ID: 480998
Sample Name: nheQqfaVcS
Cookbook: default.jbs
Time: 07:26:28
Date: 10/09/2021
Version: 33.0.0 White Diamond

Table of Contents

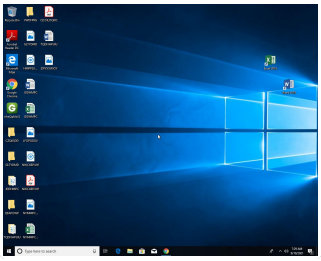
Windows Analysis Report nheQqfaVcS

Overview

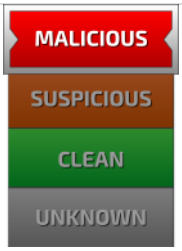
General Information

Sample Name:	nheQqfaVcS (renamed file extension from none to exe)
Analysis ID:	480998
MD5:	2926d2ff62efaa0…
SHA1:	dc5ebad8503139..
SHA256:	041d5d8edb6064..
Tags:	exe FORTHPROPERTYLTD
Infos:	

Most interesting Screenshot:



Detection



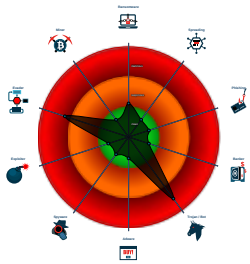
Ursnif Ursnif v3

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Ursnif
- Multi AV Scanner detection for subm…
- Detected unpacking (changes PE se…
- Multi AV Scanner detection for doma…
- 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…

Classification



Process Tree

- **System is w10x64**
- nheQqfaVcS.exe (PID: 6572 cmdline: 'C:\Users\user\Desktop\nheQqfaVcS.exe' MD5: 2926D2FF62EFAA0FBFDCC3FB7E77C6D2)
- iexplore.exe (PID: 6256 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6444 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6256 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 5720 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5888 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5720 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.313661419.00000000036D0000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000002.533943454.00000000036D0000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.313428934.00000000036D0000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.313350824.00000000036D0000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.312765827.00000000036D0000.00000004.00000040.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
0.2.nheQqfaVcS.exe.1000000.0.unpack	JoeSecurity_Ursnifv3	Yara detected Ursnif	Joe Security	
0.3.nheQqfaVcS.exe.ea9d7c.0.raw.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

Multi AV Scanner detection for domain / URL

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:

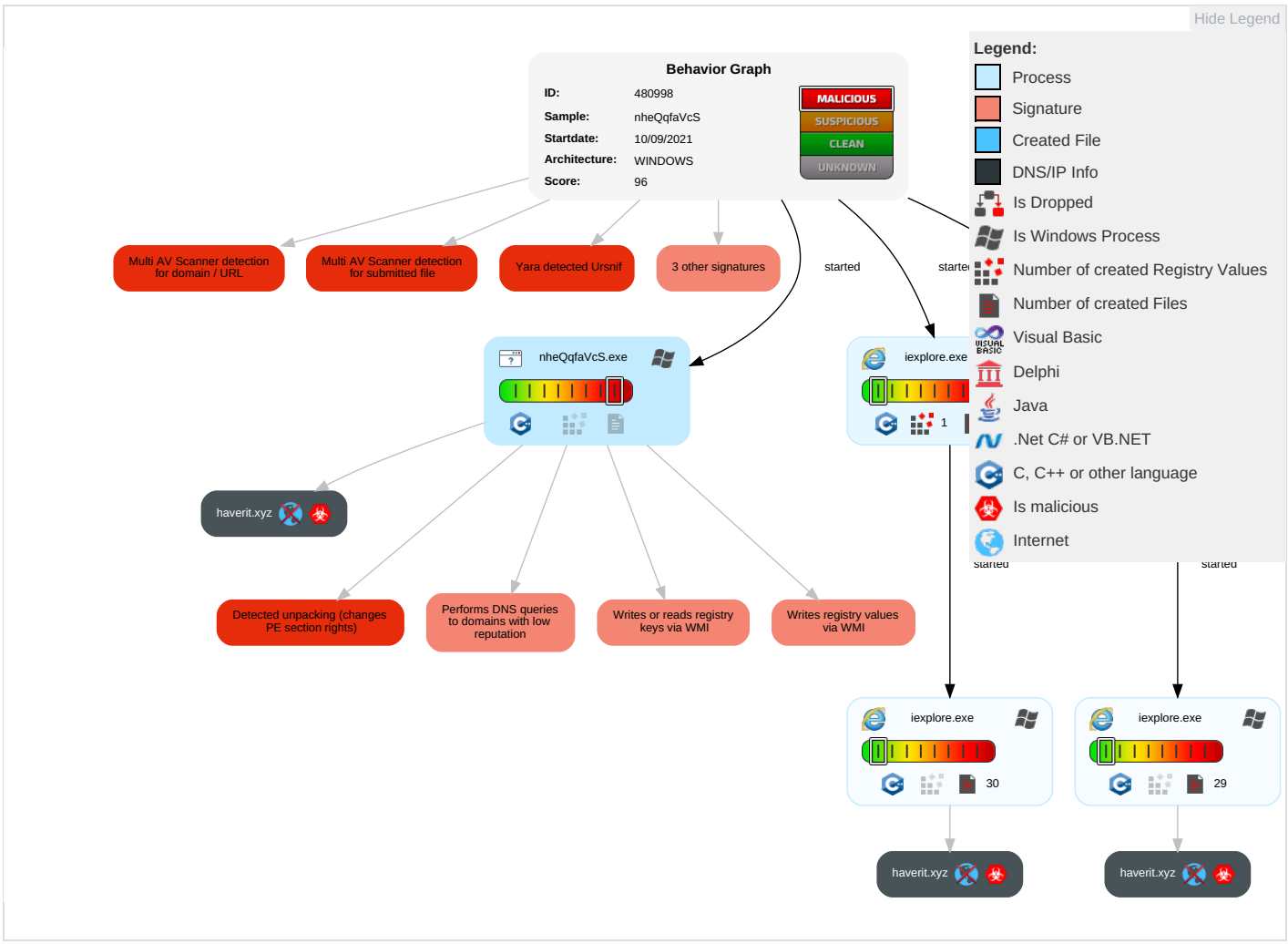
Yara detected Ursnif

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	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 1	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

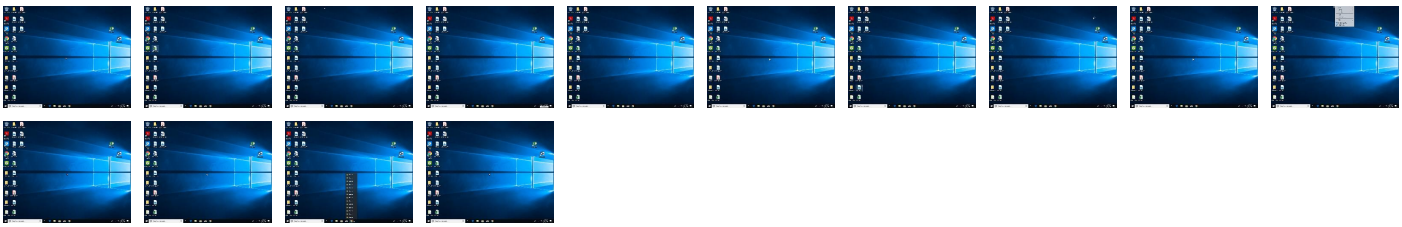
Behavior Graph



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
nheQqfaVcS.exe	19%	Virustotal		Browse
nheQqfaVcS.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.nheQqfaVcS.exe.1000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
0.3.nheQqfaVcS.exe.ea9d7c.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
haverit.xyz	6%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://haverit.xyz/index.htm	4%	Virustotal		Browse
http://https://haverit.xyz/index.htm	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://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	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	• 6%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	480998
Start date:	10.09.2021
Start time:	07:26:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	nheQqfaVcS (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:	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:	mal96.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
07:28:20	API Interceptor	2x Sleep call for process: nheQqfaVcS.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.{506886DB-1243-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.771427654928644
Encrypted:	false
SSDEEP:	96:rBZWZL2OBWO9tOFbfOsw3KMONfhziTqOnwMB:rBZWZL2OBWO9tOZfOshMOr9ODB
MD5:	E8166AD9C4D6191DD8C51030C263321E
SHA1:	61AD14E0A1D4BF14E711A26E241F5F060A40E8C3
SHA-256:	72336C9DED2DC7C99135FC983ABF3780D99B828FAA1FF57CB8065F91DA33A82A
SHA-512:	78642E04288D2E3AEA575EAE6439B8E456BC530724B50FA278753E2FF0039B0723BD65C9775C2C7E78D53A93F37A4E0211CB49609F499A920162396C5EC851BF
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.{7678AF55-1243-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{7678AF55-1243-11EC-90E5-ECF4BB570DC9}.dat	
Size (bytes):	29272
Entropy (8bit):	1.7678202020698055
Encrypted:	false
SSDEEP:	96:rAZ3Zj2xAWxutxebfxU2dKMxX1szbpqxe2MB:rAZ3Zj2xAWxutxOfxUlMx+0xcB
MD5:	7148254D4FADD6EDD26BC42BB795B2BB
SHA1:	5F8D1A30EF81D47F76BD2D9DF20D45A2C111D41C
SHA-256:	C5427B07D6C5EED675B24B4D78E6396059F3F3B7789E85C403D8171090E1EA89
SHA-512:	A784604EEF93D41E5C96ECC8EB05AEE70F27D8F03DB111EFE87CE501A9D96DB598A2BF59102BF6C8CABE7A8E8E0C7AD9F3CA1B7F5A8B05161D0008A60E75B572
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\{506886DD-1243-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26240
Entropy (8bit):	1.6577965569535396
Encrypted:	false
SSDEEP:	48:IwTGcprhGwpa9G4pQ1GrapbSpGQpBKGHHpcSTGUp8bGzYpm/jGopORyDGGqXpHRA:rpZ7Q/6lBSjjR2CWhM9kDVpA
MD5:	C892D13DD1CD1998B7477CFE1FCDC3C9
SHA1:	32C026788A88FCAC8F0B5A9C35ED93D84B599259
SHA-256:	60799FB8BC177347E5FDD2EA561AE534E71E9BE501346CB9F96C595CB03CC2B5
SHA-512:	3C4F587D9FA8BCBFE6DE40D5E8CCAA4C87ECB687FD4E595E5BB195087EDC8CB1D19F1A21A8FA265234DD6D3859C113666DD21D1521DB19DB84B688ADAD763A7
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\{7678AF57-1243-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26240
Entropy (8bit):	1.6594241652982409
Encrypted:	false
SSDEEP:	48:Iw5GcprsGwpaAG4pQIGrapbS3GQpBSGHHpcDTGUp8MxGzYpm8kyGopOayDHGqXpo:rfZEQg6WBSBjp2dWYMAkRVfA
MD5:	291690DBD83163CCA5FD3E0D02BB1F36
SHA1:	B95DF0F5F82CE3679FBD865D376FECE6100F0A10
SHA-256:	D208D5CDCC082B127052B55A8AF6DFA11A0CCD45D1C6E854099AC772108756ED
SHA-512:	3AD8EB543A7267A882D838D6896A7EA9D6A27D0E454A5260C3ECEBF6F3A8E5B807ED5553B7A36F95004B87F996284E2F6EDB791F349D2D3A49F37ECE1B83E1C0
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):	657
Entropy (8bit):	5.113905124514613
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEMaraMnWimI002EtM3MHdNMNxOEMaraMnWimI00ONVbkEtMb:2d6NxOA2MSZHKd6NxOA2MSZ7Qb
MD5:	7012472634EB96820B6EEC294FFA2AB2
SHA1:	46B70A08F8F0B7C210D7E2016C79505166019066

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
SHA-256:	C5EC7B30B03613C6450AA1953B7F13B82163B3CDEF0ADD1D83D771346BCA0F24
SHA-512:	B55B9BCE216DE90290FDA211C0F561C7BA5EE5403E93C473003DCCA84728BA82F8C3956D67894CB1C71805E1CD79DC314929C1CF0E68019A20E955941BED76E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x26189557,0x01d7a650</date><accdate>0x26189557,0x01d7a650</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>0x26189557,0x01d7a650</date><accdate>0x26189557,0x01d7a650</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):	654
Entropy (8bit):	5.126785934700775
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kMugougHnWimI002EtM3MHdNMNxe2kMugougHnWimI00ONkak6EtMb:2d6NxrgSZHKd6NxrgSZ72a7b
MD5:	036A6E3282047CFBD313BC951C0FDCC6
SHA1:	FACC78394DC05D4584A2C59D45409D28C0EC2528
SHA-256:	C87DB800F390409FF72B1C096495CAFF04E708187F7646559CE7BF2D882C5DAD
SHA-512:	1C1F7F565131612E1B0DB5B6ABF19676756BAAAA1C34E2F483AAF0607185D39735B6B44814C4B4D2D5F7D3E2656E66CC3898651A812D6277AC72E6DC44B4D02
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x260a44b2,0x01d7a650</date><accdate>0x260a44b2,0x01d7a650</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>0x260a44b2,0x01d7a650</date><accdate>0x260a44b2,0x01d7a650</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):	663
Entropy (8bit):	5.132943576775603
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLMaraMnWimI002EtM3MHdNMNxvLMaraMnWimI00ONmZEtMb:2d6Nxv12MSZHKd6Nxv12MSZ7Ub
MD5:	0810F0747527C354F4C7B878EC6C037D
SHA1:	0CE70619C66F00ED1A5FD6B7421358B9CABC4E13
SHA-256:	F97424B8D542DAA2736F2142CBC911B99AE4D09A3B382D336831F9110CAC8D80
SHA-512:	58102F88EACDF34CBF1F04A782BC60DA0DDEEE3AE7FE73F668435FD5D2B314BF21EB0E9BBDE3AFADC1B75FBB58692CBB585BD3E58061655A10E35178FED7C9EF
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x26189557,0x01d7a650</date><accdate>0x26189557,0x01d7a650</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>0x26189557,0x01d7a650</date><accdate>0x26189557,0x01d7a650</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):	648
Entropy (8bit):	5.123568335705859
Encrypted:	false
SSDEEP:	12:TMHdNMNxiMrMnWimI002EtM3MHdNMNxiMrMnWimI00ONd5EtMb:2d6Nx8SZHKd6Nx8SZ7njb
MD5:	5DA483F61304960D0F776FB1C0AC546E
SHA1:	F6FB15F9FE4A2B2CECAE1219CDCC214002C36E03
SHA-256:	1770B45C0925C77FCB065FB7D79A3D7DCC249F395EFFB214E6EE1583DE63B7B8
SHA-512:	BB0D0B8F4F43AE2878DDA27B7D4653794645B10B9437C11061C77F759B2D085AEF1075627BB8E250128E3CEAFB2870929C478B17750CF13220FC4A890D971F36
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x26116b42,0x01d7a650</date><acc date>0x26116b42,0x01d7a650</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>0x26116b42,0x01d7a650</date><accdate>0x26116 b42,0x01d7a650</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):	657
Entropy (8bit):	5.1481543684655335
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwMaraMnWimI002EtM3MHdNMNxhGwMaraMnWimI00ON8K075EtMb:2d6NxQc2MSZHKd6NxQc2MSZ7uKajb
MD5:	5E414D55D9C5C113853E0245A19215C1
SHA1:	C4EF265F1D3977769CBC094CCE02FD5DEDE6545D
SHA-256:	7B41E8602389BE61D50ADAC69C387146B3C29F2D34BEA8999D0CC5F40F35E88D
SHA-512:	3364A941E12C6D76EE67BBB4223ED009129D6A89794F2D39C9F3CB79A2E9FD049989A781F04307955ED51D3D128253A87012E40DC77EB848E7C3183C4D4E0E42
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x26189557,0x01d7a650</date>< accdate>0x26189557,0x01d7a650</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>0x26189557,0x01d7a650</date><accdate>0 x26189557,0x01d7a650</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):	654
Entropy (8bit):	5.112015487709611
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nMrMnWimI002EtM3MHdNMNx0nMrMnWimI00ONxEtMb:2d6Nx0bSZHKd6Nx0bSZ7Vb
MD5:	5DB865CF1E6A450A7E3E42EB09234DC4
SHA1:	0D6EA71BF5715A483214C89E8E1FD8514ACFAD46
SHA-256:	C2DCB2A500F9235E55C2750262BC304FC7454304A466F44DE6BC219C88DA38B4
SHA-512:	92E6885A9DF1131578F120C997E3C583D4AF54DE78614C4E92E930F0158565E7E6617196319B272B99B518484495C5BEC38FF86ADDB7750FFB0D4913BB5F8E0F
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x26116b42,0x01d7a650</date><a ccdate>0x26116b42,0x01d7a650</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>0x26116b42,0x01d7a650</date><accdate>0x2 6116b42,0x01d7a650</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	657
Entropy (8bit):	5.147778589604081
Encrypted:	false
SSDEEP:	12:TMHdNMNxxMrMnWimI002EtM3MHdNMNxxMrMnWimI00ON6Kq5EtMb:2d6NxtSZHKd6NxtSZ7ub
MD5:	B1BB196FF5EDF1BC272963AB21FCABB5
SHA1:	6B5D418C755223D69CF07CF4362C6F7DD01187E3
SHA-256:	BC5CCB9E63BC889CE68A41461AAF3AD5A90FC3DE632F3405C3FCCC9DE605DB75
SHA-512:	DF824DE32328A196D51A4CE489F19D175930751EA153C71C8C23740EFF46F4032ABEBD209AB66E030628FE287F0DBCB464722101E6B41EF48007698B9B82CA8E
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x26116b42,0x01d7a650</date>< accdate>0x26116b42,0x01d7a650</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>0x26116b42,0x01d7a650</date><accdate>0 x26116b42,0x01d7a650</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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Category:	dropped
Size (bytes):	660
Entropy (8bit):	5.124275386432658
Encrypted:	false
SSDEEP:	12:TMHdNMNxcMrMnWimI002EtM3MHdNMNxcMrMnWimI00ONVEtMb:2d6Nx+SZHKd6Nx+SZ71b
MD5:	6E42AC1028D8AB88EFB8CAA36B282D89
SHA1:	688B731F70840DFD8EC1464B1F7829DDD3675D49
SHA-256:	6541E1956991734ED55917912A40D64DDFAD6607440705CBA4E8DDD95780B7CF
SHA-512:	AFD585A1BDD6224744BF41D43B0918B847A02905623D6AE95DABAA0185527B9254F7974BE6F706D17A8001B291E4E59909CADB913957E5B7195DCC33BD8041E/
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x26116b42,0x01d7a650</date><accdate>0x26116b42,0x01d7a650</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>0x26116b42,0x01d7a650</date><accdate>0x26116b42,0x01d7a650</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):	654
Entropy (8bit):	5.1087139086941935
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnMrMnWimI002EtM3MHdNMNxfnMrMnWimI00ONe5EtMb:2d6NxDSZHKd6NxDSZ7Ejb
MD5:	B130923143DF009BD3DBE0EB65452958
SHA1:	4794E0BA69ABBFC18985B69796F925B384939EFA
SHA-256:	5F6E2870EEE5B52FA68DE47B4C15F5B30F060F064313ED9854748BD44FAAC1AD
SHA-512:	5713FCE4DC67B3F526CC8850E55F1BF00161BB96C20EEC63254B2043C19839FEB3DFE818AAEA9D80D91AA9DF7552DF35F712936137CAFF5B0F2B78C929250D1
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x26116b42,0x01d7a650</date><accdate>0x26116b42,0x01d7a650</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>0x26116b42,0x01d7a650</date><accdate>0x26116b42,0x01d7a650</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\4PB7FJMT\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:vlIJ6G7Ao8Ra
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\4PB7FJMT\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\errorPageStrings[1]	
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\4PB7FJMT\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.su bstring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var pound Index = 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\NUEPGTR9\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\NUEPGTR9\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\httpErrorPagesScripts[1]	
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\PEJLKQA8\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: #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\PEJLKQA8\NewErrorPageTemplate[2]	
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: #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\PEJLKQA8\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\dnserror[1]	
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\PEJLKQA8\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..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....#+....l..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\PEJLKQA8\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\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):	4.224587757977836
Encrypted:	false
SSDEEP:	3:oVXUpjGrpEH8JOGXnEpjGrU7n:o9Up2p4qEp2g
MD5:	03064E3244A4514F8AA241D46356725E
SHA1:	A7EB233C8F4C96653926FBB83A75850023AADEC4
SHA-256:	46B83B9473554CD475F07746945F6E70B2F892E581BD04354024B0050F32E359
SHA-512:	360B1BF6340283B8EF4D99A9E388CEADC24C27CF2C26B53D04070A97AA1CB464AFF958F5F394532E7B84089E7B3E3F5AE44CA385D895C24DE97F662870937FA
Malicious:	false
Preview:	[2021/09/10 07:29:12.207] Latest deploy version: ..[2021/09/10 07:29:12.207] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF04D35234F04DF89A.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38737

C:\Users\user\AppData\Local\Temp\~DF04D35234F04DF89A.TMP	
Entropy (8bit):	0.37172545806157037
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+tzxQ8I8wayDZayDbayDU:kBqoxKAuvScS+tzxQTbLpa
MD5:	B1843149433FC41DF0EFE9263ED154F7
SHA1:	4316C4FB4DB1846095CA848A325571CADE049A5D
SHA-256:	3822E398E5C6FB036F326BC322DE411C4A4A330BFAE0B7C52490F4A9C55A8C46
SHA-512:	B6CB2620D3D5120A0BE2336E07AB9E62D6F0BBCB92677731AF360400C80E53750E24A7897D154A52C435ACFAC44F43E45E8F2E3ABF7A773375BC47BE1DB1036D
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF165B26F914703F17.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38737
Entropy (8bit):	0.37049313974713743
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+2wqD/I/wRyDZRyDbRyDU:kBqoxKAuvScS+2wqDwIwqX
MD5:	2C7140FAB24D2288CC34CC904663D3EF
SHA1:	4A7C0F021D2B0442BFE31BF1505DAFB109366005
SHA-256:	8C0486AF2E2FCB5AE3E0CCC853BE52C25F361376541027BE62E0455BDD485DCC
SHA-512:	899E67BAC8F5749CA9312E3BBC24F2EF44B327E098984870FB3D93F4FB295FC851D76360C45906723B3563DADF8683D365355A2FF27C8CF8E492737D3281C944
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF65FC542F93EC8AEB.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4092348646167777
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loET9loET9lWECM/PDy/O7nE:kBqoljVx5
MD5:	F3FB9D4A2F87340D0E3B8FB18F3B2922
SHA1:	F039854E0419799C7653095805BF099BE1B22E89
SHA-256:	D69CC8BF9FEA5B6A2FD2333303DBAE774E3DCBEB9E21325FA3B050339375B93E
SHA-512:	A5123B626E879D8100140439AC0BB7CC50B384BC6BC21C956BAD8E6D48F7FD66464B5420CF488A58E0D76F3A5D0076AA4B6F3B495A5E0B27310C5FE5A38EBF04
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFCDB1AD29A328B9E8.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.40841972555186656
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fRj9l8fRj9lTqOZOeq:c9lLh9lLh9lIn9lIn9loj9loj9lWOZ6
MD5:	1819126BFFACD56CF744DB7D42C47680
SHA1:	010E551B291C05657DBCBFA833109E2102DFF41A
SHA-256:	C0DE1F200170DFA47C1C87589CAB0B63BF7A82A5AFEC9BE3A1425E7714B95539
SHA-512:	843E114EFD05E6BB6D3A7655DF38A16CEB4B345A4CF293439664F1A11EBAA98F4B75287040EF514A3104DDF34E93824D196BE60FFAA85D4C82E4F31F93664EC
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DFCDB1AD29A328B9E8.TMP	
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):	6.614401628444266
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:	nheQqfaVcS.exe
File size:	901960
MD5:	2926d2ff62efaa0fbfdcc3fb7e77c6d2
SHA1:	dc5ebad8503139f8ce84927fda0ec9adb5b77200
SHA256:	041d5d8edb606415cdcb6670b69ed4b2a2d80a8eb3e4dc 75f0a9b2d558bedf60
SHA512:	1c122a0a63f010e55765f32c0495611c48eec7f7f076a36 44e4ddc37763b5c6984e3ef62cf27f3e2b771b8b3a4917e 998a88e1ec94e679cdc891e490cc20ec07
SSDEEP:	24576:g9PsA9vHAYobFGQdRHylSk61LXXhtxvZPmtk1/ GqgLG4:NYKJk61bRrZPmWGG4
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.......Zm.f...5. ..5...5..r5...5..w5...5..v5...5...5...5.{.5...5..t5...5..v5...5..j5- ..5..p5...5..u5...5Rich...5......................

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:	6e09f5ea9222053b840f418fc7379964

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	• 4/12/2021 5:00:00 PM 4/13/2022 4:59:59 PM
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	0.623954269208	data	6.85141828955	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x6a000	0x23f8a	0x24000	False	0.64170328776	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 07:28:09.204570055 CEST	192.168.2.5	8.8.8.8	0x8102	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 07:28:09.247970104 CEST	192.168.2.5	8.8.8.8	0x3467	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 07:28:09.286760092 CEST	192.168.2.5	8.8.8.8	0xd1fe	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 07:28:20.653501987 CEST	192.168.2.5	8.8.8.8	0xcc39	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 10, 2021 07:28:30.802565098 CEST	192.168.2.5	8.8.8.8	0x2628	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 07:29:12.638621092 CEST	192.168.2.5	8.8.8.8	0x3cc1	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 07:29:12.688169003 CEST	192.168.2.5	8.8.8.8	0xf6a9	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 07:29:12.749125004 CEST	192.168.2.5	8.8.8.8	0x4222	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 07:28:09.240426064 CEST	8.8.8.8	192.168.2.5	0x8102	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:28:09.274013996 CEST	8.8.8.8	192.168.2.5	0x3467	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:28:09.311476946 CEST	8.8.8.8	192.168.2.5	0xd1fe	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:28:20.687736034 CEST	8.8.8.8	192.168.2.5	0xcc39	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:28:30.835525990 CEST	8.8.8.8	192.168.2.5	0x2628	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:29:12.675548077 CEST	8.8.8.8	192.168.2.5	0x3cc1	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:29:12.725872040 CEST	8.8.8.8	192.168.2.5	0xf6a9	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:29:12.782552004 CEST	8.8.8.8	192.168.2.5	0x4222	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: nheQqfaVcS.exe PID: 6572 Parent PID: 5380

General

Start time:	07:27:39
Start date:	10/09/2021
Path:	C:\Users\user\Desktop\nheQqfaVcS.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\nheQqfaVcS.exe'
Imagebase:	0x1000000
File size:	901960 bytes
MD5 hash:	2926D2FF62EFAA0FBFDCC3FB7E77C6D2

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: 00000000.00000003.313661419.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.533943454.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.313428934.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.313350824.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.312765827.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.313524102.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.313391092.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.313620745.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.313575015.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.312402940.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.313494038.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.313143533.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.313289878.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.313551158.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.313087674.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.312317005.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.313243229.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.312902480.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.311981135.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.313033304.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.313650621.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.313636918.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.312584205.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.313461705.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.312495587.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.313193145.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.312229401.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.312975464.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.312836081.00000000036D0000.00000004.00000040.sdmp, Author:

	Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.312674731.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.313595976.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.312150380.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.312065477.00000000036D0000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 6256 Parent PID: 792

General

Start time:	07:28:07
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:	0x7ff640a80000
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: 6444 Parent PID: 6256

General

Start time:	07:28:07
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:6256 CREDAT:17410 /prefetch:2
Imagebase:	0xaa0000
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: 5720 Parent PID: 792

General

Start time:	07:29:10
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:	0x7ff640a80000
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: 5888 Parent PID: 5720

General

Start time:	07:29:11
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:5720 CREDAT:17410 /prefetch:2
Imagebase:	0xaa0000
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