ID: 481298
Sample Name:
ixGWwYWQOV.exe
Cookbook: default.jbs
Time: 16:50:33
Date: 10/09/2021
Version: 33.0.0 White Diamond

Table of Contents

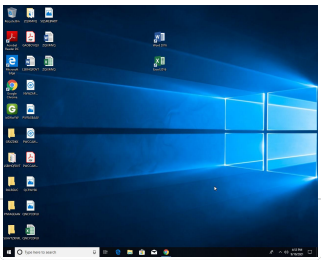
Windows Analysis Report ixGWwYWQOV.exe

Overview

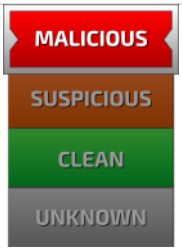
General Information

Sample Name:	ixGWwYWQOV.exe
Analysis ID:	481298
MD5:	6c4e1328230fd65.
SHA1:	9cfbf6477457d26..
SHA256:	31941577d287f74.
Tags:	exe Gozi
Infos:	

Most interesting Screenshot:



Detection



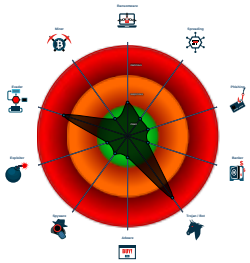
Ursnif Ursnif v3

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

Signatures

- Yara detected Ursnif
- Multi AV Scanner detection for subm…
- Detected unpacking (changes PE se…
- Yara detected Ursnif
- Writes or reads registry keys via WMI
- Writes registry values via WMI
- Machine Learning detection for samp…
- Performs DNS queries to domains w…
- Uses 32bit PE files
- Antivirus or Machine Learning detec…
- PE file contains an invalid checksum
- PE file contains strange resources

Classification



Process Tree

- **System is w10x64**
- ixGWwYWQOV.exe (PID: 5244 cmdline: 'C:\Users\user\Desktop\ixGWwYWQOV.exe' MD5: 6C4E1328230FD65C2C8232E7B9F838AE)
- iexplore.exe (PID: 6264 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6312 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6264 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 5452 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5608 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5452 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.299620365.0000000003510000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.299260696.0000000003510000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.299197344.0000000003510000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.298965891.0000000003510000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.300025842.0000000003510000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 29 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.3.ixGWwYWQOV.exe.da9d7c.0.raw.unpack	JoeSecurity_Ursnifv3	Yara detected Ursnif	Joe Security	
0.2.ixGWwYWQOV.exe.1000000.0.unpack	JoeSecurity_Ursnifv3	Yara detected Ursnif	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

Performs DNS queries to domains with low reputation

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

Yara detected Ursnif

System Summary:

Writes or reads registry keys via WMI

Writes registry values via WMI

Data Obfuscation:

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

Yara detected Ursnif

Remote Access Functionality:

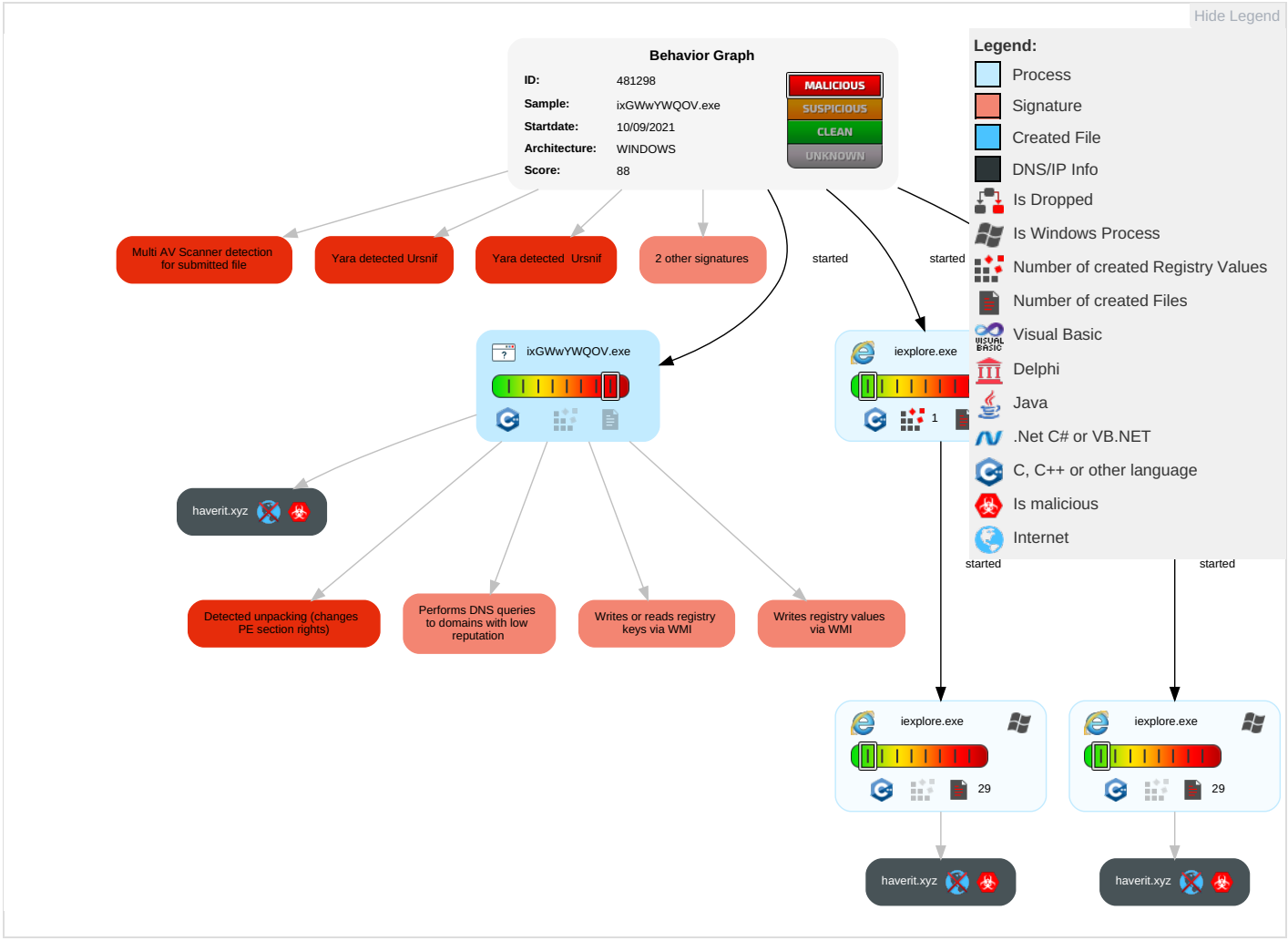
Yara detected Ursnif

Yara detected Ursnif

Mitre Att&ck Matrix

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

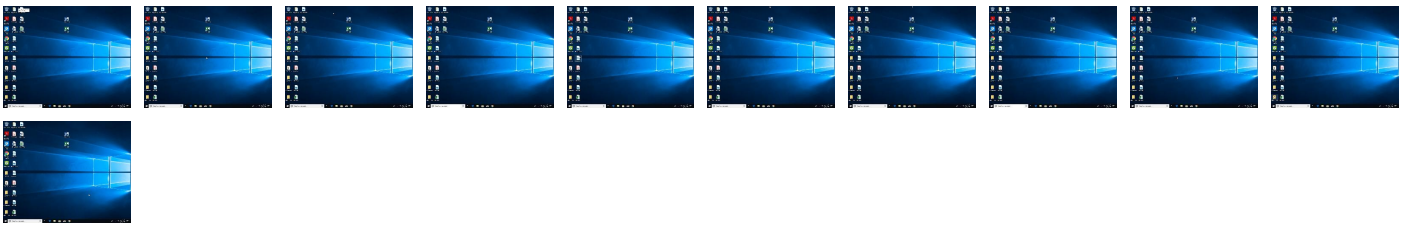
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ixGWwYWQOV.exe	22%	Virustotal		Browse
ixGWwYWQOV.exe	27%	ReversingLabs	Win32.Trojan.Ursnif	
ixGWwYWQOV.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.ixGWwYWQOV.exe.1000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
0.3.ixGWwYWQOV.exe.da9d7c.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
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		unknown

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	481298
Start date:	10.09.2021
Start time:	16:50:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ixGWwYWQOV.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:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal88.troj.evad.winEXE@7/29@8/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:52:14	API Interceptor	2x Sleep call for process: ixGWwYWQOV.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.{16F18D88-1292-11EC-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7737306665376058
Encrypted:	false
SSDEEP:	192:rjZoZE2yhWyRtyCifykzV7zMyXzDL6pHBycvUpB:rloTyQyjyrylyXAyx
MD5:	781F276B44A8E17354185949A21D8C3C
SHA1:	9654B76E8FD3D9AC6AC7AE4051986AFB1F2181A5
SHA-256:	7841062D570F0D1B8524354E8536641B2374CB5510784C3C938C1073F959D108
SHA-512:	12793FD515D79C6ED1BC7AC785737CD22E5AB4227A49990A728132AE8895BD8467D325D23BBEF27CD90BDDC095847AD19C44D69910F0953E51B6E321D70595F
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{3D493850-1292-11EC-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{3D493850-1292-11EC-90E6-ECF4BB82F7E0}.dat	
Entropy (8bit):	1.765517080326876
Encrypted:	false
SSDEEP:	48:IwJGcprAGwpLIhG/ap8xGIpcqJWGvnZpvqNGoiqAUPqp9q3Go4eqAU8qAUzpmqDR:rPZIZII2zWgztaifXB/zMind6vzBjQpB
MD5:	EEC80F35B63DB711708504028E912724
SHA1:	48C8921EDE35B83A0FA78B5ADA20CC3125443AF0
SHA-256:	63FC13C9B966AA62963E2829CD77144C25CEF4BFD26228CBEF809215BCDF2DA3
SHA-512:	DD2C3D2E061F35504FA584E6B8FD171B28C3A39833359A044642580EF8C28EEE556E01AAAB2784C4B85CBCEAA190C6A6396B2D943B4EEE900F24D41986CBA0 E
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{16F18D8A-1292-11EC-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26240
Entropy (8bit):	1.6609542346766522
Encrypted:	false
SSDEEP:	48:IwjGcpr6GwpaHG4pQzGrapbSeGQpBVohGHHpcVGWTGUp8VoGzYpmVkzGopOjkyD8:rZZiQp6XBS2jVoc2VGmWVsMVYkjaVjAA
MD5:	D15C7DCCA03F662ABBA13326034EE2CC
SHA1:	E6649D0C5BF0A723BD5B1F5BFD8250AD2CAACF74
SHA-256:	C0B23A85A1C4FAB1B4BA0F537136BA217F555E791B8459D84811CD91516DAF57
SHA-512:	C83788F35BFE661EDC8FD8734CE9FD12A312FB15F7B619F452B2FAE0C2F0F072486228F71326DCC5EEB15C18ED8B76C04329F6788E1B81159BFD9193E8ACCE5
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{3D493852-1292-11EC-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	26240
Entropy (8bit):	1.6546105666555921
Encrypted:	false
SSDEEP:	48:IwJGcprcGwpawG4pQEhGrapbSUGQpBzWGHHpcPTGUp8n5GzYpmbQ6GopO5yDXGqg:rPZUQw6ExBSMjzV2ZWnXMcikwV5A
MD5:	E7E83814597FBC0CEA7CB06FD76819FB
SHA1:	C6ADB3DF64FD6CB745C1310EC2265D1A0DC8403D
SHA-256:	F3675A3785D1A56496077919D4C9A05ADF3C6BCAB01421A821F67340E73BF51C
SHA-512:	B382BC73466A0E8971DCA5A6A2FCF362ABFD294BD8A13E3A83D87CE930E11FB2027132D8146B6B0CE8C8D912BD18B8B4865DC235FF9F9244D7962150FE7DD2 E
Malicious:	false
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):	660
Entropy (8bit):	5.0265966732661065
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEuDE/ADE/1nWimI002EtM3MHdNMNxOEuDE/ADE/1nWimI00OYVbkEty:2d6NxOM/z/1SZHKd6NxOM/z/1SZ7xb
MD5:	41F6EBBA395AE38837406560C6D36607
SHA1:	5D5A9FD4CCBE24EBF26058FF7045AE11FE96912C
SHA-256:	B410B865AE942AD7D0EEAD7334E30628AB8E9FFCDFB0EB65DA248C267208B45D
SHA-512:	E10C08054D51B6847CAD29BE0C99DCBD124DC2EC443CE6BB3FF83E9B3F7653CFD90184E4B38D96DBEE8C6DD0AC06571EB2DB76C98FB67BA786F392B9AEB3 CAF
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xecafcbfa,0x01d7a69e</date><accdate>0xecafcbfa,0x01d7a69e</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>0xecafcbfa,0x01d7a69e</date><accdate>0xecafcbfa,0x01d7a69e</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):	657
Entropy (8bit):	5.078646596942958
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kci1nWimI002EtM3MHdNMNxe2kci1nWimI00OYkak6EtMb:2d6NxrPi1SZHKd6NxrPi1SZ7Ja7b
MD5:	F40F5D67C662A19AD2D73B468506F6D9
SHA1:	F6A86DCC1295C78D9D815107576B39D004CC8DEE
SHA-256:	1E3D604C498576E68B98F2CA2F8B40E7429B8BD2853099595B186B0C966530B0
SHA-512:	B16427C940CC602F88F6D976B250A8C5D6AC28A9574D86E270F302E40DCEF8BFED73FE4C21218D70AF79B33D7D5071ED057885338040279E2C5EB66079E2B21
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xeca8a590,0x01d7a69e</date><accdate>0xeca8a590,0x01d7a69e</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>0xeca8a590,0x01d7a69e</date><accdate>0xeca8a590,0x01d7a69e</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):	666
Entropy (8bit):	5.040746518556224
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLuDE/ADE/1nWimI002EtM3MHdNMNxvLuDE/ADE/1nWimI00OYmZEtMb:2d6NxvR/z/1SZHKd6NxvR/z/1SZ7Zb
MD5:	C084CB65CEF16B602B09FA59AF50CA7F
SHA1:	341568119C29118A98053312E1596F218E57E685
SHA-256:	FDDF4CAA2768775E2192885C58252FF7F052B523F110B01FA3A8F03D8E04F294
SHA-512:	540FF71D9F5DEEE230DE927EA5F7A05D7C3C0BF799702ED7477657338506FF8C9A4A15B94482849604D47CBB2845E49565F2B62C8B2D700E72AD99935AB48F1F
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xecafcbfa,0x01d7a69e</date><accdate>0xecafcbfa,0x01d7a69e</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>0xecafcbfa,0x01d7a69e</date><accdate>0xecafcbfa,0x01d7a69e</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):	651
Entropy (8bit):	5.0417849545777695
Encrypted:	false
SSDEEP:	12:TMHdNMNxiuDE/ADE/1nWimI002EtM3MHdNMNxiuDE/ADE/1nWimI00OYd5EtMb:2d6Nx2/z/1SZHKd6Nx2/z/1SZ7qjb
MD5:	EF04CC90833F2413FFB863B6EE9E8A02
SHA1:	9DFA53752370EA2DE0F3F94BB59973748B82BF53
SHA-256:	1EAB68F9529D0F7556A7A3C94C23A54FD5BA8C2A6C58E60660672E2342F6D2C5
SHA-512:	088FFD247D89316BD4E376FD336B9C02475E4FA20F5158C9F00D929C313500BB75DB23675A03EE36CADC85DE199E2A7DBE524DE636FA34F4B22151525C9D4D8
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xecafcbfa,0x01d7a69e</date><accdate>0xecafcbfa,0x01d7a69e</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>0xecafcbfa,0x01d7a69e</date><accdate>0xecafcbfa,0x01d7a69e</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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Category:	modified
Size (bytes):	660
Entropy (8bit):	5.057678286753301
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwuDE/ADE/1nWimI002EtM3MHdNMNxhGwuDE/ADE/1nWimI00OY8K0z:2d6NxQA/z/1SZHKd6NxQA/z/1SZ7RKa/
MD5:	D76D335B10470B164C89B77313127F0E
SHA1:	164F978A7F68DFC91FFEF7E68C8B7FAC49CE1A70
SHA-256:	C2410A372EED63231E11F0240D2F271A8896B0D445CA1141DB9F86696FFA6DA7
SHA-512:	DA4C2E74DE3ED9B13FCA67C8C180D86FFA0C3F9D8B50C24F7F63F7D12A3EE3BD33DA93BBD3EBB4ADFBF75E7AA7810A53876CC5B26E51249A21DED51BBD4D5848
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xecafcbfa,0x01d7a69e</date><accdate>0xecafcbfa,0x01d7a69e</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>0xecafcbfa,0x01d7a69e</date><accdate>0xecafcbfa,0x01d7a69e</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):	657
Entropy (8bit):	5.029742539991567
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nuDE/ADE/1nWimI002EtM3MHdNMNx0nuDE/ADE/1nWimI00OYxEtMb:2d6Nx0F/z/1SZHKd6Nx0F/z/1SZ7+b
MD5:	98F3FE72EE82FE7E0809F0B4821002FE
SHA1:	2D4E09A7782E1A111E359BB2875C44425E2D663C
SHA-256:	C6DD72E42B44A085A47821C6DACDD392D6F3CD3CC5E50252E2ADABC269A2B492
SHA-512:	E2D82BB8F5BA0A680573FB3F359F4085058E2B0B4F49C28BFE438EE9A1BFC63591683B8625E4340277CB90168290D18E89979A37E7A8CC4D4DBE9328F7A9DCA3
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xecafcbfa,0x01d7a69e</date><accdate>0xecafcbfa,0x01d7a69e</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>0xecafcbfa,0x01d7a69e</date><accdate>0xecafcbfa,0x01d7a69e</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):	660
Entropy (8bit):	5.066694970514444
Encrypted:	false
SSDEEP:	12:TMHdNMNxxuDE/ADE/1nWimI002EtM3MHdNMNxxuDE/ADE/1nWimI00OY6Kq5EtMb:2d6Nxr/z/1SZHKd6Nxr/z/1SZ7Xb
MD5:	E27832EBF5F063985F12DBD31670842D
SHA1:	382D352A9DC3D1DA9619FF2422F3E9FA175D867E
SHA-256:	B11EA1FC8D2FAA73CF746C854E0EF310E439947C3312CA0D61863CB0544904B9
SHA-512:	47A7C5C3D965C887F3296128822878944FED1B999914E80A4117A70251D2769B1341D92BFCAB9FA04610B7B514A154EC2FFB0FBD3FA66C9A98D834C192576767
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xecafcbfa,0x01d7a69e</date><accdate>0xecafcbfa,0x01d7a69e</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>0xecafcbfa,0x01d7a69e</date><accdate>0xecafcbfa,0x01d7a69e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.066617002549845
Encrypted:	false
SSDEEP:	12:TMHdNMNxcci1nWimI002EtM3MHdNMNxcci1nWimI00OYVEtMb:2d6Nx3i1SZHKd6Nx3i1SZ7Gb
MD5:	98F5F73CF2EE738F3D3641DB83398EF0
SHA1:	854C595288333709B6B0C4DBF70D405FCDE621AF
SHA-256:	4EAA1438F49007B9D30C9AF00DFEDF4CD3FE00C29E8A29B9B8F1ED162ECF0202

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
SHA-512:	7D526E6A9F91095AE2F7EE28AB306A990EB6DE63BB869E5745349BDF7BFDE781CBE347D14F5C5E821269C06647B4EBC330A1EB625DD8E3B2DDF63AE022D7AD CB
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xeca8a590,0x01d7a69e</date> <accdate>0xeca8a590,0x01d7a69e</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>0xeca8a590,0x01d7a69e</date><accdate >0xeca8a590,0x01d7a69e</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):	657
Entropy (8bit):	5.0543220403445765
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnci1nWiml002EtM3MHdNMNxfnci1nWiml00OYe5EtMb:2d6Nxki1SZHKd6Nxki1SZ7Fjb
MD5:	DDD8A7424249B413E6AC1A01E3843FC1
SHA1:	E9C076045981074FDFBAD957DD418C9F3DA0CE94
SHA-256:	BDBCA3540F5D55B65F1F719482CA9252E4C26D7318CAA39F2B3B3F2B1AE7D991
SHA-512:	A3C76D1B4548266E6341CD7D1F7B34974341ED8F35A3B3460D874CBD5F7E9823D77341B33534D54ADC911776B99FC6AF942663CFCD250F9B8159C106530A7FC
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xeca8a590,0x01d7a69e</date><a ccdate>0xeca8a590,0x01d7a69e</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>0xeca8a590,0x01d7a69e</date><a ccdate>0xeca8a590,0x01d7a69e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Go ogle.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\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\2K7JPOQS\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\2K7JPOQS\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\2K7JPOQS\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";....//used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\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\6M6D1PMD\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\down[1]	
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\6M6D1PMD\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\VAHFWDJC\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:5m73jcJqQep89TEw7Ukk
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\VAHFWDJC\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\errorPageStrings[1]	
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\VAHFWDJC\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):	4.440534734931472
Encrypted:	false
SSDEEP:	3:oVXUpfYV2IqAW8JOGXnEpfYV2Ign:o9UpQMqEpQ+
MD5:	3FB5291B91C6AD22FE8A57C77D1DA276
SHA1:	FD32C99851C94D34211AF3A8A7ABDFA4AA6020DA
SHA-256:	0200729CA3A7B9971CF7D91AFCCE662C3DE0EB3D1D39ADFEA5573C5CB9FFF7FF
SHA-512:	D6EA7206A2DE140A13CF22AD27D8192FC8AEFD99A7680AAF54D87A4D5C1B83A63F3E5D6028E314F29750BC9A003DF9D6D93CDFAB2DA1AF21192EDA2AA4795 BB
Malicious:	false
Preview:	[2021/09/10 16:53:06.933] Latest deploy version: ..[2021/09/10 16:53:06.933] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DFA52BA84DB18EF3E4.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.40900281620806456
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fRI9l8fRY9lTqy+Nnv:c9lLh9lLh9lIn9lIn9loI9loY9lWy+Rv
MD5:	27159C71B39BC35A35D2AE2C5A352055
SHA1:	1FBC9B88A786399AD1B1035C76078774D02208FE
SHA-256:	8918194C84939FC06E43C122CCF625F1DA6EE0236899A094AB0BD7353FD029F7
SHA-512:	B3835117CCD31DB497CFE62192E4BE4104EE2F2CDD89A124399AD5C1A250CE35B3EF035A81700489C987D766232139AF622A3879A528D8C67F70B1FC1A576CF
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFB8A0D879113F03C7.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data

C:\Users\user\AppData\Local\Temp\~DFB8A0D879113F03C7.TMP	
Category:	dropped
Size (bytes):	38737
Entropy (8bit):	0.36876329153462023
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+U50e3bIbw5yDZ5yDb5yDU:kBqoxKAuvScS+S0e3Ecoyf
MD5:	DA3A6AC514DF883080CA2F98F007442D
SHA1:	A0F2645B6F930E1BF23A38C1DAA8CF69CE97C324
SHA-256:	0AD20F9438A75BE483BD3D252FFD3DFD950399E49CE76FD297BCDB28566AE3FF
SHA-512:	6E1DBFC069DC58262CE3E151271067A48408A82378305F7CDA9FF78C32B57989D470CFC6E3AE5739DAEF42AB086B2D44E33931A96EB45497E3AAE6BFEDC6ED D
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFE1308D1C5805163F.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4069783134723913
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loW9loG9lWLJEMmJQ:kBqoIRXV
MD5:	A7480C3C91FF1C3922B399950A67A23B
SHA1:	498201767377A978E524B08196D9C4EE8FD9EE76
SHA-256:	D895686EAD90A5AB9D2B7888E2C5D4B832D8231973565EC8371F38FE0AADB994
SHA-512:	E9F104A71F271AF42D7CF1C94BB22F967F01B513DEC227C66A0C17E867474CC5D94B0EF96E545BBAC13206AA9C01DEAE69BDDA008F4A81C5E22C6F51FD87E4 BA
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFE30A9991DB7FBF1E.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38737
Entropy (8bit):	0.372600979825686
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+V1VbVZVIVkIVkwjkyDZjkyDbjkyDU:kBqoxKAuvScS+V1VbVZVIVLVjj1j3jg
MD5:	8F7B57036A1806980D21B85DA312515A
SHA1:	1F4282A80509BAAB6EA569DFEC656B0F7A9A519E
SHA-256:	2380DDA787E183076CFFD1944757975B10F5DB8685EEEEB40EF8E199D723AB61
SHA-512:	5127D50ACF7464057C9023859FD70BC5FFC590B46C84ED59B9FB9F1D99CCB8191F5E114C5AA952A1EA8AC6F81EE9963AF0D30634706E73BAAF1537F9AD02344
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):	6.614457028856633
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%

General

File name:	ixGWwYWQOV.exe
File size:	901960
MD5:	6c4e1328230fd65c2c8232e7b9f838ae
SHA1:	9cfbf6477457d26555e37ad3717cccd3aadc7dbe
SHA256:	31941577d287f7445f2791c78da17ffcd54baee40acf61dc0ff27a3f1d5253e6
SHA512:	062c9fa2241227752ead4f15d05e3c3df8f685538765e527f4929ed3e94f3f37f89f60764b531a0c935e878b7710ea4174ae6f9b48e7c8aa8066176e57fdf733
SSDEEP:	24576:P9PsA9vHAYobFGQdRLylSk61LXXhtxvZPmtk1/GqgLGT:wYWJk61bRrZPmWGGT
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9..D}...}...}....{q.....{t.n....{u.~...}.....x....{w.v....#u.|....{i.G....{s.|....{v.|...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:	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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x681b9	0x68200	False	0.623956613896	data	6.85142443524	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 16:52:03.141858101 CEST	192.168.2.7	8.8.8.8	0xa6b8	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 16:52:03.186640024 CEST	192.168.2.7	8.8.8.8	0x6aeb	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 16:52:03.230904102 CEST	192.168.2.7	8.8.8.8	0xb2a1	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 16:52:14.641695023 CEST	192.168.2.7	8.8.8.8	0xee60	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 16:52:24.870857000 CEST	192.168.2.7	8.8.8.8	0xb3d7	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 16:53:07.855437994 CEST	192.168.2.7	8.8.8.8	0x1a4b	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 16:53:07.898761988 CEST	192.168.2.7	8.8.8.8	0x74a	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 16:53:07.977636099 CEST	192.168.2.7	8.8.8.8	0xbd05	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 16:52:03.177349091 CEST	8.8.8.8	192.168.2.7	0xa6b8	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 16:52:03.225603104 CEST	8.8.8.8	192.168.2.7	0x6aeb	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 10, 2021 16:52:03.264877081 CEST	8.8.8.8	192.168.2.7	0xb2a1	Server failure (2)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 16:52:14.685658932 CEST	8.8.8.8	192.168.2.7	0xee60	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 16:52:24.905440092 CEST	8.8.8.8	192.168.2.7	0xb3d7	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 16:53:07.891165972 CEST	8.8.8.8	192.168.2.7	0x1a4b	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 16:53:07.936516047 CEST	8.8.8.8	192.168.2.7	0x74a	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 16:53:08.011830091 CEST	8.8.8.8	192.168.2.7	0xbd05	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: ixGWwYWQOV.exe PID: 5244 Parent PID: 1820

General

Start time:	16:51:33
Start date:	10/09/2021
Path:	C:\Users\user\Desktop\ixGWwYWQOV.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ixGWwYWQOV.exe'
Imagebase:	0x1000000
File size:	901960 bytes
MD5 hash:	6C4E1328230FD65C2C8232E7B9F838AE
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: 00000000.00000003.299620365.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.299260696.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.299197344.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.298965891.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.300025842.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.300187569.0000000003510000.00000004.00000040.sdmp, Author:

	Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.299926777.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.299677009.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.299128367.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.298447630.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.298720367.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.299959474.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.522375595.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.299054889.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.300165850.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.299450851.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.299720559.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.298639407.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.298803166.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.298555276.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.300135492.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.300105036.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.299988986.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.299384530.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.299782953.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.299827410.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.298884838.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.300078539.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.300048451.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.299508546.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.299863512.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.299563221.0000000003510000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.299326737.0000000003510000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 6264 Parent PID: 792

General

Start time:	16:52:00
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:	0x7ff663720000
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: 6312 Parent PID: 6264

General

Start time:	16:52:01
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:6264 CREDAT:17410 /prefetch:2
Imagebase:	0xca0000
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: 5452 Parent PID: 792

General

Start time:	16:53:05
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:	0x7ff663720000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 5608 Parent PID: 5452

General

Start time:	16:53:06
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:5452 CREDAT:17410 /prefetch:2
Imagebase:	0xca0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Disassembly

Code Analysis