ID: 338189
Sample Name: OgQJzDbLce.dll
Cookbook: default.jbs
Time: 19:16:27
Date: 11/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

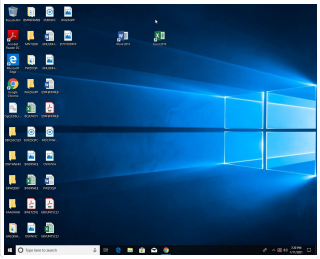
Analysis Report OgQJzDbLce.dll

Overview

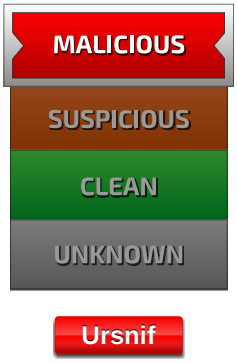
General Information

Sample Name:	OgQJzDbLce.dll
Analysis ID:	338189
MD5:	5268c190b3a694..
SHA1:	56b1b5066f88e07.
SHA256:	8e34c697b60378..
Tags:	dll Gozi

Most interesting Screenshot:



Detection

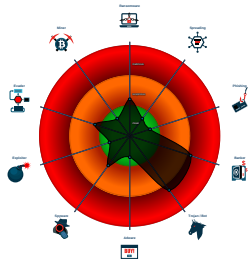


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Creates a COM Internet Explorer ob…
- Writes or reads registry keys via WMI
- Writes registry values via WMI
- Antivirus or Machine Learning detec…
- Contains functionality to call native f…
- Creates a DirectInput object (often fo…
- Detected potential crypto function
- Monitors certain registry keys / valu…
- PE / OLE file has an invalid certificate
- PE file contains sections with non-s…
- Sample file is different than original

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 6140 cmdline: loaddll32.exe 'C:\Users\user\Desktop\OgQJzDbLce.dll' MD5: 2D39D4DFDE8F7151723794029AB8A034)
- iexplore.exe (PID: 6572 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6832 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6572 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 6392 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4632 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6392 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 3480 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6284 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3480 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 6128 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6708 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6128 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

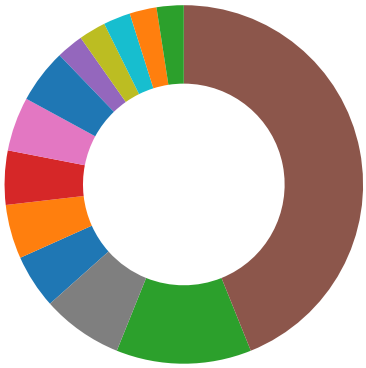
Source	Rule	Description	Author	Strings
00000000.00000003.777109164.0000000003AD8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.776993803.0000000003AD8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.777131098.0000000003AD8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.777071428.0000000003AD8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000003.777173919.0000000003AD8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 4 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

Creates a COM Internet Explorer object

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

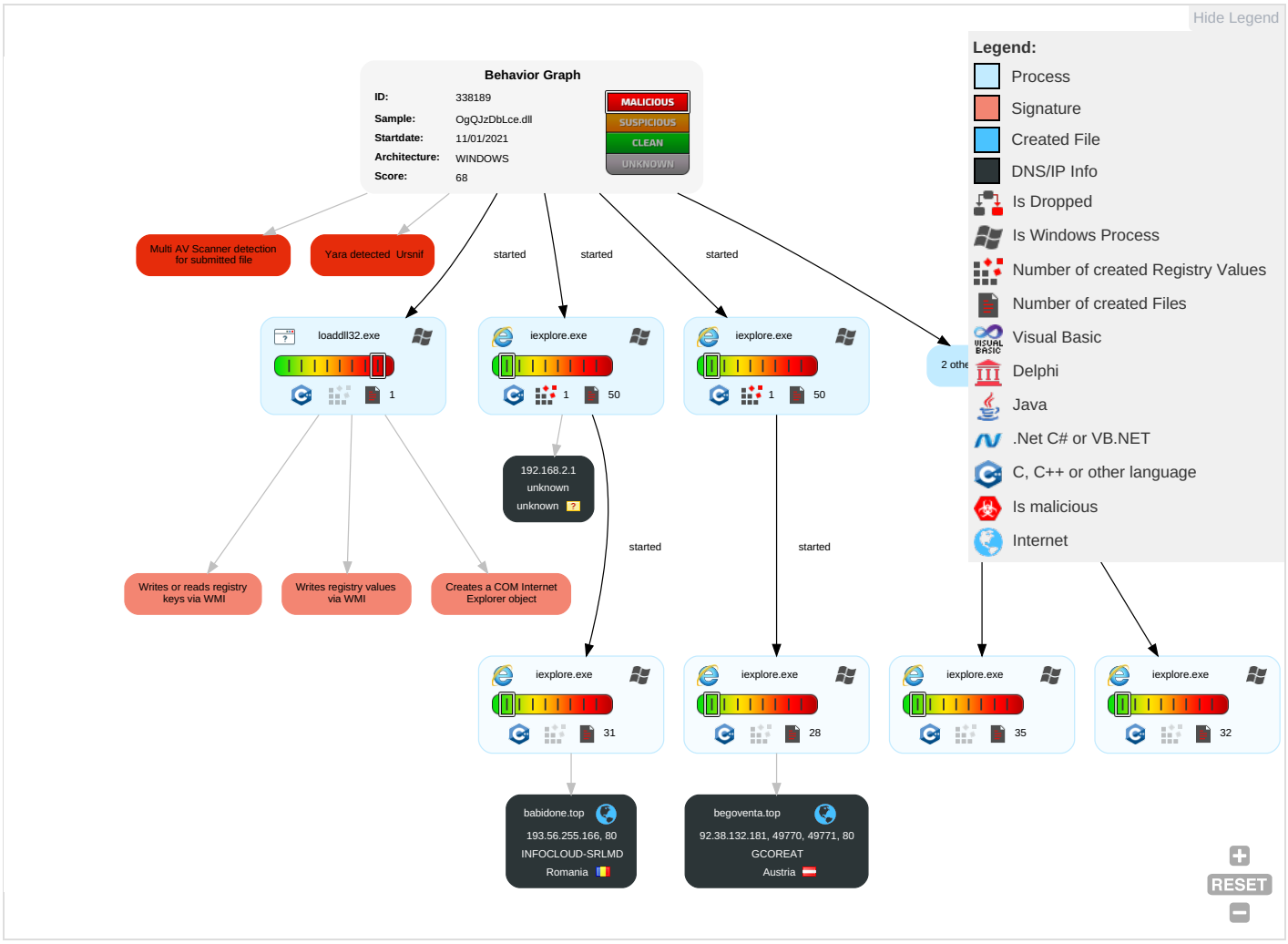
Remote Access Functionality:

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	Remote Service Effects	Im
Valid Accounts	Windows Management Instrumentation 2	Path Interception	Process Injection 2	Masquerading 1	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mo Sy Pa
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	De Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	De De Da
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap		Ca Bill Fra
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	System Information Discovery 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Ma Ap Ra or

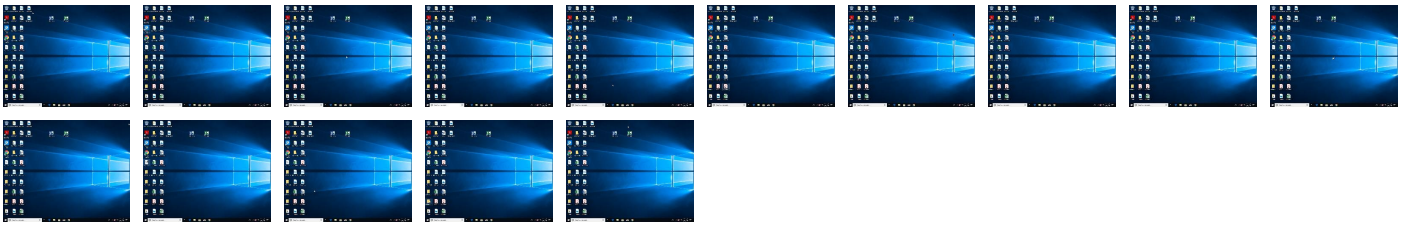
Behavior Graph



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
OgQJzDbLce.dll	22%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.10000000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
0.2.loaddll32.exe.15b0000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

