ID: 481103
Sample Name: CGd7lq6RDL.dll
Cookbook: default.jbs
Time: 11:05:32
Date: 10/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report CGd7lq6RDL.dll 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 5
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
Public 9
Private 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: CGd7lq6RDL.exe PID: 6948 Parent PID: 6008 21
General 21
File Activities 23

Analysis Process: iexplore.exe PID: 6672 Parent PID: 792 23
General 23
File Activities 23
Registry Activities 23
Analysis Process: iexplore.exe PID: 6824 Parent PID: 6672 23
General 23
File Activities 23
Analysis Process: iexplore.exe PID: 5656 Parent PID: 792 24
General 24
File Activities 24
Registry Activities 24
Analysis Process: iexplore.exe PID: 6136 Parent PID: 5656 24
General 24
File Activities 24
Disassembly 24
Code Analysis 24

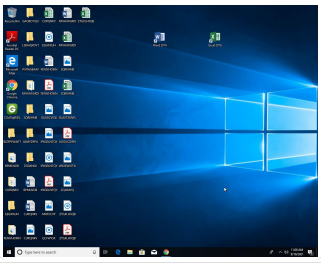
Windows Analysis Report CGd7lq6RDL.dll

Overview

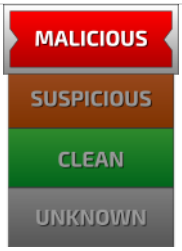
General Information

Sample Name:	CGd7lq6RDL.dll (renamed file extension from dll to exe)
Analysis ID:	481103
MD5:	c7b71f03f190a5d..
SHA1:	8e750d01e1a5ed..
SHA256:	930d54df724f163..
Infos:	

Most interesting Screenshot:



Detection



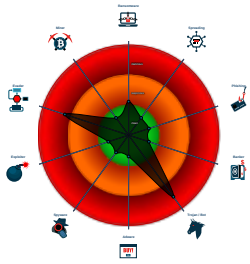
Ursnif Ursnif v3

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Process Tree

- **System is w10x64**
- CGd7lq6RDL.exe (PID: 6948 cmdline: 'C:\Users\user\Desktop\CGd7lq6RDL.exe' MD5: C7B71F03F190A5DA3E4976F37194419F)
- iexplore.exe (PID: 6672 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6824 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6672 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 5656 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6136 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5656 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000003.385018366.0000000003610000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.384548084.0000000003610000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.383601456.0000000003610000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.385072202.0000000003610000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.384483225.0000000003610000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 29 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
1.3.CGd7lq6RDL.exe.da9d7c.0.raw.unpack	JoeSecurity_Ursnifv3	Yara detected Ursnif	Joe Security	
1.2.CGd7lq6RDL.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:

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:

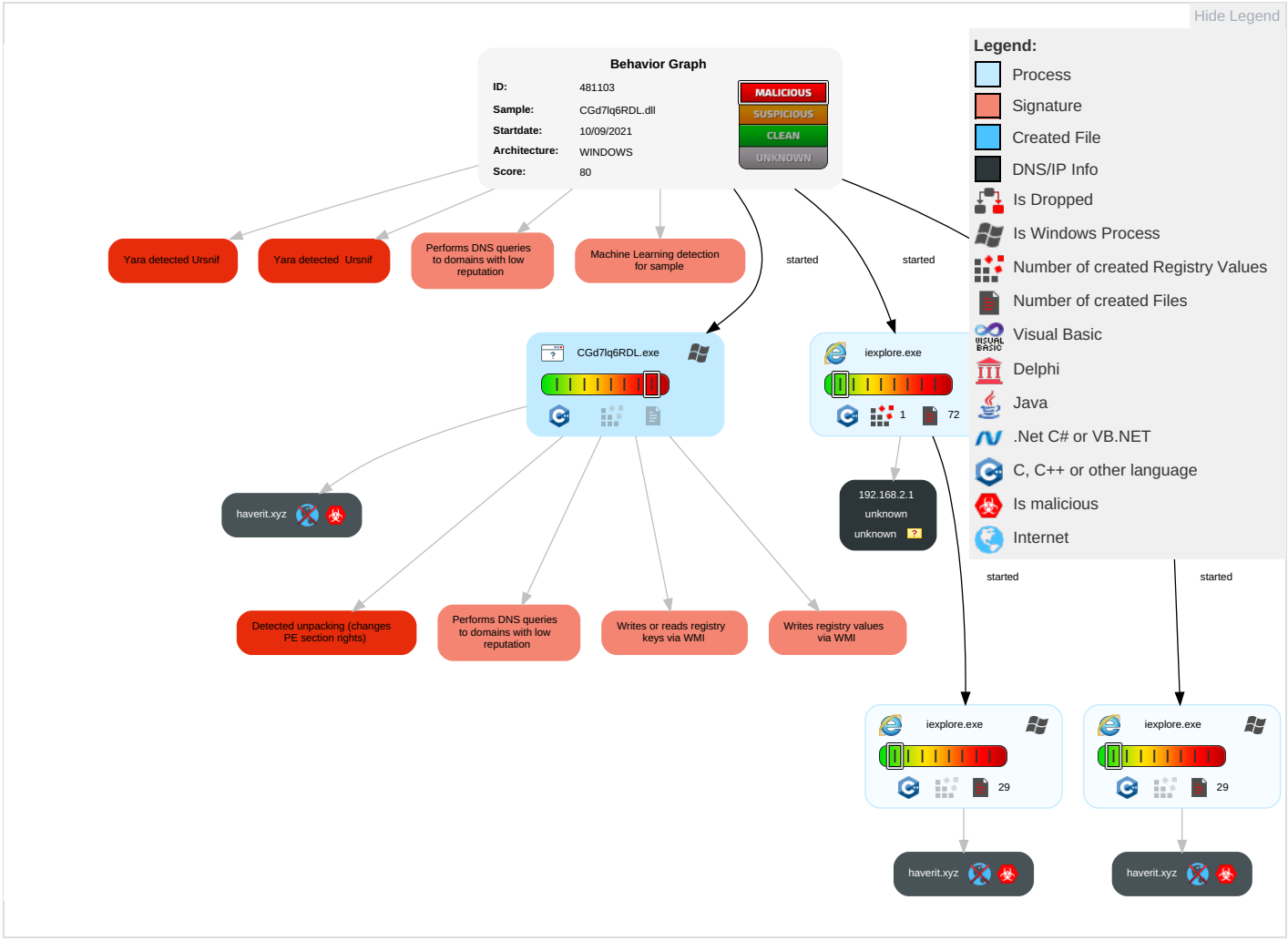
Yara detected Ursnif

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

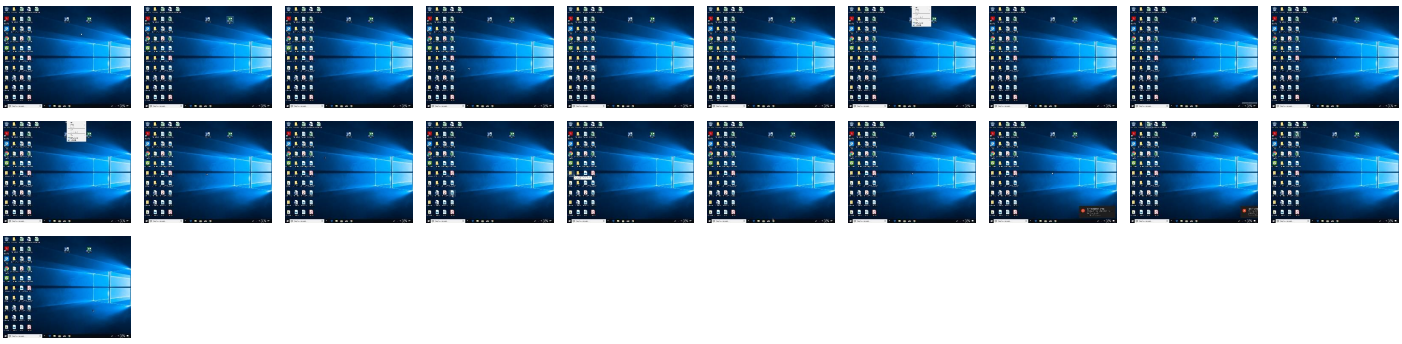
Behavior Graph



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
CGd7lq6RDL.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.3.CGd7lq6RDL.exe.da9d7c.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.CGd7lq6RDL.exe.1000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://haverit.xyz/index.htm	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	481103
Start date:	10.09.2021
Start time:	11:05:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CGd7lq6RDL.dll (renamed file extension from dll to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	26
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:	mal80.troj.evad.winEXE@7/29@8/1
EGA Information:	Failed

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

Simulations

Behavior and APIs

Time	Type	Description
11:07:06	API Interceptor	2x Sleep call for process: CGd7lq6RDL.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.{06650DBE-1262-11EC-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7678852739688395
Encrypted:	false
SSDEEP:	48:Iw7GcprqGwpL7G/ap8jGIpcHGvnZpvDHGoERqp9p1QGo4w01pmQGWEz41ZGWEBTK:rhZyZb2lW4twAf7zw01Mfs+IqcTA2PDB
MD5:	91D74D68B43CCDAE94C1706D038C8A1A
SHA1:	8227029E9BA7F0E28E4DCC141EB41BBA47EF138A
SHA-256:	C866FCEBE96AF3868188B0AC5293E9AE25A2D08CDBAD0933AE71F2F37BCDF248
SHA-512:	476AF38E28FDF7F43F0C947BDCA7FC6EBAF67788997749C0661B13DB2A77B76DDADA362A4BF3D52162A66E0A8093557C71C62DFBFDD04E10DF1EF3AD4BA6C62
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{06650DBE-1262-11EC-90E5-ECF4BB2D2496}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{E0443E1A-1261-11EC-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7653086061397365
Encrypted:	false
SSDEEP:	48:IwcGcprlGwpLVG/ap8AGIpcnGvnZpvQ8Go7zRqp9TuQGo4/zrz1pm3GW7zznz1YK:rAZvZx2wWYtDAfyzrv1MBnWIeXThRkDB
MD5:	0E5636275C441CD90C269D5C6EF99D80
SHA1:	7F044DC2479A60F9AA3AC28957322EB0E1669E4D
SHA-256:	A71C123B695592F824A3E57997E78CA48F243820109E60294A8170227E8BD53E
SHA-512:	6586B3C502ED21B6D94A343D0FA42639E3C4EED575EE88BE945350D6D3641212C410522B4020194EFDF07A26538A5BF866FCA5EDF4FE16F3B6D90ACF216E49E
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\{06650DC0-1262-11EC-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26240
Entropy (8bit):	1.6570043927330005
Encrypted:	false
SSDEEP:	48:IwO0GcprAfGwpap0G4pQ/mGrapbS0GQpBKGHHpcWTGUp8OGzYpmxQGopO3yDpGq2:rZZKQq6ABSsjR2mWiMGkMVfA
MD5:	7FA8DD3F4FB00A17B2C41F231E9A0E07
SHA1:	BDCEB0136D5E5C3394AFF432B30CF297D9A32E33
SHA-256:	15E70B605701F421505DFC949C2F0273418CB913CDF5A2376B3E44354A21FF56
SHA-512:	9EC4CD119B8E109C9ED5DDE75F6E32B6CC4D7E82E9B2CECBC4557EE2F644F23B6F82B60DC7D01CE81568890338C9348091AE92B757C65E4FF596D4AD6BB82BC
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\{E0443E1C-1261-11EC-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26240
Entropy (8bit):	1.6575667429961585
Encrypted:	false
SSDEEP:	48:IwaGcprnkGwpawPG4pQ2dGrapbSiGQpBOGHHpcLTGUp81GzYpm5DGopOTyDLGqXZ:reZcQg6yBSqjd2lWLM/kWVoA
MD5:	C81D77FE65821897EC6BDED4CDDB1153
SHA1:	AB2D019A9C9E781534D1ED5358C5A46C801AF633
SHA-256:	1DA4003576AAD9DECA1E93655F7FFF67F88E1EEFAB0FED707374B867A076029A
SHA-512:	5A282CA90671A48F6BF08F62E3CE021CD9D4F652E0C2E81577283C1CE829345AA6FC582FDB115F8720A651D4203356C6B79AF8E30099A48E624BCDBBD3BC406
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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.0673004512682684
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE84l74lMnWimI002EtM3MHdNMNxOE84l74lMnWimI00OVbVbkEtMb:2d6NxOC0MSZHKd6NxOC0MSZ7V6b
MD5:	720C1B6AE76C69288735B54685FF20F6
SHA1:	116894018C32921C13272B3442A02A97B84FF73A
SHA-256:	7EF6FCC9BC4CBBDFD4D6FFA5348FCC30187B5DFDC00DA7F7D7097196BBD227F9
SHA-512:	325BC40B2D093D892362D6112F4C3A4BD46CA95DC34A184881B666124E33724FEB11E44CF9C84C28E9CE693E4F208A465A8ADA131CB6BC521D87B1125EB5524
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xb603e652,0x01d7a66e</date><accdate>0xb603e652,0x01d7a66e</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>0xb603e652,0x01d7a66e</date><accdate>0xb603e652,0x01d7a66e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.088537313641816
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kjBtBRnWimI002EtM3MHdNMNxe2kjBtBRnWimI00OVbkak6EtMb:2d6NxrIBtBRSZHKd6NxrIBtBRSZ7VAan
MD5:	6E339B98FAEC4B8200B314938FD4C7F6
SHA1:	B6572CF80F6BECD31325FA024BCF4029DBD3A5AA
SHA-256:	C6104511DC96081C1E30333DC40B46D18CF336049BE480FDBE454A4CABA52BAF
SHA-512:	90AA84F8B5CCFBC800C1CDC28E46BB12B1F586AD1B012122DBAAB9323EF17A5AA6D9B5E6F20491F302D577565507EAF2A5BC67D81BAF320EB8ED2339F22BD409
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xb5fcbe9d,0x01d7a66e</date><accdate>0xb5fcbe9d,0x01d7a66e</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>0xb5fcbe9d,0x01d7a66e</date><accdate>0xb5fcbe9d,0x01d7a66e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	665
Entropy (8bit):	5.086871044550789
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL84l74lMnWimI002EtM3MHdNMNxvL84l74lMnWimI00OVbmZEtMb:2d6Nxv/0MSZHKd6Nxv/0MSZ7Vmb
MD5:	9F1828F27A4F7BED74A2D84A6130EDB4
SHA1:	B312E021BC2C22E7E4B8A8E641C97A488C18261D
SHA-256:	32E1858AEB47481FDF276C220FB0B9B4C94DEDED69F767F180A17C579437A805
SHA-512:	6FF87F1A06F870FB0B7E752B790B6314FB742A637689A77523A335054694EFDD56EDBA543E848BF1FAFD10FAA28C5BA18959E68781262AAA02B03A76EC975F6A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xb603e652,0x01d7a66e</date><accdate>0xb603e652,0x01d7a66e</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>0xb603e652,0x01d7a66e</date><accdate>0xb603e652,0x01d7a66e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	650
Entropy (8bit):	5.075595889238291
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
SSDEEP:	12:TMHdNMNxijBtBRnWimI002EtM3MHdNMNxijBtBRnWimI00OVbd5EtMb:2d6NxKBtBRSZHKd6NxKBtBRSZ7VJjb
MD5:	6D86F9B2BC32E5AAD8FDB49FFD43F94A
SHA1:	B2CD5F8A87D637F5C6E2C87C5CE4C459F9C7476E
SHA-256:	C507957165F8EFB8BBD112C908FCADEB73E9C692A74F5029C760F2833DC91C3D
SHA-512:	F98ADC890C978F2F0EBF298A459196C5CA846791B93219E20B6850CE9DC5F4F4A4795CC47815B0A048B423C261F5DA18D9CC8DD48C8582974E6F2162672F9B5
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xb5fcbe9d,0x01d7a66e</date><acc date>0xb5fcbe9d,0x01d7a66e</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>0xb5fcbe9d,0x01d7a66e</date><accdate>0xb5fcb e9d,0x01d7a66e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.09846477693444
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGw84l74lMnWimI002EtM3MHdNMNxhGw84l74lMnWimI00OVb8K075Es:2d6NxQ20MSZHKd6NxQ20MSZ7VYKajb
MD5:	8558B33EC3D187F4FEF608A562E12D80
SHA1:	C23BFD2A6FF524C8A9715E511AADE7098557E533
SHA-256:	BCC0B19E079D29D80757A892E266CBA59A1995B3DC3A35ECAD56734F3BBA2C90
SHA-512:	4C4899BB375B036EA6E4A1EFD368DB3A7B35C35C5183F47100E67294E333812B174DB5F76DE6DBEEEF2CE8274A9BF71D7E266CB7CC902576479A8F70E573F78 B
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xb603e652,0x01d7a66e</date>< accdate>0xb603e652,0x01d7a66e</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>0xb603e652,0x01d7a66e</date><accdate>0 xb603e652,0x01d7a66e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.070985183767182
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n84l74lMnWimI002EtM3MHdNMNx0n84l74lMnWimI00OVbxEtMb:2d6Nx0D0MSZHKd6Nx0D0MSZ7Vnb
MD5:	94B687BCE7F42C5FCE98156DCCFE1165
SHA1:	EA18499D3B3777B83145C8110A688BDBE3536772
SHA-256:	6CDFB7D1E0467264EE8C0418794EAADE5209140F06B5721B921F4FC81BD7EE93
SHA-512:	844CD404DEFA95E66544CBE8CF705313587932E32BB694CA967ED66B70C483D816042A2C18D35BC29D3A0DA2BA08DE54DDFCEEE8BC56DF45B4DBEBC870135 AD1
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xb603e652,0x01d7a66e</date><a ccdate>0xb603e652,0x01d7a66e</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>0xb603e652,0x01d7a66e</date><accdate>0xb 603e652,0x01d7a66e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.109499180513016
Encrypted:	false
SSDEEP:	12:TMHdNMNxxjBtBRnWimI002EtM3MHdNMNxxjBq4lMnWimI00OVb6Kq5EtMb:2d6NxRBtBRSZHKd6NxRBtMSZ7Vob
MD5:	D1BB70C7AEC00622B4B93AAF50742418
SHA1:	3D191B22DE45823A85E2B2151842F88EA2DD159B
SHA-256:	F25615F8A56F3B23763B8A7DD15C1C117909C685F3B7CAF6D071107EA2FCC28D
SHA-512:	16B4312C6D7E2410B88035B923CC410CE6C80D1C17F8C58981E1E73BFEFE387E76FBAAEB1BEF9659CFC31C5890C582E64BA9F1966C50C0DBE728246A18ACE3 F
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xb5fcbe9d,0x01d7a66e</date><accdate>0xb5fcbe9d,0x01d7a66e</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>0xb5fcbe9d,0x01d7a66e</date><accdate>0xb603e652,0x01d7a66e</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):	662
Entropy (8bit):	5.0736778920006635
Encrypted:	false
SSDEEP:	12:TMHdNMNxcjBtBRnWimI002EtM3MHdNMNxcjBtBRnWimI00OVbVEtMb:2d6NxQBtBRSZHKd6NxQBtBRSZ7VDb
MD5:	8FFB06B03840C41C277CF7B6C3EDF51C
SHA1:	1ABDF733FB6F9183040F0443B3206FBBBB0BB692
SHA-256:	E53959D9D9012CBD7602EA6E30B632AF76113536B96855F7D88602B2E770BC17
SHA-512:	2D9DF8B20A60115E9F3414823CF4BCFA432D6DEF3CF992EA797BE5F5E8D83702A8D8961EE85F1F1AC67C6AAA6C3732DBB913AD4DBA2B4A766842104EA3527E87
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xb5fcbe9d,0x01d7a66e</date><accdate>0xb5fcbe9d,0x01d7a66e</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>0xb5fcbe9d,0x01d7a66e</date><accdate>0xb5fcbe9d,0x01d7a66e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.061334817329456
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnjBtBRnWimI002EtM3MHdNMNxfnjBtBRnWimI00OVbe5EtMb:2d6NxLBtBRSZHKd6NxLBtBRSZ7Vijb
MD5:	8A8289DB3625D7AFB565EC722F6AA989
SHA1:	2551F20C55637F97DCE84BA7A9B74F5C06C474AD
SHA-256:	537D95D201DD28532C259CAC26D3A9E917CBBE6B4D39B25FA265B291D139802D
SHA-512:	71D9011162826FB05745B5FA32F94E824809588AD2155D91436853D3257FE86F51BC19F2DB6527CE4C6C8B1B97B3734EAB3781E7DE438ACF169959D94584CEB7
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xb5fcbe9d,0x01d7a66e</date><accdate>0xb5fcbe9d,0x01d7a66e</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>0xb5fcbe9d,0x01d7a66e</date><accdate>0xb5fcbe9d,0x01d7a66e</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
Malicious:	false
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet 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\9QTQHWWN\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D
Malicious:	false
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #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\9QTQHWWN\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\dnserror[1]	
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vllJ6G7Ao8Ra
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\9QTQHWWN\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vllJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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(); initMo reInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";....//used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.su bstring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var pound Index = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	89
Entropy (8bit):	4.45974266689267
Encrypted:	false
SSDEEP:	3:oVXUp0f2c8JOGXnEp0f2TLun:o9UpGqEpU
MD5:	2255590FBF7B2B2DE3B8ABF420E87CE1
SHA1:	49D48DC36BAC1FE9D0AC98A2C981451B3A3B213F
SHA-256:	9230DC2F04354883072E5A1F94D04C9F618E863937CAC067992C5500F937E91C
SHA-512:	540B6B368FD1173F9635D3E05B936F713593123A44738FCC9C25E9D8AC8DCEC38607BA952BFA10578FA444C964EB0C5142FBF4DA653B24783CF93B040210A945
Malicious:	false
Preview:	[2021/09/10 11:07:58.739] Latest deploy version: ..[2021/09/10 11:07:58.739] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF54FE3B7C7FD18873.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data

C:\Users\user\AppData\Local\Temp\~DF54FE3B7C7FD18873.TMP	
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4085493096259837
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo/9lo/9lWsSKMJ:kBqoIg+J
MD5:	EBBDD5B53D8E906796F7500DD2255B8D
SHA1:	134C6ED30946D5C9B8D052EF9D3F5D6FEEE45602
SHA-256:	578F3EE53F83BF3D32B9D77EE25801BF0F7885C1878BD52DA67151936CCFFE70
SHA-512:	F96DFD204FB925AEC0381AB1F9F204A1888A54300671D0B3142B5DC1C7954262DB1940F9A5853D9A877EC8AC7392B28D484C3CA4F8F48299CFBE010020E2605D
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF849AFB3A04ECE3BF.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38737
Entropy (8bit):	0.37139184013210086
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+Ye0F5I5wTyDZTyDbTyDU:kBqoxKAuvScS+Ye0FO2KQN
MD5:	D02335560B534BE6D104EB2EB3FB9272
SHA1:	3C720A2CB2EEC0F62A256E4FA314E5CD2195312F
SHA-256:	1602942D59034772849BAE5AF52258B4D4EFA68E4F0172BB634E09A4F551617E
SHA-512:	878F942F89977EFABDA185E151D19DA95B64C4696EC0E72A1043FEED165706BA4D1CD95C2CB9F7C9B11A70125173D8D706938732089399D18D5E8AA5CA21A93
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF9956526A696EBC76.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.40921707933435686
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fR29l8fRm9lTqRQQlF3RQlU1:c9lLh9lLh9lIn9lIn9lo29lom9lWJRqK
MD5:	E579AF038EA387295A731A257EA4BC05
SHA1:	9AF1A8BF9BDF61AEEE4C4264C454414A36B8D1C4
SHA-256:	6B2DA325B9D1F280C27A0E08061DD874D86BBD80A8FF4A2282A36FF2F04471EA
SHA-512:	2B55CCF8366BF98FC6C5D83662C0E360B0CF4B92A91EC277C6527ABA1EB03E1C47D7B3E83BF4BC61E3309D1DCB45E783E63130821C01584FD32BAA8FB0E28E 78
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFD9B906886E0EC1C2.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38737
Entropy (8bit):	0.3715571594200072
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+QWMNxIxw3yDZ3yDb3yDU:kBqoxKAuvScS+QWMNWu+EB
MD5:	7AC15FDA26FE401C71736DE922177826
SHA1:	FCC5B6B4616DE0E693444C8720BDBA92E4EB8FB9
SHA-256:	2A0C19E55C64CB545BC8A80D78C406AD56B6477CAE0EBC9866A0E4155D1913CE
SHA-512:	7B2AE9C4B42A1EC744B01B7040179785CF5F90B167EBC13340E5D06B2707E535B5936B45BBD7EEA8BB56B4B74AE70D7A116C20CE8290915EE9F0F33CCF28FD1 D

C:\Users\user\AppData\Local\Temp\~DFD9B906886E0EC1C2.TMP	
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.61438464019549
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:	CGd7lq6RDL.exe
File size:	901960
MD5:	c7b71f03f190a5da3e4976f37194419f
SHA1:	8e750d01e1a5edb2c320e1b0b703b5823f241587
SHA256:	930d54df724f1637f38d840e1822fa8f5cccedceb4b86d0e737e2311162e0921
SHA512:	d274bcc78a5916220e51036b8a24b82f165a03736fb829a76a01d96bd5c224b0624b3ebf592a5b06a5bd9d04cc5c7aff0e47bca908782dd27b226fb953f2cc6e
SSDEEP:	24576:v9PsA9vHAYobFGQdRPylSk61LXXh5xvZjmtk1/GqgLGS:QYyJk61bRnZjmWGGS
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.........p.............`.......`.......`..........o............`......m8.......`.......`.......`......Rich...........................

File Icon

Icon Hash:	f0b0e8e4e4e8b2dc

Static PE Info

General

General	
Entrypoint:	0x1005725
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x1000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x55E85856 [Thu Sep 3 14:25:26 2015 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	264c61a35ad2f260d533f2d7b897c2a5

Authenticode Signature

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

Signature Validation Error:	**No signature was present in the subject**
Error Number:	-2146762496
Not Before, Not After	• 4/12/2021 5:00:00 PM 4/13/2022 4:59:59 PM
Subject Chain	• CN=FORTH PROPERTY LTD, O=FORTH PROPERTY LTD, L=Edinburgh, C=GB
Version:	3
Thumbprint MD5:	8AB6A86211EE700AA961C3292ADB312D
Thumbprint SHA-1:	A533DFA7E6AED2A9FFBE41FCEC5A8927A6EAFBBB
Thumbprint SHA-256:	9E0611728595A506CC2A55486FDD88ECA0971EF0B08F74CB3B3B6F5F6F3C7E27
Serial:	239664C12BAEB5A6D787912888051392

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x681b9	0x68200	False	0.623956613896	data	6.85142771967	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x6a000	0x23f8a	0x24000	False	0.641723632812	data	6.36645327435	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x8e000	0x1e3ac	0x7a00	False	0.527792008197	data	6.51367686644	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xad000	0x41028	0x41200	False	0.240744211852	data	5.36312234805	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xef000	0x4d50	0x4e00	False	0.730168269231	data	6.65913941378	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 10, 2021 11:06:55.753245115 CEST	192.168.2.6	8.8.8.8	0x8a0a	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 11:06:55.787014008 CEST	192.168.2.6	8.8.8.8	0x12f1	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 11:06:55.827631950 CEST	192.168.2.6	8.8.8.8	0x1e50	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 11:07:07.075915098 CEST	192.168.2.6	8.8.8.8	0x1875	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 11:07:17.181979895 CEST	192.168.2.6	8.8.8.8	0x5c25	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 11:07:59.157938004 CEST	192.168.2.6	8.8.8.8	0xa945	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 11:07:59.203895092 CEST	192.168.2.6	8.8.8.8	0xb867	Standard query (0)	haverit.xyz	A (IP address)	IN (0x0001)
Sep 10, 2021 11:07:59.246572971 CEST	192.168.2.6	8.8.8.8	0x195d	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 11:06:55.780266047 CEST	8.8.8.8	192.168.2.6	0x8a0a	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 11:06:55.822834015 CEST	8.8.8.8	192.168.2.6	0x12f1	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 11:06:55.860533953 CEST	8.8.8.8	192.168.2.6	0x1e50	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 11:07:07.111475945 CEST	8.8.8.8	192.168.2.6	0x1875	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 11:07:17.209393978 CEST	8.8.8.8	192.168.2.6	0x5c25	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 11:07:59.194992065 CEST	8.8.8.8	192.168.2.6	0xa945	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 11:07:59.235157013 CEST	8.8.8.8	192.168.2.6	0xb867	Name error (3)	haverit.xyz	none	none	A (IP address)	IN (0x0001)
Sep 10, 2021 11:07:59.282083988 CEST	8.8.8.8	192.168.2.6	0x195d	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: CGd7lq6RDL.exe PID: 6948 Parent PID: 6008

General

Start time:	11:06:27
Start date:	10/09/2021
Path:	C:\Users\user\Desktop\CGd7lq6RDL.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\CGd7lq6RDL.exe'
Imagebase:	0x1000000

File size:	901960 bytes
MD5 hash:	C7B71F03F190A5DA3E4976F37194419F
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: 00000001.00000003.385018366.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.384548084.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.383601456.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.385072202.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.384483225.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.384261011.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.385265307.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.385224495.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.384337083.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.383794745.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.385278956.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.383290755.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.385120189.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.385245280.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.384188109.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.384802369.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.383702783.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.383888043.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.384673722.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.384849581.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.385191377.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.383501926.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.384938347.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000002.606209100.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.384982348.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.385155225.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.384003623.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.384615803.0000000003610000.00000004.00000040.sdmp, Author:

	Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.384747658.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.383189063.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.384415120.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.384102374.0000000003610000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.384895266.0000000003610000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 6672 Parent PID: 792

General

Start time:	11:06:53
Start date:	10/09/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff721e20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 6824 Parent PID: 6672

General

Start time:	11:06:54
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:6672 CREDAT:17410 /prefetch:2
Imagebase:	0x910000
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: 5656 Parent PID: 792

General

Start time:	11:07:57
Start date:	10/09/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff721e20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 6136 Parent PID: 5656

General

Start time:	11:07:58
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:5656 CREDAT:17410 /prefetch:2
Imagebase:	0x910000
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