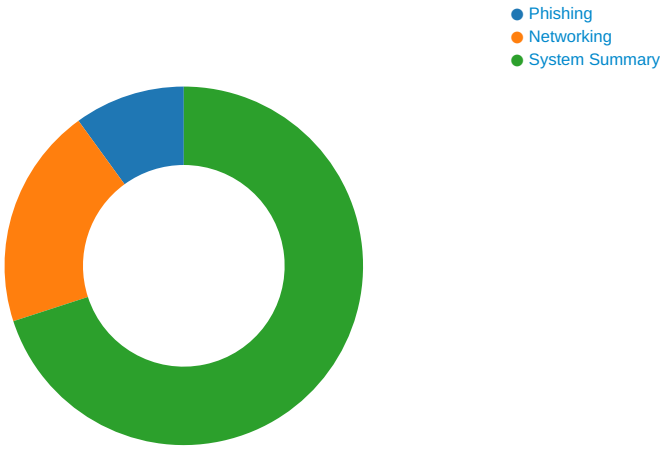
Initial Sample

Source	Rule	Description	Author	Strings
#U260eVoiCeCALLER@ensono.com.htm	JoeSecurity_Phisher_2	Yara detected Phisher	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

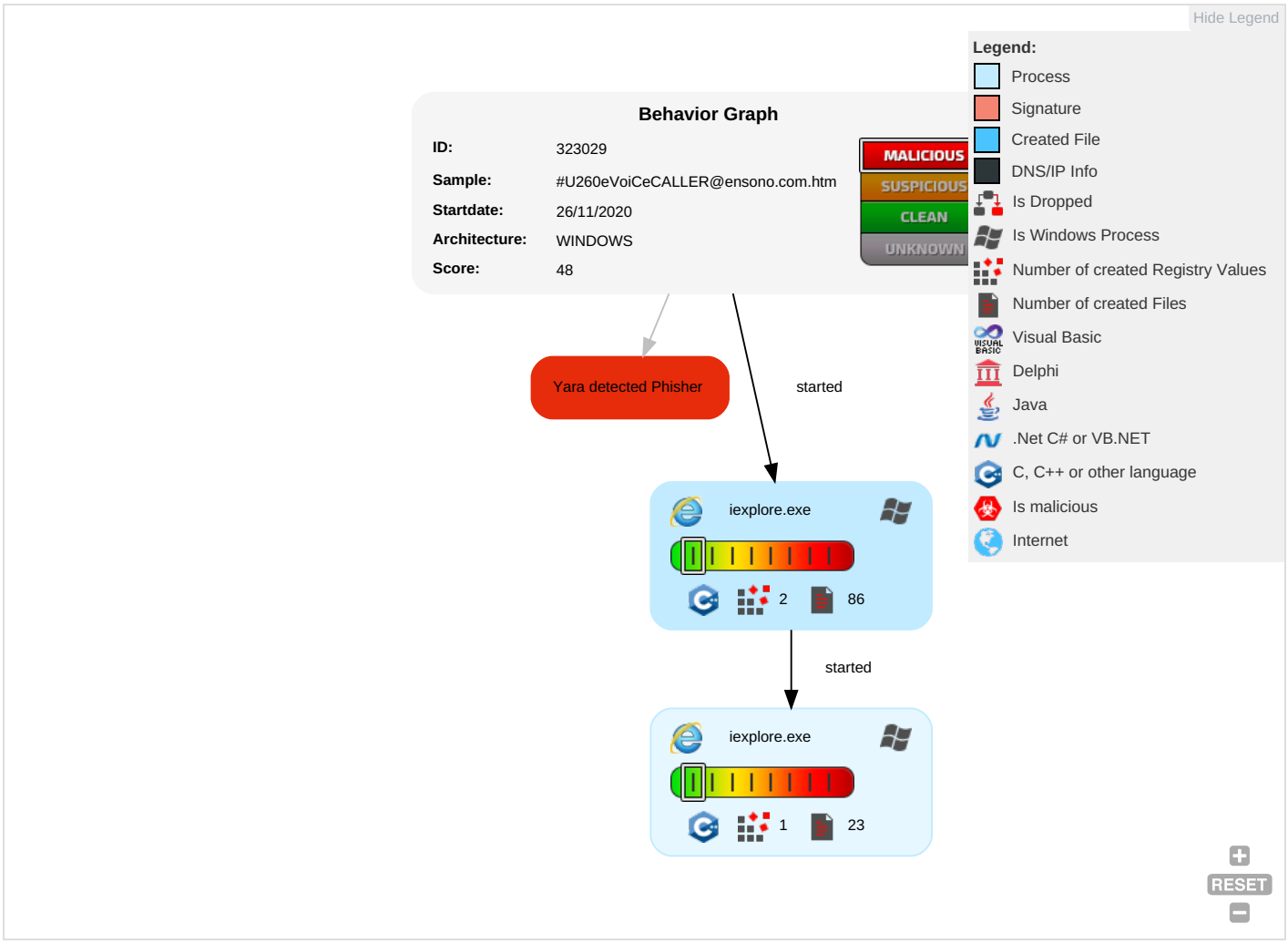
Phishing:

Yara detected Phisher

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	Impact
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	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
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	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

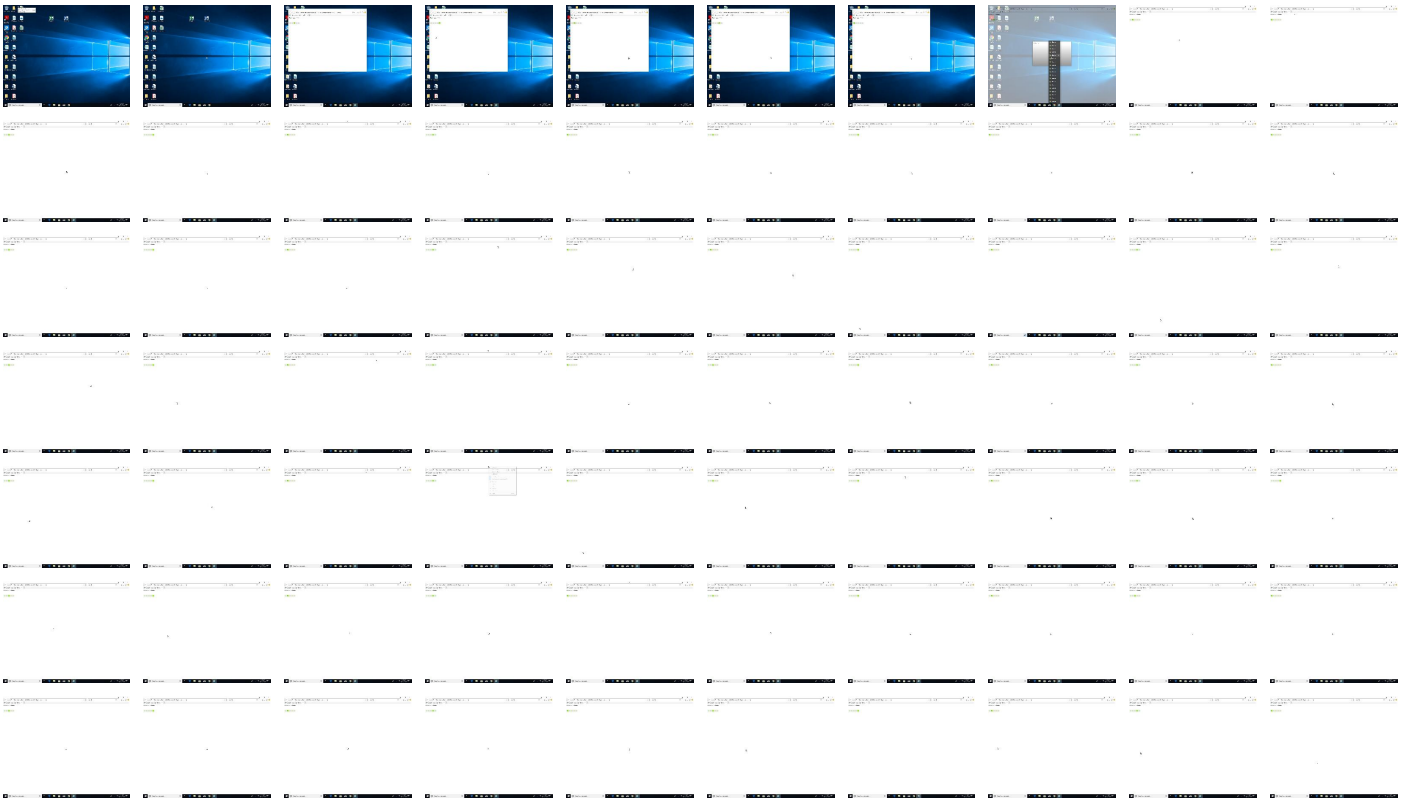
Behavior Graph

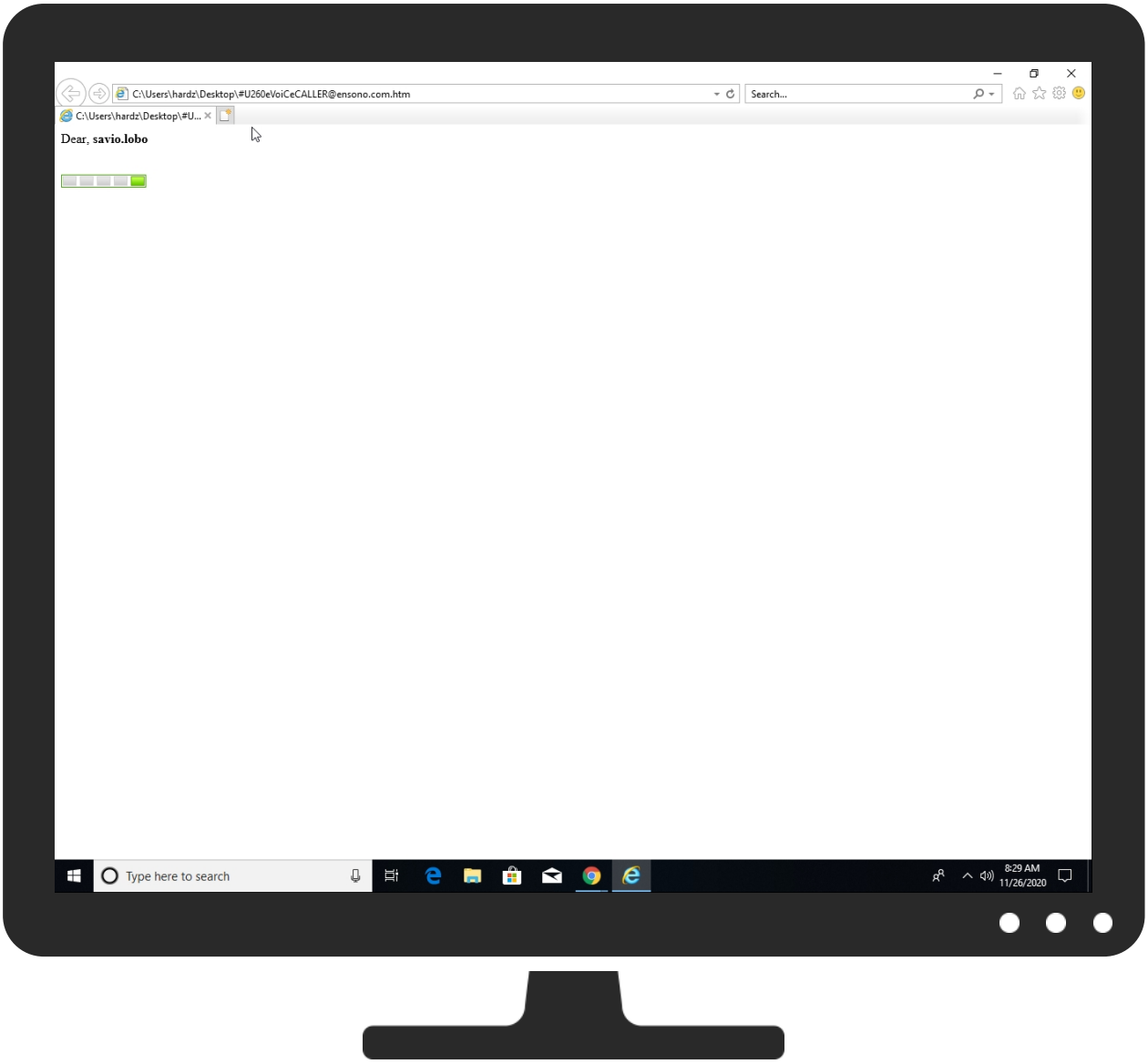


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

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	
http://https://uesb9.com.my/c2F2aW8ubG9ib0BlbnNvbm8uY29t	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/%23U260eVoiCeCALLER@ensono.com.htm	true		low