Source	Detection	Scanner	Label	Link
begoventa.top	2%	Virustotal		Browse
babidone.top	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://babidone.top/images/PPpwiauX_2BIh4oFWqX/Djwkz7R93cFnDrrKCEfupn/1lc9UumTDGjRL/5auxQAs_/2B38Hwp	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://begoventa.top/images/HRdOnZXQubvEpiF/dnOBFJ5ijbSGwRmyqM/h51pT26O9/4EIbVpHBFlOcgrt0TShq/p	0%	Avira URL Cloud	safe	
http://begoventa.top/favicon.ico	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://begoventa.top/images/HRdOnZXQubvEpiF/dnOBFJ5ijbSGwRmyqM/h51pT26O9/4EIbVpHBFlOcgrt0TShq/pPJJGC5mrcZE6ZGUWjS/LKs0W_2FZrtLgELoKDEbZR/8X1_2FxjVbkZk/tVcM_2Bd/jQmX3NhgeWRqCDsfD_2BayQ/lSPwdIYz4P/81sFvcaWcXolUgVkt/y_2B1p3Gvpg_/2F0X2_2F87o/JZseyqJj/p.avi	0%	Avira URL Cloud	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://begoventa.top/images/HRdOnZXQubvEpiF/dnOBFJ5ijbSGwRmyqM/h51pT26O9/4EIbVpHBFlOcgrt0TShq/pPJJGC	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
begoventa.top	92.38.132.181	true	false	• 2%, Virustotal, Browse	unknown
babidone.top	193.56.255.166	true	false	• 2%, Virustotal, Browse	unknown

Contacted URLs

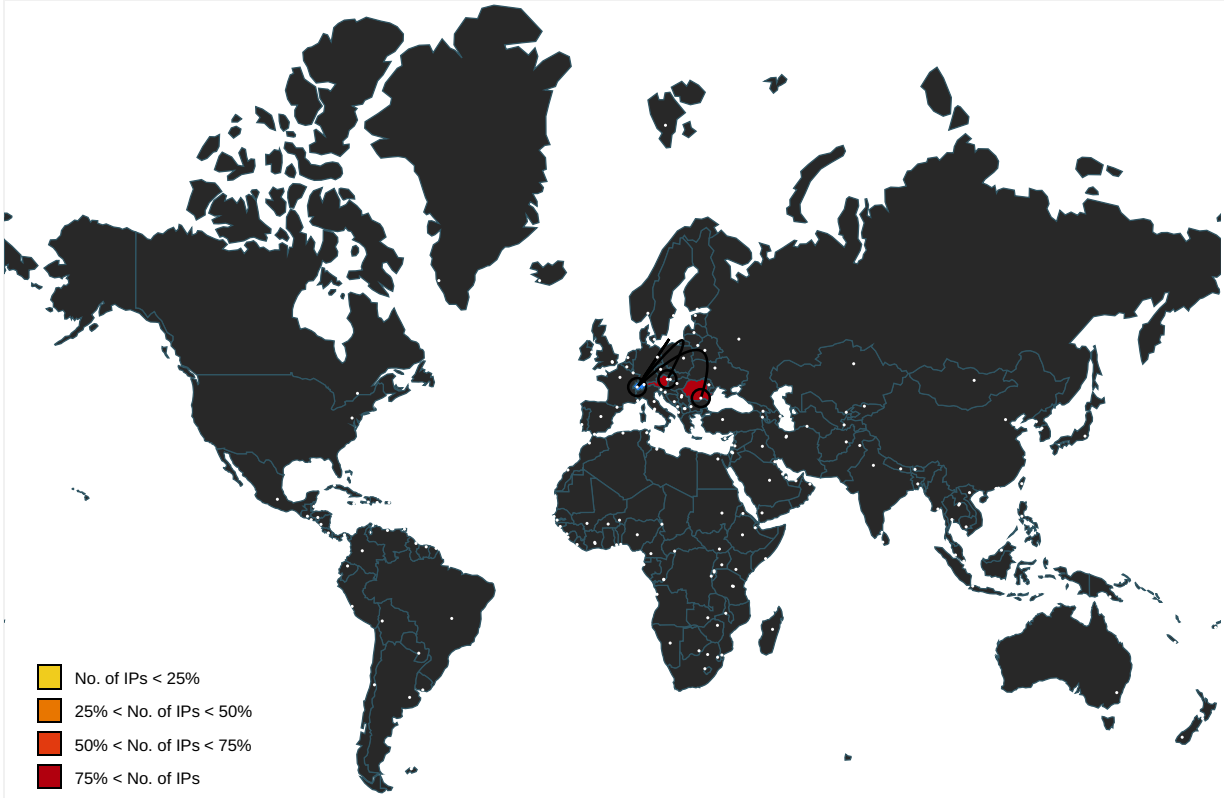
Name	Malicious	Antivirus Detection	Reputation
http://begoventa.top/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://begoventa.top/images/HRdOnZXQubvEpiF/dnOBFJ5ijbSGwRmyqM/h51pT26O9/4EIbVpHBFlOcgrt0TShq/pPJJGC5mrcZE6ZGUWjS/LKs0W_2FZrtLgELoKDEbZR/8X1_2FxjVbkZk/tVcM_2Bd/jQmX3NhgeWRqCDsfD_2BayQ/lSPwdIYz4P/81sFvcaWcXolUgVkt/y_2B1p3Gvpg_/2F0X2_2F87o/JZseyqJj/p.avi	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	OgQJzDbLce.dll	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.nytimes.com/	msapplication.xml3.13.dr	false		high
http://babidone.top/images/PPpwiauX_2BIh4oFWqX/Djwkz7R93cFnDrrKCEfupn/1lc9UumTDGjRL/5auxQAs_/2B38Hwp	~DFD4CA446EF33C2D57.TMP.20.dr, {77F8D092-5439-11EB-90EB-ECF4BBEA1588}.dat.20.dr	false	• Avira URL Cloud: safe	unknown
http://ocsp.sectigo.com0	OgQJzDbLce.dll	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://begoventa.top/images/HRdOnZXQubvEpiF/dnOBFJ5ijbSGwRmyqM/h51pT26O9/4EIbVpHBFlOcgrt0TShq/p	loaddll32.exe, 00000000.00000002.1018176446.0000000001C10000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	OgQJzDbLce.dll	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.youtube.com/	msapplication.xml7.13.dr	false		high
http://https://sectigo.com/CPS0D	OgQJzDbLce.dll	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.wikipedia.com/	msapplication.xml6.13.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.com/	msapplication.xml.13.dr	false		high
http://begoventa.top/images/HRdOnZXQubvEpiF/dnOBFJ5ijbSGwRmyqM/h51pT26O9/4EIbVpHBFlOcgrt0TShq/pPJJGC	loaddll32.exe, 00000000.00000002.1018085048.0000000001697000.00000004.00000020.sdmp, ~DF4EBD4894B35EDD90.TMP.25.dr, {9B722639-5439-11EB-90EB-ECF4BBEA1588}.dat.25.dr	false	• Avira URL Cloud: safe	unknown
http://www.live.com/	msapplication.xml2.13.dr	false		high
http://www.reddit.com/	msapplication.xml4.13.dr	false		high
http://www.twitter.com/	msapplication.xml5.13.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.56.255.166	unknown	Romania		213137	INFOCLOUD-SRLMD	false
92.38.132.181	unknown	Austria		199524	GCOREAT	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	338189
Start date:	11.01.2021
Start time:	19:16:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OgQJzDbLce.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:	27
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:	mal68.bank.troj.winDLL@13/44@3/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 96.1% (good quality ratio 90.2%) • Quality average: 78.5% • Quality standard deviation: 29%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.64.90.137, 104.42.151.234, 52.255.188.83, 51.104.139.180, 92.122.213.247, 92.122.213.194, 52.155.217.156, 20.54.26.129, 2.20.142.209, 2.20.142.210, 51.11.168.160, 88.221.62.148, 152.199.19.161 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, ie9comview.vo.msecnd.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, updates.microsoft.com, ctldl.windowsupdate.com, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
INFOCLOUD-SRLMD	5fd9d7ec9e7aetar.dll	Get hash	malicious	Browse	• 193.56.255.167
GCOREAT	8WLxD8uxRN.exe	Get hash	malicious	Browse	• 5.188.6.146
	http://https://kiankaziataad.com/shop/images/homebanners/err	Get hash	malicious	Browse	• 185.105.3.162
	LmlSW3qU2x.exe	Get hash	malicious	Browse	• 92.223.105.117
	http://https://sleekearflap.com//shareform/index.php	Get hash	malicious	Browse	• 92.38.163.8
	http://https://www.google.com/url?q=https://canadian-pills-store.su/?cp%3Dsalesx&sa=D&ust=1608032187237000&usg=AOvVaw2CTXjcE4npPvhliuTL-Itl	Get hash	malicious	Browse	• 5.188.0.147
	http://https://ofd.beeline.ru/check-order/oxjsoinmq	Get hash	malicious	Browse	• 92.223.97.97
	http://https://www.wunba.com/	Get hash	malicious	Browse	• 92.223.97.97
	http://https://ngor.zlen.com.ua/Restore/Click here to restore message automatically.html	Get hash	malicious	Browse	• 92.223.97.97
	mXlHxlkrkB.exe	Get hash	malicious	Browse	• 146.185.219.29
	Rawan inquiry.doc	Get hash	malicious	Browse	• 92.223.93.172
	5e3Dtdp1dU.exe	Get hash	malicious	Browse	• 185.101.139.252
	KqVNXoOE85.exe	Get hash	malicious	Browse	• 45.135.229.212
	xl.png.exe	Get hash	malicious	Browse	• 5.188.38.80
	corp-fin.xlsb	Get hash	malicious	Browse	• 5.188.38.80
	Ghj736i4Ht.exe	Get hash	malicious	Browse	• 185.105.1.149
	slip copy.exe	Get hash	malicious	Browse	• 45.135.229.212
	Receipt+00034587583883.exe	Get hash	malicious	Browse	• 92.223.105.174
	Angebot_09082020_148.xls	Get hash	malicious	Browse	• 5.188.0.171
	INV15 .docm	Get hash	malicious	Browse	• 92.38.135.61
	Tagesprotokoll_G0001_20200911.xlsm	Get hash	malicious	Browse	• 5.188.0.251

