ID: 480999
Sample Name: p47bG25tTf
Cookbook: default.jbs
Time: 07:26:31
Date: 10/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Windows Analysis Report p47bG25tTf

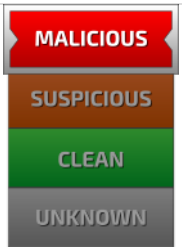
Overview

General Information

Sample Name:	p47bG25tTf (renamed file extension from none to exe)
Analysis ID:	480999
MD5:	d0cb3af3f2f9bbb…
SHA1:	3a1006610fc6e98.
SHA256:	31f5ee68e7548cd.
Tags:	exe FORTHPROPERTYLTD
Infos:	

Most interesting Screenshot:

Detection



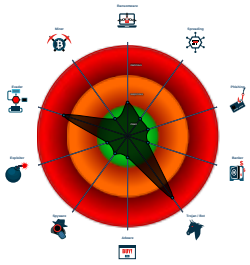
Ursnif Ursnif v3

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

Classification



- **System is w10x64**
- p47bG25tTf.exe (PID: 6576 cmdline: 'C:\Users\user\Desktop\p47bG25tTf.exe' MD5: D0CB3AF3F2F9BBB89FABA16F41585E7C)
- iexplore.exe (PID: 5348 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5388 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5348 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 2584 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4060 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2584 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.631812823.0000000003750000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.411680498.0000000003750000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.412285957.0000000003750000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.411095451.0000000003750000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.412774183.0000000003750000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 29 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.p47bG25tTf.exe.1000000.0.unpack	JoeSecurity_Ursnifv3	Yara detected Ursnif	Joe Security	
0.3.p47bG25tTf.exe.db9d7c.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:

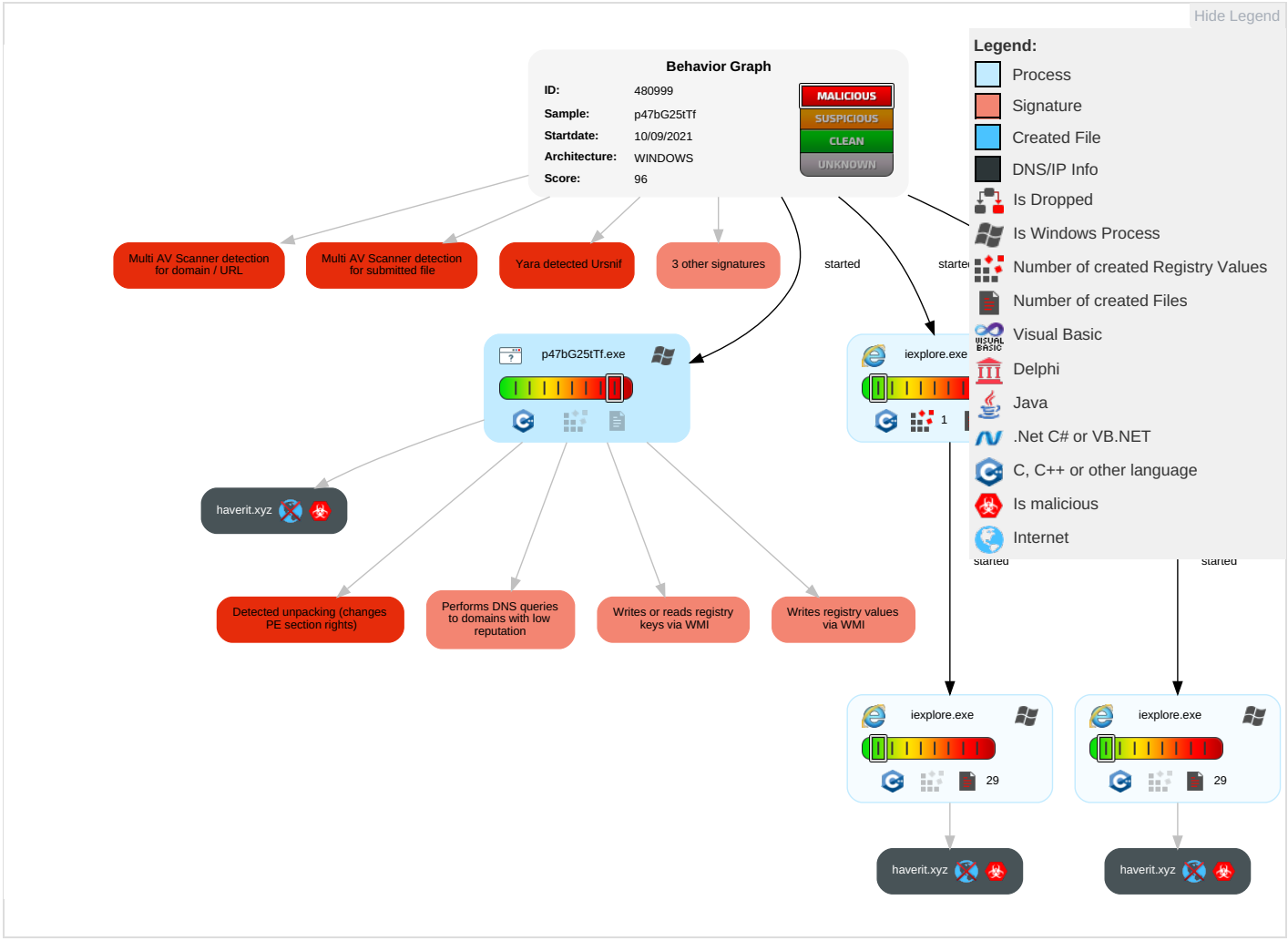
Yara detected Ursnif

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

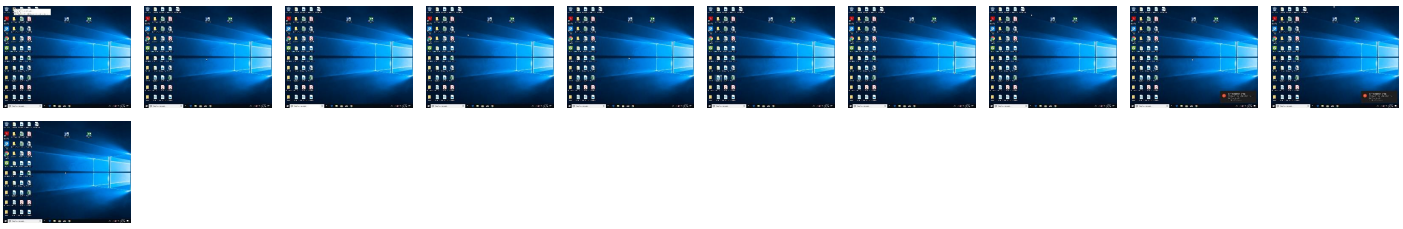
Behavior Graph



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
p47bG25tTf.exe	15%	Virustotal		Browse
p47bG25tTf.exe	18%	ReversingLabs	Win32.Infostealer.Gozi	
p47bG25tTf.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.3.p47bG25tTf.exe.db9d7c.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.p47bG25tTf.exe.1000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		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:	480999
Start date:	10.09.2021
Start time:	07:26:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	p47bG25tTf (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:	25
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
07:28:28	API Interceptor	2x Sleep call for process: p47bG25tTf.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.{54E1EBED-1243-11EC-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.769301021732044
Encrypted:	false
SSDEEP:	96:r9ZmZo/2oFWovtopnAfoiYnMn1Mo8n0nrnIDnEnToUnnnDB:r9ZmZW2kWyt3fNlMdylB
MD5:	32F915F644D0303AD4FF52854EDAC775
SHA1:	8CC5C68DAC1423ED28DDC612A192F38D68A43D47
SHA-256:	8A54441EA01342A6700F45E981FC505A9650BCEFF2DDEED9A30D131599F94544
SHA-512:	D52F74B71D730F2874FDD6CB41F7E7AA37CF6345600656D7C32C89430B15F083C15690EF97040475D682B08FAD658465EC60680114DAD9598E4D90BCFE0188B7
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.{7B4B21B1-1243-11EC-90E5-ECF4BB2D2496}.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.{7B4B21B1-1243-11EC-90E5-ECF4BB2D2496}.dat	
Size (bytes):	29272
Entropy (8bit):	1.764398028666985
Encrypted:	false
SSDEEP:	96:rbZoZU2hrWhBthBAfhROy1MhVqfIL6Th0dDB:rbZoZU2hrWhBthSfhRhMhrkhSB
MD5:	DECDC9404C44D35851F7DF1F6DEAF5CD
