ID: 498828
Sample Name: 50.dll
Cookbook: default.jbs
Time: 15:14:09
Date: 07/10/2021
Version: 33.0.0 White Diamond

Table of Contents

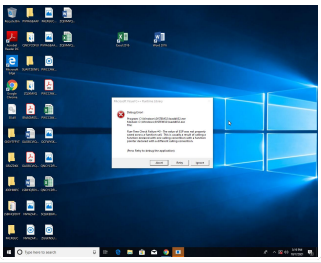
Windows Analysis Report 50.dll

Overview

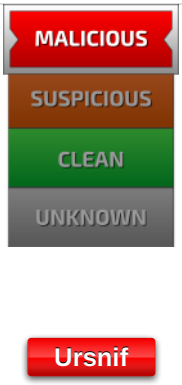
General Information

Sample Name:	50.dll
Analysis ID:	498828
MD5:	03a4adf216161ac.
SHA1:	5b37a2bdc58279..
SHA256:	e0e9821e1c172e..
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection

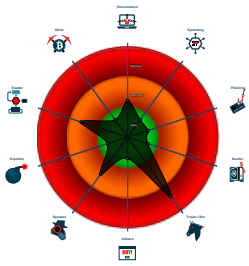


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for doma…
- Writes or reads registry keys via WMI
- Writes registry values via WMI
- Uses 32bit PE files
- Contains functionality to check if a d…
- Contains functionality to query locale…
- Uses code obfuscation techniques (…
- Queries the installation date of Wind…
- Internet Provider seen in connection…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5416 cmdline: loaddll32.exe 'C:\Users\user\Desktop\50.dll' MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 4604 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\50.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 3148 cmdline: rundll32.exe 'C:\Users\user\Desktop\50.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 3348 cmdline: rundll32.exe C:\Users\user\Desktop\50.dll,@DllRegisterServer@0 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5364 cmdline: rundll32.exe C:\Users\user\Desktop\50.dll,@DllUnregisterServer@0 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 3324 cmdline: rundll32.exe C:\Users\user\Desktop\50.dll,@Properwhat@8 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 7056 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 3644 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7056 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 6992 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 2332 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6992 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 3892 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4676 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3892 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 5580 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6336 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5580 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 6888 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6004 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6888 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "lang_id": "RU, CN",
  "RSA Public Key":
"spMgSJlMsbtyYJa7J98r3sDVnAauyYqUMJmfcOwftrNnR0Q/C00j0nLxLEQJJp6q/6NEKbKUj0/JgWKRbzzHEB4F6RQgzHtMFW3wSImU2nYZ9tLVzVwdEUFZI5FukXQ3NiY2htJmxqUn2twjM931KOxXZ4RzDvIB/4hTvpsWTDF+n4G7
YGtk1nZlke9r+CWY",
  "c2_domain": [
    "golang.feel500.at/api1",
    "api10.laptok.at/api1"
  ],
  "botnet": "2200",
  "server": "730",
  "serpent_key": "wyzQ2rMFkB7aXutb",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0",
  "dga_base_url": "constitution.org/usdeclar.txt",
  "dga_tld": "com ru org",
  "DGA_count": "10"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000003.479416380.0000000004CD8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.479376627.0000000004CD8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.621232674.00000000044C9000.00000004.00000040.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000000.00000002.804482994.0000000003F08000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.495439556.0000000003F08000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 20 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.loaddll32.exe.13a0000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.2.rundll32.exe.2590000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
6.3.rundll32.exe.51b94a0.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.3.rundll32.exe.44c94a0.1.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.4eb94a0.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 10 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for domain / URL

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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:

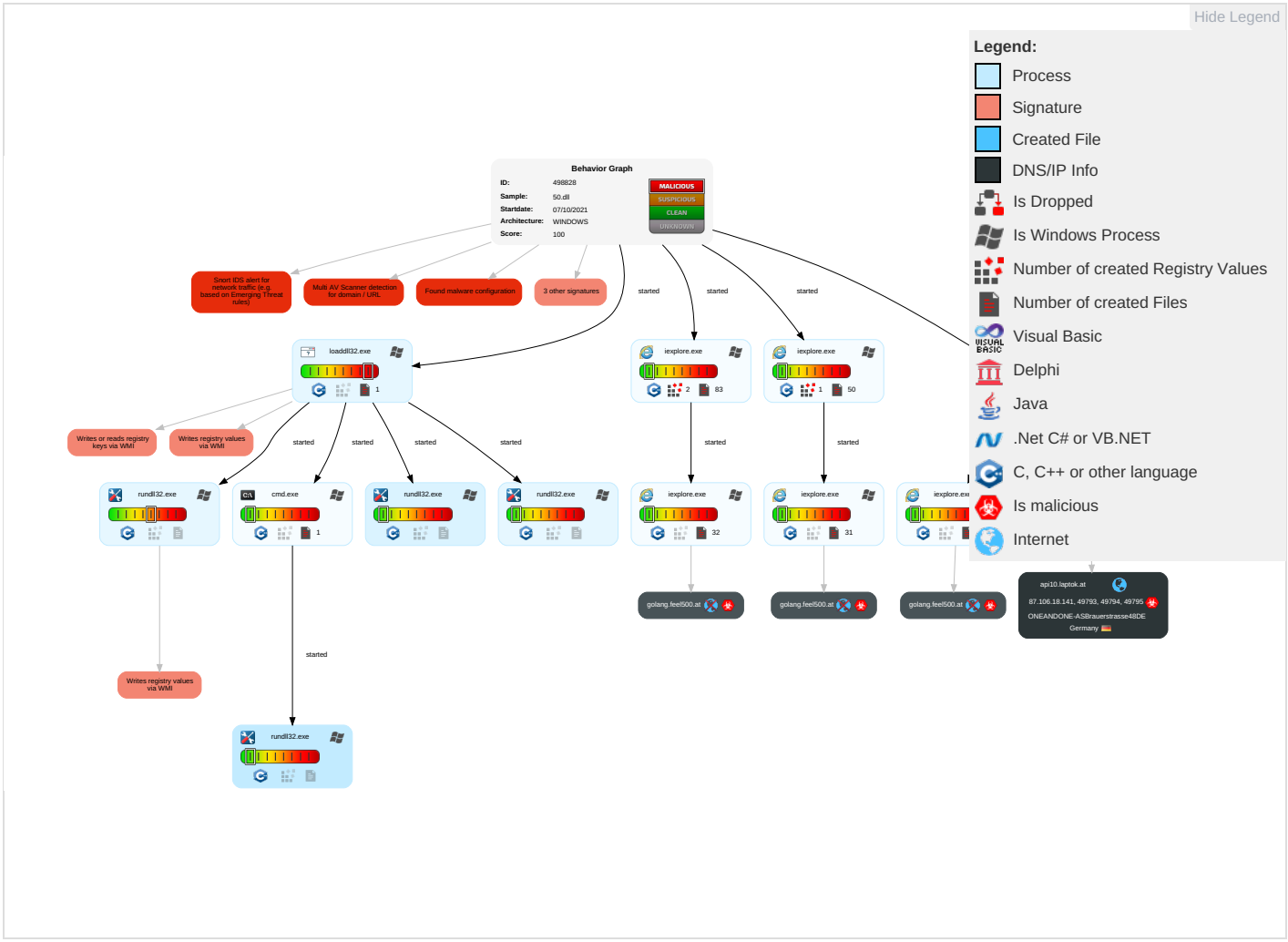
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	F S E
Valid Accounts	Windows Management Instrumentation 2	DLL Side-Loading 1	Process Injection 1 2	Masquerading 1	Input Capture 1	System Time Discovery 2	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	F T V A
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 1 2	LSASS Memory	Security Software Discovery 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS	F V V A
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location	C D C E
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Rundll32 1	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	F S E
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 2	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	System Information Discovery 3 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	