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://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
http://https://uesb9.com.my/c2F2aW8ubG9ib0BlbnNvbm8uY29t	#U260eVoiCeCALLER@ensono.com.htm	false	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323029
Start date:	26.11.2020
Start time:	08:28:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	#U260eVoiCeCALLER@ensono.com.htm
Cookbook file name:	default.jbs
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:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.phis.winHTM@3/15@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .htm
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 13.64.90.137, 168.61.161.212, 204.79.197.200, 13.107.21.200, 104.83.120.32, 51.11.168.160, 104.42.151.234, 23.210.248.85, 152.199.19.161, 8.241.122.126, 67.26.139.254, 8.248.113.254, 8.253.95.249, 67.27.234.126, 51.104.144.132, 92.122.213.247, 92.122.213.194, 20.54.26.129, 92.122.145.220 • 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, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, go.microsoft.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, dual-a-0001.a-msedge.net, ie9comview.vo.msecnd.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.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.{79F938E5-3004-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8462538458492341
Encrypted:	false
SSDEEP:	96:roZjZm209WmQtmDfmj9MmvmLMmLLfmLhMX:roZjZm209WXtYfS9Ma5Mf0MX
MD5:	0B46341101F77303CBDB6A2B91A57076
SHA1:	B41F2B298795DB087A4FD739316A369CE8402AD3
SHA-256:	DE0737D5CA9132EE3E72367C5FB948055D1DE1E77264385E3F08F84C30C044FE
SHA-512:	93B76B4FAEA00DEE02615895CE7D94E12335C1F748F540374FDF548026F0B5A95F4E3DB74E37C770038DDDC5B620D81E053F9AAEEC2861F3E2B32AECDAD9FA6
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\{79F938E7-3004-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24236
Entropy (8bit):	1.6430986567580008
Encrypted:	false
SSDEEP:	48:IwuGcprzjGwpa7G4pQXGrapbSbrGQpBH2GHHpc+sTGUp8uAGzYpm24cYGopum4LY:ryZBQd6rBSbFjV2+kWu0MrcYPGg
MD5:	CE0B34CE65DC8871FACED8CDD7D15B55
SHA1:	EBFE017EA82370938E9FEC9DEE842B74792D8E5E
SHA-256:	A76C137D66EEA1B9C342A4DDAAF5D989E9BF103CEDFAD4E17796089D110AEB7F
SHA-512:	A5F65194F639B6523B1310F2DBD7D59FAA04F90D4FB97F2D8F8B98A958EA7F40D506308C5BF5917735DBB63DAD30454DCF1743D8510316CD09548D382801B6B1
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\{79F938E8-3004-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5653866960988418
Encrypted:	false
SSDEEP:	48:IwXGcprKjGwpaoG4pQwGrapbSZrGQpKPG7HpRcsTGIpG:rdZ2Q46OBSZFAeTc4A
MD5:	EB5BE5A2BE6FCCFBC763B83CB98A5C50

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{79F938E8-3004-11EB-90E4-ECF4BB862DED}.dat	
SHA1:	19AF6F4FCB9EF3F983F7543CF0342D078E4F53A6
SHA-256:	A1D275F3CE51D222F828CDEB084273B37D555B79AF9F24896E3F4F9F1F6FACA8
SHA-512:	31E03425D8F4A64EACEA6FEAA15362287F253848C3217A23F2AC47BE445351689EDD4ADBACDAFA6522625ADD95D05D06B6FA24E03D3F9EB905107C8A02C112C
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):	5.112628846520527
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEDVVnWimI002EtM3MHdNMNxOEDVVnWimI00ObVbkEtMb:2d6NxOGVVSZHKd6NxOGVVSZ76b
MD5:	922BDA453A5BCA8F3645E23CF1E7C9C8
SHA1:	2BE09A51CC61D6AB69309AC99875895BB5D97463
SHA-256:	054AB0611CDED58C5E84F4DFDF995084CB1628316B5E850AF9073F41FA73F410
SHA-512:	E7220B14B4C6996C917F679128C4941035A64E7F9639CE72D4430A85E6BB7EB3BEED7ED9ECF1853700545BFA4C9B3067E3C4BB9211D267879D75F538F471FC79
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x4f36f274,0x01d6c411</date><accdate>0x4f36f274,0x01d6c411</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>0x4f36f274,0x01d6c411</date><accdate>0x4f36f274,0x01d6c411</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):	5.124112807930566
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kXnWimI002EtM3MHdNMNxe2kXnWimI00Obkak6EtMb:2d6Nxr2SZHKd6Nxr2SZ7Aa7b
MD5:	DA7721A4C9EC6E363CA882BA2DE5E765
SHA1:	99C5039E70D5500061FAD1C22AF1BDD6DEF09AEE
SHA-256:	CC4B563FABE54938C16BACA7BE932F1534331B7527911547C231DEC0576AA16F
SHA-512:	D9A10CBFE08F7DF1B47771A797AA022C666C15B08FA99DD1E159DB0CC909FEB77325B81982A3E5B806AFCFE1AF6698A2DDC994B545A804696A77F0A6B51A001
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x4f322dcb,0x01d6c411</date><accdate>0x4f322dcb,0x01d6c411</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>0x4f322dcb,0x01d6c411</date><accdate>0x4f322dcb,0x01d6c411</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):	5.130432463955484
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLRnWimI002EtM3MHdNMNxvLRnWimI00ObmZEtMb:2d6NxvNSZHKd6NxvNSZ7mb
MD5:	84E36CB7A63CB9C63C7A318E4A513924
SHA1:	69690C94902ACED658D21AFA5C8A257043F38285
SHA-256:	10DA7FA624BB9491DABA72D0F105DD0EF911B392D187C6E04DDB95698F295E15
SHA-512:	89A95ECA7286DED7DA4DD9122D1BCD933AE1C9FA9A9353D15FE35C97ED4A143815400952260 0A1187D382601CF3A5D05245ECC7C3B7011CE091059E64F9F8B4
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x4f3954c7,0x01d6c411</date><accdate>0x4f3954c7,0x01d6c411</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>0x4f3954c7,0x01d6c411</date><accdate>0x4f3954c7,0x01d6c411</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):	5.098359640098819
Encrypted:	false
SSDEEP:	12:TMHdNMNxiDEtEVnWimI002EtM3MHdNMNxiDEtEVnWimI00Obd5EtMb:2d6NxQEtEVSZHKd6NxQEtEVSZ7Jjb
MD5:	4A6A99B3FF60E20E146F61768316789A
SHA1:	B3FAC4733227E3E3DEFBA7453D5743015893EC2E
SHA-256:	E685FDFA2C2AD0E7D946A457CE07A748F275034FA4CD59EB67459330FFB840C7
SHA-512:	AB54F37CC4231A249890E68F23A0D5DE91DB754B30AD6D52848024F1EBD8CE04A744959CFE8BEB3DC052C5D21CE2197882D73182E826EBD0E40E67E9FB8DD7B
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x4f348ffd,0x01d6c411</date><accdate>0x4f348ffd,0x01d6c411</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>0x4f348ffd,0x01d6c411</date><accdate>0x4f348ffd,0x01d6c411</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):	5.1453374744177225
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwRnWimI002EtM3MHdNMNxhGwRnWimI00Ob8K075EtMb:2d6NxQASZHKd6NxQASZ7YKajb
MD5:	6D83D69E3111FF5F58280BA6E289F519
SHA1:	2FAF12ABFFF77DC8875C135CEA9117572A214421
SHA-256:	60A1DC282D4112504A3D1E7BE2DED5EE10C838741023907BA6D45BA8990E6427
SHA-512:	C292BDCE89CE45FB18F7276AB96F5B862A22398CC616A3514D17E1F4EA744EEC9C9F84A590E8323F879C53F39DA1BD99829381241EF758A3A2D01CC9C28B6B6
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x4f3954c7,0x01d6c411</date><accdate>0x4f3954c7,0x01d6c411</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>0x4f3954c7,0x01d6c411</date><accdate>0x4f3954c7,0x01d6c411</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):	5.11588367311809
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nDVVnWimI002EtM3MHdNMNx0nDVVnWimI00ObxEtMb:2d6Nx0DVVSZHKd6Nx0DVVSZ7nb
MD5:	189B2F60393EC15334564B3FA4DFB8CB
SHA1:	9800209A37A64C14D5DC6C5B0E3505D793D42D5B
SHA-256:	19B328C3E10AD1B031DB57B22F332228424D7BD05BFD2D75065136E3D724E8C7
SHA-512:	CFAD928D88A8DB5BBBD3FC5B581023264AA494FD504A3291F67639EBA2ABD1D7EA8364AE5EBB12479C0F576CCBFE2BF38F530995C9FCEE898C4BDC975220EA55
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x4f36f274,0x01d6c411</date><accdate>0x4f36f274,0x01d6c411</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>0x4f36f274,0x01d6c411</date><accdate>0x4f36f274,0x01d6c411</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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.153052547791224
Encrypted:	false
SSDEEP:	12:TMHdNMNxxDVVnWimI002EtM3MHdNMNxxDVVnWimI00Ob6Kq5EtMb:2d6NxNVVSZHKd6NxNVVSZ7ob
MD5:	553ABA2FC623F5AA3DD005AB5EC835F4
SHA1:	B2C86AE9E1B6A90BD8245861166BA2573CE61B43
SHA-256:	F7E406248BC0BA56022E2A6D961B38ABE543B40D7B4F67152BE837D2819703C3
SHA-512:	83EF175D75D624D2B2F70FACE9472CB4CB50177F744CEEEF3898AFA5C552968DFDE9FC709143C919841F5B30692A527B8146E573E6F51E812E4ADF779103E3E1
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x4f36f274,0x01d6c411</date><accdate>0x4f36f274,0x01d6c411</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>0x4f36f274,0x01d6c411</date><accdate>0x4f36f274,0x01d6c411</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):	5.100540654745781
Encrypted:	false
SSDEEP:	12:TMHdNMNxcDEtEVnWimI002EtM3MHdNMNxcDEtEVnWimI00ObVEtMb:2d6NxKEtEVSZHKd6NxKEtEVSZ7Db
MD5:	913F4189464B36165DB91F8DA85CC7D5
SHA1:	3146F1F889F00F3631811E8EC0FD18B3C74625A4
SHA-256:	34684A292B8AA3AD027BE84468362F84CD295A0EE073EE6B6FAB66C33B88B59B
SHA-512:	251B86EF3B8CE72376ED22ECD206BB78EF6B0D2E63B31F865352420C7BFE487A6D363129E2AE5F99282DD32E63AFEDA181A17BC867302B941618AF5D9177FF8
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x4f348ffd,0x01d6c411</date><accdate>0x4f348ffd,0x01d6c411</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>0x4f348ffd,0x01d6c411</date><accdate>0x4f348ffd,0x01d6c411</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):	5.084140486836328
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnDEtEVnWimI002EtM3MHdNMNxfnDEtEVnWimI00Obe5EtMb:2d6Nx7EtEVSZHKd6Nx7EtEVSZ7ijb
MD5:	F632D28EF2CE861070AEF573FD9F7DF3
SHA1:	9256ABD220594DFE1AA0237574E06C993C2749A7
SHA-256:	ED3802C925861B574AB20712B35265D26ABC35BD480E9D35756BCAB3ADBA646F
SHA-512:	50D66DD806293DE5EC134BF83D5AB2DFA1274D67F92CC42CEA99CE3CABD6F9AD9C6F96FA3DF8934FD090343D3A2FD971C415E75CDD55F06E4597DE25EEAF807
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x4f348ffd,0x01d6c411</date><accdate>0x4f348ffd,0x01d6c411</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>0x4f348ffd,0x01d6c411</date><accdate>0x4f348ffd,0x01d6c411</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Temp\~DF1219ADD9DE056562.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34429
Entropy (8bit):	0.363756786559758
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwNO9lwNhk9l2Ng9l2N2:kBqoxKAuvScS+nHJLC2l2Ym4Lrf
MD5:	91F5BF25669958E9D86DD5209406E559
SHA1:	FEF1696C465ADE1AED96E2F071ACCD70BEF149AD

C:\Users\user\AppData\Local\Temp\~DF1219ADD9DE056562.TMP	
SHA-256:	4F15C18E656AE47FE59E4760176829E47198C9F835A90348BADF1CED53E20197
SHA-512:	E7B488E8C3401A5FCFF9D16A36B871712285FE6B3EFE6C918F238DFC7C6D268CC02BBE2101F3E30AB8E22EF2A49C21172DC03B16C66E6DEB9EBF86E58209A1 9
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF45D7CA75BC90EE11.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47392922299431395
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loE0rF9loE0R9lWE0k6+pl6+Gaa+GA3SDrlSDre:kBqoIV6VEVk6+pl6+GF+GA3SDrlSDre
MD5:	B7AB348265E877DA404967A0A74C0220
SHA1:	995C1A454BE9F5FEF8A34FD9223EA9B9A7D95737
SHA-256:	8234EBC0AB48EE0ADF0124D1A0D026716C811A337127467E4A04C2F10A580D9F
SHA-512:	74598D50DEBA13D4D2532BD46DE4A32F3F1FBA0819768514D812B7C42C654427F03FF08201C85F0817971D46C0C96620EE1F0DB3775D135897FAEAFC93B07E61
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF94A290286564D177.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.3356481730520129
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAR4St/2B:kBqoxxJhHWSVSEabKSt/2B
MD5:	C82DD48F9AA46CCC8AD75A2D91662A76
SHA1:	1E8FC4D7F86641375373EC3E8BDFB4A75BD40004
SHA-256:	224139951E434E051F118C1563819FD374C6ABEB85D0F4212D1A41864B9A61A0
SHA-512:	556EEBED08ECD1309ED84EED6F172043FEF79E9B5BCBFC53D3A25E7F45DF33547FEDADDB8321466FA6143D3D9694D47DCF94736EBCE746FA0306F15498948C F0
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

File type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	5.952468986029711
TrID:	
File name:	#U260eVoiCeCALLER@ensono.com.htm
File size:	2308
MD5:	854acf66612439963bb33ef491392419
SHA1:	769e490db70e392d2fbdd12eb2d9005ad8e23206
SHA256:	9953401e31b3e8dc22d887342c31944556c39aa5664f0c9603ad4f4862519626
SHA512:	2b3de6a2835c394d3561800c06329da28caa0a83915fb6893d555e80235c20d58e640ac12a07f88f6bf4d8d1a80cb9d1b68cf0f3a5ae22cf744d34e9daa05f2b
SSDEEP:	48:PCTGoyH5kWQV1COFF8fm9HJH19HJW9HJu9HgM:PfH5kW2C01aej

General

File Content Preview:	..<p> Dear, savio.lobo..<p> <img src="

File Icon

Icon Hash:	f8c89c9a9a998cb8

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 08:28:50.360934019 CET	50620	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:28:50.388154984 CET	53	50620	8.8.8.8	192.168.2.3
Nov 26, 2020 08:28:51.459927082 CET	64938	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:28:51.487122059 CET	53	64938	8.8.8.8	192.168.2.3
Nov 26, 2020 08:28:52.476577997 CET	60152	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:28:52.503772974 CET	53	60152	8.8.8.8	192.168.2.3
Nov 26, 2020 08:28:52.664201021 CET	57544	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:28:52.691349983 CET	53	57544	8.8.8.8	192.168.2.3
Nov 26, 2020 08:28:53.798378944 CET	55984	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:28:53.834079981 CET	53	55984	8.8.8.8	192.168.2.3
Nov 26, 2020 08:28:55.710737944 CET	64185	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:28:55.737803936 CET	53	64185	8.8.8.8	192.168.2.3
Nov 26, 2020 08:28:56.667603970 CET	65110	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:28:56.706897020 CET	53	65110	8.8.8.8	192.168.2.3
Nov 26, 2020 08:28:56.977842093 CET	58361	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:28:57.004975080 CET	53	58361	8.8.8.8	192.168.2.3
Nov 26, 2020 08:28:58.558607101 CET	63492	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:28:58.585697889 CET	53	63492	8.8.8.8	192.168.2.3
Nov 26, 2020 08:28:59.890789032 CET	60831	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:28:59.917829990 CET	53	60831	8.8.8.8	192.168.2.3
Nov 26, 2020 08:29:00.938994884 CET	60100	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:29:00.966155052 CET	53	60100	8.8.8.8	192.168.2.3
Nov 26, 2020 08:29:04.565270901 CET	53195	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:29:04.600756884 CET	53	53195	8.8.8.8	192.168.2.3
Nov 26, 2020 08:29:05.738580942 CET	50141	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:29:05.765605927 CET	53	50141	8.8.8.8	192.168.2.3
Nov 26, 2020 08:29:06.743398905 CET	53023	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:29:06.770673037 CET	53	53023	8.8.8.8	192.168.2.3
Nov 26, 2020 08:29:07.928845882 CET	49563	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:29:07.955996037 CET	53	49563	8.8.8.8	192.168.2.3
Nov 26, 2020 08:29:15.344160080 CET	51352	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:29:15.371169090 CET	53	51352	8.8.8.8	192.168.2.3
Nov 26, 2020 08:29:15.868882895 CET	59349	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:29:15.896030903 CET	53	59349	8.8.8.8	192.168.2.3
Nov 26, 2020 08:29:16.174379110 CET	57084	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:29:16.210007906 CET	53	57084	8.8.8.8	192.168.2.3
Nov 26, 2020 08:29:17.206300020 CET	58823	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:29:17.241585970 CET	53	58823	8.8.8.8	192.168.2.3
Nov 26, 2020 08:29:22.723738909 CET	57568	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:29:22.760658979 CET	53	57568	8.8.8.8	192.168.2.3
Nov 26, 2020 08:29:26.676382065 CET	50540	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:29:26.711931944 CET	53	50540	8.8.8.8	192.168.2.3
Nov 26, 2020 08:29:27.489046097 CET	54366	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 08:29:27.524657011 CET	53	54366	8.8.8.8	192.168.2.3
Nov 26, 2020 08:29:27.674766064 CET	50540	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:29:27.710248947 CET	53	50540	8.8.8.8	192.168.2.3
Nov 26, 2020 08:29:28.483772039 CET	54366	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:29:28.519190073 CET	53	54366	8.8.8.8	192.168.2.3
Nov 26, 2020 08:29:28.687252045 CET	50540	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:29:28.722913027 CET	53	50540	8.8.8.8	192.168.2.3
Nov 26, 2020 08:29:29.615122080 CET	54366	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:29:29.650598049 CET	53	54366	8.8.8.8	192.168.2.3
Nov 26, 2020 08:29:31.306096077 CET	50540	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:29:31.341527939 CET	53	50540	8.8.8.8	192.168.2.3
Nov 26, 2020 08:29:31.624773026 CET	54366	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:29:31.660295963 CET	53	54366	8.8.8.8	192.168.2.3
Nov 26, 2020 08:29:32.897578001 CET	53034	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:29:32.924732924 CET	53	53034	8.8.8.8	192.168.2.3
Nov 26, 2020 08:29:34.121901989 CET	57762	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:29:34.157501936 CET	53	57762	8.8.8.8	192.168.2.3
Nov 26, 2020 08:29:35.312748909 CET	50540	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:29:35.339773893 CET	53	50540	8.8.8.8	192.168.2.3
Nov 26, 2020 08:29:35.410517931 CET	55435	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:29:35.438069105 CET	53	55435	8.8.8.8	192.168.2.3
Nov 26, 2020 08:29:35.640870094 CET	54366	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:29:35.676460981 CET	53	54366	8.8.8.8	192.168.2.3
Nov 26, 2020 08:29:38.790831089 CET	50713	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:29:38.818062067 CET	53	50713	8.8.8.8	192.168.2.3
Nov 26, 2020 08:29:51.582416058 CET	56132	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:29:51.609508991 CET	53	56132	8.8.8.8	192.168.2.3
Nov 26, 2020 08:29:57.101052046 CET	58987	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:29:57.138128042 CET	53	58987	8.8.8.8	192.168.2.3
Nov 26, 2020 08:30:28.241914988 CET	56579	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:30:28.269040108 CET	53	56579	8.8.8.8	192.168.2.3
Nov 26, 2020 08:30:41.597552061 CET	60633	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:30:41.632930040 CET	53	60633	8.8.8.8	192.168.2.3
Nov 26, 2020 08:30:42.735198975 CET	61292	53	192.168.2.3	8.8.8.8
Nov 26, 2020 08:30:42.772702932 CET	53	61292	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6048 Parent PID: 792

General

Start time:	08:28:55
Start date:	26/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff62a6e0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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: 4812 Parent PID: 6048

General

Start time:	08:28:56
Start date:	26/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6048 CREDAT:17410 /prefetch:2
Imagebase:	0xd40000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	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