ID: 480992
Sample Name: y5ACIMK3tT.exe
Cookbook: default.jbs
Time: 07:14:12
Date: 10/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report y5ACIMK3tT.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 4
Sigma Overview 5
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
E-Banking Fraud: 5
System Summary: 5
Data Obfuscation: 5
Hooking and other Techniques for Hiding and Protection: 5
Stealing of Sensitive Information: 5
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 19
General 19
File Icon 19
Static PE Info 19
General 19
Authenticode Signature 19
Entrypoint Preview 20
Data Directories 20
Sections 20
Resources 20
Imports 20
Version Infos 20
Possible Origin 20
Network Behavior 20
Network Port Distribution 20
UDP Packets 20
DNS Queries 20
DNS Answers 21
Code Manipulations 21
Statistics 21
Behavior 21
System Behavior 21
Analysis Process: y5ACIMK3tT.exe PID: 5412 Parent PID: 5676 21
General 21
File Activities 23
Analysis Process: iexplore.exe PID: 4648 Parent PID: 792 23
General 23

File Activities 23
Registry Activities 23
Analysis Process: iexplore.exe PID: 1392 Parent PID: 4648 23
General 23
File Activities 23
Analysis Process: iexplore.exe PID: 4176 Parent PID: 792 24
General 24
File Activities 24
Registry Activities 24
Analysis Process: iexplore.exe PID: 1488 Parent PID: 4176 24
General 24
File Activities 24
Disassembly 24
Code Analysis 24

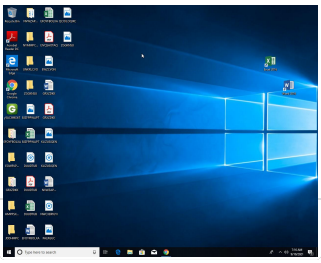
Windows Analysis Report y5ACIMK3tT.exe

Overview

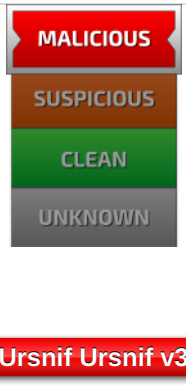
General Information

Sample Name:	y5ACIMK3tT.exe
Analysis ID:	480992
MD5:	72fb1d021cfaa3e..
SHA1:	7de81647d41ef9c.
SHA256:	b7a9576a80944c..
Tags:	exe Gozi ISFB RM3
Infos:	

Most interesting Screenshot:



Detection



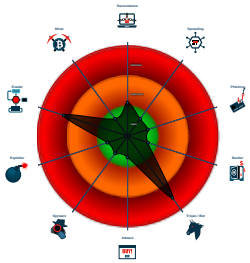
Ursnif Ursnif v3

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**
- y5ACIMK3tT.exe (PID: 5412 cmdline: 'C:\Users\user\Desktop\y5ACIMK3tT.exe' MD5: 72FB1D021CFAA3EF3EA5DDD2AA6EDC86)
- iexplore.exe (PID: 4648 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 1392 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4648 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 4176 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 1488 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4176 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.501326750.00000000036E0000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.280081187.00000000036E0000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.280494462.00000000036E0000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.281430952.00000000036E0000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.280426403.00000000036E0000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 30 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.y5ACIMK3tT.exe.1000000.0.unpack	JoeSecurity_Ursnifv3	Yara detected Ursnif	Joe Security	
0.3.y5ACIMK3tT.exe.c79d7c.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

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:

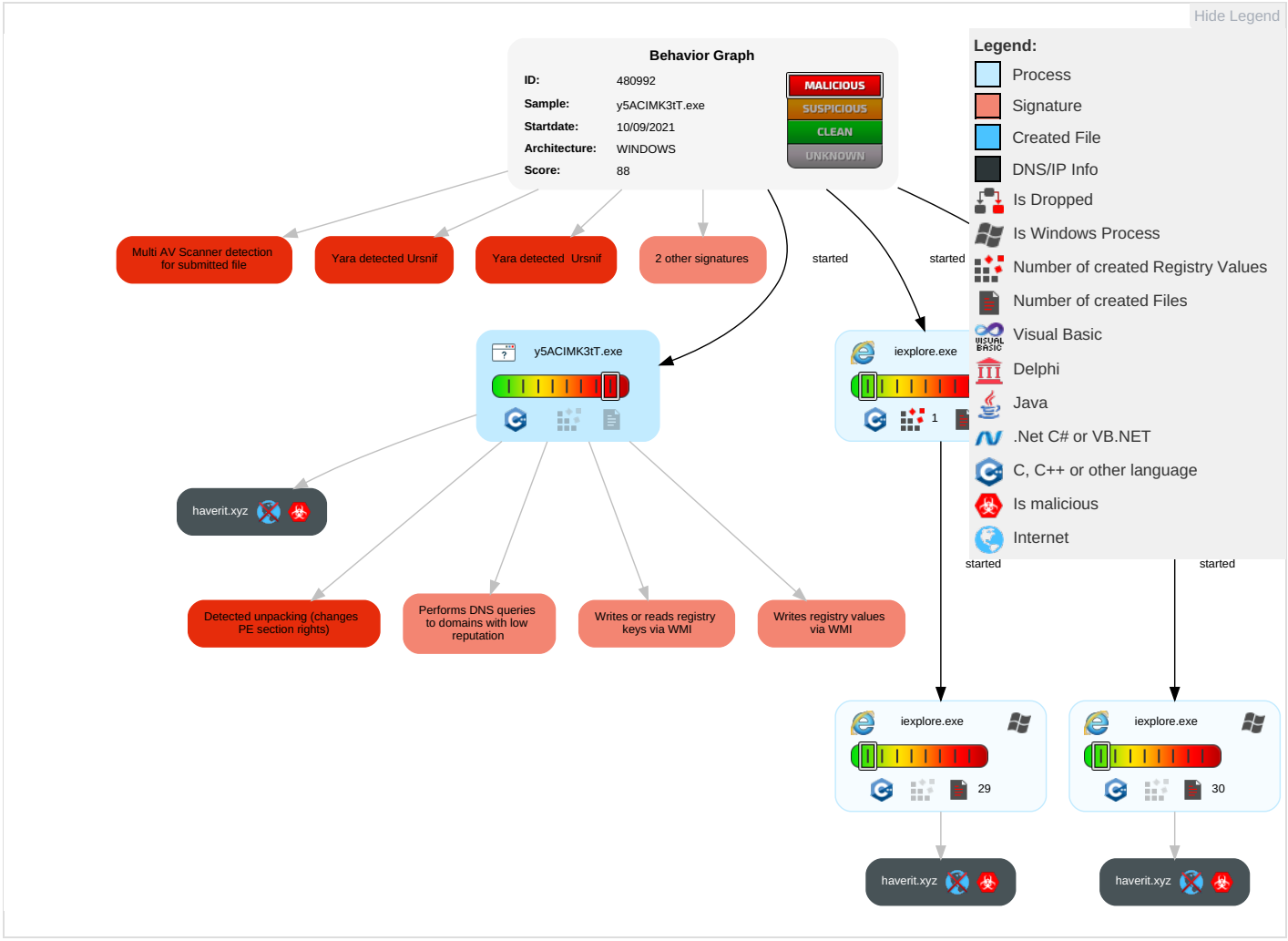
Yara detected Ursnif

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

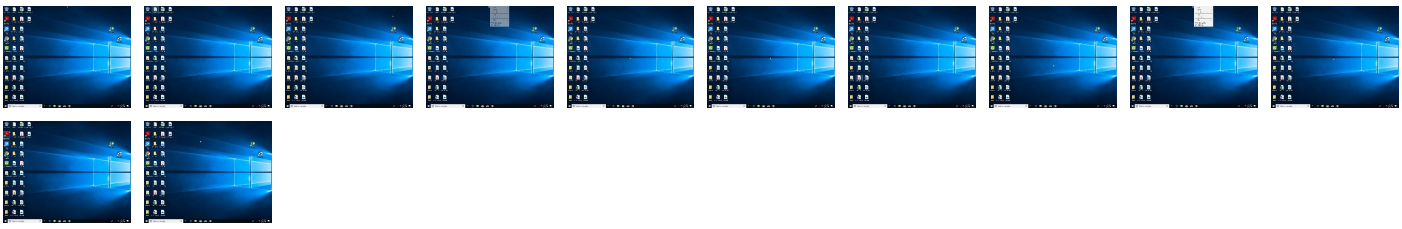
Behavior Graph



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
y5ACIMK3tT.exe	14%	Virustotal		Browse
y5ACIMK3tT.exe	7%	ReversingLabs		
y5ACIMK3tT.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.y5ACIMK3tT.exe.1000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
0.3.y5ACIMK3tT.exe.c79d7c.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:	480992
Start date:	10.09.2021
Start time:	07:14:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	y5ACIMK3tT.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:	21
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
07:15:45	API Interceptor	2x Sleep call for process: y5ACIMK3tT.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.{8E70C929-1241-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7669382848733182
Encrypted:	false
SSDEEP:	48:IweGcprvGwpLxG/ap8PGIpcdtJGvnZpvdtTGo3zCqp9dtnGo4TzMzKpmStjGW3ze:rCZZZ12RWut3bf43AKMaIAzfUqb3MB
MD5:	7945358580CE004301B14ECCF33C17D2
SHA1:	F9F713A23F41C627008836FA4F85BA3F7F8FDA69
SHA-256:	CEF37EA620615897A045CEEFFCBA0D5381E42F9C0DF7497CB8B06D8F7E625C19
SHA-512:	280D5388D9252CFD5B88BAE3860E19B4608F377D6384715D590E4801CD936A01E473A7C23E70018647CDD9ADA571798ABA69FDDBFE3409ED92719BDE2CC1E9
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.{B494046A-1241-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{B494046A-1241-11EC-90E5-ECF4BB570DC9}.dat	
Size (bytes):	29272
Entropy (8bit):	1.7655222910227881
Encrypted:	false
SSDEEP:	96:rlZ+ZP2qWNtW27mbfYE27mj27mKMd27mL27mn27mzc27mX27mqLy27mE27mMB:rlZ+ZP2qWNtWpfYElcMdNthclsOyuB
MD5:	D88CD82AC1F60895D1EB6EC62F06F333
SHA1:	DF56E8606A2179574B2B5D80DA05E65DA51A04CB
SHA-256:	8DAE15F4846A28D19541A9514629C22DAA0BDA2A6865BC7599BD8E572F42E4CD
SHA-512:	6C6F7899D8FC77627E5AA35E4F490DE7328E374181D07820DD006A3B105F57FDDCBCE23B674732A026DD766CFB5BE79FE8DE34C2F9BCFDE48A9C03ECDD12CDE
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\{8E70C92B-1241-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26240
Entropy (8bit):	1.6584600639370661
Encrypted:	false
SSDEEP:	48:IwDGcpreGwpalG4pQFGrapbSuGQpBVyxGHHpcVBTGUp8VFGzYpmVTNGopOHTyDF8:r5ZWQ361BSmjt2lWVMlksVhA
MD5:	CD8936B512AAD306702B9FC86A416B85
SHA1:	0A3F2D76086B86BBFD6E90182AEC239EA8BBA810
SHA-256:	9E97C5A637B3EB9021DC6B64CA7657660039D58DD89C3A19B12A2A834C864991
SHA-512:	0AE78E8367CBCA2420D85FCD468C8BA8428EC23BCCA1B50BF8B1D5518966634928E444C0DD247B2EC302B8091056CA7527542AC0BF5B485738DD3D354E78F7E
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\{B494046C-1241-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26240
Entropy (8bit):	1.6582689479333252
Encrypted:	false
SSDEEP:	48:Iw6GcprnGwpazG4pQrGrapbSiGQpBktGHHpcLTGUp8hzGzYpm1Q4GopOPyDcGqXw:r+ZxQF6fBSqjF2lW7Mzk7VFA
MD5:	B5CA7495FC9582571052CC861577079B
SHA1:	C468E4E826A65275A8813D6A753923541A33F2E9
SHA-256:	CD7558C1567C5551B69316C19AFE67521F86BD98D7980B7023BDE39A3172D63C
SHA-512:	69B9F5D0EDCE121D66C5E65C9D700CC1C6AB2246FF309E9391986A543EAD96123FD4E413CBF0CC327D07D0549FB598E963DC39F854A903D6F95093485867AEC
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	657
Entropy (8bit):	5.112698068858243
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE/tnWiml002EtM3MHdNMNxOE/tnWiml00ONVbkEtMb:2d6NxOUtSZHKd6NxOUtSZ7Qb
MD5:	56C04B2170D0DEFFB06A9B9F6F37B575
SHA1:	CA85A57216773C46A9D92517AB8F81AD03C85373

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
SHA-256:	C8CFD500E2C71690947B8A4C4CF79B313ACC1678111541A9AAAF2F3968C87E99
SHA-512:	3909594FAE2FDB23A1DA8DB925B6CB7FE58C33F72BCD04878CD5816A42E5B430423ABA83D6DE828F118E12EB0A3683ACFA3FEB83B49E4E622B931420D04AF9F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x64348842,0x01d7a64e</date><accdate>0x64348842,0x01d7a64e</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>0x64348842,0x01d7a64e</date><accdate>0x64348842,0x01d7a64e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.105781907353887
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2ko3rN3EnWimI002EtM3MHdNMNxe2ko3rN3EnWimI00ONkak6EtMb:2d6NxrDr9ESZHKd6NxrDr9ESZ72a7b
MD5:	D5284D0B09924DC9096DEEA434C09981
SHA1:	4353BD8DFBD0A1BF36017203DD9A71A4DC87EAA0
SHA-256:	693BB50D3FCA8AB0CEFBDD40107BBF4025ABC5024B409865B1208394BEEAACC4
SHA-512:	4E2269FA633C9AAA2ADBE6C29C76A7F0818793362CE6FA313D46FFF53CCE3C089BAD588375B805124F3CCE19DCEDE601DCAA1BAFA34A0B14B6C1343B920FAB70
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x642d42ea,0x01d7a64e</date><accdate>0x642d42ea,0x01d7a64e</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>0x642d42ea,0x01d7a64e</date><accdate>0x642d42ea,0x01d7a64e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.131747444699833
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL/tnWimI002EtM3MHdNMNxvL/tnWimI00ONmZEtMb:2d6NxvTtSZHKd6NxvTtSZ7Ub
MD5:	30FC25A36A0471ECCE7D48FDD6D0E12B
SHA1:	D4733C92D8009793A25661271027590392427A99
SHA-256:	34A03EE1D7D5C07C1EFFD920C88860F4384FF00C4AE95F95BF7809363E5FD4FA
SHA-512:	61C3B6910CC576CC5E137E0ABBEC0676DCC40AE4D8A2720A96B6F0CA64FB73BEC1C9C73DFEC7B61EEC436F20436E40BAC5916524770A868D95B56615642AA912
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x64348842,0x01d7a64e</date><accdate>0x64348842,0x01d7a64e</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>0x64348842,0x01d7a64e</date><accdate>0x64348842,0x01d7a64e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	648
Entropy (8bit):	5.107580769884397
Encrypted:	false
SSDEEP:	12:TMHdNMNxio3rN3EnWimI002EtM3MHdNMNxio3rtnWimI00ONd5EtMb:2d6NxJr9ESZHKd6NxJrtSZ7njb
MD5:	78930A6B474FF3C6FC92CF65473DF93A
SHA1:	1A8D5302E7135E943C109F993296164AA252F93B
SHA-256:	73C8C3A7ACF4B48F77369F1EB3EE51C913327D428B6A93D5B142B5782A42C1AC
SHA-512:	B10FAAFE8E2FC9FF7DB456D617682C01E2611E237B894AFD4BA04E43AE79584A012A5C075D42C62121C5A2AAE4C30C5B892B856E38EA89FA8B0053DD59B7A76
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>0x642d42ea,0x01d7a64e</date><acc date>0x642d42ea,0x01d7a64e</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>0x642d42ea,0x01d7a64e</date><accdate>0x64348 842,0x01d7a64e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	657
Entropy (8bit):	5.146947312809163
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGw/tnWimI002EtM3MHdNMNxhGw/tnWimI00ON8K075EtMb:2d6NxQQtSZHKd6NxQQtSZ7uKajb
MD5:	19BAA0AA4F7B42F1CA9D58F85F36A67B
SHA1:	9113B73F91E064873E1DA1247118B80D78373BA9
SHA-256:	F430FA5EF7272D5879B8CD143C25B32B5439972DBA3D7AE3AD04C66A234E086F
SHA-512:	CD6CBE7CDF9AD6DB223C18D560D4264FA8DEDC609F68F254E0D90B4905AF9E93676B7427071604F4DF0C51F2D6184242ECEC16503AFC819D76222A8E5BA991 3
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x64348842,0x01d7a64e</date>< accdate>0x64348842,0x01d7a64e</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>0x64348842,0x01d7a64e</date><accdate>0 x64348842,0x01d7a64e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.116530535276916
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n/tnWimI002EtM3MHdNMNx0n/tnWimI00ONxEtMb:2d6Nx0/tSZHKd6Nx0/tSZ7Vb
MD5:	A1AFD5D082D3C856A670C9986D04420A
SHA1:	C8C810DE09A02D662C07CD1E7A49B66ADDBF59B1
SHA-256:	87D3D0F83FB4DAE3EA812108E1B2F6D61983D66BC58AFF67E720D3C604C15009
SHA-512:	0D50713677B1B2C0807EDF39715E3C9F42A1C323EFCF6DEF4C7AE3DDB6EBC6276D61C1A8EEA4597C9516B93081C02A300E96BEE2E4B7A8B69707EDF071DD65 2E
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x64348842,0x01d7a64e</date><a ccdate>0x64348842,0x01d7a64e</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>0x64348842,0x01d7a64e</date><accdate>0x6 4348842,0x01d7a64e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin202591677780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	657
Entropy (8bit):	5.152273020515827
Encrypted:	false
SSDEEP:	12:TMHdNMNxx/tnWimI002EtM3MHdNMNxx/tnWimI00ON6Kq5EtMb:2d6NxttSZHKd6NxttSZ7ub
MD5:	22B48B7DDFCE42C42EA81FBD0846B662
SHA1:	111B0CAAB4F2F1C67000C0731CC9CC4B2EC1B6BE
SHA-256:	70D89213EF2CF2C2075483C7E79D01DC921200B20A8BDE99A5D91FAA782097E3
SHA-512:	9D2DDB1124CA4A70739BD5A930CD0C897EE3CEA48A96731FB703B9B5672238B48CB9964B33900E26D90252A79E3ACCDCF71F460652AA041D9E897D27AA75FE E
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x64348842,0x01d7a64e</date>< accdate>0x64348842,0x01d7a64e</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>0x64348842,0x01d7a64e</date><accdate>0 x64348842,0x01d7a64e</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):	660
Entropy (8bit):	5.099005968693941
Encrypted:	false
SSDEEP:	12:TMHdNMNxco3rN3EnWimI002EtM3MHdNMNxco3rN3EnWimI00ONVEtMb:2d6Nx7r9ESZHKd6Nx7r9ESZ71b
MD5:	770028D27C9FDE5B0995D0D63E48142E
SHA1:	D87004D71F531D5E4CE044E48F6E5028886C8825
SHA-256:	77FB3B0296E9681AE26C13093A761F1DE6F5F5F55D23A8F1A2A60A10FEFF4A04
SHA-512:	FB282B9B497FE481DB14455B1D627E21C4B081395AFABFB17C337C85F04C9CF19AC1C1D1456F2811566E90BDA4C6F0647B133F2DB72316DBF4C1338940F84C1
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x642d42ea,0x01d7a64e</date><accdate>0x642d42ea,0x01d7a64e</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>0x642d42ea,0x01d7a64e</date><accdate>0x642d42ea,0x01d7a64e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.080308113402304
Encrypted:	false
SSDEEP:	12:TMHdNMNxfno3rN3EnWimI002EtM3MHdNMNxfno3rN3EnWimI00ONe5EtMb:2d6NxYr9ESZHKd6NxYr9ESZ7Ejb
MD5:	24F51F3EF9833D6BBC19AE0B21CEA66F
SHA1:	9457E5D590C1F5EEEDCA4432966C594AD9949FE4
SHA-256:	55A7188A06693632F606D862C04ED6140F787C8AEBFA5539CDEE69620FB38100
SHA-512:	00BF15D1BF9C3C398C6ABF96D8C45572A9C495A968CCE6E74F6CCD011FBED5B9CB4BF50C35E1E578D0D58E07AADBC8C99D29E78A5B9AD44460A5D2A6DEE8EEEF
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x642d42ea,0x01d7a64e</date><accdate>0x642d42ea,0x01d7a64e</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>0x642d42ea,0x01d7a64e</date><accdate>0x642d42ea,0x01d7a64e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\errorPageStrings[1]	
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\4PB7FJMT\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.su bstring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var pound Index = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\httpErrorPagesScripts[1]	
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D
Malicious:	false
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\NewErrorPageTemplate[2]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D
Malicious:	false
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493 AC6D
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\dnserror[1]	
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....l..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";....//used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	89
Entropy (8bit):	4.48547855515619
Encrypted:	false
SSDEEP:	3:oVXUpPvTEH8JOGXnEpPvuSun:o9UpoHqEpOSu
MD5:	D83E06FE427751E9BDB33BB4973DDAE4
SHA1:	D3B5FD3B9CC417D6C9104133BD4D208B271E3539
SHA-256:	2560DB494FC84A2E3B784C92C6D21A6E2326B6C022EC01751E3EC1B2D3977051
SHA-512:	665DED2E622C649F7B540499A542AE24835CD4E32077E584E118279013D35B6E88AB0591AC7BE38EFBF3C63C570245203AF3B7431F2AB965DC62DF05D91361E2
Malicious:	false
Preview:	[2021/09/10 07:16:37.656] Latest deploy version: ..[2021/09/10 07:16:37.656] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF56EA5AC75B303922.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38737

C:\Users\user\AppData\Local\Temp\~DF56EA5AC75B303922.TMP	
Entropy (8bit):	0.37178213318940906
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+VqVyRVWVfVTIVTwHTyDZHTyDbHTyDU:kBqoxKAuvScS+ouk1emqwt
MD5:	4CFC78871AA73B44EF10B660F7B9A647
SHA1:	110C151CC0DF69ABDE3C5FB7B92366EF33C72F73
SHA-256:	EE8635C8F7336AB4769C1F836FE2099EF0EFBAC3B9086AFF3F8B2C1F4796F865
SHA-512:	BFE2CB219AF232EBD8108A1C0AB1844D7EFCCD6CB6806F29B8806406162104FE816C00FBA58F5CAFB6BDFA6A780B205512E6F94734AFD740C7F8CEBD2E7FC 3D
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF58B12BFEC36A6D12.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4083961078857369
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fR3C9l8fR3y9lTq3nnh:c9lLh9lLh9lIn9lIn9loS9loC9lW3h
MD5:	724E1A38416982867DB7435AF11BE17C
SHA1:	F664B8739825A1AFBEC4F311F03B01742EC36EEA
SHA-256:	2BA5B6F622CD7C3D745C61D4CF754E18784D818EDE82EFA121A85501500B52A1
SHA-512:	5A13C7A97A8A4E1567D7B4503BD36482D23FA3947E3B907908516C5D1F2C3DC7D72C26F2650CF09FE2891D9ED5EE0E83FE254E5C03E55ABDB1D2798153F16A9
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFA5C652E686E58888.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+EkRIZ1I1wPyDZPyDbPyDU:kBqoxKAuvScS+EiIZCaG8Z
MD5:	334468D3CF49CDFE2CCAC8920F29206F
SHA1:	9E61FA62581B40C30BD11BF92BECA809689157ED
SHA-256:	EA945154C25F0CE7ABEC89280E9419AFE8F82C2E3C3FDC6D7FF27DF0152ECBD4
SHA-512:	F8C7833DDF8F0204CAAD36CA56A29F7BB32D965076C6263F7C75C27ACA1999CE7AD0E1611BB510388C8A50978ADAA81A8BA445166AD7E847119CE9C7DA3167 1
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFEAB2FBB4231FF1CC.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.40716309839094866
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loIT9loIT9lWINvinev6WnE:kBqoIv59SE
MD5:	5217D7AB6A9D794AAC70438D98666715
SHA1:	DB061C2C7A891FC61AEFC4D9586D6259E91ABF99
SHA-256:	66EBFEDA3EF90C4EEE430B0738C08546A62BE6EAE13B1C77918B900BAF9878D3
SHA-512:	CF2C8FB599D15499CE609B1187CDF10E133FFCA0EC96FE183BA60D514691732A740807FE5F0FF084E4163BEA1916CAA0EA294B975FFFFC1004E91DD7B73590E A
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DFEAB2FBB4231FF1CC.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.614360119917732
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:	y5ACIMK3tT.exe
File size:	901960
MD5:	72fb1d021cfaa3ef3ea5ddd2aa6edc86
SHA1:	7de81647d41ef9c982920e119ebaf27b5affcf26
SHA256:	b7a9576a80944c203ddb7a1fbfbfa2a5806c2419ad193f22b84d0fa4f078a725
SHA512:	f487c205746f3b9de76de7029fb9fab108c384e55c8d1918120a76feccd1284ab566eedacd5c7b279a8a9ba16c8c357e56dd6c0497866cb3a41d098d9618cd4e
SSDEEP:	24576:y9PsA9vHAYobFGQdRHylSk61LXXhNxvZXmtk1/GqgLGu:3YqJk61bRLZXmWGGu
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........s/>..Am..Am..Am...m..Am...m..Am...m..Am..@mb.Am.e.m..Am...m..Amn..m..Am...m..Am...m..Am...m..AmRich..Am......................

File Icon

Icon Hash:	f0b0e8e4e4e8b2dc

Static PE Info

General

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

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=Sectigo RSA Code Signing CA, O=Sectigo Limited, L=Salford, S=Greater Manchester, C=GB

Signature Validation Error:	**No signature was present in the subject**
Error Number:	-2146762496
Not Before, Not After	• 4/12/2021 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	0.62395192452	data	6.85141956597	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x6a000	0x23f8a	0x24000	False	0.641872829861	data	6.36645327435	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x8e000	0x1e3ac	0x7a00	False	0.527792008197	data	6.51367686644	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xad000	0x41028	0x41200	False	0.240744211852	data	5.36312234805	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xef000	0x4d50	0x4e00	False	0.730168269231	data	6.65913941378	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 10, 2021 07:15:34.716731071 CEST	192.168.2.5	8.8.8.8	0x1bcc	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 07:15:34.768047094 CEST	192.168.2.5	8.8.8.8	0xaf32	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 07:15:34.820358038 CEST	192.168.2.5	8.8.8.8	0xe91b	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 07:15:46.217190027 CEST	192.168.2.5	8.8.8.8	0xb663	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 10, 2021 07:15:56.312530041 CEST	192.168.2.5	8.8.8.8	0x9483	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 07:16:38.532948971 CEST	192.168.2.5	8.8.8.8	0x528f	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 07:16:38.567085028 CEST	192.168.2.5	8.8.8.8	0xf2	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 07:16:38.613707066 CEST	192.168.2.5	8.8.8.8	0x9562	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)

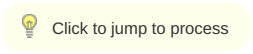
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 10, 2021 07:15:34.752845049 CEST	8.8.8.8	192.168.2.5	0x1bcc	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:15:34.803451061 CEST	8.8.8.8	192.168.2.5	0xaf32	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:15:34.854804039 CEST	8.8.8.8	192.168.2.5	0xe91b	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:15:46.254637003 CEST	8.8.8.8	192.168.2.5	0xb663	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:15:56.348328114 CEST	8.8.8.8	192.168.2.5	0x9483	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:16:38.560961962 CEST	8.8.8.8	192.168.2.5	0x528f	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:16:38.603250980 CEST	8.8.8.8	192.168.2.5	0xf2	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 07:16:38.646589994 CEST	8.8.8.8	192.168.2.5	0x9562	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: y5ACIMK3tT.exe PID: 5412 Parent PID: 5676

General

Start time:	07:15:04
Start date:	10/09/2021
Path:	C:\Users\user\Desktop\y5ACIMK3tT.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\y5ACIMK3tT.exe'
Imagebase:	0x1000000
File size:	901960 bytes
MD5 hash:	72FB1D021CFAA3EF3EA5DDD2AA6EDC86

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: 00000000.00000002.501326750.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.280081187.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.280494462.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.281430952.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.280426403.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.281014480.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.280263191.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.281416323.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.425935885.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.280831725.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.281148827.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.281353274.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.280639725.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.280563706.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.281240518.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.279765747.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.281062590.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.280698259.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.281191378.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.280772678.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.281330244.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.279863384.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.279650602.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.280906581.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.279954452.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.281398809.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.281439514.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.280341081.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.280961190.00000000036E0000.00000004.00000040.sdmp, Author:

	Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.281272411.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.281107458.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.281302346.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.281376823.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.280182518.00000000036E0000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 4648 Parent PID: 792

General

Start time:	07:15:32
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:	0x7ff7cbd60000
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: 1392 Parent PID: 4648

General

Start time:	07:15:32
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:4648 CREDAT:17410 /prefetch:2
Imagebase:	0xd50000
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: 4176 Parent PID: 792

General

Start time:	07:16:36
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:	0x7ff7cbd60000
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: 1488 Parent PID: 4176

General

Start time:	07:16:36
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:4176 CREDAT:17410 /prefetch:2
Imagebase:	0xd50000
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