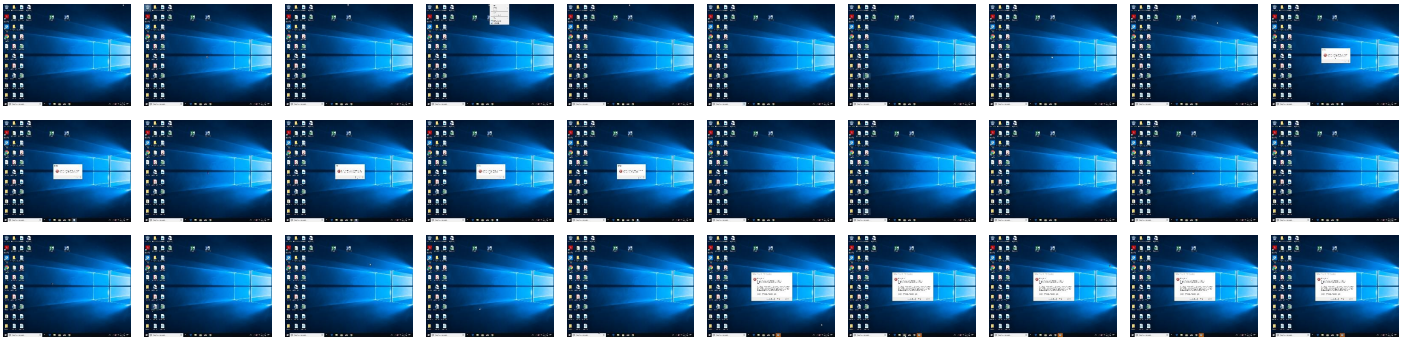
Behavior Graph

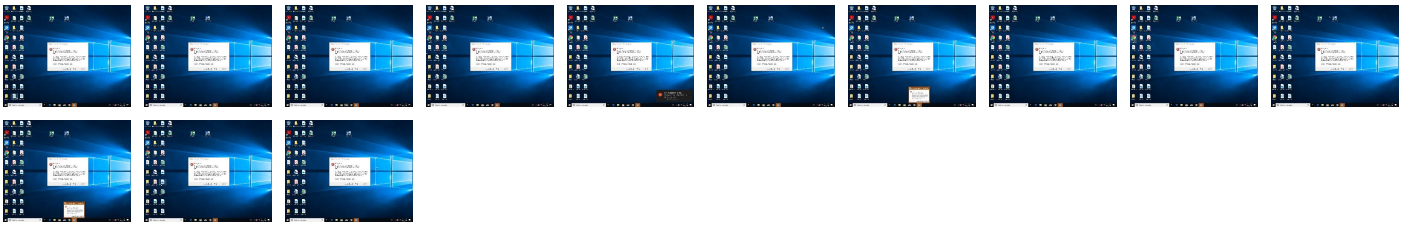


Screenshots

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
50.dll	60%	Virustotal		Browse
50.dll	28%	Metadefender		Browse
50.dll	71%	ReversingLabs	Win32.Trojan.Masson	
50.dll	100%	Avira	TR/AD.UrsnifDropper.yqyps	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
api10.laptok.at	14%	Virustotal		Browse
golang.feel500.at	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://api10.laptok.at/api1/Jq38ICaRqPy/g8cT5EDuzQRTfd/bDaQidhBmNREYWZABcNxO/6xll5SLapn_2FusJ/iHdi_2	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/Jq38ICaRqPy/g8cT5EDuzQRTfd/bDaQidhBmNREYWZABcNxO/6xll5SLapn_2FusJ/iHdi_2FbiOmTGGb/BXo7JAZFG1eu_2FtyI/cNFtxMNBR/zYGeZfeXbEOB1SyQFsvB/rB0Q_2FZQZ0YZi_2FRO/tidnHoD06Cgh_2FRad0Stl/qK8jV1z_2FTo2/PBtT0ki_/2BubNruXDtYtZ2wLQ_2BEya/1EtRRJfeUI/5CMi0T2vwqXTEyNz1/lyOJ_2BtNXg9/d_2B7LGgvGV/55GaKjfY_2FDfj/svm_0A_0DtNmhHj6ls2X4/2lW3OzRcv2PkceFw/VNJ6ep7w_2FRmj_2FWh4Js/N	0%	Avira URL Cloud	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://api10.laptok.at/favicon.ico	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/Jq38ICaRqPy/g8cT5EDuzQRTfd/bDaQidhBmNREYWZABcNxO/6xll5SLapn_2FusJ/i	0%	Avira URL Cloud	safe	
http://golang.feel500.at/api1/YLF22kb3qppYj0qV_2FrBA/gmsmY04uRW1XV/l2QyGLGA/GtEQ6XjZAWGXWxCNpGcTaDx/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api10.laptok.at	87.106.18.141	true	true	• 14%, Virustotal, Browse	unknown
golang.feel500.at	unknown	unknown	true	• 11%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://api10.laptok.at/api1/Jq38ICaRqPy/g8cT5EDuzQRTfd/bDaQidhBmNREYWZABcNxO/6xll5SLapn_2FusJ/iHdi_2FbiOmTGGb/BXo7JAZFG1eu_2FtyI/cNFtxMNBR/zYGeZfeXbEOB1SyQFsvB/rB0Q_2FZQZ0YZi_2FRO/tidnHoD06Cgh_2FRad0Stl/qK8jV1z_2FTo2/PBtT0ki_/2BubNruXDtYtZ2wLQ_2BEya/1EtRRJfeUI/5CMi0T2vwqXTEyNz1/lyOJ_2BtNXg9/d_2B7LGgvGV/55GaKjfY_2FDfj/svm_0A_0DtNmhHj6ls2X4/2lW3OzRcv2PkceFw/VNJ6ep7w_2FRmj_2FWh4Js/N	true	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/favicon.ico	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
87.106.18.141	api10.laptok.at	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	498828
Start date:	07.10.2021

Start time:	15:14:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	50.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:	40
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:	mal100.troj.winDLL@26/49@11/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 23.7% (good quality ratio 22.3%) • Quality average: 77.9% • Quality standard deviation: 29.3%
HCA Information:	• Successful, ratio: 68% • 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

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
87.106.18.141	08dVB7v4wB6w.vbs	Get hash	malicious	Browse	• chat.allager.at/jvassets/xl/t64.dat
	http:// far.gaploop.at/api1/m9Nm6sQ5MZ2/kV1dHuUchwgj0p/w9B514uuWuNRu_2Fovw1B/iJjn_2FjOcMhSdO6/hY1viFbhIYH_2BS/FrMYbmCHgkAwm_2Btu/e29igvEBi/gLOHtqdBI_2B3sibC3Cg/z_2F8IFoCH_2BWJVdUY/ri7hwzyuAx2q5RHXJmbXhc/ygopWPWJKwti5/IOOS1u46/4ZXFc4Ok4SPekiO7ot2QyT_/2FJdMyYfAP/7FTqw0rQZL_2B1pan/wh8ruTp3dham/UlLIzAZ_2Fn/esHGZHp93qljV_/0A_0DvFEgD08oveRu1RDL/3nPBhZLduxccr2_2/FS5iRLSxGBo44/0xUc	Get hash	malicious	Browse	• far.gaploop.at/api1/m9Nm6sQ5MZ2/kV1dHuUchwgj0p/favicon.ico
	4EyIHmLYEBBs.vbs	Get hash	malicious	Browse	• chat.allager.at/jvassets/xl/t64.dat

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
api10.laptok.at	11.dll	Get hash	malicious	Browse	• 35.228.184.80
	documentation_27396.vbs	Get hash	malicious	Browse	• 35.189.93.117
	info_70397.vbs	Get hash	malicious	Browse	• 35.189.93.117
	SecuriteInfo.com.Win32.Kryptik.HJSQ.12709.dll	Get hash	malicious	Browse	• 35.189.93.117
	SecuriteInfo.com.Trojan.Win32.Save.a.30469.dll	Get hash	malicious	Browse	• 35.189.93.117
	22.dll	Get hash	malicious	Browse	• 34.65.108.95
	2200.dll	Get hash	malicious	Browse	• 34.65.108.95
	urban.dll	Get hash	malicious	Browse	• 34.65.25.23
	SecuriteInfo.com.BScope.TrojanBanker.IcedID.dll	Get hash	malicious	Browse	• 34.65.15.6
	SecuriteInfo.com.Generic.mg.3964ec2fe493ed56.dll	Get hash	malicious	Browse	• 34.65.144.159
	SecuriteInfo.com.Generic.mg.f76b81b0397ae313.dll	Get hash	malicious	Browse	• 34.65.144.159
	SecuriteInfo.com.Generic.mg.f77e7bd43f365593.dll	Get hash	malicious	Browse	• 34.65.144.159
	NJPcHPuRcG.dll	Get hash	malicious	Browse	• 34.65.144.159
	Ne6A4k8vK6.dll	Get hash	malicious	Browse	• 34.65.144.159
	File_78476.xlsb	Get hash	malicious	Browse	• 35.228.31.40
	u8xtCk7fq8.dll	Get hash	malicious	Browse	• 35.228.31.40
	2200.dll	Get hash	malicious	Browse	• 35.228.31.40
	SecuriteInfo.com.Trojan.Win32.Wacatac.Bml.dll	Get hash	malicious	Browse	• 35.228.31.40
	Attached_File_898318.xlsb	Get hash	malicious	Browse	• 35.228.31.40
	Presentation_68192.xlsb	Get hash	malicious	Browse	• 47.89.250.152

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ONEANDONE-ASBrauerstrasse48DE	Quote -0071021.exe	Get hash	malicious	Browse	• 217.160.0.7
	DHL SHIPMENT.HTML	Get hash	malicious	Browse	• 217.160.0.196
	hwIILTIn0n.exe	Get hash	malicious	Browse	• 217.160.0.17
	just.exe	Get hash	malicious	Browse	• 212.227.15.158
	2WK7SGkGVZ.exe	Get hash	malicious	Browse	• 74.208.236.156
	0n1pEFuGKC.exe	Get hash	malicious	Browse	• 74.208.236.145
	VmbABLKNbD.exe	Get hash	malicious	Browse	• 74.208.236.108
	Update-KB250-x86.exe	Get hash	malicious	Browse	• 74.208.5.20
	Update-KB2984-x86.exe	Get hash	malicious	Browse	• 74.208.5.20
	justifi4c.exe	Get hash	malicious	Browse	• 213.165.67.118
	CY2075400.exe	Get hash	malicious	Browse	• 213.165.67.115
	Justificante de la transfer.exe	Get hash	malicious	Browse	• 212.227.15.142
	IMAGE1001.exe	Get hash	malicious	Browse	• 213.165.67.115
	Exq3dXFDHe.exe	Get hash	malicious	Browse	• 217.160.0.243
	MIN8gr0eOj.exe	Get hash	malicious	Browse	• 74.208.236.228
	solicitud de presupuesto.exe	Get hash	malicious	Browse	• 217.160.0.21
	Payment Requisition October 4.xlsx	Get hash	malicious	Browse	• 74.208.236.226
	ZFQ06Cz6TT.exe	Get hash	malicious	Browse	• 217.160.0.48
	justificante de la transfer.exe	Get hash	malicious	Browse	• 212.227.15.158
	DHL_Online_Receipt.doc	Get hash	malicious	Browse	• 74.208.236.241

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{391FBB81-27BC-11EC-90E9-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7671859583920144

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{391FBB81-27BC-11EC-90E9-ECF4BB862DED}.dat	
Encrypted:	false
SSDEEP:	96:r8ZfZ6D26soW6sy3zt6sy3Fxf6sy3FPCVM6sy3TBP/a6sv3TBP/B:r8ZfZU2KW2tyf3VMYajB
MD5:	9209EAE3279AC2632916580688128590
SHA1:	901CC40A9F371BA45651EF85872EBBACFB20AFC3
SHA-256:	12BBBDF5F2B1BC161F903CFE8EE991C037F3E162053DCD0225127A6DB15D724D
SHA-512:	91C775683D95C75FBCAB3FE75B834D16D214B5FE46C5436C2705B0C091C674752CA8089AF710139FA4E93CD2E06D287528ACD317CCDEDA5FCB74251EF9EC16 8
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{531DF9CA-27BC-11EC-90E9-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7741769984095097
Encrypted:	false
SSDEEP:	96:r0ZTZvH2v/kWv/Z3Ntv/Z3eMFfv/Z3em27EAMv/Z3iSmJ84tLsov/G3iSmzlqB:r0ZTZf20W7t9fcRMmHUB
MD5:	152CAA28B65E3A45B85101AE5126DC5D
SHA1:	294F05F91972C1B70894BE60A591AFBFF4903038
SHA-256:	D542F8D642B5E28208759CC5CCA3CD784EC922A056CFE093881CDBD2ED366898
SHA-512:	A3A529E8667AC1E8916F95FB2F1BA70B39016562E4B583B184182F1C53885D5767DCD79192063EA2360389D2A5B71A05CD1B9BB1D759D813B97E80D7DB889EEA
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{57B5605C-27BC-11EC-90E9-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7711462578805588
Encrypted:	false
SSDEEP:	96:reZpZal2aO6WaOI3DtaOI3z9faOI3zTWRMaOI33PTXoaOz33PT9B:reZpZ22WWCtsftRMWoBB
MD5:	9F9833212C5E9817F794703F10445DEF
SHA1:	26F8E909E6680294702D19E1BAFFFA065E7B1FB2
SHA-256:	7356A72ECD8003BCACFBB6932A60F2094B87B4EA1A4DA6489F09CEDC45B80DC4
SHA-512:	AA3F5B7B19CB37BF8E0A59E1C243DD32D5CA37D8DE3B5FEB54CA526B38CCCF162F49A2DF9760C4E852B6257204F87ACE9E8EE7F7E55B52245258F511DD0D7 C7
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{60EB543E-27BC-11EC-90E9-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.772265508005362
Encrypted:	false
SSDEEP:	96:ruZ1Z3B23nxW3nx3Wt3nx3Ejf3nx3EquFM3nx3uAqqF3nK3uAqaB:ruZ1Zx2BWgtwfmFMpFcB
MD5:	72ECE26DBB9A78B7E7B10E6A7EB18E12
SHA1:	4200701E0E0A8B97EB84275D2F3179A6A71889DA
SHA-256:	0C005DC1275F8B3743AB25E3F01FE3073DE2DEDF9D4C25320CC1B525B5EE00C3
SHA-512:	0C5474DC63C2563835C14D70AE07041EBD45A50F7270DA56F2EA56A82CCF40C145768A15D3218FAAEA22EC17119FEB22BB3AB6CC4C367A62D3B371EE89D70B A
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{60EB543E-27BC-11EC-90E9-ECF4BB862DED}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{654BE4A9-27BC-11EC-90E9-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.766403454897482
Encrypted:	false
SSDEEP:	96:rjZ0Zrc2rx3WrxT3DtrxT3NefrxT3N+tlMrxT3qp+Uk/Xrxe3qp+P0B:rjZ0ZA2dW1tCfglM3fDB
MD5:	A2DA837EF8E44D6066F39FC2C5AB8344
SHA1:	A2163278AE2B2DDCFCDD3407F8C3D2245D14272D
SHA-256:	2CB6FAD41B545B9DEE032D3EE9E55A05522529FC56B133E92F88A6866BD53487
SHA-512:	AF1477EB47897925871E8F4BE179B03DB3484B80050F99C0C63F1793175A27F629CF8BB2F61D61DFE3E2365947915A58C817D136FBBA6FF45951425DA6AAEDCB
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{391FBB83-27BC-11EC-90E9-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28132
Entropy (8bit):	1.9127599655484808
Encrypted:	false
SSDEEP:	192:rJZiQF6rkOjx2VWIMYCmZDdiEAyZSDdi4A:r/PwwIgstcZTZSK
MD5:	C0F79B2CFBB0EF0E29C18856F7AF8A5E
SHA1:	2FFAA171EA1F12D3F51B4E5BF859371A355317AA
SHA-256:	094721AB6B007155A44DE1A5858ACD3262868CCC4514AD563D26303D6AD61A08
SHA-512:	FF09BA7618A864917A62152FF3078B0D1261F4E40603D38322D627C34321372A52CF4E3FE2C645B4B6D07BF29FDC1C100A901D240F7EE4B245C0E82F03B79D22
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{531DF9CC-27BC-11EC-90E9-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28164
Entropy (8bit):	1.9260382633891415
Encrypted:	false
SSDEEP:	192:rWZVQ567kmjx2lWYvMVqViH3qMDJvViHEH3qMDJBA:rSKUAgg8YkVOiH3q4iHEH3qx
MD5:	52BA7C2A651F7BE462F5658189C9D057
SHA1:	79024D0C933882D0E7A36B87C8EE4BDA14EAD041
SHA-256:	07A30F5B29F2FED1F44D84F99FDB7D03BC00B877CA25290D9FB9BC16F667D935
SHA-512:	E698FE3ABF742178622FC7A61755104549B7AA84E6F22BED564A76CED65298DDAB50A6588B4AD6722B90EB13D81247134632C02D76FCCABE007756E79FCAB31
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{57B5605E-27BC-11EC-90E9-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27592
Entropy (8bit):	1.9156973078754163

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{57B5605E-27BC-11EC-90E9-ECF4BB862DED}.dat	
Encrypted:	false
SSDEEP:	96:r8ZRQ567BS+jV2lWlfMe6B0Vllp6l0VllpcV1A:r8ZRQ567k+jV2lWlfMe6BikliCA
MD5:	B5DEB904336437E2DEBDDBC23C6055FF
SHA1:	6B48F712B640701E43E03F922F9D8DFC85DE63A8
SHA-256:	96051E804562B509D1BF8F7B5FA6C03EDAF7F248AAD674C9323057E2B779CE5E
SHA-512:	F79D736C1FC0037D008273F72336DA7D0E9FA717CE8518FA3FF6DBECA4044DDAB1E6713CA4B6C94ACACCC000C932D6D11B736A0C63D2D3E962B9C28A59CE8 15
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{60EB5440-27BC-11EC-90E9-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28140
Entropy (8bit):	1.9187067585244182
Encrypted:	false
SSDEEP:	192:rqZJQB6XkmjFn2FbWFgMFQNXUZezelXU3cezt4A:rWucUgF2FyF1FcXhqXevBb
MD5:	A6C76D6C29F8165E5A1FFDB71D60871C
SHA1:	9CAD9FC162A428A1A9A6D9760079492A5A385540
SHA-256:	38ADFB366FD3E4FA4E805236EE100687873D74D3779716623C725C4015B2E399
SHA-512:	0F42FCF15DCA505FE564A969F9661E4B4850239D36FD3F00372F0D1DD7428646C30BFADD79C9AC381559585C2CAF93CBF557ECF69332507D6C78A6D9A86386E
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{654BE4AB-27BC-11EC-90E9-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28152
Entropy (8bit):	1.9222727393523877
Encrypted:	false
SSDEEP:	96:r7ZUQA6SBSmjR2FWlMRxtSDjvd2p5kstSDjvjDjvd2pQ4A:r7ZUQA6SkmjR2FWlMRxuUp5luLUpTA
MD5:	02CD78794142B261DFC91EA448CCBF31
SHA1:	543870E71426C5AAF61836B584812A96B9E6A446
SHA-256:	29D605E80CEEE45B9531561FD1910753D35A9B9238FD2BE55A41AB0DC85C3B12
SHA-512:	A29131D5D5AE0B985670D84B4035D94ECC5D3F103476885636F0BBBF7D8FC634CD6FD4E6F75096BD6497088DB8951210875489EFCE213A51F05447FE65E56B70
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):	5.040920354804753
Encrypted:	false
SSDEEP:	12:TMHdNMNxOElG4oqG4nnWimI002EtM3MHdNMNxOElG4oqG4nnWimI00ObVbkEtMb:2d6NxOeG4oqG4nSZHKd6NxOeG4oqG4np
MD5:	2B16AADA42D1B1D5A38A03CFF0AC0DA7
SHA1:	46A5FB0C844FE8DC7B3189ECCDF7091BC9550DBE
SHA-256:	170D75FDE23833A80C9BE56DD29A61A22FA7C68563E8A3D5F816D09580ACB2E7
SHA-512:	A8C239EEA8993EB2AD6FAFB91E6953F6347686798AD4CBA499C227ABDBCA780C7D737E6A51D246E7DD20A95E0BD96531B8026A3165FA952770835273AD27955
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x0ed20c0d,0x01d7bbc9</date><accdate>0x0ed20c0d,0x01d7bbc9</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>0x0ed20c0d,0x01d7bbc9</date><accdate>0x0ed20c0d,0x01d7bbc9</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):	5.116344047260175
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2k4dl9BdlMnWimI002EtM3MHdNMNxe2k4dl9BdlMnWimI00Obkak6Es:2d6Nxr179B7MSZHKd6Nxr179B7MSZ7AS
MD5:	F61301BB91342CC794746636BB5771D2
SHA1:	A59399DD7FFC48C9F636B202C53758F1C5956FF3
SHA-256:	85B84EC1AE06E8333B53F5B9C74A525C0980CDD4BC1AB3EBDAA46F6FBEEDC6D7
SHA-512:	E9525B7206ADB1DF721224044D6BAE0734F97C34EAA4738541BE61B7509F55EBC3612D42DE24115D6C84777CB806F19350A41C1833204EF765873BEACA696813
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x0ec88392,0x01d7bbc9</date><accdate>0x0ec88392,0x01d7bbc9</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>0x0ec88392,0x01d7bbc9</date><accdate>0x0ec88392,0x01d7bbc9</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):	5.111861488801107
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLIcnWimI002EtM3MHdNMNxvLIcnWimI00ObmZEtMb:2d6Nxv0cSZHKd6Nxv0cSZ7mb
MD5:	A9536414C0EC35670D89764EF1AC7B7C
SHA1:	EE58FB2E9E2A1755578E27938BDF2D9CEF4161F8
SHA-256:	5C6C57F02BEF2FE1C748E86D168D43F43F3969F92EDB9D74545A480AEFD4AAC4
SHA-512:	642C6D12F8CF9062D63DD6B0FC6DA791FABE19F75483B687F9FADC941AB96850B072D3902F1CD49A3D8E47A85E609D20269185C2D6181E8987DC4FEB95D6EDB
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x0ed932f5,0x01d7bbc9</date><accdate>0x0ed932f5,0x01d7bbc9</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>0x0ed932f5,0x01d7bbc9</date><accdate>0x0ed932f5,0x01d7bbc9</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):	5.055936308181912
Encrypted:	false
SSDEEP:	12:TMHdNMNxilG4oqG4nnWimI002EtM3MHdNMNxilG4oqG4nnWimI00Obd5EtMb:2d6NxEG4oqG4nSZHKd6NxEG4oqG4nSZ5
MD5:	2AD0C9D4415C7FFF68B643E23220411F
SHA1:	76863C2FCAB19A75D0A19B1C4551C180BCDD377A
SHA-256:	F220F1DFC7E20643FED56720271FE6EE251F8671B3A71B60173436B08BA008C5
SHA-512:	1C4344F80ED78438C1EB6CECCA25471C34F71054A3B0C3CC9AC0B9B7295D8316F0CAC2C63662D464CD2024BB9B8D9A8AD3A3DB80AA1E66650D083569E7FAB46
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x0ed20c0d,0x01d7bbc9</date><accdate>0x0ed20c0d,0x01d7bbc9</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>0x0ed20c0d,0x01d7bbc9</date><accdate>0x0ed20c0d,0x01d7bbc9</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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.12189605752625
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwIcnWimI002EtM3MHdNMNxhGwIcnWimI00Ob8K075EtMb:2d6NxQVcSZHKd6NxQVcSZ7YKajb
MD5:	15230B4213E11682E3FC025BE12A7100
SHA1:	68AB26F9E75F0340B158696F0FFE31A5462425CC
SHA-256:	7C9A3A595A2A9C537C52ADC0739EB4407D775479578A7BDA9439C7064725EB46
SHA-512:	1346DF8697EB126248AC94B61479BDC2937E7C6789876D10E8C25A64F320DB78E6A4EBDF86ED3DDA6E51532275AB4860E7A5959D52A7442DDB56E769E61517E
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x0ed932f5,0x01d7bbc9</date><accdate>0x0ed932f5,0x01d7bbc9</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>0x0ed932f5,0x01d7bbc9</date><accdate>0x0ed932f5,0x01d7bbc9</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):	5.039360863385906
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nlG4oqG4nnWimI002EtM3MHdNMNx0nlG4oqG4nnWimI00ObxEtMb:2d6Nx0lG4oqG4nSZHKd6Nx0lG4oqG4nI
MD5:	F0AB12241C4580B19982A410A9A04A04
SHA1:	73ED57DA5C0701DFA71BF6D484A898F0AB41FC4B
SHA-256:	09C0B7AF4F6829D3F74ADFA0CBC2A938D0A0302C4CF0606252CD642EEBA0EFB5
SHA-512:	319C9FE3F4BCA342D60579A3B76B8FB1C5C8A5C95AE11FBD2B0C0991EE1772180597C1085626C7B39B2087AFA5525F0DB10169FFEA66DECF44B8B92C8EB3B2 4
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x0ed20c0d,0x01d7bbc9</date><accdate>0x0ed20c0d,0x01d7bbc9</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>0x0ed20c0d,0x01d7bbc9</date><accdate>0x0ed20c0d,0x01d7bbc9</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):	5.081344056075451
Encrypted:	false
SSDEEP:	12:TMHdNMNxxlG4oqG4nnWimI002EtM3MHdNMNxxlG4oqG4nnWimI00Ob6Kq5EtMb:2d6NxvG4oqG4nSZHKd6NxvG4oqG4nSZ6
MD5:	3C555F3DD99378421AE73BDD90AF9A5A
SHA1:	7AAC028E56FAF91971828036EDD350FCDE42E418
SHA-256:	61AAA0C2A330052756F58C2841B372FA9E7A92ED8C894BC04EDC729D2C08527B
SHA-512:	AB0175811070ABB6070178F313E8139F1EF2CE8F1A1E71317CC9BF7654297B8056D6F2E2A706FA78F318B05057ABEC15F036D2A78BFED16865C421CA85B63EBD
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x0ed20c0d,0x01d7bbc9</date><accdate>0x0ed20c0d,0x01d7bbc9</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>0x0ed20c0d,0x01d7bbc9</date><accdate>0x0ed20c0d,0x01d7bbc9</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):	5.1066330360173335
Encrypted:	false
SSDEEP:	12:TMHdNMNxc4dl9BdlMnWimI002EtM3MHdNMNxc4dl9BdlMnWimI00ObVEtMb:2d6NxN79B7MSZHKd6NxN79B7MSZ7Db
MD5:	125E062B512CDE919E9736470AF2B0EE
SHA1:	2B3DFB992B0DF64691C3FAEFBCDF12B9FDAFE49C

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
SHA-256:	E59B9F4CA80C0EEA35586C0C593C04188618B97A96080374800B1A8FDCBBA4C8
SHA-512:	8ABC97C6AADE306965EAE84F6F3CCB687DBE93AECB9524ECA378971E06648BAF867547FD966A0EEB988FAA7ADC7C554295FFA4B2CCFBB483DAE244D6351F589E
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x0ec88392,0x01d7bbc9</date><accdate>0x0ec88392,0x01d7bbc9</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>0x0ec88392,0x01d7bbc9</date><accdate>0x0ec88392,0x01d7bbc9</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):	653
Entropy (8bit):	5.0421069558252425
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnlG4oqG4nnWimI002EtM3MHdNMNxfnlG4oqG4nnWimI00Obe5EtMb:2d6Nx9G4oqG4nSZHKd6Nx9G4oqG4nSZa
MD5:	53F94EFBA358D9AB4FC69DD095D0EEF8
SHA1:	E2347A13E23FB9EF3574D612BC7E205482C657F7
SHA-256:	79C76FA69C53DC7E4E418C9064BC945EAF85B610248A0456A2DBB865205A31C2
SHA-512:	70AD340A5153F40B950FC46F66A4C9EABB8D3E6AAF122D78556343153E4F1FA4C41723F5C81A7BCAA96F09D799F9ECBABE80C899C7D6DC06D83981B958B4F505
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x0ed20c0d,0x01d7bbc9</date><accdate>0x0ed20c0d,0x01d7bbc9</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>0x0ed20c0d,0x01d7bbc9</date><accdate>0x0ed20c0d,0x01d7bbc9</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\0W10PBUV\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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\0W10PBUV\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\0W10PBUV\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.su bstring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var pound Index = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493 AC6D
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(); 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\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....#+....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\PSUEOSZZ\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D
Malicious:	false
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #00 0000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\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
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493 AC6D
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(); initMo reInfo('infoBlockID');">.. .. Can’t reach this page .. <div class="taskSection" id="taskSection">.. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address <span id= "webpage" class="webpageURL">is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\down[1]	
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\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\PSUEOSZZ\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\WJ8I2OL4\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\down[1]	
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\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:	modified
Size (bytes):	89
Entropy (8bit):	4.45974266689267
Encrypted:	false
SSDEEP:	3:oVXUYzKUS59X6Fi8JOGXnEYzKUS59X6FZun:o9UYzKUSjqFiqEYzKUSjqFZu
MD5:	3873E593E1934969F5926C13BFEE66F9
SHA1:	3B82F081F2FBEDFC8B86988B4DA73505E76268A9
SHA-256:	235FC7D5B4516318DD3F5EB58BA6DA1BF2E99430B422D02DE391CF681D223D8C
SHA-512:	A36071FBAF1763DDAECBCF8EAEBF0559979C3551E50CCCF6BA87EC6E9FF2E895D32BD281C7F511B5CD74F8FD32B6C9D8083CB155BEF7F4B0B8EEB0DDDBBB8328
Malicious:	false
Preview:	[2021/10/07 15:17:46.828] Latest deploy version: ..[2021/10/07 15:17:46.828] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF0FD44A9046836784.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4090730852277953
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo3YF9lo3g9lW3sU/53Eq/53uAx:kBqoI3r3N3n/53Eq/53uAx
MD5:	4424ED0732D7B13F792CA43D85C5537E
SHA1:	52BEC0FAAF21A348BE6EF0A7A1950CC02AE0F761
SHA-256:	F031C482728659DF537260765815F088CE7262656AF8A1274D08B5BA5F161EEC
SHA-512:	8A137169BD136EE865CE5D20679BDAC08B74D07C372718B54A8E2D0EDE07EBB30E3CDDC0BFBD910644AA188D0F1EC0421F448A91074ED22BEB52C37B9E45FAD6
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF1FC87509FACB1AE5.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40177

C:\Users\user\AppData\Local\Temp\~DF1FC87509FACB1AE5.TMP	
Entropy (8bit):	0.6759162670930271
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+pHVEnOtJsDjvd2pOtJsDjvd2pMstJsDjvd2pe:kBqoxKAuqR+pHVEnObiUpObiUptbiUpe
MD5:	105FC8363C4F2B383C9D87AE12D3B6F7
SHA1:	3946A1DC57A770DE2BFD3A0F5C46B952CBBED388
SHA-256:	0A6ECFE1EFF015E01B8387814C892C65B77CFF09661DFDB14823091422AFDBB5
SHA-512:	07AB089D54F2AF75271BDB4D720ED1B69541703B67CD04126A650FED874A9B94BBD998E73816FA993BA89DFF6D6C68231D8A9A5E1ABB926F1F0262CF5AE24E3 7
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF3A2D95194B6E56C4.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4070097347943249
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lln9lln9lorYF9lorg9lWrxz3N+z3qkYx:kBqoIrrrNrxz3N+z3qpx
MD5:	8DD8549101EA31B20DE9CAA33E494DEF
SHA1:	6B63C1D3F92DF9A0D4056827F43DA55B7968AB27
SHA-256:	AB53172A6B0839E568EC4F72515E36FE14C54670218CA2238D435DA449E54B72
SHA-512:	7BBC6C095FD33080AFC5D90748EA8D83F034D11F30DBE6816CD219E31A030741F9D5D595E1C36B7CCAA45688CFA6C3C434DEAF102FCAEC666B5513A6D7504E 1
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF4BC159430978B235.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4103658984651203
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lln9lln9loaYF9loag9lWa7Ko3HTTo33DTx:kBqoIaraNaOo3zTo33Px
MD5:	ADAD04E19A7B2F0F98CCBA72C3109DD7
SHA1:	F8B70831718581E7522EC400D1101029D7B77DA6
SHA-256:	4CF8C5D721114247B9A827B31452B34BA3B7463C443D837AA77264891A789DAA
SHA-512:	3D3C957DFCC91EEC5CD25CB46D02AD97D76B7DE15982D4A5FDE853AA816FD3C0F23D367696240469F24378B9B5C3D42069C47C9945501A6B3AEFBAF7AE334E 5
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF614A578B8A0039D2.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40201
Entropy (8bit):	0.6820865447942543
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+MqwRaPoNH3qMDJnoNH3qMDJAoNH3qMDJt:kBqoxKAuqR+MqwRaPiH3q2iH3q5iH3qq
MD5:	01837F3500E010DA204417219CF40F3A
SHA1:	5300E7DD0E93ED6186C6604D346DAC648BC3D576
SHA-256:	0BB4C60955DAF7AB952609C2F12E49CC7A81DF2DDF4B22F8E2BB143CEF6D65A6
SHA-512:	283C95E3A38932718B80D2892B0E6781C3C61A7B2FE46D82C8EDE47CEC19A63120E0AAE5415B36D87199EFFB36B2C492CE5D4F9486212C3D9A866E3BB8C660A 7
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DF614A578B8A0039D2.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF724E8AB2918CB9FB.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40137
Entropy (8bit):	0.6659647436059842
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+Ddvmtlm3JDdiom3JDdixy3JDdiR:kBqoxKAuqR+DdvmtMZEZHZY
MD5:	50426BF40EB19BE2D8AB973861D3B862
SHA1:	05C7AC8B548A968350A1B8046A7555AEAF45FACC
SHA-256:	E295AAB9E9B30391591F2C741AA48C9EB4B614C519209A35AA20A0917B34B44A
SHA-512:	B27A1183024B1C1861F6F57E75BE6F20AB6388E900B3184DFE3AA0C2E47D2D9AD379248BD22D262787C4A6B1A1983FF2E4D33A636232130AB476DDFB7EAA281
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF91CFCEBEAE749A87.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4101528862094827
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lokUYF9lokUg9lWkU/53M7Tm53i47Tx:kBqoIvrvNv/53Mnm53i4nx
MD5:	D3E17153E374EB42DA249B89E19CCC9D
SHA1:	E431E2356EBC6C6DCC3A6C66E7241FC005C237D9
SHA-256:	D48ED09CCF435C020B708552DA0223E604B23A2B888585C90C3480BF96A2DA08
SHA-512:	8058BD76384B0136A4B08FC40D7AC866868AAB8EF81655EF973C5CC8A2E2AAF983002E12382DC7BAB186DC515CF6C16409D73D30034338B65F5E4CF22CBE116
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF9E71909E92B794F9.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40081
Entropy (8bit):	0.6592702145716053
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+4+UluHmPVllpEmPVllpDmPVllpM:kBqoxKAuqR+4+UluHmlemlNml+
MD5:	CF5E1077CA891CB0FC5A5371994EA7A4
SHA1:	DC4D89A6D8F0803F1A37F0C4C5E8955905DE1C7C
SHA-256:	BB1A7A0C2CB3B83B25BEC3BAE7C21B6660BA03D91EAC929055DA7F5D5E4BA02A
SHA-512:	A8F282B093CF026191D20A8AFF066E7F008361BE3CB04295CF7AA45C38A866A7121975D37276710FC2F02E1684E1E42BD16D6C36065ABD3FA7F7616A5209A2D8
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFB26ED506A2ACFD75.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.40645366442558867

C:\Users\user\AppData\Local\Temp\~DFB26ED506A2ACFD75.TMP	
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo6YF9lo6g9lW6vUS3FPS3TBx:kBqoI6r6N6vUS3FPS3TBx
MD5:	6363274396A80C0D545ACDE52E13C6CC
SHA1:	69BC5DCAB07B01B1AF12F4266EDDFF88C199B20E
SHA-256:	D175243C58EF103FD15B57BF0F68B84E3D6B3CB550A72DBC807084540C39F571
SHA-512:	BC756689673A5516B44214D7D6509049FF12A9F673309C4EE474697919174EBFA9F6802DDAC3ADE4190A713033D1DE95A5E39BB46A8BE5037D4025B412C334F4
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

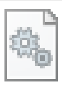
C:\Users\user\AppData\Local\Temp\~DFE194E450F56592B9.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40153
Entropy (8bit):	0.670314920418402
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+FuFoFCFLFYFRXUBvezQXUBvezTXUBvezk:kBqoxKAuqR+FuFoFCFLFYFRXhMXh3Xho
MD5:	3BC585FD3C5B18CA6438E27A656EFC7D
SHA1:	D6AA2B2A21658F630E1BA65A3D11800BC768F524
SHA-256:	FE8D12052AE9E3EB0F9485215C9C743D40A78C4B61ACF850280F282E33371013
SHA-512:	624C65F4E4BA7ED4C07470C739495494F352F2C7AD9424D105D7FA98CC368EE17F42612260BD56DCCBC06536E4749ACDD538718E21EB1E50792FAF9D314EA91
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):	6.737385098522604
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:	50.dll
File size:	351232
MD5:	03a4adf216161aceabaf8b9cbde58308
SHA1:	5b37a2bdc58279f1f1e31038fff1f859eec76cf6
SHA256:	e0e9821e1c172ee90b6ea27d96a0e9053269fb48bcbe7ec4fb42e048da9f4e8a
SHA512:	3ec128c3c3208aeaf480de750c55f11e0d188ae1bbc32db4b6dbb11353da7fe08efd873e335da4085129fe5dbd8882f8400b1f3d57ed37419015a6a70fe0a8ce
SSDEEP:	6144:tgx+Fh1vq19DeXOKKGEH6xmID/u2rA5QcGqWtyXaNc:Wx+F6FehKXH6xmIDs5QcDW0Xn
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........$...Ea..Ea..Ea......Ea......Ea......Ea......Ea..E`..Ea......Ea......Ea......Ea......Ea.Rich.Ea.........PE..L...{n.T...........

File Icon



Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x12f014
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x100000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x548D6E7B [Sun Dec 14 11:03:23 2014 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:	388c18203ba7cd9d5e6bbc1e635bd8d1

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x439ab	0x43a00	False	0.712439348429	data	6.87960232272	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x45000	0xd75e	0xd800	False	0.41040943287	data	5.24834717721	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x53000	0xa9ac	0x1c00	False	0.321149553571	data	3.83064778866	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x5e000	0x558	0x600	False	0.41796875	data	3.83355470058	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x5f000	0x2388	0x2400	False	0.768988715278	data	6.64336652157	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Version Infos

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/07/21-15:17:40.389493	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49793	80	192.168.2.3	87.106.18.141
10/07/21-15:17:40.389493	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49793	80	192.168.2.3	87.106.18.141
10/07/21-15:17:47.836744	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49795	80	192.168.2.3	87.106.18.141

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 7, 2021 15:16:34.269242048 CEST	192.168.2.3	8.8.8.8	0xb0b3	Standard query (0)	golang.feel500.at	A (IP address)	IN (0x0001)
Oct 7, 2021 15:16:34.292124033 CEST	192.168.2.3	8.8.8.8	0x2f1	Standard query (0)	golang.feel500.at	A (IP address)	IN (0x0001)
Oct 7, 2021 15:16:34.341847897 CEST	192.168.2.3	8.8.8.8	0x3623	Standard query (0)	golang.feel500.at	A (IP address)	IN (0x0001)
Oct 7, 2021 15:17:17.651487112 CEST	192.168.2.3	8.8.8.8	0x4bf	Standard query (0)	golang.feel500.at	A (IP address)	IN (0x0001)
Oct 7, 2021 15:17:17.675950050 CEST	192.168.2.3	8.8.8.8	0x6dd1	Standard query (0)	golang.feel500.at	A (IP address)	IN (0x0001)
Oct 7, 2021 15:17:17.734096050 CEST	192.168.2.3	8.8.8.8	0x6df6	Standard query (0)	golang.feel500.at	A (IP address)	IN (0x0001)
Oct 7, 2021 15:17:25.078634977 CEST	192.168.2.3	8.8.8.8	0x1dc4	Standard query (0)	golang.feel500.at	A (IP address)	IN (0x0001)
Oct 7, 2021 15:17:25.106987000 CEST	192.168.2.3	8.8.8.8	0xf5cc	Standard query (0)	golang.feel500.at	A (IP address)	IN (0x0001)
Oct 7, 2021 15:17:25.138366938 CEST	192.168.2.3	8.8.8.8	0x570d	Standard query (0)	golang.feel500.at	A (IP address)	IN (0x0001)
Oct 7, 2021 15:17:40.324491024 CEST	192.168.2.3	8.8.8.8	0xf18f	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Oct 7, 2021 15:17:47.759160995 CEST	192.168.2.3	8.8.8.8	0x2141	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 7, 2021 15:16:34.286691904 CEST	8.8.8.8	192.168.2.3	0xb0b3	Name error (3)	golang.feel500.at	none	none	A (IP address)	IN (0x0001)
Oct 7, 2021 15:16:34.311359882 CEST	8.8.8.8	192.168.2.3	0x2f1	Name error (3)	golang.feel500.at	none	none	A (IP address)	IN (0x0001)
Oct 7, 2021 15:16:34.360780954 CEST	8.8.8.8	192.168.2.3	0x3623	Name error (3)	golang.feel500.at	none	none	A (IP address)	IN (0x0001)
Oct 7, 2021 15:17:17.669847012 CEST	8.8.8.8	192.168.2.3	0x4bf	Name error (3)	golang.feel500.at	none	none	A (IP address)	IN (0x0001)
Oct 7, 2021 15:17:17.708945990 CEST	8.8.8.8	192.168.2.3	0x6dd1	Name error (3)	golang.feel500.at	none	none	A (IP address)	IN (0x0001)
Oct 7, 2021 15:17:17.752178907 CEST	8.8.8.8	192.168.2.3	0x6df6	Name error (3)	golang.feel500.at	none	none	A (IP address)	IN (0x0001)
Oct 7, 2021 15:17:25.101989031 CEST	8.8.8.8	192.168.2.3	0x1dc4	Name error (3)	golang.feel500.at	none	none	A (IP address)	IN (0x0001)
Oct 7, 2021 15:17:25.125339031 CEST	8.8.8.8	192.168.2.3	0xf5cc	Name error (3)	golang.feel500.at	none	none	A (IP address)	IN (0x0001)
Oct 7, 2021 15:17:25.158637047 CEST	8.8.8.8	192.168.2.3	0x570d	Name error (3)	golang.feel500.at	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 7, 2021 15:17:40.343003988 CEST	8.8.8.8	192.168.2.3	0xf18f	No error (0)	api10.laptok.at		87.106.18.141	A (IP address)	IN (0x0001)
Oct 7, 2021 15:17:47.784818888 CEST	8.8.8.8	192.168.2.3	0x2141	No error (0)	api10.laptok.at		87.106.18.141	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- api10.laptok.at

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49793	87.106.18.141	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Oct 7, 2021 15:17:40.389492989 CEST	5487	OUT	GET /api1/Jq38ICaRqPy/g8cT5EDuzQRTfd/bDaQidhBmNREYWZABcNxO/6xll5SLapn_2FusJ/iHdi_2FbiOmTGG b/BXo7JAZFG1eu_2FtyI/cNFtxMNBR/zYGeZfeXbEOB1SyQFsvB/rB0Q_2FZQZ0YZi_2FRO/tidnHoD06Cgh_2FRad 0Stl/qK8jV1z_2FTo2/PBtT0ki_/2BubNruXDtYtZ2wLQ_2BEya/1EtRRJfeUI/5CMi0T2vwqXTEyNz1/lyOJ_2BtNXg9/d_2B7L GgvGV/55GaKjfY_2FDfj/svm_0A_0DtNmhHj6ls2X4/2lW3OzRcv2PkceFw/VNJ6ep7w_2FRmj_2FWh4Js/N HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Oct 7, 2021 15:17:40.437324047 CEST	5487	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Thu, 07 Oct 2021 13:17:40 GMT Content-Type: text/plain Transfer-Encoding: chunked Connection: keep-alive Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Oct 7, 2021 15:17:40.771373034 CEST	5487	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: api10.laptok.at Connection: Keep-Alive
Oct 7, 2021 15:17:40.837850094 CEST	5488	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Thu, 07 Oct 2021 13:17:40 GMT Content-Type: text/plain Transfer-Encoding: chunked Connection: keep-alive Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49795	87.106.18.141	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Oct 7, 2021 15:17:47.836744070 CEST	5489	OUT	GET /api1/9RmUtQcDZhfIk1c/nHzONe5_2BBvJ2yBiQ/7EpiCVM7W/f4E0uY3D227v2RDuExxP/zjYG_2FjR1JK0C dmuq7/JUrUMl2hsVJQOhQQrJjdjl/lE7jBPvrlvBD9/Eqgu2Y0S/_2FHxlBiKM99DvrRblH0nvV/kCN2W88lpy/lXYy2rxZX1fnU 6LEk/1F2dsOnkIM4n/gevEdeTc_2F/PmNNaIgvx9qczG/o0sHDdRiEaK9_2F3dDlYN/KN8GHFQNDyxdo2UR/PPq4SU NELaWLIO_/0A_0DzqmFbCxXnCfo4/lNkWBFYtG/ncFEw74zm9E4h83K_2FU/jx5qA20TXkJiA0KWOxZ/VG0Riowa/X HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Oct 7, 2021 15:17:47.883217096 CEST	5489	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Thu, 07 Oct 2021 13:17:47 GMT Content-Type: text/plain Transfer-Encoding: chunked Connection: keep-alive Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Timestamp	kBytes transferred	Direction	Data
Oct 7, 2021 15:17:48.092147112 CEST	5490	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: api10.laptok.at Connection: Keep-Alive
Oct 7, 2021 15:17:48.149419069 CEST	5490	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Thu, 07 Oct 2021 13:17:48 GMT Content-Type: text/plain Transfer-Encoding: chunked Connection: keep-alive Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 5416 Parent PID: 5308

General

Start time:	15:14:59
Start date:	07/10/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\50.dll'
Imagebase:	0x1150000
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: 00000000.00000002.804482994.0000000003F08000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.495439556.0000000003F08000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.496320513.0000000003F08000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.496294032.0000000003F08000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.496277018.0000000003F08000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.495483618.0000000003F08000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.496244695.0000000003F08000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.496057082.0000000003F08000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.804033989.0000000003359000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.496215226.0000000003F08000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 4604 Parent PID: 5416

General

Start time:	15:15:00
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\50.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: 3348 Parent PID: 5416

General

Start time:	15:15:00
Start date:	07/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\50.dll,@DllRegisterServer@0
Imagebase:	0x40000
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: 00000002.00000003.478390389.0000000004EB9000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 3148 Parent PID: 4604

General

Start time:	15:15:00
Start date:	07/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\50.dll',#1
Imagebase:	0x40000
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, Description: Yara detected Ursnif, Source: 00000003.00000003.479416380.0000000004CD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.479376627.0000000004CD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000003.621232674.00000000044C9000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.479510909.0000000004CD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.479453127.0000000004CD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.479614184.0000000004CD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.479576032.0000000004CD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.479548431.0000000004CD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.479596189.0000000004CD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.622172269.0000000004CD8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 5364 Parent PID: 5416

General

Start time:	15:15:05
Start date:	07/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\50.dll,@DllUnregisterServer@0
Imagebase:	0x40000
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: 00000005.00000003.492977892.00000000044B9000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 3324 Parent PID: 5416

General

Start time:	15:15:13
Start date:	07/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\50.dll,@Properwhat@8
Imagebase:	0x40000
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: 00000006.00000003.503835282.00000000051B9000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 7056 Parent PID: 744

General

Start time:	15:16:31
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:	0x7ff70bcc0000
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: 3644 Parent PID: 7056

General

Start time:	15:16:32

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:7056 CREDAT:17410 /prefetch:2
Imagebase:	0x820000
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: 6992 Parent PID: 744

General

Start time:	15:17:15
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:	0x7ff70bcc0000
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: 2332 Parent PID: 6992

General

Start time:	15:17:15
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:6992 CREDAT:17410 /prefetch:2
Imagebase:	0x820000
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: 3892 Parent PID: 744

General

Start time:	15:17:22
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:	0x7ff70bcc0000
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: 4676 Parent PID: 3892

General

Start time:	15:17:23
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:3892 CREDAT:17410 /prefetch:2
Imagebase:	0x820000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 5580 Parent PID: 744

General

Start time:	15:17:38
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:	0x7ff70bcc0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 6336 Parent PID: 5580

General

Start time:	15:17:38
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:5580 CREDAT:17410 /prefetch:2
Imagebase:	0x820000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 6888 Parent PID: 744

General

Start time:	15:17:45
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:	0x7ff70bcc0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 6004 Parent PID: 6888

General

Start time:	15:17:46
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:6888 CREDAT:17410 /prefetch:2
Imagebase:	0x820000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis