ID: 480997
Sample Name: VjLfUM5cMx
Cookbook: default.jbs
Time: 07:26:27
Date: 10/09/2021
Version: 33.0.0 White Diamond

Table of Contents

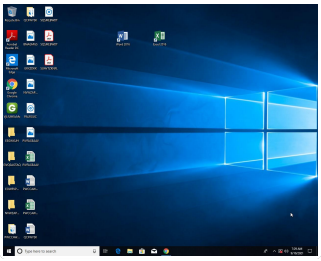
Windows Analysis Report VjLfUM5cMx

Overview

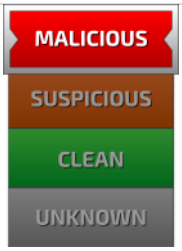
General Information

Sample Name:	VjLfUM5cMx (renamed file extension from none to exe)
Analysis ID:	480997
MD5:	c07d4f7dcac497a..
SHA1:	f9910595a15ee0c.
SHA256:	82aabb70809394..
Tags:	exe FORTHPROPERTYLTD
Infos:	

Most interesting Screenshot:



Detection



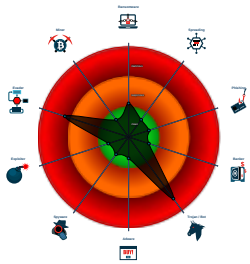
Ursnif Ursnif v3

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Ursnif
- Multi AV Scanner detection for subm…
- Detected unpacking (changes PE se…
- Yara detected Ursnif
- Writes or reads registry keys via WMI
- Writes registry values via WMI
- Machine Learning detection for samp…
- Performs DNS queries to domains w…
- Uses 32bit PE files
- Antivirus or Machine Learning detec…
- PE file contains an invalid checksum
- PE file contains strange resources
- May sleep (evasive loops) to hinder …
- Checks if Antivirus/Antispyware/Fire…
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- VjLfUM5cMx.exe (PID: 6120 cmdline: 'C:\Users\user\Desktop\VjLfUM5cMx.exe' MD5: C07D4F7DCAC497A3C06CBBA9E6E9E711)
- iexplore.exe (PID: 2856 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6960 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2856 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 1492 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 3740 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1492 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.743054194.0000000003640000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.742911268.0000000003640000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.742353433.0000000003640000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.743093279.0000000003640000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.743313694.0000000003640000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 29 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.3.VjLfUM5cMx.exe.dc9d7c.0.raw.unpack	JoeSecurity_Ursnifv3	Yara detected Ursnif	Joe Security	
0.2.VjLfUM5cMx.exe.1000000.0.unpack	JoeSecurity_Ursnifv3	Yara detected Ursnif	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

Performs DNS queries to domains with low reputation

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

Yara detected Ursnif

System Summary:

Writes or reads registry keys via WMI

Writes registry values via WMI

Data Obfuscation:

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

Yara detected Ursnif

Remote Access Functionality:

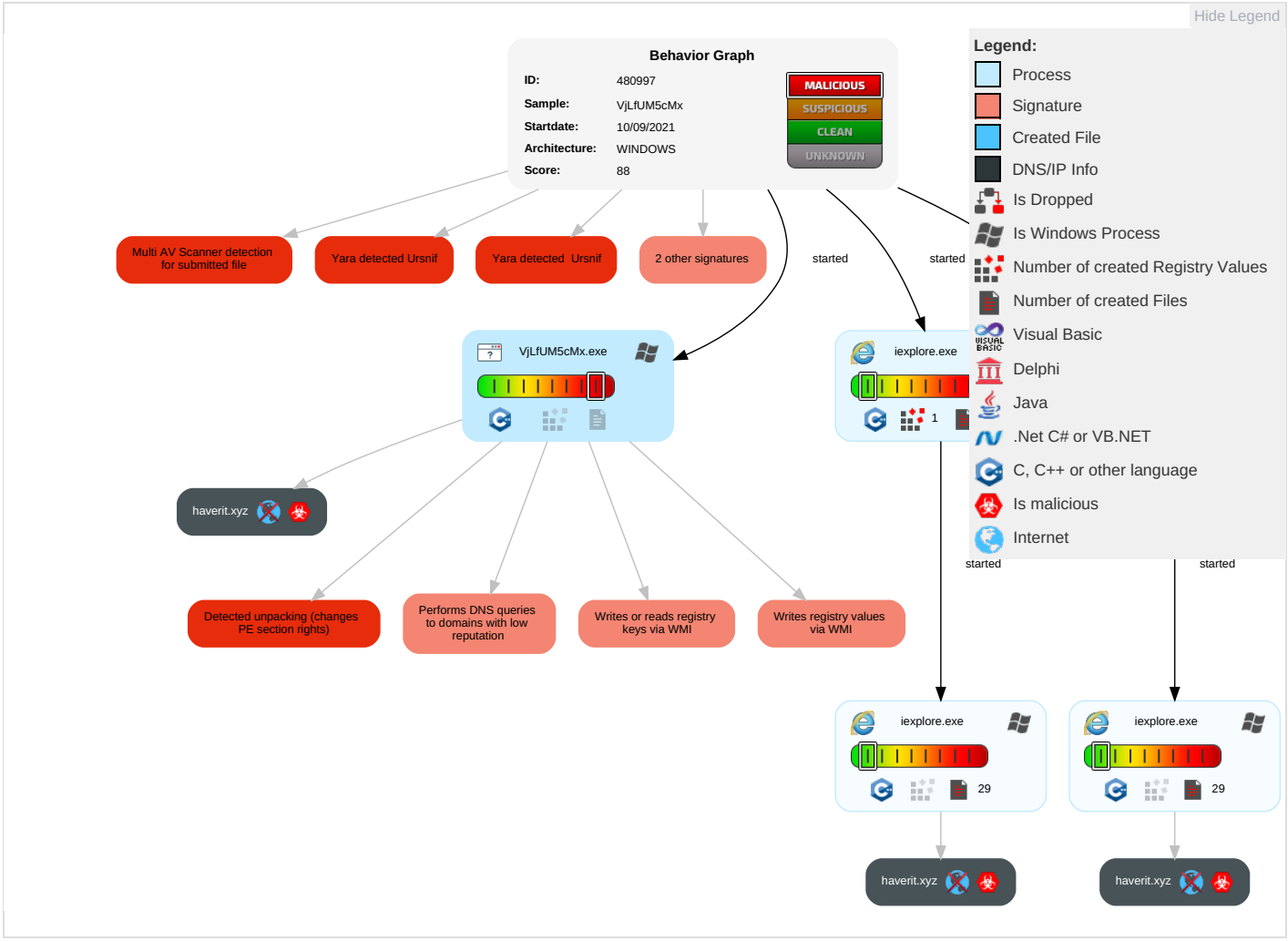
Yara detected Ursnif

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 2	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces

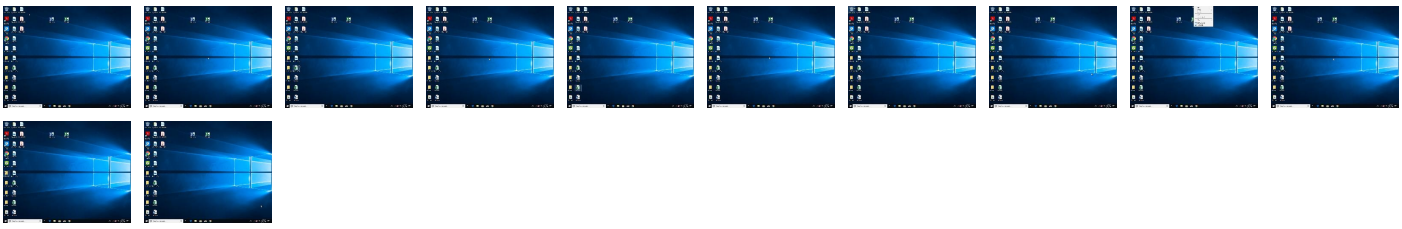
Behavior Graph



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
VjLfUM5cMx.exe	13%	Virustotal		Browse
VjLfUM5cMx.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.3.VjLfUM5cMx.exe.dc9d7c.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.VjLfUM5cMx.exe.1000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://haverit.xyz/index.htm	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://haverit.xyz/index.htmr#	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://https://haverit.xyz/index.htmdex.htm	0%	Avira URL Cloud	safe	
http://%s=%s&file://&os=%u.%u_%u_%u_x%uindex.html;	0%	Avira URL Cloud	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://https://haverit.xyz	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://https://haverit.xyz/0b	0%	Avira URL Cloud	safe	
http://https://haverit.xyz/Q	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://https://haverit.xyz/index.htm&E	0%	Avira URL Cloud	safe	
http://https://haverit.xyz/index.htmRoot	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
haverit.xyz	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	480997
Start date:	10.09.2021
Start time:	07:26:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	VjLfUM5cMx (renamed file extension from none to exe)
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:	18
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:	mal88.troj.evad.winEXE@7/29@8/0
EGA Information:	Failed
HDC Information:	Failed

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
07:28:22	API Interceptor	2x Sleep call for process: VjLfUM5cMx.exe modified

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.{077FA0D4-11F8-11EC-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7687952691507924
Encrypted:	false
SSDEEP:	192:rZZe9Zi2z1WzMtzJifzzU2zMzwOg62CBzMlpB:rPezBzMz4zmz+zlzq
MD5:	E92FD7DF6802E331C7A855D3A78FEFEA
SHA1:	80610D98C43B9F68C370E37224AA9D5A25CC650A
SHA-256:	D1E5051E0E89115F43C3EB87B41D8EE0272787B84AA7936A41CB4E39B031B4AD
SHA-512:	05E023DF86A9A6ADBA94FE937A96493B2B89FE69DACF871FC9F370D28CB0EFA12B5E8811B3D43427D55F7368F46080900F5F966F42FB61C88D6C93345EA1D91
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\RecoveryStore.{E1A18F6F-11F7-11EC-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7653733500022424
Encrypted:	false
SSDEEP:	192:rSZX9Za2lWRtJHifJ3jxvzM9353+6YjBxw34gpB:rOXzZ/jawYu
MD5:	D24E24FB19663AB8E7C73D6587EFFF6C
SHA1:	B82737BFA7A49BA4BCF3A0C81C14962DAEEDBAF1
SHA-256:	B08D2BC882D1E7ECCC639CD0054218DE9BF9B7DD213335A776E96D876A2CD96D
SHA-512:	D2F202639C2A74152BC1DE4AA9F2AB33240A2C09E25D4196C6A2EEBD50EC0458A5680A35B05F46FC064EF2C87BBAE6421AF14E84DC4753798C74E31B6AD696 1
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\{077FA0D6-11F8-11EC-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26240
Entropy (8bit):	1.6585521788268434
Encrypted:	false
SSDEEP:	48:IwDGcprCjGwpaCG4pQqGrapbSAGQpBtcBGHHpct62TGUp8tdGzYpmtEOGopOzEyq:r5ZC9Qy6cBSojt2lWNMFk+V2A
MD5:	8C6512EF426D5BB96705D87CC986C2D3
SHA1:	F3EC5C5DF2C53E864807177BA6F9FDA27D3CFCD1
SHA-256:	6999B248C19B53968E3EAB2BCB6D7DCB82D1263108B80FF236D032245D633799
SHA-512:	FD5798A38BB65D6975E9F59A8BBC0D6A0D2194D52798F67702DE11B97DD6DF68CACBBE2D050A11B39D3632B9982C1A767F0BE620B4364EE300EB91595DB523 0
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\{E1A18F71-11F7-11EC-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26240
Entropy (8bit):	1.6568915553272197
Encrypted:	false
SSDEEP:	48:IwXGcprqjGwpaeG4pQ6GrapbSZGQpByGHHpcrTGUp8kGzYpmb0GopOdyDCGqXpHR:rdZq9Qe6sBSzjJ2FWAMQkPVGA
MD5:	976CE6A118BC49942D4F83A41795AF60
SHA1:	0886BB24D61554692CF98EB0DAEF152B8D82130C
SHA-256:	C1363B5295C4FC934787D3D95811D426B5009EFCAE0004611A2F9FC9CE36C4D9
SHA-512:	51ED9BB236F9FD16CBD91C63689B10EB504C61366F2B628CD43F27176E285F7619019DF2781F97C91F5213FD1D26291548EDB6857D01DE1A693124C83C431EF5
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):	5.097103490576207
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
SSDEEP:	12:TMHdNMNxOEjwanWimI002EtM3MHdNMNxOEjwanWimI00OYGVbkEtMb:2d6NxOcwaSZHKd6NxOcwaSZ7YLb
MD5:	01FB138155392A0403F38515CE0F9A89
SHA1:	3870F06CE96AA652A0E4291609CB3538AB309936
SHA-256:	24D93C2842111FE151324DA082D5C8559AA307AF5F185AF9DA4E468956E4D585
SHA-512:	E9D30B7E77328CD6733E95C137A6996EEAF3FDEB8F317C6940D36A190DF0508D98EEDC1F5130F6E3B15677755E77724EE698656E775D151A3F1FEF2D208D99F1
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xb71b6d91,0x01d7a604</date><accdate>0xb71b6d91,0x01d7a604</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>0xb71b6d91,0x01d7a604</date><accdate>0xb71b6d91,0x01d7a604</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):	5.119386841314523
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kRqanWimI002EtM3MHdNMNxe2kRqanWimI00OYGkak6EtMb:2d6NxrGqaSZHKd6NxrGqaSZ7Yza7b
MD5:	78C567EB422B95A55974D3844C4E3A25
SHA1:	4A043CD69791CB35A7BBE32E0A019B1024DA867C
SHA-256:	DB54273546F218206DDCADD0D68EF38F3922184C700AE0F5180F22733C6A626E
SHA-512:	340977812B58FF75C72FB24707C819A1831D83F7D95D4740EA3D21735A28B20472966F2046BD458D3A9E58005AABC7547D729FE3BB54065D144BDFB0B8A61CD3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xb714465a,0x01d7a604</date><accdate>0xb714465a,0x01d7a604</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>0xb714465a,0x01d7a604</date><accdate>0xb714465a,0x01d7a604</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):	5.167162589928272
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL1pSpanWimI002EtM3MHdNMNxvL1pSpanWimI00OYGmZEtMb:2d6NxvjYaSZHKd6NxvjYaSZ7Yjb
MD5:	95E9AFC9B0CA3948C096400220F6E2FC
SHA1:	ED40EE9CBEF489E1A0937B55484C50004366147A
SHA-256:	2637059B1F09E429B62D3442314CC96CD1D0D031173BFE42C04790E26ED3F3C6
SHA-512:	35F4FFFADAEC9EC48833FCE35C5B9B3BD9BAE7D14E22CED33FD549DB4A97B644603D92D79F3FAB26FFE2A3413C777AFC41E85AF4C3F7FB62DAE0271F30292DB2
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xb7229583,0x01d7a604</date><accdate>0xb7229583,0x01d7a604</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>0xb7229583,0x01d7a604</date><accdate>0xb7229583,0x01d7a604</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):	5.11260966532361
Encrypted:	false
SSDEEP:	12:TMHdNMNxijwanWimI002EtM3MHdNMNxijwanWimI00OYGd5EtMb:2d6Nx2waSZHKd6Nx2waSZ7YEjb
MD5:	4ADAE51FDF242ACCBA0BA603E37F65C8
SHA1:	096307D1C70E2E3AFE1651ECF0A009BB24062841
SHA-256:	A112CC8C0B606E3D96F3985A70B44BC93ED0CD87EA3C8A19A3F225B2B7BD6B71
SHA-512:	AAB1906DBE98B8F6C21A4C10EE06C82C93565B9CB5DD6E690BFD8D947650C0BE8A9665C36681E5FF1C9C312E39386DFF9102AD9D4F0FDCBEB7DA0C8038B5ED4E

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xb71b6d91,0x01d7a604</date><accdate>0xb71b6d91,0x01d7a604</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>0xb71b6d91,0x01d7a604</date><accdate>0xb71b6d91,0x01d7a604</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):	5.178861223167003
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGw1pSpanWimI002EtM3MHdNMNxhGw1pSpanWimI00OYG8K075EtMb:2d6NxQYYaSZHKd6NxQYYaSZ7YrKajb
MD5:	A32AA08FE4957F980C25BA02B088C7A3
SHA1:	9C0B720474A1BCFE89045161D504C6A1F19DCDD0
SHA-256:	1C39487B76D89749483D67B722E091B8A159D75A7B0CFD126627218126A103F5
SHA-512:	79638801E8F940CDD4FB7F98D4D54C74E0613BEDBD8BB6DC7C076635DCE08ED84FAD73D66C5358137AA88845630FDC1D1AD79FA730E7A2F2443516A9C19F392
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xb7229583,0x01d7a604</date><accdate>0xb7229583,0x01d7a604</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>0xb7229583,0x01d7a604</date><accdate>0xb7229583,0x01d7a604</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):	5.0983299559903665
Encrypted:	false
SSDEEP:	12:TMHdNMNx0njwanWimI002EtM3MHdNMNx0njwanWimI00OYGxEtMb:2d6Nx0jwaSZHKd6Nx0jwaSZ7Ygb
MD5:	30009857A260CBF0B20FAA19AEED39DC
SHA1:	31E15FD67D29A6BB7BA93456B319C1F311D1423D
SHA-256:	22E514DBB72F0368497D4E14279F41CEC6E42D5D1DEA55434C9D7849BC11DC77
SHA-512:	DD691F1D0820CCF54A52A8F1F6C520AC085514B305606F73E62814EDF041F47D8886CF08ED13301BE0A999ACDEA11CF38EB77DE932547120BB304A8676D49CD
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xb71b6d91,0x01d7a604</date><accdate>0xb71b6d91,0x01d7a604</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>0xb71b6d91,0x01d7a604</date><accdate>0xb71b6d91,0x01d7a604</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\pin202591677780\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):	5.136738769904
Encrypted:	false
SSDEEP:	12:TMHdNMNxxjwanWimI002EtM3MHdNMNxxjwanWimI00OYG6Kq5EtMb:2d6NxBwaSZHKd6NxBwaSZ7Yhb
MD5:	9443E152D8CB24CCE6B18B7FB82AF0CC
SHA1:	A7A4916172C5A0FF545F1192057DA50246E2FD9C
SHA-256:	F4ACB9872F7882249023FDFA21CA78B8267B0E277701467281EFFC6AE805AD03
SHA-512:	B348117CCFC016FD9FBB101EEC1E53899E4087C665F7B4A0E846E198D9838A71FB2DEC497EEA70A8576013174C2C95F581EF3663C38AD614883CF8D3FE9F6DE
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xb71b6d91,0x01d7a604</date><accdate>0xb71b6d91,0x01d7a604</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>0xb71b6d91,0x01d7a604</date><accdate>0xb71b6d91,0x01d7a604</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):	5.111475006436849
Encrypted:	false
SSDEEP:	12:TMHdNMNxcjwanWiml002EtM3MHdNMNxcjwanWiml00OYGVEtMb:2d6NxEwaSZHKd6NxEwaSZ7Ykb
MD5:	DE14F026220BC4AD975589A143D4862D
SHA1:	D4B22718CF721228E0CDB1C10489148FD3DF0CBC
SHA-256:	696399FD8895D1AAE33915A14619DEC5B7C8744AD37E1C99E56DF656A9EFBF70
SHA-512:	E98BE0BFC148546AE0191E54C96931639D12DE30A9821A1C529002CF681B932DF1968A1D2CCC38B3B9F48C81D69810A7E389F20C4589E339144785EB89219BC0
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xb71b6d91,0x01d7a604</date><accdate>0xb71b6d91,0x01d7a604</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>0xb71b6d91,0x01d7a604</date><accdate>0xb71b6d91,0x01d7a604</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):	5.097923317006781
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnjwanWiml002EtM3MHdNMNxfnjwanWiml00OYGe5EtMb:2d6NxLwaSZHKd6NxLwaSZ7YLjb
MD5:	2505F5CDDDEC582665E57DD8138AE8FE
SHA1:	580DF47543557FB9077349D0BA0ACAC798857786
SHA-256:	ED9E4F3EBF559EC0BBB0B52FC9E6E83EA099648AB523B97904A4E3F95A3729F7
SHA-512:	E233567EC2DE9325ED0AE16EA3B43721B67EA77ECD8F17B32746B94BE2C64A788542E91F4880EDFC8D8923673C53CBCC17AAE1921538CB3744EF3F7736367D7
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xb71b6d91,0x01d7a604</date><accdate>0xb71b6d91,0x01d7a604</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>0xb71b6d91,0x01d7a604</date><accdate>0xb71b6d91,0x01d7a604</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\2WF3MMUU\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
Malicious:	false
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt;..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vllJ6G7Ao8Ra

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\dnserror[1]	
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\down[1]	
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D
Malicious:	false
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #00 0000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493 AC6D
Malicious:	false
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMo reInfo('infoBlockID');">.. .. Can’t reach this page .. <div class="taskSection" id="taskSection">.. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address <span id= "webpage" class="webpageURL">is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	89
Entropy (8bit):	4.412554678800313
Encrypted:	false
SSDEEP:	3:oVXUpjHLTMW8JOGXnEpjHLTBn:o9UpLLVqEpLLV
MD5:	C1257D744F3D940640B1C3A5B5AFD9E7
SHA1:	9A590780CAC06216357B82052A64909D1C3C44B2
SHA-256:	DBDCE1B51B72E8776ECD1B4CAE2223360B2059257442B2CFE8EE031D0B18046B
SHA-512:	61B08C8D7975445BAFB761369756E2DA18AC35ED934AE61B690CE2CBCDCE0B7C86E60AD5A606F4D7ED2571AABC4B0FDC74C2B8718F0ED05C08E4443B53CE2 9E3
Malicious:	false
Preview:	[2021/09/10 07:29:13.693] Latest deploy version: ..[2021/09/10 07:29:13.693] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF53DFCC907A82F6AE.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38737
Entropy (8bit):	0.3709746847672781
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+tVt7t5totEltEwzEyDZzEyDbzEyDU:kBqoxKAuvScS+j9PGNVRDc
MD5:	48B207ABB84ABD21E374BF3B0BC629E5
SHA1:	9BA15FD9C6856628363D65CD9A28881F8BB17F7F
SHA-256:	8C3149638C6002175CFB043340B3CDDFD45176DDA6107DE00DAE2D7CD441E0EB
SHA-512:	483EC9170E76167B87E298712AC45E6F82DAF33B571A1486233C36DBE8B464207E53FF287D43281FDE824074558C86399483A08C7565DB34DFB653E5C739BABC

C:\Users\user\AppData\Local\Temp\~DF53DFCC907A82F6AE.TMP	
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFB3B5364D27108BD7.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.40524698605679654
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loha9lohK9lWhFR9qc9Yd2f:kBqoIhFhzhFR9qc9A2f
MD5:	F20C0B95ECC352ED980E564C0785243D
SHA1:	6841084009F9D90222280DD230F23D1E1D42B7EB
SHA-256:	886BFFC3541110649828420D7529FEC5E40BA180BD48719B3C54E693E5DBDC16
SHA-512:	57F02927448FDA4B144FF81A7A82A2632FB11D4DCEF1D1F3C8B02C30AFA8B05B16870BC3B10610FFA8CE0816AF03E073DF7AD2BAFC6B8CCA08ED4671DD4C5 17
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFCE99751527B74E99.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.40712809719208554
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo2A9lo2Q9lW26xiSHibOB:kBqoI272d26xiSHibOB
MD5:	E8C95AF8D3A8F841CC5EA3B6E1BDC24E
SHA1:	7A6869487B6DC66DC8038E2790CCB35238E741F7
SHA-256:	A0D8599D0CFBE862CF3B689A7BBBC70B9DE9B6DE02DE139B27DB3AD9E9D89004
SHA-512:	AF8E65D1D7F61414D7260ABB7DCDDFD34DC50547EE48DA26BF002B1141B0C8166FF6CD3B0255738C4C89DCCDC475ABC270CC2D8B244429552C24330F5A344 1
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFD3F956B20687A278.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38737
Entropy (8bit):	0.37078044094891244
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+S0e3bIbwdyDZdyDbdyDU:kBqoxKAuvScS+S0e3Ec8GT
MD5:	122B6346770EE93D6C99E259ACAADEF4
SHA1:	61DFF47B74EC6657F8103666A0142F372367155F
SHA-256:	11A757AA78EEFF90A2EC39FA8DE22BC95284EE5CF0F7A5813C553D11C967DA11
SHA-512:	2335BE3DCB0C1A1470E076582F4DA12678992AC4017109ECF8B0C04B96BC562A816C3EAAA8B8931ADE41E2842EBED5C08C96DA7C84A4713A7775C9B979F231 7
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.614337368439923
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	VjLfUM5cMx.exe
File size:	901960
MD5:	c07d4f7dcac497a3c06cbba9e6e9e711
SHA1:	f9910595a15ee0ca41871bda8f1a23a3aa7f9360
SHA256:	82aabb70809394ec910ecdff3dfe4982d652c6d65f7fa65e7da16b83ebf87192
SHA512:	0eafdb6efe6a117ed331d828613131509cd9d0d5b6be3bfc010b4af0cf809b5f8866dc0362cc853ba8d13fd2f15716e2e4d4d437b7a4503c064c2b15c653417d
SSDEEP:	24576:49PsA9vHAYobFGQdRGylSk61LXXhNxvZXmtk1/GqgLGr:VYLJk61bRLZXmWGGr
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Hl..Hl..Hl..../.Jl....*.Xl....+.Kl..Hl...l....].Ml....).Cl....+.Il....7.zl....-.Il....(.Il..RichHl.....

File Icon

Icon Hash:	f0b0e8e4e4e8b2dc

Static PE Info

General

Entrypoint:	0x1005725
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x1000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x55E85856 [Thu Sep 3 14:25:26 2015 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	e256626a548828ef6c76be7957372a60

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=Sectigo RSA Code Signing CA, O=Sectigo Limited, L=Salford, S=Greater Manchester, C=GB
Signature Validation Error:	**No signature was present in the subject**
Error Number:	-2146762496
Not Before, Not After	• 4/13/2021 2:00:00 AM 4/14/2022 1:59:59 AM
Subject Chain	• CN=FORTH PROPERTY LTD, O=FORTH PROPERTY LTD, L=Edinburgh, C=GB
Version:	3
Thumbprint MD5:	8AB6A86211EE700AA961C3292ADB312D
Thumbprint SHA-1:	A533DFA7E6AED2A9FFBE41FCEC5A8927A6EAFBBB
Thumbprint SHA-256:	9E0611728595A506CC2A55486FDD88ECA0971EF0B08F74CB3B3B6F5F6F3C7E27
Serial:	239664C12BAEB5A6D787912888051392

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x681b9	0x68200	False	0.62395192452	data	6.85141546298	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x6a000	0x23f8a	0x24000	False	0.641872829861	data	6.36645327435	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x8e000	0x1e3ac	0x7a00	False	0.527792008197	data	6.51367686644	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xad000	0x41028	0x41200	False	0.240744211852	data	5.36312234805	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xef000	0x4d50	0x4e00	False	0.730168269231	data	6.65913941378	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 10, 2021 07:28:11.163975954 CEST	192.168.2.4	8.8.8.8	0xa173	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 07:28:11.213056087 CEST	192.168.2.4	8.8.8.8	0xf9a7	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 07:28:11.255109072 CEST	192.168.2.4	8.8.8.8	0x35ab	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 07:28:22.515371084 CEST	192.168.2.4	8.8.8.8	0x1438	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 07:28:32.627718925 CEST	192.168.2.4	8.8.8.8	0x105	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 07:29:14.412585020 CEST	192.168.2.4	8.8.8.8	0x2194	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 07:29:14.453455925 CEST	192.168.2.4	8.8.8.8	0x24	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 07:29:14.488106012 CEST	192.168.2.4	8.8.8.8	0x17ae	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 10, 2021 07:28:11.196463108 CEST	8.8.8.8	192.168.2.4	0xa173	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:28:11.245542049 CEST	8.8.8.8	192.168.2.4	0xf9a7	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:28:11.283317089 CEST	8.8.8.8	192.168.2.4	0x35ab	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:28:22.552726030 CEST	8.8.8.8	192.168.2.4	0x1438	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:28:32.662878990 CEST	8.8.8.8	192.168.2.4	0x105	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:29:14.448110104 CEST	8.8.8.8	192.168.2.4	0x2194	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:29:14.481364012 CEST	8.8.8.8	192.168.2.4	0x24	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:29:14.512888908 CEST	8.8.8.8	192.168.2.4	0x17ae	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: VjLfUM5cMx.exe PID: 6120 Parent PID: 4984

General

Start time:	07:27:43
Start date:	10/09/2021
Path:	C:\Users\user\Desktop\VjLfUM5cMx.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\VjLfUM5cMx.exe'
Imagebase:	0x1000000
File size:	901960 bytes
MD5 hash:	C07D4F7DCAC497A3C06CBBA9E6E9E711
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.743054194.0000000003640000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.742911268.0000000003640000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.742353433.0000000003640000.00000004.00000040.sdmp, Author: Joe Security

- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.743093279.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.743313694.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.742958135.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.743290829.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.741931302.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.742268425.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.743331263.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.743266389.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.742496222.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.743239058.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.743391740.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.961646531.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.743211426.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.742430984.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.742097013.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.743177986.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.743353889.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.742801405.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.742634138.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.743003429.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.742749222.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.742570614.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.743401742.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.743138802.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.742692154.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.742188110.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.742014211.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.743370213.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.742861166.0000000003640000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.741849479.0000000003640000.00000004.00000040.sdmp, Author: Joe Security

Reputation:	low

File Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 2856 Parent PID: 800

General

Start time:	07:28:08
Start date:	10/09/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7cd730000
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 Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 6960 Parent PID: 2856

General

Start time:	07:28:09
Start date:	10/09/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2856 CREDAT:17410 /prefetch:2
Imagebase:	0xd90000
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 Show Windows behavior

Analysis Process: iexplore.exe PID: 1492 Parent PID: 800

General

Start time:	07:29:12
Start date:	10/09/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7cd730000
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 Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 3740 Parent PID: 1492

General

Start time:	07:29:13
Start date:	10/09/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1492 CREDAT:17410 /prefetch:2
Imagebase:	0xd90000
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 Show Windows behavior

Disassembly

Code Analysis