SHA1:	F557C8E3E26C47AE01F3A8CB1DC5DD95F8730AF7
SHA-256:	BE7BA463E72FA89F211B9C25E8302E278C541D637446F65F1113F0FA0A0AA3E6
SHA-512:	E09670998AA40F1AC8D311F4191333C483B9A6B20D7B36EC4F9A5142989CA13AF165CA4D0834E813F0B4B97B07A3D62D632019545AEEDEB5B6C3808B62198B0E
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\{54E1EBEF-1243-11EC-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26240
Entropy (8bit):	1.659600944701321
Encrypted:	false
SSDEEP:	48:IwvGcprjGwpaHG4pQTGrapbSxAGQpBqGHHpcTTGUp8jGzYpmn7GopOByD7GqXpHr:rlZ9Qp63BS+jx2tW5MdkQVoA
MD5:	4071FCD40650175D24DD5998725A6FFF
SHA1:	159412F8607724683B8DBAF4B57AE3F669A405E0
SHA-256:	11D7FAF519AE6FA4463D0FC79FE2C3745BD061395D588CEF77BDEE0C57BB50F8
SHA-512:	18B5AABF8058687B8EB6215B550E993CC6289B8F2D0562881421364242D4CEA9D11951D098EFF4A0E65E110012A402C371976F7CFFDEA461ACBAC1988ED5E55
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\{7B4B21B3-1243-11EC-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26240
Entropy (8bit):	1.6596269041483662
Encrypted:	false
SSDEEP:	48:Iw5GcprRGwpaRG4pQVGrapbSKGQpBeGHHpcETGUp8kGzYpmGxGopOgyD8GqXpHg7:rfZLQD6FBSyjt28WAMEkiVpA
MD5:	2FFE83F0271D9386F3A78653738CB2EA
SHA1:	A0760867AF5D35E5CCB87A642E00FBC30EE3079E
SHA-256:	ADB941AEB59FBEEE861F3403FB29AF6D7081B1D0FF261EF4AB2AF2C019B915D2
SHA-512:	0CBEFC835AF6BAC9C70C2ED9994F616517CC3D8BD17AEF3BFA51B41E0717532AA11EF5ECC659F0A9F316EFBF44E67BDE582075874905DCC8474C99F9F9658F5
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):	659
Entropy (8bit):	5.063499204381996
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEpjhnWimI002EtM3MHdNMNxOEpjhnWimI00OVbVbkEtMb:2d6NxO6jhSZHKd6NxO6jhSZ7V6b
MD5:	CBC2DB9A877E0D7C64FEDF2FECB7E10C
SHA1:	AAFA7ACE14E0D8723D5487F00A0B6B66228DB2BF
SHA-256:	D22CFBDD19DCD996BFD62221786F4174525A6AEB1949A4653035A9FD5B928502

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
SHA-512:	92003F61828D5ECA7896ECC1AD1C91014B7DF7FE06C56147349C843717DF0229F0A093F45087E80C15ECD70C13EEA8EF93AE205694B1384A73DCE516EDE2008
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x2aa299ee,0x01d7a650</date><accdate>0x2aa299ee,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>0x2aa299ee,0x01d7a650</date><accdate>0x2aa299ee,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):	656
Entropy (8bit):	5.117776941839032
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2ktnWimI002EtM3MHdNMNxe2ktnWimI00OVbkak6EtMb:2d6NxrsSZHKd6NxrsSZ7VAa7b
MD5:	D8636A8BAF043132CD3993B8447AC27C
SHA1:	B2859A643B39A88894AF321BAD5ED5C525C25B4B
SHA-256:	FF5955446C17EF457442CD561F3228A67107215A955D654AD7DDD17488A68347
SHA-512:	DA6D5DC9D104FBB5E6C3117FD7829615A380BF26F8E111AB27179D192AFFF63C89E4A0A3AC10AA849B1E42D5BF6DD91ADBB2023E817E7704B68C8B2339E77FA
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x2a9b72c5,0x01d7a650</date><accdate>0x2a9b72c5,0x01d7a650</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>0x2a9b72c5,0x01d7a650</date><accdate>0x2a9b72c5,0x01d7a650</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):	665
Entropy (8bit):	5.072324302275548
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLiIdnWimI002EtM3MHdNMNxvLiIdnWimI00OVbmZEtMb:2d6Nxv+IdSZHKd6Nxv+IdSZ7Vmb
MD5:	17CDBF7D4E0179CA4AFB71EBEC2671F9
SHA1:	18CFF5A64AAAA9AD1CB422EA9387FE326115BB86
SHA-256:	797443ED0C8E86E29597EE7F7DC5AC59900D93C8915EC1F850DDED065522904B
SHA-512:	CB84CD42AAC8F11A50AB9C56D46BE3227AAA7BA26E7DC000571F2E3F7DDBA73EDD98E5E895621CD0A2C1DA2D579C0DF01563DBBE1205DD9929A03F04D1245225
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x2aaa0d44,0x01d7a650</date><accdate>0x2aaa0d44,0x01d7a650</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>0x2aaa0d44,0x01d7a650</date><accdate>0x2aaa0d44,0x01d7a650</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):	650
Entropy (8bit):	5.078666709638152
Encrypted:	false
SSDEEP:	12:TMHdNMNxipjhnWimI002EtM3MHdNMNxipjhnWimI00OVbd5EtMb:2d6NxEjhSZHKd6NxEjhSZ7VJjb
MD5:	BA48D6130DEEDF0227A354C4FAAB69A9
SHA1:	C2368AD50B729A583EFA505C871B742B6FB24778
SHA-256:	4904567132105BB5B50ABEA614EABDF44D10FCF7D51D42669995B81619AC3F67
SHA-512:	7E87846F0E1EEDAE67B55E7A709C00F0963D20BA3CBDECF7306BA095F096170390754F77DBE26130C544DE70D2DF5B957EE6ABFCD76D66637D79C13F2991F48
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>0x2aa299ee,0x01d7a650</date><acc date>0x2aa299ee,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>0x2aa299ee,0x01d7a650</date><accdate>0x2aa299ee,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):	659
Entropy (8bit):	5.090906642763367
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwIdnWimI002EtM3MHdNMNxhGwIdnWimI00OVb8K075EtMb:2d6NxQ/IdSZHKd6NxQ/IdSZ7VYKajb
MD5:	1C9D261E74E0E31B53A779040773103F
SHA1:	22AC19A7151E5D2E4E77EA2DE137E5A26ED63B69
SHA-256:	C36B97B0D3FC6134410DB9A66D273B0623C0C9AC747B6692E7A40022679357DA
SHA-512:	5CC9292B535C3E69B029D1A3480BE51F6D7CA82B40FF2D39E85B8D4EB9534009240FFC752374E8879EA90EE32C990488EC454B391F4895279DA6D532A517775F
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x2aaa0d44,0x01d7a650</date><accdate>0x2aaa0d44,0x01d7a650</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>0x2aaa0d44,0x01d7a650</date><accdate>0x2aaa0d44,0x01d7a650</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):	656
Entropy (8bit):	5.067166553129904
Encrypted:	false
SSDEEP:	12:TMHdNMNx0npjhnWimI002EtM3MHdNMNx0npjhnWimI00OVbxEtMb:2d6Nx0pjhSZHKd6Nx0pjhSZ7Vnb
MD5:	DFF76B7B695CDD42F920EB8619B8F0D1
SHA1:	B60BF03B2B24834A3F8AAB67AC8BC72751593F3B
SHA-256:	0648EEF317FF46AE29DAB7B62F4800B8FBF8779FEF61A631EBA42C3B77530961
SHA-512:	843EC3C6E2DA14151AE1286DB0FEC62D06746DDDF8612DB5E5C81799031977C9D164DB6E34370E560F376233DF94287A9210CFCBAFB4BD0A22BF04A6671340D
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x2aa299ee,0x01d7a650</date><accdate>0x2aa299ee,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>0x2aa299ee,0x01d7a650</date><accdate>0x2aa299ee,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):	659
Entropy (8bit):	5.103300306344195
Encrypted:	false
SSDEEP:	12:TMHdNMNxxpjhnWimI002EtM3MHdNMNxxpjhnWimI00OVb6Kq5EtMb:2d6Nx3jhSZHKd6Nx3jhSZ7Vob
MD5:	367253BEC154A52D863DAFDB0782AE08
SHA1:	46E0E37E012794458E8944FD1368CDF2C3A04409
SHA-256:	B70893BDF4156FC4CD010110B8F6AA0F20F34651A645C63B61C7C7B751EF8753
SHA-512:	91E5B62D362E8E3C0B983E0F42DADEA90D4CC32E725922057B7DDE9178A8E125B15BB73C5BFE737F90D806188835E24ABF07D7FF440FFD87FB3356D1210147F
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x2aa299ee,0x01d7a650</date><accdate>0x2aa299ee,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>0x2aa299ee,0x01d7a650</date><accdate>0x2aa299ee,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):	662
Entropy (8bit):	5.10803413076142
Encrypted:	false
SSDEEP:	12:TMHdNMNxctnWimI002EtM3MHdNMNxctnWimI00OVbVEtMb:2d6Nx0SZHKd6Nx0SZ7VDb
MD5:	ECCDFAE90D63FBF7231A68FE2FE4F8CB
SHA1:	BA789C2EA29A90550B41AEF00314BD6DBE7B8E43
SHA-256:	8376C2D3BB4968F8DF6B9E8FC601AEF3B63348529F8B329AEDFEC640C70D4FE4
SHA-512:	3FEC1745EC49A3637A10DF1ED6B94E258F020C4D2BB0D74168B67E091F8B8D936782DB66D643DDB801B47385DBDFAB967761D5B20E6750D0B256870E2D1D690E
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x2a9b72c5,0x01d7a650</date><accdate>0x2a9b72c5,0x01d7a650</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>0x2a9b72c5,0x01d7a650</date><accdate>0x2a9b72c5,0x01d7a650</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):	656
Entropy (8bit):	5.0931945398264675
Encrypted:	false
SSDEEP:	12:TMHdNMNxfntnWimI002EtM3MHdNMNxfntnWimI00OVbe5EtMb:2d6Nx1SZHKd6Nx1SZ7Vijb
MD5:	38E9D1EA4A6D6DDE4FC0979F4D869994
SHA1:	6FD7424F9F9A0A3A751EF341DE4F0E1C36A11139
SHA-256:	6C41EAA479E65C789C3E1A682BB87E41786D2253AA597B4D6EE230D6659E3F13
SHA-512:	C608F9EDC1FE4F8BE473F383B9AEE99EC4797BD4A90293BC1AC06C4C10672066C04FFDBF4DDA0788696860A26BDC70089CDEEC738AD46690251A739EB422C2E
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x2a9b72c5,0x01d7a650</date><accdate>0x2a9b72c5,0x01d7a650</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>0x2a9b72c5,0x01d7a650</date><accdate>0x2a9b72c5,0x01d7a650</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\3Y2ADQKS\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\3Y2ADQKS\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\down[1]	
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\3Y2ADQKS\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\9QTQHWWN\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\9QTQHWWN\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\9QTQHWWN\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\9QTQHWWN\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....#+....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\9QTQHWWN\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\G62TDH9B\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:	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\OTUW0Q90\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\OTUW0Q90\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\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):	4.393346746839115
Encrypted:	false
SSDEEP:	3:oVXUpj1UER98JOGXnEpj1p7n:o9UpJ9qEpH7
MD5:	A2B7AD8390CE4353328431196B7C7E67
SHA1:	787E491F5EEE64CDDB1F9A46403D4D57571E8FAC
SHA-256:	E9F8316B380EFB562E124FC3CEED78F7DC6C37DE52E9F42110A906FF0EC46D8E
SHA-512:	698D2EE9310C76E4F2145C9916C656BD7237ADDFAA3231B1CE31AD9CD1D952B5F67637F888D3A5283C0EDB3F43618DDB6E8F8660D88DB6603540CB94CC5F69B
Malicious:	false
Preview:	[2021/09/10 07:29:20.886] Latest deploy version: ..[2021/09/10 07:29:20.886] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF173DAD1FEFCCC031.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38737
Entropy (8bit):	0.37131414924692396
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+eYSbnInwByDZByDbByDU:kBqoxKAuvScS+eYSbIwg6n
MD5:	85A96C33A4D0D986D4695979A2893E2B
SHA1:	ADB7EF717CA0B73338A3E5CE3FF01FCB2BD59A8B

C:\Users\user\AppData\Local\Temp\~DF173DAD1FEFCCC031.TMP

SHA-256:	AA21F1D72887F021E816F98EE6DB74296226819752D3F6A7A39565883558DF09
SHA-512:	2A5C89DE9A657CB292D69ACC05A0E885B27ACE1BFED6FBE58617AF2297EF0767C437D84B3EBE70EB08C47699A7E4A122841454EF6445E13D4D996EC86A9822 A
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF29513E450399A0E6.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38737
Entropy (8bit):	0.37144306557840784
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+357yGIGwgyDZgyDbgyDU:kBqoxKAuvScS+357yZBhzM
MD5:	B27950A47D3C84FA6E074FCBE1936C1A
SHA1:	2D764B05EC5F6FA90D85E664A468D994D3AA9789
SHA-256:	CF25D8F1611843D169DE538A0B3D9E82DA2FFBF6C6F90BE7C5D519228076E209
SHA-512:	DC64C7AB4DD00FD2AF9A6E6FDAFEF29F0B6BFAC5B338A58B645E35B3CE738B9AF487E2D978A9FD20641BD56D69D1BCADDEAE842C08E569B90D20B6DC5450 E2B5
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF904617D6CF584C8C.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4070458951298893
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loU9lok9lWhJ9kfS1:kBqoIfphrb1
MD5:	2EBD710925DF5B3DFE76C07D8F0DE84F
SHA1:	16977BBE653EC66C3D7BCB546214DC1DD1EBA0AA
SHA-256:	7EDE8C824769552CE616FE3A0DDA3271FF9770D38BBC79AFE9F3D806F8161A03
SHA-512:	3572973D135472311CDEDDB97F7338D8E2E70B64DAA1A47DA454D54F541FED4BF2CAD98F9AA26AA2BC7D37FD14864E75BC916468F64A974B14CFA19FDCED9 37
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF9DEA79CED7C13093.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.40624672850090743
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9losJ69losJq9lWsJBRYx1:kBqoIoloToHU1
MD5:	F648059D56199311B49614A202316819
SHA1:	7FE1FE80D07EAC9350C4605CF5A1C7666DEBBD10
SHA-256:	3441BF87926E7F7E2940E4010BCC6B4604F35703051757EAA603FB0AE8AEBA0E
SHA-512:	0CC4BEBA2738B72281D4F2AD9566C0B1079770252B817EC761A52EACC0C900C6F92EAA4B10A4B10FA08681E041FC401E8D691F20EF4B7A5ED7883B9E52437A1 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):	6.614404253395742
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:	p47bG25tTf.exe
File size:	901960
MD5:	d0cb3af3f2f9bbb89faba16f41585e7c
SHA1:	3a1006610fc6e98670cfd6f01744e4623eeedd9b
SHA256:	31f5ee68e7548cd1d49720492502877466b35241cd441b48eefbddffc74a5475
SHA512:	c0865d84c4b60dbb257e2486a0928d984c0595fe505ddb79998efe57b5302855403b5e2dc884c47a3eade3e90ad4c3ac10033a05ed22ac80413b21828899d0d3
SSDEEP:	24576:H9PsA9vHAYobFGQdRoylSk61LXXh5xvZjmtk1/GqgLG0:4YVJk61bRnZjmWGG0
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z.....\b.....\b.....\b....."...Q.....\b.....7:.....\b.....\b.....\b.....Rich.....

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:	264c61a35ad2f260d533f2d7b897c2a5

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	6.85140338901	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x6a000	0x23f8a	0x24000	False	0.641723632812	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 07:28:16.863847017 CEST	192.168.2.6	8.8.8.8	0xf71	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 07:28:16.908354998 CEST	192.168.2.6	8.8.8.8	0x19c3	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 07:28:16.953681946 CEST	192.168.2.6	8.8.8.8	0x20d3	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 07:28:28.848757982 CEST	192.168.2.6	8.8.8.8	0x2712	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 07:28:39.090675116 CEST	192.168.2.6	8.8.8.8	0xebb5	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 07:29:21.577091932 CEST	192.168.2.6	8.8.8.8	0x877c	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 07:29:21.610570908 CEST	192.168.2.6	8.8.8.8	0xe616	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 07:29:21.668625116 CEST	192.168.2.6	8.8.8.8	0x70cf	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 07:28:16.900222063 CEST	8.8.8.8	192.168.2.6	0xf71	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:28:16.943964005 CEST	8.8.8.8	192.168.2.6	0x19c3	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:28:16.986730099 CEST	8.8.8.8	192.168.2.6	0x20d3	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:28:28.884125948 CEST	8.8.8.8	192.168.2.6	0x2712	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:28:39.124855042 CEST	8.8.8.8	192.168.2.6	0xebb5	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:29:21.604587078 CEST	8.8.8.8	192.168.2.6	0x877c	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:29:21.643030882 CEST	8.8.8.8	192.168.2.6	0xe616	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:29:21.696573019 CEST	8.8.8.8	192.168.2.6	0x70cf	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: p47bG25tTf.exe PID: 6576 Parent PID: 5192

General

Start time:	07:27:47
Start date:	10/09/2021
Path:	C:\Users\user\Desktop\p47bG25tTf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\p47bG25tTf.exe'
Imagebase:	0x1000000
File size:	901960 bytes
MD5 hash:	D0CB3AF3F2F9BBB89FABA16F41585E7C
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: 00000000.00000002.631812823.0000000003750000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.411680498.0000000003750000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source:

00000000.00000003.412285957.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.411095451.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.412774183.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.412569620.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.411978196.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.411758460.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.412426058.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.412785825.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.411605521.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.412680066.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.412607752.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.412384175.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.412743237.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.411442677.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.411526814.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.411908339.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.412640219.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.410999353.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.412334976.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.411184929.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.412120238.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.412463340.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.412538373.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.411360711.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.412177885.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.411273329.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.412722714.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.412702712.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.412499004.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.411834632.0000000003750000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.412228113.0000000003750000.00000004.00000040.sdmp, Author:

	Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 5348 Parent PID: 792

General

Start time:	07:28:14
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:	0x7ff721e20000
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: 5388 Parent PID: 5348

General

Start time:	07:28:15
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:5348 CREDAT:17410 /prefetch:2
Imagebase:	0xc30000
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: 2584 Parent PID: 792

General

Start time:	07:29:18
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:	0x7ff721e20000
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: 4060 Parent PID: 2584

General

Start time:	07:29:20
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:2584 CREDAT:17410 /prefetch:2
Imagebase:	0xc30000
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