ID: 498857
Sample Name: 0f.dll
Cookbook: default.jbs
Time: 15:51:49
Date: 07/10/2021
Version: 33.0.0 White Diamond

Table of Contents

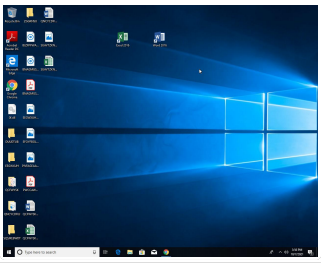
Windows Analysis Report 0f.dll

Overview

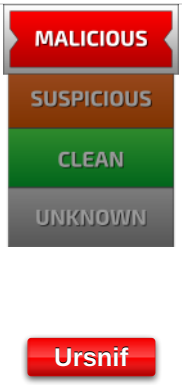
General Information

Sample Name:	0f.dll
Analysis ID:	498857
MD5:	0f90b21a2cdc355..
SHA1:	1293aa454365b3..
SHA256:	95dbbfc33223e8e.
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection



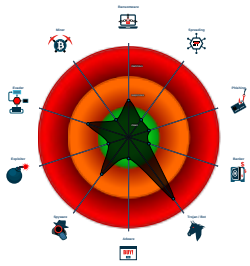
Ursnif

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

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Multi AV Scanner detection for subm…
- 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…
- Creates a DirectInput object (often fo…
- Uses 32bit PE files
- Antivirus or Machine Learning detec…
- Contains functionality to query locale…
- Contains functionality to read the PEB
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5268 cmdline: loaddll32.exe 'C:\Users\user\Desktop\0f.dll' MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 5160 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\0f.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 4760 cmdline: rundll32.exe 'C:\Users\user\Desktop\0f.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 2316 cmdline: rundll32.exe C:\Users\user\Desktop\0f.dll,Start MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 2988 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 2964 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2988 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"YspyHla3Q+Y+mL+jkDMPo0K37HDx3ZQpkC6iMQ9FB0Jvz67qLEuPPd+7itRbk+5jPXxEvcc4HELzBbK+zEpcnk3gfkFepE47XU1UkIqwsz5EFKG4uDfy9jLX4cSD4IKUeWVT2AmhhkhIjXebeVqL2cavKIWzE+O11PlMSJB8CPxu3rcoXlZgOw7DYBYyTHdQlEkgzTqDwlIzW3bdSDtO0jlb1GqIU5jAVZj0nusFmwufXbMRHKThAuzV0SiB8H0jceNWGALcy01VeCV7PJrnPe8wCvy64gODn28q2topDihJ51KGWbMNR5jWjFp/LTmfqJ9+UqlA3XrMm4Ht2D3DJEE72pdtZyqrd+EuqZEvdjw=",
  "c2_domain": [
    "app5.folion.xyz",
    "wer.defone.click",
    "app10.laptok.at",
    "apt.feel500.at",
    "init.in100k.at"
  ],
  "botnet": "2500",
  "server": "580",
  "serpent_key": "lOrlLLFRkSMi2UOq",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "10"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000003.739535676.00000000040A8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.706311406.0000000005BB9000.00000004.00000040.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000001.00000003.739521647.00000000040A8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.739458564.00000000040A8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.739502896.00000000040A8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.loaddll32.exe.38f94a0.3.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.2.loaddll32.exe.10000000.4.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.2.loaddll32.exe.f60000.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.2.loaddll32.exe.38f94a0.3.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
4.2.rundll32.exe.11f0000.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 6 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Found malware configuration

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

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Writes or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

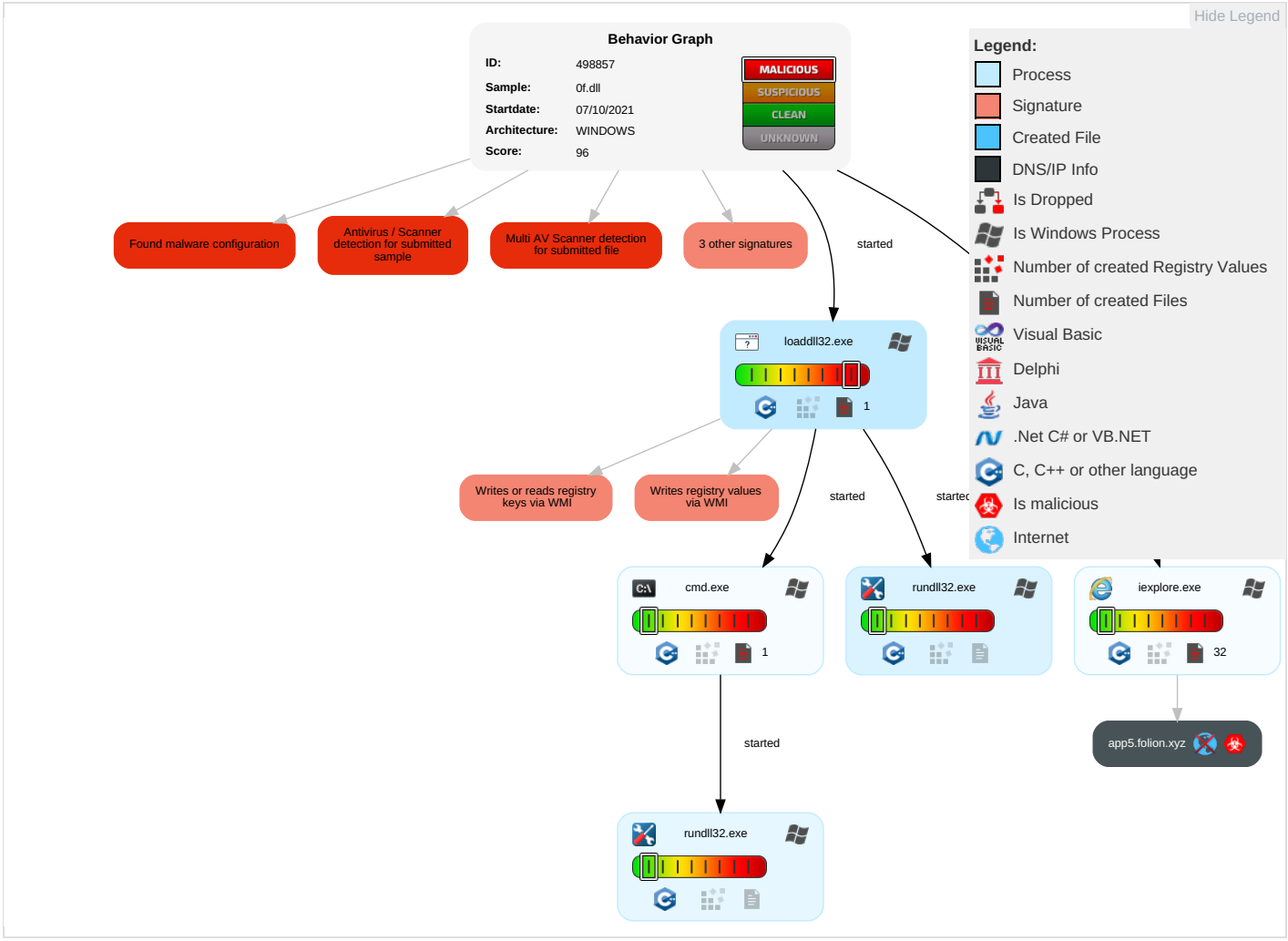
Remote Access Functionality:

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	Network Effects	Rem Serv Effe
Valid Accounts	Windows Management Instrumentation 2	Path Interception	Process Injection 1 2	Masquerading 1	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Rem Trac With Auth
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Rem Wipe With Auth
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Account Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obta Devi Clou Back
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	NTDS	System Owner/User Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 3 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

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
0f.dll	24%	Metadefender		Browse
0f.dll	79%	ReversingLabs	Win32.Trojan.GenericML	
0f.dll	100%	Avira	TR/AD.Ursnif.uxgkb	
0f.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.loaddll32.exe.f90000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
4.2.rundll32.exe.5150000.2.unpack	100%	Avira	HEUR/AGEN.1142655		Download File
5.2.rundll32.exe.10000000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
4.2.rundll32.exe.1370000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
5.2.rundll32.exe.4af0000.1.unpack	100%	Avira	HEUR/AGEN.1142655		Download File
1.2.loaddll32.exe.2e90000.2.unpack	100%	Avira	HEUR/AGEN.1142655		Download File
1.2.loaddll32.exe.10000000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File

Domains

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://app5.folion.xyz/C6VmqHmn62rFCww6y4ysR/P0nI5lbrE_2FoyZm/BDBmvveWjO3LK9Q/55XxQq6CmCPdNvBaEz/m5n	0%	Avira URL Cloud	safe	
http://app5.folion.xyz	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
windowsupdate.s.llnwi.net	178.79.242.128	true	false		unknown
app5.folion.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:	498857
Start date:	07.10.2021
Start time:	15:51:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	0f.dll
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:	mal96.troj.winDLL@10/19@3/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 61.2% (good quality ratio 59.3%) • Quality average: 80.6% • Quality standard deviation: 27.3%

HCA Information:	• Successful, ratio: 59% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:55:54	API Interceptor	1x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
windowsupdate.s.llnwi.net	KVx62u3gsv.exe	Get hash	malicious	Browse	• 178.79.242.128
	rKQTea8DKe.exe	Get hash	malicious	Browse	• 178.79.242.0
	NESMA RFQ EQUIPMENTS AND DOCUMENTS REQUIRED.doc	Get hash	malicious	Browse	• 178.79.242.128
	6dfce00750c09d7a9927dab4bed6b81a4043fab36fba5.exe	Get hash	malicious	Browse	• 178.79.242.128
	GT09876545678.exe	Get hash	malicious	Browse	• 178.79.242.0
	REVISED PI 7-10-2021.xlsx	Get hash	malicious	Browse	• 178.79.242.128
	FACTURA.exe	Get hash	malicious	Browse	• 178.79.242.128
	uNCouz6hx8.exe	Get hash	malicious	Browse	• 178.79.242.0
	cBPH5n4T38.exe	Get hash	malicious	Browse	• 178.79.242.0
	DcF5xuhMNO.exe	Get hash	malicious	Browse	• 178.79.242.0
	BSQ4wRQciB.dll	Get hash	malicious	Browse	• 178.79.242.128
	Factura Pendiente.exe	Get hash	malicious	Browse	• 178.79.242.128
	nEwkr1dC74.exe	Get hash	malicious	Browse	• 178.79.242.0
	uN85v8VI8X.exe	Get hash	malicious	Browse	• 178.79.242.128
	OXkB3xMeAr.exe	Get hash	malicious	Browse	• 178.79.242.128
	new price quote inquiry FOB sgz67889 dfx46667.exe	Get hash	malicious	Browse	• 178.79.242.0
	IokJ1Ttx1O.dll	Get hash	malicious	Browse	• 178.79.242.0
	eZCQoOpWRX.exe	Get hash	malicious	Browse	• 178.79.242.0
	x1Y6mEs1uM.dll	Get hash	malicious	Browse	• 178.79.242.0
	DeqrIfxzHW.exe	Get hash	malicious	Browse	• 178.79.242.0

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.{C5D724C1-27C1-11EC-90E9-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7726504473662315
Encrypted:	false
SSDEEP:	96:rlZyZqS2qwVWqwi35ytqwi35pRSfqwi35pXR0xMqwi3D9pXjDqw33D9pXAB:rlZyZN2vWBtWSfu0xMeDOB
MD5:	94F9B5C28E9B149EB46ADF9F2AEF671C
SHA1:	D980F86F0CB9D559D4511FE48DF6DC551FA7EE8E
SHA-256:	18C6860293D7ED805DAE18A5C77E6B816ECF9C7952B6588E2E5278CCA7E9B7BB
SHA-512:	BC178D27576935281ED3E3F4F6EB34D4E3E843AFCC54569766CB5A97189B3E2FC9CB8FFD5C63EE6D437F41F2F1AC71360BFAA5CC670A62B144A8EFFC9E3B482
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{C5D724C3-27C1-11EC-90E9-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28124
Entropy (8bit):	1.9114461517774022
Encrypted:	false
SSDEEP:	192:rUrZmmQhn6P7kcjB2NWIMc9Rh8CVslgh8CVcA:rU9mzh6PAOwktYRh8CVQgh8CVX
MD5:	AEB3A15AEDBCF9FB5FA5B95E2DEB6649
SHA1:	ECFA0B9E79EE11ACA8CB3E5D5A3650CEC7471C19
SHA-256:	0FD03A33686DDBC1905354E97A0449F8E2937910F7C545F13F55FDBA1F0D5099
SHA-512:	C2AC69F2D0EC27A8353FA1E60B4C4AE96EC0812CB3A2E2CEE7C57B9E7AFF420D7B781B1DBAD33A2CD6CD26EC83B318EFA79CC4855D69D13D5B6BC9788BCD739F
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.107543499804657
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEWCnWimI002EtM3MHdNMNxOEWCnWimI00ObVbkEtMb:2d6NxOWSZHKd6NxOWSZ76b
MD5:	DC395B2AEFBEDD9A677BD175271E1437
SHA1:	878FD1F33DF98EF507658F2A95279CC4ED1B7539
SHA-256:	9FDD3722C364EE0FB6936FA96D61709E1C800150A8C22B43760D1D0250D1181B
SHA-512:	941CC2033EB271DFC340CFB7C936F425B4B9293F79FAA99DD7584B4090FF78BB301878AEF6978003F7E045D75546E42E357AE102C84724C67D1A51D805427644
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x9b4f4795,0x01d7bbce</date><accdate>0x9b4f4795,0x01d7bbce</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>0x9b4f4795,0x01d7bbce</date><accdate>0x9b4f4795,0x01d7bbce</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):	653
Entropy (8bit):	5.145246967420208

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kL8ijnWimI002EtM3MHdNMNxe2kL8ijnWimI00Obkak6EtMb:2d6NxrGzjSZHKd6NxrGzjSZ7Aa7b
MD5:	B75797E660E655043C9F8ABB4B4D25B6
SHA1:	E726052E9AB9C4C81B05049B04E399017A0C512E
SHA-256:	D6477BBF5E39AA393F596BBD590C2977F5652E08AF0C78F557E8CC788CF13858
SHA-512:	185AF0953A8DBFAF81564B0411908AAAB8E3FB9D73C09573541B2B87BC1366628493A7BA632A9861BC788132DFCAE4ADF7D87F6ADE2D3A737AEDACEB768E8E68
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x9b482054,0x01d7bbce</date><accdate>0x9b482054,0x01d7bbce</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>0x9b482054,0x01d7bbce</date><accdate>0x9b482054,0x01d7bbce</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):	662
Entropy (8bit):	5.119905113075047
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLD8GjnWimI002EtM3MHdNMNxvLD8GjnWimI00ObmZEtMb:2d6NxvfSZHKd6NxvfSZ7mb
MD5:	2544FD05527C054C8DF3BA23EE41EC7B
SHA1:	E831E81CC7D44B0136DCDB28B43D205F7ACB2373
SHA-256:	B01039E1F635638B2F6EA1E9A71206D07523634A4F7320C9BCA1CBBAAB1EA218
SHA-512:	631A1F882E0CBC94CF2DFB723FCA701959F14C70641A7E27DD8ACA1421312DE649277C101CD74827307A18156919C29CE686C5E9721F01E017D6BA1958AD668
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x9b566f66,0x01d7bbce</date><accdate>0x9b566f66,0x01d7bbce</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>0x9b566f66,0x01d7bbce</date><accdate>0x9b566f66,0x01d7bbce</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):	647
Entropy (8bit):	5.123486204812417
Encrypted:	false
SSDEEP:	12:TMHdNMNxiWCnWimI002EtM3MHdNMNxiWCnWimI00Obd5EtMb:2d6NxESZHKd6NxESZ7Jjb
MD5:	E0B40BCD3C29E9C1843BBF53A62255A3
SHA1:	E4ACD05178FA797D64DBF9E4C97BF38D9995F726
SHA-256:	30E079AA2536B1FDE438410443824E67DA7996D7B788BA171191004E96666421
SHA-512:	A44146F71F634E7AF699D20EFECAD2889B3CC476B46FBAEEC762CD11C305F1013A0278A3C0770635E8E3808E4AC61D50B32C8259D5B8063788DB20A92F2A6BCA
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x9b4f4795,0x01d7bbce</date><accdate>0x9b4f4795,0x01d7bbce</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>0x9b4f4795,0x01d7bbce</date><accdate>0x9b4f4795,0x01d7bbce</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):	656
Entropy (8bit):	5.127001735722792
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwD8GjnWimI002EtM3MHdNMNxhGwD8GjnWimI00Ob8K075EtMb:2d6NxQmSZHKd6NxQmSZ7YKajb
MD5:	2A79317507DCC843A39E305AF8AFDE32
SHA1:	70A060E42DCFA217398616C5745D15446B2505C1
SHA-256:	AF625B0D3CDA31324047ED4ABC78F4B15C73AFA5E26082A7164196A30BEBD9DE
SHA-512:	7FCBDAD8CA0C438FC1327D8D4950B471492EFBFACCD2C2B8186CAB5AFDC7BE909CACCC7F97B6DF38B97397660848BF2AD2F6A93AE49F37D118F583123915F67

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x9b566f66,0x01d7bbce</date><accdate>0x9b566f66,0x01d7bbce</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>0x9b566f66,0x01d7bbce</date><accdate>0x9b566f66,0x01d7bbce</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):	653
Entropy (8bit):	5.110774963400463
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nWCnWimI002EtM3MHdNMNx0nWCnWimI00ObxEtMb:2d6Nx0zSZHKd6Nx0zSZ7nb
MD5:	BE0E56E5768CB1791890ED689C01B1BE
SHA1:	3A1A25EAC0B613D8EA41AD6DA0130FEBBDD2DFE4
SHA-256:	DC668F7C29E2F40537610A5D7D7FC3C77F6E6DDED2657488D35880B946703D7A
SHA-512:	982C545F3416C26C80852796D3320FCF36759EA0F32DEDA695634D6BCC4D92D3B02E9856FCE981014679A1F2F9760A7EEB64AEA0AFEE1637199C62296A0F79C4
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x9b4f4795,0x01d7bbce</date><accdate>0x9b4f4795,0x01d7bbce</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>0x9b4f4795,0x01d7bbce</date><accdate>0x9b4f4795,0x01d7bbce</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):	656
Entropy (8bit):	5.147967201075354
Encrypted:	false
SSDEEP:	12:TMHdNMNxxWCnWimI002EtM3MHdNMNxxWCnWimI00Ob6Kq5EtMb:2d6NxlSZHKd6NxlSZ7ob
MD5:	F74D7428F32B2F62DE287ACC75B6D49A
SHA1:	BFA99A67ECC10AC006FAB791E7F97147458C66F4
SHA-256:	DE3EE199535C258A56FDB933EE6665804B4207B36D88EFA7ED3DCAF8449BD1B6
SHA-512:	F91DB48C540AF354BF54375F87D3B4308FF10AFA69884F607EF39217D559AF4EE10DA1DDA2746B3C2FE7A42F8616DC8D4501A8475D52F3BE04034DA3CABF99F
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x9b4f4795,0x01d7bbce</date><accdate>0x9b4f4795,0x01d7bbce</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>0x9b4f4795,0x01d7bbce</date><accdate>0x9b4f4795,0x01d7bbce</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):	659
Entropy (8bit):	5.134325724897167
Encrypted:	false
SSDEEP:	12:TMHdNMNxcL8ijnWimI002EtM3MHdNMNxcL8ijnWimI00ObVEtMb:2d6NxuzjSZHKd6NxuzjSZ7Db
MD5:	0B59888F018D85C6AF868C51B39B0603
SHA1:	3F61342FFB6A4D827187B09D6E013CB480889FAA
SHA-256:	0008F44CA9738270DFFF72E1FF1ED004C5DDE062A4A430E94CEF86F8F2F72DB2
SHA-512:	940277E01D5EE301866E29AC126EA88A2AEF94604AA612C6882D3052255C23A61239BB074D9E516A8B4B382BB029FABAFFDAA2863804EE0258DA364C2810C5A
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x9b482054,0x01d7bbce</date><accdate>0x9b482054,0x01d7bbce</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>0x9b482054,0x01d7bbce</date><accdate>0x9b482054,0x01d7bbce</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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.123476990133076
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnL8ijnWimI002EtM3MHdNMNxfnL8CnWimI00Obe5EtMb:2d6NxTzjSZHKd6NxTJSZ7ijb
MD5:	C0CECA743047E53995B308329C42B758
SHA1:	80F5FA1AB8CF709D2DEA1DDE221C9F5AB9656F0C
SHA-256:	B1BB9FE8C5741A24D45511004CEA2B082CA438DB2B8028777E6A640E86313A0F
SHA-512:	DBD1F04B3E3D5240AD9E07FD632C7EC1A57412A852932D605722F80632041CF647CE05A5BFB4F579B53279C00CA0B36CDBA2C41B89B9840F4D1F3519B48F556
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x9b482054,0x01d7bbce</date><accdate>0x9b482054,0x01d7bbce</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>0x9b482054,0x01d7bbce</date><accdate>0x9b4f4795,0x01d7bbce</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\0W10PBUV\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\MEEXW4H4\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....#+....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\PSUEOSZZ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\dnserror[1]	
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\PSUEOSZZ\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\WJ8I2OL4\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\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	89
Entropy (8bit):	4.39783508257439
Encrypted:	false
SSDEEP:	3:oVXUYzKQTfFphW8JOGXnEYzKQTfFpbLun:o9UYzKQTX0qEYzKQTXbC
MD5:	96CE80CB02C302A441DE74AF8A06EED5
SHA1:	3AC02A600B79AF8ABAFD5C57CC1A996915FC21FC
SHA-256:	48026BED77C076952F9F5AC2FAC05B4840EBABC3D4F26E23424CF27ED1E9D87C
SHA-512:	75B05A3627467E68DA9FF10CF9C8F923E4E77F99629C99674B5991C7ED040866A018F92E053CA047ECDD17ECCCE836BBB37E79AFBE5671CB5D6B65DFB2FB4FB
Malicious:	false
Preview:	[2021/10/07 15:56:16.503] Latest deploy version: ..[2021/10/07 15:56:16.503] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log

C:\Users\user\AppData\Local\Temp\~DFA1D11EC49A94A948.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40121
Entropy (8bit):	0.6662066462562781
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+AGcdGLRh8CVZRh8CVaRh8CVP:N8G8B8W
MD5:	A10F00C96C90A98D5AD726F315D7E8EC
SHA1:	DDC4214284F24081022316EAB9A06F30D7F20A33
SHA-256:	5CD7342F83768F33EC03EED2017C885D7AF4D2C88F569514BAA896D409935B37
SHA-512:	1DB71E92C872F324D337B5DEA3D7D1C106AB59000B98E55C0D1EC3C3B4FA3DD326E666B5CF553ED63829908DA8FB80BF3F1AC78BF249CCF60A5BF16CCA4E581
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFCB4F6EF3903B6C34.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4079157710343825
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lol4YF9lol4g9lWl4P4Dh43Q4w4Dh4304M4x:kBqoIqrqNqwC33XC3DLx
MD5:	C93DA6F6188C47D44D61BA6CE2A636FE
SHA1:	A88F5F64B15D7C3D192BEA14E7273C0B82F48F74
SHA-256:	96CB17E675B019E40C198AA6F29DDF5BA747FA6F36916D120E963A61B48D675F
SHA-512:	3CF67AEDC23A7CD9710DF6DDAFE8FBBE99FAC8C9BE336B30588BFD1AB529F509BB3AB1F0518EFE16BC5B2E97B24F5E9258517B3215EFD28DA7ADE4DA7A1CEEBE
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	2.5822820478796022
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	0f.dll
File size:	397824
MD5:	0f90b21a2cdc35511626509c67c8cbf5
SHA1:	1293aa454365b3679afd77b34749ce8e175c997a
SHA256:	95dbbfc33223e8e670b4f25d086d65a41d67f0434d3fe37469a7bd23e134f1f6
SHA512:	0c46cceb3e716e995eb043e8f59b0883406954e6628602969a5c8c53088e018e2ae49f27942ee44aef0553d772c0fc33f33d974ce720dce8396ae85c89a11d3e
SSDEEP:	3072:/NCW8aQutBgN/+bz37UGw+24RwFBatjKqe0FucS:/1oig+TRwTYKqe

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....^7...Vl..Vl..Vl..I...Vl..v~..Vl.Rich.Vl.....PE..L.....m`.....I.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1000810a
Entrypoint Section:	.code
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x606D96B2 [Wed Apr 7 11:25:38 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	6a47c078cd001e32ce158eef785cbcae

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.code	0x1000	0x19e78	0x1a000	False	0.617760291466	data	6.43604242524	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1b000	0x49	0x200	False	0.1328125	data	0.802850919454	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rdata	0x1c000	0x673a50	0x45c00	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.data	0x690000	0xe70	0x1000	False	0.395751953125	data	4.74218170739	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Imports

Exports

Network Behavior

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 7, 2021 15:56:17.487533092 CEST	192.168.2.3	8.8.8.8	0xe998	Standard query (0)	app5.folion.xyz	A (IP address)	IN (0x0001)
Oct 7, 2021 15:56:17.519701958 CEST	192.168.2.3	8.8.8.8	0xa495	Standard query (0)	app5.folion.xyz	A (IP address)	IN (0x0001)
Oct 7, 2021 15:56:17.570930004 CEST	192.168.2.3	8.8.8.8	0x4ca5	Standard query (0)	app5.folion.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 7, 2021 15:53:32.710131884 CEST	8.8.8.8	192.168.2.3	0x4da5	No error (0)	windowsupdate.s.llnwi.net		178.79.242.128	A (IP address)	IN (0x0001)
Oct 7, 2021 15:56:17.510956049 CEST	8.8.8.8	192.168.2.3	0xe998	Name error (3)	app5.folion.xyz	none	none	A (IP address)	IN (0x0001)
Oct 7, 2021 15:56:17.542115927 CEST	8.8.8.8	192.168.2.3	0xa495	Name error (3)	app5.folion.xyz	none	none	A (IP address)	IN (0x0001)
Oct 7, 2021 15:56:17.589647055 CEST	8.8.8.8	192.168.2.3	0x4ca5	Server failure (2)	app5.folion.xyz	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 5268 Parent PID: 5800

General

Start time:	15:52:44
Start date:	07/10/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\0f.dll'
Imagebase:	0x800000
File size:	893440 bytes
MD5 hash:	72FCD8FB0ADC38ED9050569AD673650E
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: 00000001.00000003.739535676.00000000040A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.739521647.00000000040A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.739458564.00000000040A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.739502896.00000000040A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.739363916.00000000040A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000002.813265596.00000000040A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.739321134.00000000040A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000001.00000002.813125689.00000000038F9000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.739404580.00000000040A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000001.00000002.810063319.0000000000F60000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.739481698.00000000040A8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 5160 Parent PID: 5268

General

Start time:	15:52:45
Start date:	07/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\0f.dll',#1
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 2316 Parent PID: 5268

General

Start time:	15:52:45
Start date:	07/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\0f.dll,Start
Imagebase:	0x1380000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000004.00000003.706311406.0000000005BB9000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000004.00000002.706735766.00000000011F0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 4760 Parent PID: 5160

General

Start time:	15:52:45
Start date:	07/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\0f.dll',#1
Imagebase:	0x1380000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000005.00000002.809626071.0000000000A30000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: iexplore.exe PID: 2988 Parent PID: 744

General

Start time:	15:56:15
Start date:	07/10/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff62f1c0000
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: 2964 Parent PID: 2988

General

Start time:	15:56:15

Start date:	07/10/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2988 CREDAT:17410 /prefetch:2
Imagebase:	0x11a0000
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