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{5E3D54B5-5439-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{5E3D54B5-5439-11EB-90EB-ECF4BBEA1588}.dat	
Entropy (8bit):	1.7677795101409812
Encrypted:	false
SSDEEP:	48:IwchGcpru6GwpL0TG/ap8SXrGIpcdGvnZpvpGo/Pqp9AGo4LlzpmBGW/5zTUCGWP:roZfZs2y9W6tVifDLlzML94O6vZBX2pB
MD5:	F19EB8802FE83029B13BCFB8D2C6C307
SHA1:	0D661CEF7AAD0B1567866B0C476D9256F1164241
SHA-256:	E5EFDD1A001C6136C17563097E5018D0AF6407B53B9E82E29220228A345A7010
SHA-512:	54E35057744434433BF64ED4DB17BB0C2185B5DAE63E55F4E21BBC52369BB6C7626F7B3320E315307B337B3F479DD7355A7DFD7E0A4651A9C515E1B5B1FF8646
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{77F8D090-5439-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7727430226053469
Encrypted:	false
SSDEEP:	96:r/ZQZgV2gRO9WgRPztgRPA8ifgRPA2zeszMgRPCU2VEeN68gBgR2CU2hDpB:r/ZQZ62d9WOtWifmeszMrEG68gBSDpB
MD5:	83E4BBBE72AD06F58B5B436C654DD4F9
SHA1:	D9E6660D3F2750BC06D3399A9A74EF5F0B9E6D5A
SHA-256:	80F10776BF6323447A2448168B3BB752ECB5E0DA4DC2300F61B1F239B51871AB
SHA-512:	CB1ADE72BCFDBF4950BDF392CD62E539A695B7FD4A310946179AF67E220A9592AEF70E42F96BE7251915F378B1DC813E1CC66E5B61DE29AFA52A2791FE13EE 3
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{8DCAF18E-5439-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.767609996176377
Encrypted:	false
SSDEEP:	192:rHZtZo2y9W4mt4Uif4cVrzM4XDp6j3BLEpB:r5D/yUBamrM
MD5:	40625874579526CBE836AA9E298C4BCC
SHA1:	72242BC794C34E86D9F6D273F42D393ECC5AFE68
SHA-256:	4E1165C23BD8EE6B5EB26D8C9D4E14D8E2AE86A672A0467522A735A13C1EB8E5
SHA-512:	EABE9A27C1F0FD2EC0FCCFFD46248C7D609E096CBB10EE34FEE2183DE53E1CA53E40FF09287BE6D5A9DC258EB957B533896720555CB5EB8B4029D8CB6E47D 97A
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{9B722637-5439-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7689336572294374
Encrypted:	false
SSDEEP:	48:IwcGcprJGwpLL6G/ap8LmrGIpcLGGvnZpvL7GolPqp9LGGo4h/zpmLxGWl5ZT+GP:rAZjZ0269WXtVifdh/zM9Ho6NzBIgpB
MD5:	26964069B5AB1183C6F019622544C827
SHA1:	2F4BA0A68FF90B1FF1AC3AA69DCCC64BEFFA7E66
SHA-256:	66F84454F3368C4080EDF55E3EE6CD0E7DE2A6F568CD156F02B2D13615716C5B
SHA-512:	C12F1922535948BA26B21EA9C5ED9246C869EC684A30561C62DB2AB485501F0F2FDBE202AEB1880CAC42BCC9996513F3EBB66EA4E0B4C845CB2976D7F623BF 5
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{9B722637-5439-11EB-90EB-ECF4BBEA1588}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{5E3D54B7-5439-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27368
Entropy (8bit):	1.8430070309605113
Encrypted:	false
SSDEEP:	96:r4ZLQt6DBSIFjZ2QkWBMwYiy6R9xy6RWWciA:r4ZLQt6DkIFjZ2QkWBMwYiyOxy/iA
MD5:	513141E5326F0E8893D18F6B6CF4ECC9
SHA1:	34E8DB4E1CA1B189129034CCFFC2F89D28B1141B
SHA-256:	33863CF59E31800B4A818618BF56BF1E408310CF474B079583065CE3268F8168
SHA-512:	1D4C9751793F1B566192A614E9265CF2B017C4B511024244862260619F861FC1A1C30BBAA6EB0EDA9369B6DFF3608C93FDEE07294F4A9D58C6531614D0538DD3
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{77F8D092-5439-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27360
Entropy (8bit):	1.841214254937248
Encrypted:	false
SSDEEP:	192:r4ZfQ761k7FjV24kWXeMISYqxboZRxbo6b2KA:r4Y++7hM8X3ISfxbuxbBb2t
MD5:	EFC9DBE9B1A00BC2B3183437EABF9EA3
SHA1:	0012ACD6D98242CF5187119CE7514975FB2FF588
SHA-256:	16D2B449F031BFFECEB7AD22C8367515B1D83DD80DC95ABFAA8B94A500B63937
SHA-512:	6F43DFFC3E0AF0B68CD13E0D7A5C70FD8F895AED60D6D46CF88DF6C47202138CF2BA3F7A6912FF8B938CC8F915F8B4162D52CFCCACA7AF10972D3920A87A8 A8
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{8DCAF190-5439-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27376
Entropy (8bit):	1.8472568777610467
Encrypted:	false
SSDEEP:	192:rqZBQt6Hk1Fjh2TkWoMHY6ewpJxewp56A:rWWYE1hQ3NHvewpXewp59
MD5:	D33C7184E23B721DCFC9E112AACACDC0
SHA1:	83E519B4B762340A3C01618B9C6BB15F6E926E4D
SHA-256:	B1F97C3D3BA1233DA5EE5D52FEB6378519CE2320E648C38746CC13A6F95C392D
SHA-512:	1CBD446F3DA475E2213B965C121EE73B03FBC9AA05B725B085C2B2526DD78743F9BBAEFFAA65E657F3EB04DE901D4AF14B4E9AC3BBBB78C2D467FC63871763 EE
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9B722639-5439-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27368

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9B722639-5439-11EB-90EB-ECF4BBEA1588}.dat	
Entropy (8bit):	1.8403358832338321
Encrypted:	false
SSDEEP:	192:r9ZmQC6QkiFjp2jkWwMPYin4Ozxn4Oc8iA:rTztdih4HFPH4O4qV
MD5:	34D74AFEC96FDAF1AC3EC81B56E035A4
SHA1:	1D41B818ADAA1D9D1F974EEB0CD963D4921E0334
SHA-256:	FDD9D1EB2FA4628FC123AF5515F053BF4F6A5296C657D783509809CC4C1BB814
SHA-512:	DC4199F013F4A0C4B7085D38DC5919CB85276FE80BF7FF435445C84E62980AE6F9CAE8BCB686FF163C983FF2146A7B0FFF59E8F848E87E9BA4A9DA53D6B8EB0 4
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):	5.123118361083354
Encrypted:	false
SSDEEP:	12:TMHdNMNxOECDr8nWimI002EtM3MHdNMNxOECDr8nWimI00OYGVbkEtMb:2d6NxORDr8SZHKd6NxORDr8SZ7YLb
MD5:	7E6B49EEC0BEB1BC27E4DED68249CE03
SHA1:	66533E523D676017CA1AC096F01B45EFC432D5B3
SHA-256:	92AB2E98CCA3A2E4DBFEFD4A84B850B7F9E47391B88B5FB2329DA36A5C82BEB6
SHA-512:	0DE3346DC82FB930C4A0F4D4E293003CB914F8CD9D8CBAD5F98FBCC0E20B9974DEEDB6EACFFE3A2857BF17609F3585FF8EB8BF6DF7346D0E2BFCB77E794C0 3CD
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x33a85989,0x01d6e846</date>< accdate>0x33a85989,0x01d6e846</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>0x33a85989,0x01d6e846</date><accdate>0 x33a85989,0x01d6e846</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):	5.11901366828337
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kDfcDqfc8nWimI002EtM3MHdNMNxe2kDfcDqfc8nWimI00OYGkak6t:2d6NxrLDd8SZHKd6NxrLDd8SZ7Yza7b
MD5:	CF6C928DA3DBC3459C96F4CC79D40C92
SHA1:	9A12BC347C3F0BEDA3725FD6DD42DD4DEF73FE5C
SHA-256:	26AF633EFA78F94B59A2ED6E838C1A29D982D1D13B04410B6FBDDAC187EEB7ED
SHA-512:	C4A20F0013DBACDD1D09DCF593CA1C4F312402077B881317384D27744043C0B7D8B93BE6221DB6C11FB97FD7B4ABFEE32365F08E821F1132BBE28FE8035AAB2 6
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x33a132c6,0x01d6e846</date><a ccdate>0x33a132c6,0x01d6e846</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>0x33a132c6,0x01d6e846</date><a ccdate>0x33a132c6,0x01d6e846</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Am azon.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):	5.142286717418112
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLCDr8nWimI002EtM3MHdNMNxvLCDr8nWimI00OYGmZEtMb:2d6Nxv2Dr8SZHKd6Nxv2Dr8SZ7Yjb
MD5:	8AA7C1AE009F7157E9C6CEA1B4FE8BB3
SHA1:	CCD372C471932E57785792BB622A12D4842AEF90
SHA-256:	41F1F5F4B50D4CAF46FC5B1E2C086FA7A8D189CD3A77F958F1DB30E966F22541
SHA-512:	865D8552587DABD0550923067AC8CF21F0302C61E522F6158E45F496F10FD3104C4BCF5D8EB69B61FD29DCBAC00EF49A0B7BB35AB32E24433F54C54942A84CC

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x33a85989,0x01d6e846</date><accdate>0x33a85989,0x01d6e846</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>0x33a85989,0x01d6e846</date><accdate>0x33a85989,0x01d6e846</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):	5.132012535046788
Encrypted:	false
SSDEEP:	12:TMHdNMNxiqVVDXVV8nWimI002EtM3MHdNMNxiqVVDXVV8nWimI00OYGd5EtMb:2d6NxDLDXL8SZHKd6NxDLDXL8SZ7YEjb
MD5:	95C939A865C8101F80CEDC1DE98A4361
SHA1:	BDEC37EE7FE60CAABE53594F681A3A0FB54E570E
SHA-256:	A825DE7F2D3734780282ECAD82F28538A9F0F12E974EBE63A5E3F9B699C4FBEB
SHA-512:	A478801B40A0AA5B391BC6607390AF931EC2BC11CC6AA7480799282A76FA9D4B545EBE2C87D79DCE8290E7B4FF7A59D75625B8E5EB438C91478C1C4669EE80FC
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x33a5f732,0x01d6e846</date><accdate>0x33a5f732,0x01d6e846</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>0x33a5f732,0x01d6e846</date><accdate>0x33a5f732,0x01d6e846</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):	5.157419814247615
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwCDr8nWimI002EtM3MHdNMNxhGwCDr8nWimI00OYG8K075EtMb:2d6NxQdDr8SZHKd6NxQdDr8SZ7YrKajb
MD5:	8930BB5A619E764D208825B40ADB9C1B
SHA1:	4BEB28A7403DD7AE4AA4E2716423295C92B1AA85
SHA-256:	603EBB0035DEB07CAE4A5C1047A0497858413F8F8DBEE33B1538DC93AB5A7FD0
SHA-512:	80A1313C37CF49532395952CD44C20431C28476EB822FAE565A06E6133CA888D5D1497D95551B2D6778AE00B4AA1B9D4F5BF6A0A30F99F0E895856914D707B30
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x33a85989,0x01d6e846</date><accdate>0x33a85989,0x01d6e846</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>0x33a85989,0x01d6e846</date><accdate>0x33a85989,0x01d6e846</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):	5.120104889948707
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nqVVDXVV8nWimI002EtM3MHdNMNx0nqVVDXVV8nWimI00OYGxEtMb:2d6Nx0qLDXL8SZHKd6Nx0qLDXL8SZ7Yu
MD5:	900F7E70BF1A18DEF2B8F775034AD5C0
SHA1:	16A95BB43A7CC44A2D1CC3A7C658A7EE87BF59A7
SHA-256:	33BB8311F998AB5963614127CFCD20CB4FB815F895717981136AFEAD57B0E081
SHA-512:	A013E2F164B9567401D259EFE4B91EA555B4B6A154B948819A0BBE75CFD315722FABC2BBEBF8B6AC0FE59A6927745CFE17764D9E6270879DBC72C2F1874847D9
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x33a5f732,0x01d6e846</date><accdate>0x33a5f732,0x01d6e846</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>0x33a5f732,0x01d6e846</date><accdate>0x33a5f732,0x01d6e846</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):	5.155875441719391
Encrypted:	false
SSDEEP:	12:TMHdNMNxxqVVDXVV8nWimI002EtM3MHdNMNxxqVVDXVV8nWimI00OYG6Kq5EtMb:2d6NxILDXL8SZHKd6NxILDXL8SZ7Yhb
MD5:	94DEE2D982F6B090513529E3C081F2BB
SHA1:	A2AB3F04ED9CCC98B45D647F164CF17068C330E6
SHA-256:	B8F299722A651BFB5B335B51ED6C0843010CE50707E8E0EA256A5DA4CBDBD0EA
SHA-512:	911E6624B3FDFD109BB9C89EC2A6572FCF1C5A110D9484D05A2626E93CFCC59AFE868B3E6A37FB65F8CDE780D7772B0035E1F6C2CDE7CE63BB107E4D296624 0
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x33a5f732,0x01d6e846</date> accdate>0x33a5f732,0x01d6e846</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>0x33a5f732,0x01d6e846</date><accdate>0 x33a5f732,0x01d6e846</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):	5.104813971265666
Encrypted:	false
SSDEEP:	12:TMHdNMNxcvRfDKRf8nWimI002EtM3MHdNMNxcvRfDKRf8nWimI00OYGVEtMb:2d6NxIRfDKRf8SZHKd6NxIRfDKRf8SZ9
MD5:	C8FD4280CD70F937103A9AF732E3DD4E
SHA1:	A374A611046247FF1857B101DB71DC443824FA19
SHA-256:	8B141F38B3ACF2D58766274C0133B878ECEA2EDBC4B78F057A441EBD2E3E903F
SHA-512:	A50A5D49DC8A11B9A121E7B66BE8FC3C0115D56105B81EEE85DA791D4F11CB8E8D293AA216ADFC6147E3FB76E8D532358760E15A6E520BB537E08066D8DC76 5
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x33a394ee,0x01d6e846</date> <accdate>0x33a394ee,0x01d6e846</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>0x33a394ee,0x01d6e846</date><accdate >0x33a394ee,0x01d6e846</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):	5.100792594048622
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnvRfDKRf8nWimI002EtM3MHdNMNxfnvRfDXVV8nWimI00OYGe5EtMb:2d6NxXRfDKRf8SZHKd6NxXRfDXL8SZ7Q
MD5:	7A0858FCBFC03AA1DBCCFF36133AD9DB
SHA1:	034E9AB92DB4EEE559E84C9760F470954D3A4422
SHA-256:	EC63AB7411D857A0AA038EF4D700252C5F7839DF80B2B5E5AB931486E21690FF
SHA-512:	FB3DE82F4D39726FD0F52008923CE55CBC5A734D4223C0A03E1499FA74981D16243EAC6E735A3FA98E0B80971E0BF43A4C089436840CCC4115D4492C70A4784 3
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x33a394ee,0x01d6e846</date><a ccdate>0x33a394ee,0x01d6e846</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>0x33a394ee,0x01d6e846</date><a ccdate>0x33a5f732,0x01d6e846</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Go ogle.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\NewErrorPageTemplate[1]	
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D
Malicious:	false
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
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\2WF3MMUU\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493 AC6D
Malicious:	false
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\2WF3MMUU\dnserror[2]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493 AC6D
Malicious:	false
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=9003
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\2WF3MMUU\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\down[1]	
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....l..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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\9026IKNJ\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:	downloaded
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
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....l..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
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
IE Cache URL:	res://ieframe.dll/errorPageStrings.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\errorPageStrings[1]	
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\9026IKNJ\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\CS6IXJW6\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\CS6IXJW6\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\OR0WKIO1\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\OR0WKIO1\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:	downloaded
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
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=0
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\OR0WKIO1\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\OR0WKIO1\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\httpErrorPagesScripts[1]	
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
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
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):	4.330858678274478
Encrypted:	false
SSDEEP:	3:oVXUBcNwspNW8JOGXnEBcNwsUULun:o9UBm4qEB3
MD5:	9B2F941CC234206ED52127B15C3DB5C4
SHA1:	CFA1858AE4D0BAD526EA88C088894AE87E7B68BC
SHA-256:	E62B2E85EE25A7F9675E2672D59BAE17BCF10A6E913BF5358AA4305B616F4772
SHA-512:	729D1A577343DB9EE0487DCF350241F878F815B11C91EC2FA2BB78897FE1A2B936DD35D5660BAB55511FF70D29C20E191E85793B66D88F2FEB82317B52B6BE7F
Malicious:	false
Preview:	[2021/01/11 19:19:58.275] Latest deploy version: ..[2021/01/11 19:19:58.275] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF2067CF7CEB139563.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39633
Entropy (8bit):	0.571125479592397
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+/hDqOIO+gSexjm/r310kcgSexjm/r310kcgSexjm/r310k9:kBqoxKAuvScS+/hDqxby6Rmy6RWy6Rv
MD5:	1E9C165BA8BBA336C2F29A759A8A63F4
SHA1:	196030A43DA96C58881459B13C0EC493E61714E0
SHA-256:	C30B5984EF56B3CBCF4CAC78DF3D6BFF6A773ACB643894B06B8D8931651283A9
SHA-512:	367F0BD24041967CA819E403BC99143DA2587B359743473F94533B35FF571115E89D430637E078E7FC875F03EB0AC0E2B6831B6B925168F645DF4DFE3964B87A
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF3AD4F610F2F01C17.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4073703340301186
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9loLuS9loLuC9lWLuu4ciu43A3:kBqoILmL4LmW
MD5:	9E06FBC5BBCCF4AD5560712694B4D83F
SHA1:	17EBB760CB64206E78E840D1D07EA9E218DB3810
SHA-256:	F56041664FC19EB49766B6932193151BA2E3CC4BE20C25915F1D6B4B1660FB86
SHA-512:	9D06774BFCAD97F9BB46B67B4D061CF547E7956EC70EE7C8D82F1617C3E81555F0EA25AE7CEF847E27C2D3BCEA19DEE912ACFBE85C85AD0DEDF0B6DEFD90347F
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DF3AD4F610F2F01C17.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF3BDE2C19B223BD97.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4082977278331884
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9logUS9logUC9lWgUWUzgUbUhUzgUVUXU3:kBqoIg4gmgRkgA2kgCUw
MD5:	23F6F6B07B5E7E986466E1CD2C4B5FB4
SHA1:	17E7B294F38E630D17E00A334F7B5D722A082752
SHA-256:	2376D6EBB665AB2483161DF184CD9E4B5C409030BBA45D244DAA9401CDA61352
SHA-512:	11175CB1340AD507F58D108BE07F56B3DE7A3E39EB5F518B9B8C0A5E2CF21BDF72B47DCB6E1AE0BAEEDF96A369CDA555097203F954084586857537D5B122CF 8
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF4EBD4894B35EDD90.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39633
Entropy (8bit):	0.567384082930945
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+j9PGN3334OC334Oi334Or:kBqoxKAuqR+j9PGN3n4OCn4Oin4Or
MD5:	4862725EC73842A1146F44DA0C1DCB2D
SHA1:	EFA859B3E2CAFE2EEB0528E5C37CE94337C03C06
SHA-256:	523DA11F99BDC035433B7AD42642F058492A4E63ED357D193839809F8D560A4F
SHA-512:	0EA6C157FAF1C9484A69C107E1BA43E1388BFCA3E55C93B8572E1DF6EB17B76BAF9350215504A931C6C8DD652C6743F722187FBF08031CC05559DCEA800EA86 E
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFBDDB979C06B382E7.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.40568636521364454
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loEDS9loEDC9lWEDg2oIrXR+IIrXSIF3:kBqoIwOoDrwrn
MD5:	467079A72B9542080A17D7020CEA1EA5
SHA1:	C6C24309BE84C5C36B8C154C37B4399C30FEA861
SHA-256:	B6CEF05D56E0CF94B3747781D495F1B81F445F23B4A1E12848350175554FBBC3
SHA-512:	A7B1D3E1E3480EF7BFD6A11E2D6CD923DA3418D7747D3126D9A5A7189DAD453E77D13200A831F263AFA319C17E89B76077644B4BF37B80E04EDFCD34EAE703 F
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFD4CA446EF33C2D57.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Temp\~DFD4CA446EF33C2D57.TMP	
Size (bytes):	39617
Entropy (8bit):	0.5661717333321002
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+EiIZCUxboMYxboMgxboMR:kBqoxKAuqR+EiIZCUxbonxboTxbo4
MD5:	F3F63A0DA97DF0202CBE6FB587020099
SHA1:	28EF2148B441B85BE2DDC9FBDC0EAE7233E710DC
SHA-256:	22516C1B3F3F5028D7364B248D4FDF1924FAA1BA29CF4AEEC7A1131F4E38EF4D
SHA-512:	8A9B7438433A8D15C282099A65EF4E4947E688F6F06E39D3F9CD61B69F69282346F660D14E04E731333C09C297E6705E97A1DA58441C1F49D114D4A02449A335
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFDF7FEAB4721FD8E2.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39649
Entropy (8bit):	0.5736007353148195
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+lOEV+Qejcp5ejcpNejcpy:kBqoxKAuqR+lOEV+Qewp5ewpNewpy
MD5:	1D852009F05DA7DF995E7535A4709495
SHA1:	018E6040EE0A99AE26B2141A577BDBBD8C0D8A70
SHA-256:	BA91F56D73CEFF88360862E08E54FF1B190BB918B4F25156BEF682CD061769B2
SHA-512:	34D754E5B46105510EEBF07005BA34F355A31C93BBF5B1878C55468507DA45E8B855995E6350528E49AB970ED1EFD2CBE8023DD5481C23378398384094C34184
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFF6F6BADDE9A18747.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.40633329185700595
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loyfS9loyfC9lWyf2fQfFfzfQf2YHfxf3:kBqoIys3
MD5:	7C0D373B4B13410A8135BC0B8DCCDCC0
SHA1:	B59FD3076421306B8C71FCDF0112BCA3051C0F2A
SHA-256:	F0D3ADAF55E47D21B0C9675965A8C0BEED1BA4BE1979C573A14E5EFBD66210C0
SHA-512:	CE629A4BFAD6597BA4695A5270E25DAFA25618B1A7E0C733822E07CDB507634A704228DA859D7F1BA56C6084F252C54EA67C3A5293CE1391496DA666AA80267
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):	3.911923467563189
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.39% • Win16/32 Executable Delphi generic (2074/23) 0.21% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • VXD Driver (31/22) 0.00%
File name:	OgQJzDbLce.dll

General

File size:	313176
MD5:	5268c190b3a6940bc7c8f0361f3a187f
SHA1:	56b1b5066f88e07f494e5e97f9a8b791cc9d7bd2
SHA256:	8e34c697b603788b9baeecfb375c466cb8468a322d6ae9b81fc41fb61472c3da
SHA512:	c44274ee84f9fdfdce444b36e33b2ca2db265cbc99a9ffb7fe5ebbbc79cb9b82f19cb93477d4211d9122cd7043a5964c115d2bc4adc4af0ef7c0b60b069481d0
SSDEEP:	1536:34UeRdT1u9JFuuhY03X67MMOo+xT0/7Hbo5ioQ+pQ:IUe2aW6CKE5rQ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....[._.....!...2.....4.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1002f010
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, DLL, LINE_NUMS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5FFC5BBD [Mon Jan 11 14:07:57 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:	302dc27ee8fb51d51fd455c5c954a121

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=XFYFPUHYTZABTVZNTR
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 1/11/2021 12:21:35 AM 1/1/2040 12:59:59 AM
Subject Chain	• CN=XFYFPUHYTZABTVZNTR
Version:	3
Thumbprint MD5:	BB4518AF652AB34118DB294048EC2292
Thumbprint SHA-1:	C0D055129F95529EA2B2D89554BF80520281570D
Thumbprint SHA-256:	22031A72E03D309F0C1E229440904D068D6D8F87D2CDE4DC11EC76DE301B9DA3
Serial:	5D3EDE33956CF3B547584EF32177B187

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 50h
mov dword ptr [ebp-08h], 00000001h
mov dword ptr [ebp-04h], 00000000h

Instruction
mov eax, ebp
mov ecx, dword ptr [eax+08h]
mov dword ptr [1004B4C0h], ecx
mov dword ptr [1004B4A0h], ebp
mov dword ptr [ebp-10h], 00000001h
mov dword ptr [ebp-14h], 00000001h
mov dword ptr [ebp-18h], 00000001h
mov dword ptr [ebp-0Ch], 00000001h
mov eax, dword ptr [ebp-18h]
push eax
call dword ptr [1004AB44h]
mov dword ptr [ebp-34h], 00000001h
mov dword ptr [ebp-3Ch], 00000001h
mov dword ptr [ebp-4Ch], 00000001h
mov dword ptr [ebp-24h], 00000001h
mov dword ptr [ebp-30h], 00000001h
mov dword ptr [ebp-38h], 00000001h
mov dword ptr [ebp-48h], 00000001h
mov dword ptr [ebp-20h], 00000001h
mov dword ptr [ebp-2Ch], 00000001h
mov dword ptr [ebp-40h], 00000001h
mov dword ptr [ebp-28h], 00000001h
mov dword ptr [ebp-44h], 00000001h
mov dword ptr [ebp-1Ch], 00000001h
mov ecx, dword ptr [ebp-24h]
push ecx
call dword ptr [1004AB18h]
mov edx, dword ptr [ebp-1Ch]
add edx, 33h
mov dword ptr [ebp-1Ch], edx
mov eax, dword ptr [ebp-24h]
push eax
call dword ptr [1004AB18h]
mov ecx, dword ptr [ebp-1Ch]
add ecx, 00000000h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x4a76c	0xa0	.data
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4c000	0x11a8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x4b200	0x1558	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x4e000	0x398	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x4a9fc	0x1f0	.data
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2fe9f	0x30000	False	0.279159545898	data	4.882308777	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data2	0x31000	0x64	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x32000	0x1951c	0x19600	False	0.0185691194581	data	0.340193889812	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x4c000	0x11a8	0x1200	False	0.394314236111	data	4.62126050947	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x4e000	0x398	0x400	False	0.8388671875	data	6.25576957826	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
REGISTRY	0x4c158	0x17c	ASCII text, with CRLF line terminators	English	United States
TYPELIB	0x4c2d4	0x708	data	English	United States
RT_RCDATA	0x4c9dc	0x410	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States
RT_VERSION	0x4cdec	0x3bc	data	English	United States

Imports

DLL	Import
KERNEL32.dll	QueryPerformanceFrequency, GetDateFormatW, ResetEvent, QueryPerformanceCounter, SetEvent, GetCurrentProcess, OpenEventW, ResumeThread, WaitForSingleObject, DuplicateHandle, WriteFile, GetLastError, GetExitCodeThread, CreateFileW, MoveFileW, lstrlenA, ReadFile, Sleep, GetFileSize, CreateEventW, GetLocaleInfoW, CloseHandle, GetLocalTime, LoadLibraryW, GetWindowsDirectoryW, FormatMessageW, CreateProcessW, LocalFree, FindFirstFileW, CopyFileW, FindClose, SetLastError, CreateDirectoryW, lstrlenW, GetSystemDirectoryW, GetTempPathW, GetDriveTypeW, GetFileTime, GetUserDefaultLCID, ExpandEnvironmentStringsW, GetPrivateProfileStringW, GetFileInformationByHandle, GetFileAttributesA, FileTimeToDosDateTime, GetSystemInfo, CreateFileA, WideCharToMultiByte, FileTimeToLocalFileTime, lstrcmpiW, GetTempFileNameW, GetFileAttributesW, GetProcAddress, LocalAlloc, GetModuleHandleW, GetStartupInfoW, DeleteFileW, ExitProcess, GetTickCount, LoadLibraryA, MultiByteToWideChar, FreeLibrary, GetModuleHandleA, GetStdHandle, GetConsoleScreenBufferInfo, VirtualAlloc, HeapFree, GetProcessHeap, HeapAlloc, VirtualFree, SetConsoleCtrlHandler
USER32.dll	GetClipboardData, LoadIconW
GDI32.dll	GetKerningPairsA, CreateEllipticRgn, PATHOBJ_vEnumStartClipLines, GetBoundsRect, FONTOBJ_pfdg, GetDIBColorTable, SetTextCharacterExtra, GetTextFaceW, EndPage, GetColorSpace, RealizePalette
COMDLG32.dll	GetOpenFileNameW
ADVAPI32.dll	IsTextUnicode, RegCloseKey, RegCreateKeyExW, RegOpenKeyExW, RegEnumKeyExW, RegQueryInfoKeyW, RegQueryValueExW, RegSetValueExW, RegDeleteKeyW, RegDeleteValueW, RegGetKeySecurity, RegOpenKeyW, RegSetKeySecurity, RegConnectRegistryW
SHELL32.dll	ExtractIconW, DragQueryFileAorW, SHBindToParent, DoEnvironmentSubstW, ExtractIconA, ShellExecuteA, SHCreateProcessAsUserW, SHPathPrepareForWriteW, SHPathPrepareForWriteA, SHIsFileAvailableOffline, ExtractAssociatedIconW, SHGetSpecialFolderPathA, ShellExecuteEx, DragAcceptFiles, ExtractAssociatedIconA
SHLWAPI.dll	StrChrIA, StrRChrIW, StrCmpNW, StrChrA

Version Infos

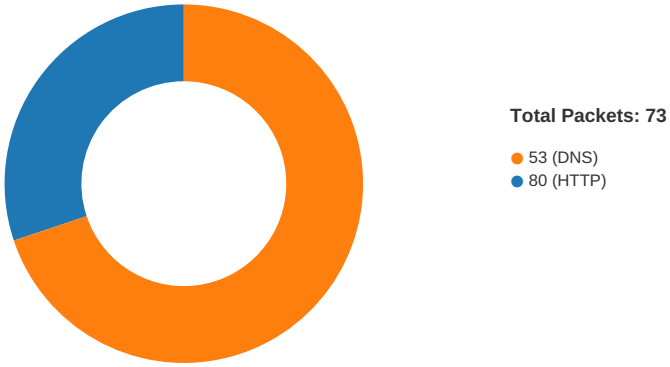
Description	Data
LegalCopyright	Microsoft Corporation. All rights reserved.
InternalName	wmprph.exe
FileVersion	12.0.7600.16385 (win7_rtm.090713-1255)
CompanyName	Microsoft Corporation
ProductName	Microsoft Windows Operating System
ProductVersion	12.0.7600.16385
FileDescription	Windows Media Player Rich Preview Handler
OriginalFilename	wmprph.exe
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 19:18:58.637449026 CET	49766	80	192.168.2.4	193.56.255.166
Jan 11, 2021 19:18:58.637895107 CET	49767	80	192.168.2.4	193.56.255.166
Jan 11, 2021 19:18:59.652379036 CET	49767	80	192.168.2.4	193.56.255.166
Jan 11, 2021 19:18:59.652384996 CET	49766	80	192.168.2.4	193.56.255.166
Jan 11, 2021 19:19:01.652669907 CET	49767	80	192.168.2.4	193.56.255.166
Jan 11, 2021 19:19:01.668169022 CET	49766	80	192.168.2.4	193.56.255.166
Jan 11, 2021 19:19:05.671752930 CET	49768	80	192.168.2.4	193.56.255.166
Jan 11, 2021 19:19:05.685636997 CET	49769	80	192.168.2.4	193.56.255.166
Jan 11, 2021 19:19:06.684380054 CET	49768	80	192.168.2.4	193.56.255.166
Jan 11, 2021 19:19:06.684417963 CET	49769	80	192.168.2.4	193.56.255.166
Jan 11, 2021 19:19:08.684454918 CET	49768	80	192.168.2.4	193.56.255.166
Jan 11, 2021 19:19:08.684526920 CET	49769	80	192.168.2.4	193.56.255.166
Jan 11, 2021 19:19:58.675662994 CET	49771	80	192.168.2.4	92.38.132.181
Jan 11, 2021 19:19:58.676135063 CET	49770	80	192.168.2.4	92.38.132.181
Jan 11, 2021 19:19:58.842180967 CET	80	49771	92.38.132.181	192.168.2.4
Jan 11, 2021 19:19:58.842485905 CET	80	49770	92.38.132.181	192.168.2.4
Jan 11, 2021 19:19:58.843215942 CET	49771	80	192.168.2.4	92.38.132.181
Jan 11, 2021 19:19:58.843277931 CET	49770	80	192.168.2.4	92.38.132.181
Jan 11, 2021 19:19:58.844620943 CET	49770	80	192.168.2.4	92.38.132.181
Jan 11, 2021 19:19:59.010343075 CET	80	49770	92.38.132.181	192.168.2.4
Jan 11, 2021 19:19:59.010474920 CET	49770	80	192.168.2.4	92.38.132.181
Jan 11, 2021 19:19:59.014595985 CET	49770	80	192.168.2.4	92.38.132.181
Jan 11, 2021 19:19:59.180378914 CET	80	49770	92.38.132.181	192.168.2.4
Jan 11, 2021 19:19:59.374355078 CET	49771	80	192.168.2.4	92.38.132.181
Jan 11, 2021 19:19:59.539839983 CET	80	49771	92.38.132.181	192.168.2.4
Jan 11, 2021 19:19:59.540218115 CET	49771	80	192.168.2.4	92.38.132.181
Jan 11, 2021 19:19:59.540604115 CET	49771	80	192.168.2.4	92.38.132.181
Jan 11, 2021 19:19:59.706584930 CET	80	49771	92.38.132.181	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 19:17:13.728465080 CET	52991	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:17:13.776426077 CET	53	52991	8.8.8.8	192.168.2.4
Jan 11, 2021 19:17:14.899044991 CET	53700	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:17:14.947060108 CET	53	53700	8.8.8.8	192.168.2.4
Jan 11, 2021 19:17:16.134349108 CET	51726	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:17:16.183490992 CET	53	51726	8.8.8.8	192.168.2.4
Jan 11, 2021 19:17:17.316296101 CET	56794	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:17:17.365488052 CET	53	56794	8.8.8.8	192.168.2.4
Jan 11, 2021 19:17:18.543859005 CET	56534	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:17:18.591643095 CET	53	56534	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 19:17:20.270620108 CET	56627	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:17:20.321528912 CET	53	56627	8.8.8.8	192.168.2.4
Jan 11, 2021 19:17:21.431942940 CET	56621	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:17:21.482697010 CET	53	56621	8.8.8.8	192.168.2.4
Jan 11, 2021 19:17:23.037543058 CET	63116	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:17:23.095849037 CET	53	63116	8.8.8.8	192.168.2.4
Jan 11, 2021 19:17:24.173182964 CET	64078	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:17:24.223839998 CET	53	64078	8.8.8.8	192.168.2.4
Jan 11, 2021 19:17:25.405437946 CET	64801	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:17:25.461977959 CET	53	64801	8.8.8.8	192.168.2.4
Jan 11, 2021 19:17:26.528758049 CET	61721	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:17:26.576582909 CET	53	61721	8.8.8.8	192.168.2.4
Jan 11, 2021 19:17:27.789350986 CET	51255	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:17:27.840101004 CET	53	51255	8.8.8.8	192.168.2.4
Jan 11, 2021 19:17:31.651175976 CET	61522	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:17:31.702140093 CET	53	61522	8.8.8.8	192.168.2.4
Jan 11, 2021 19:17:37.523211002 CET	52337	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:17:37.571157932 CET	53	52337	8.8.8.8	192.168.2.4
Jan 11, 2021 19:17:42.095158100 CET	55046	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:17:42.158015013 CET	53	55046	8.8.8.8	192.168.2.4
Jan 11, 2021 19:17:56.574376106 CET	49612	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:17:56.646744967 CET	53	49612	8.8.8.8	192.168.2.4
Jan 11, 2021 19:17:57.340466022 CET	49285	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:17:57.396816015 CET	53	49285	8.8.8.8	192.168.2.4
Jan 11, 2021 19:17:57.949260950 CET	50601	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:17:58.008524895 CET	53	50601	8.8.8.8	192.168.2.4
Jan 11, 2021 19:17:58.401261091 CET	60875	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:17:58.424139977 CET	56448	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:17:58.472059011 CET	53	60875	8.8.8.8	192.168.2.4
Jan 11, 2021 19:17:58.480787992 CET	53	56448	8.8.8.8	192.168.2.4
Jan 11, 2021 19:17:58.947978020 CET	59172	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:17:59.056448936 CET	53	59172	8.8.8.8	192.168.2.4
Jan 11, 2021 19:17:59.920516014 CET	62420	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:17:59.977058887 CET	53	62420	8.8.8.8	192.168.2.4
Jan 11, 2021 19:18:00.565299988 CET	60579	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:18:00.621866941 CET	53	60579	8.8.8.8	192.168.2.4
Jan 11, 2021 19:18:01.463937998 CET	50183	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:18:01.520250082 CET	53	50183	8.8.8.8	192.168.2.4
Jan 11, 2021 19:18:01.791364908 CET	61531	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:18:01.852602005 CET	53	61531	8.8.8.8	192.168.2.4
Jan 11, 2021 19:18:02.311281919 CET	49228	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:18:02.372957945 CET	53	49228	8.8.8.8	192.168.2.4
Jan 11, 2021 19:18:03.041776896 CET	59794	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:18:04.038800955 CET	59794	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:18:04.095683098 CET	53	59794	8.8.8.8	192.168.2.4
Jan 11, 2021 19:18:13.464627028 CET	55916	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:18:13.512702942 CET	53	55916	8.8.8.8	192.168.2.4
Jan 11, 2021 19:18:13.857961893 CET	52752	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:18:13.916877031 CET	53	52752	8.8.8.8	192.168.2.4
Jan 11, 2021 19:18:14.372106075 CET	60542	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:18:14.432737112 CET	53	60542	8.8.8.8	192.168.2.4
Jan 11, 2021 19:18:15.591245890 CET	60689	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:18:15.661892891 CET	53	60689	8.8.8.8	192.168.2.4
Jan 11, 2021 19:18:15.666835070 CET	64206	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:18:15.723268986 CET	53	64206	8.8.8.8	192.168.2.4
Jan 11, 2021 19:18:15.732852936 CET	50904	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:18:15.789099932 CET	53	50904	8.8.8.8	192.168.2.4
Jan 11, 2021 19:18:17.501837015 CET	57525	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:18:17.561764002 CET	53	57525	8.8.8.8	192.168.2.4
Jan 11, 2021 19:18:44.371268988 CET	53814	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:18:44.419553995 CET	53	53814	8.8.8.8	192.168.2.4
Jan 11, 2021 19:18:45.388396025 CET	53814	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:18:45.436148882 CET	53	53814	8.8.8.8	192.168.2.4
Jan 11, 2021 19:18:46.386667013 CET	53814	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 19:18:46.434607029 CET	53	53814	8.8.8.8	192.168.2.4
Jan 11, 2021 19:18:48.402055979 CET	53814	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:18:48.450495958 CET	53	53814	8.8.8.8	192.168.2.4
Jan 11, 2021 19:18:51.038003922 CET	53418	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:18:51.085899115 CET	53	53418	8.8.8.8	192.168.2.4
Jan 11, 2021 19:18:52.417939901 CET	53814	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:18:52.465867043 CET	53	53814	8.8.8.8	192.168.2.4
Jan 11, 2021 19:18:52.960946083 CET	62833	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:18:53.030009031 CET	53	62833	8.8.8.8	192.168.2.4
Jan 11, 2021 19:18:57.541655064 CET	59260	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:18:57.602686882 CET	53	59260	8.8.8.8	192.168.2.4
Jan 11, 2021 19:18:58.559163094 CET	49944	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:18:58.615565062 CET	53	49944	8.8.8.8	192.168.2.4
Jan 11, 2021 19:19:12.693413973 CET	63300	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:19:12.749691010 CET	53	63300	8.8.8.8	192.168.2.4
Jan 11, 2021 19:19:34.145577908 CET	61449	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:19:34.203614950 CET	53	61449	8.8.8.8	192.168.2.4
Jan 11, 2021 19:19:35.314510107 CET	51275	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:19:35.389287949 CET	53	51275	8.8.8.8	192.168.2.4
Jan 11, 2021 19:19:35.394572973 CET	63492	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:19:35.453552961 CET	53	63492	8.8.8.8	192.168.2.4
Jan 11, 2021 19:19:35.461821079 CET	58945	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:19:35.517985106 CET	53	58945	8.8.8.8	192.168.2.4
Jan 11, 2021 19:19:57.094701052 CET	60779	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:19:57.151117086 CET	53	60779	8.8.8.8	192.168.2.4
Jan 11, 2021 19:19:58.227552891 CET	64014	53	192.168.2.4	8.8.8.8
Jan 11, 2021 19:19:58.653007030 CET	53	64014	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 11, 2021 19:18:58.559163094 CET	192.168.2.4	8.8.8.8	0xdf0f	Standard query (0)	babidone.top	A (IP address)	IN (0x0001)
Jan 11, 2021 19:19:12.693413973 CET	192.168.2.4	8.8.8.8	0x9d45	Standard query (0)	babidone.top	A (IP address)	IN (0x0001)
Jan 11, 2021 19:19:58.227552891 CET	192.168.2.4	8.8.8.8	0xd523	Standard query (0)	begoventa.top	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 11, 2021 19:18:58.615565062 CET	8.8.8.8	192.168.2.4	0xdf0f	No error (0)	babidone.top		193.56.255.166	A (IP address)	IN (0x0001)
Jan 11, 2021 19:19:12.749691010 CET	8.8.8.8	192.168.2.4	0x9d45	No error (0)	babidone.top		193.56.255.166	A (IP address)	IN (0x0001)
Jan 11, 2021 19:19:58.653007030 CET	8.8.8.8	192.168.2.4	0xd523	No error (0)	begoventa.top		92.38.132.181	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- begoventa.top

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49770	92.38.132.181	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 19:19:58.844620943 CET	4752	OUT	GET /images/HRdOnZXQubvEpiF/dnOBFJ5ijbSGwRmyqM/h51pT26O9/4EIbVpHBFlOcgrt0TShq/pPJJGC5mrcZE6ZGUWjS/LKs0W_2FZrtLgELoKDEbZR/8X1_2FxjVbkZk/tVcM_2Bd/jQmX3NhgeWRqCDsfD_2BayQ/lSPwdIYz4P/81sFvcaWcXoIUgVkt/y_2B1p3Gvpg_/2F0X2_2F87o/JZseyqJj/p.avi 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: begoventa.top Connection: Keep-Alive
Jan 11, 2021 19:19:59.010343075 CET	4752	IN	HTTP/1.0 503 Service Unavailable Cache-Control: no-cache Connection: close Content-Type: text/html Data Raw: 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 3c 68 31 3e 35 30 33 20 53 65 72 76 69 63 65 20 55 6e 61 76 61 69 6c 61 62 6c 65 3c 2f 68 31 3e 0a 4e 6f 20 73 65 72 76 65 72 20 69 73 20 61 76 61 69 6c 61 62 6c 65 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 69 73 20 72 65 71 75 65 73 74 2e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <html><body> 503 Service Unavailable No server is available to handle this request.</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49771	92.38.132.181	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 19:19:59.374355078 CET	4752	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: begoventa.top Connection: Keep-Alive
Jan 11, 2021 19:19:59.539839983 CET	4753	IN	HTTP/1.0 503 Service Unavailable Cache-Control: no-cache Connection: close Content-Type: text/html Data Raw: 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 3c 68 31 3e 35 30 33 20 53 65 72 76 69 63 65 20 55 6e 61 76 61 69 6c 61 62 6c 65 3c 2f 68 31 3e 0a 4e 6f 20 73 65 72 76 65 72 20 69 73 20 61 76 61 69 6c 61 62 6c 65 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 69 73 20 72 65 71 75 65 73 74 2e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <html><body> 503 Service Unavailable No server is available to handle this request.</body></html>

Code Manipulations

Statistics

Behavior

- loaddll32.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6140 Parent PID: 6032

General

Start time:	19:17:20
Start date:	11/01/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\OgQJzDbLce.dll'
Imagebase:	0xb00000
File size:	120832 bytes
MD5 hash:	2D39D4DFDE8F7151723794029AB8A034
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.777109164.0000000003AD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.776993803.0000000003AD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.777131098.0000000003AD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.777071428.0000000003AD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.777173919.0000000003AD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.777044888.0000000003AD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.777196001.0000000003AD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.777154030.0000000003AD8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6572 Parent PID: 800

General

Start time:	19:18:14
Start date:	11/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff70f2b0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6832 Parent PID: 6572

General

Start time:	19:18:14
Start date:	11/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6572 CREDAT:17410 /prefetch:2
Imagebase:	0x260000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6392 Parent PID: 800

General

Start time:	19:18:57
Start date:	11/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff70f2b0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 4632 Parent PID: 6392

General

Start time:	19:18:58
Start date:	11/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6392 CREDAT:17410 /prefetch:2
Imagebase:	0x260000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 3480 Parent PID: 800

General

Start time:	19:19:34
Start date:	11/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff70f2b0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6284 Parent PID: 3480

General

Start time:	19:19:34
Start date:	11/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3480 CREDAT:17410 /prefetch:2
Imagebase:	0x260000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6128 Parent PID: 800

General

Start time:	19:19:57
Start date:	11/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff70f2b0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6708 Parent PID: 6128

General

Start time:	19:19:57
Start date:	11/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6128 CREDAT:17410 /prefetch:2
Imagebase:	0x260000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis