

ID: 446419
Sample Name: d7b.dll
Cookbook: default.jbs
Time: 15:22:13
Date: 09/07/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report d7b.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 5
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
E-Banking Fraud: 5
System Summary: 5
Hooking and other Techniques for Hiding and Protection: 5
Stealing of Sensitive Information: 5
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 9
Public 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 22
General 22
File Icon 23
Static PE Info 23
General 23
Entrypoint Preview 23
Rich Headers 23
Data Directories 23
Sections 23
Imports 23
Exports 23
Network Behavior 23
Snort IDS Alerts 24
Network Port Distribution 24
TCP Packets 24
UDP Packets 24
DNS Queries 24
DNS Answers 24
Code Manipulations 24
Statistics 24
Behavior 24
System Behavior 24
Analysis Process: loaddll32.exe PID: 5604 Parent PID: 5764 24
General 24
File Activities 25
Analysis Process: cmd.exe PID: 3180 Parent PID: 5604 25
General 25
File Activities 25

Copyright Joe Security LLC 2021

Analysis Process: rundll32.exe PID: 5672 Parent PID: 5604 25
General 25
File Activities 26
Analysis Process: rundll32.exe PID: 6136 Parent PID: 3180 26
General 26
File Activities 26
Analysis Process: iexplore.exe PID: 5640 Parent PID: 792 26
General 26
File Activities 27
Registry Activities 27
Analysis Process: iexplore.exe PID: 5532 Parent PID: 5640 27
General 27
File Activities 27
Analysis Process: iexplore.exe PID: 5548 Parent PID: 5640 27
General 27
File Activities 27
Analysis Process: iexplore.exe PID: 7080 Parent PID: 792 27
General 27
File Activities 28
Registry Activities 28
Analysis Process: iexplore.exe PID: 5572 Parent PID: 7080 28
General 28
File Activities 28
Analysis Process: iexplore.exe PID: 6168 Parent PID: 7080 28
General 28
File Activities 28
Analysis Process: iexplore.exe PID: 5248 Parent PID: 792 29
General 29
File Activities 29
Registry Activities 29
Analysis Process: iexplore.exe PID: 5392 Parent PID: 5248 29
General 29
Analysis Process: iexplore.exe PID: 5468 Parent PID: 5248 29
General 29
Disassembly 29
Code Analysis 30

Copyright Joe Security LLC 2021

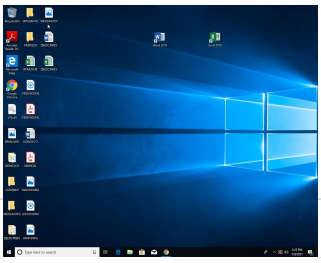
Windows Analysis Report d7b.dll

Overview

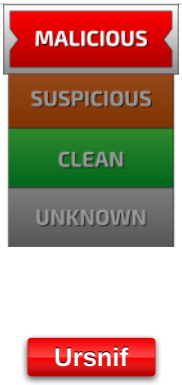
General Information

Sample Name:	d7b.dll
Analysis ID:	446419
MD5:	d7b3fe9b94d3896.
SHA1:	6b71978633aa2f9.
SHA256:	f7a1ecdd925fd1e..
Tags:	dll gozi
Infos:	

Most interesting Screenshot:



Detection

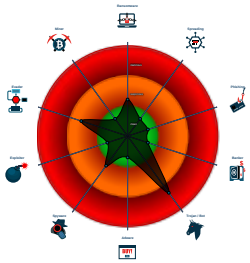


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected Ursnif
- Machine Learning detection for samp…
- Performs DNS queries to domains w…
- Writes or reads registry keys via WMI
- Writes registry values via WMI
- Contains functionality to access load…
- Contains functionality to call native f…
- Contains functionality to check if a d…
- Contains functionality to query CPU …

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5604 cmdline: loaddll32.exe 'C:\Users\user\Desktop\d7b.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 3180 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\d7b.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6136 cmdline: rundll32.exe 'C:\Users\user\Desktop\d7b.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5672 cmdline: rundll32.exe C:\Users\user\Desktop\d7b.dll,Moleculenotice MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 5640 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5532 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5640 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5548 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5640 CREDAT:17414 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 7080 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5572 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7080 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6168 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7080 CREDAT:17414 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 5248 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5392 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5248 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5468 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5248 CREDAT:17414 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000003.384867126.0000000005308000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Copyright Joe Security LLC 2021

Source	Rule	Description	Author	Strings
00000000.00000003.386739440.0000000003458000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.384991598.0000000005308000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.386787805.0000000003458000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000002.596356802.0000000005308000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 15 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:



Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:



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

Performs DNS queries to domains with low reputation

Key, Mouse, Clipboard, Microphone and Screen Capturing:



Yara detected Ursnif

E-Banking Fraud:



Yara detected Ursnif

System Summary:



Writes or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:



Yara detected Ursnif

Stealing of Sensitive Information:



Yara detected Ursnif

Copyright Joe Security LLC 2021

Remote Access Functionality:

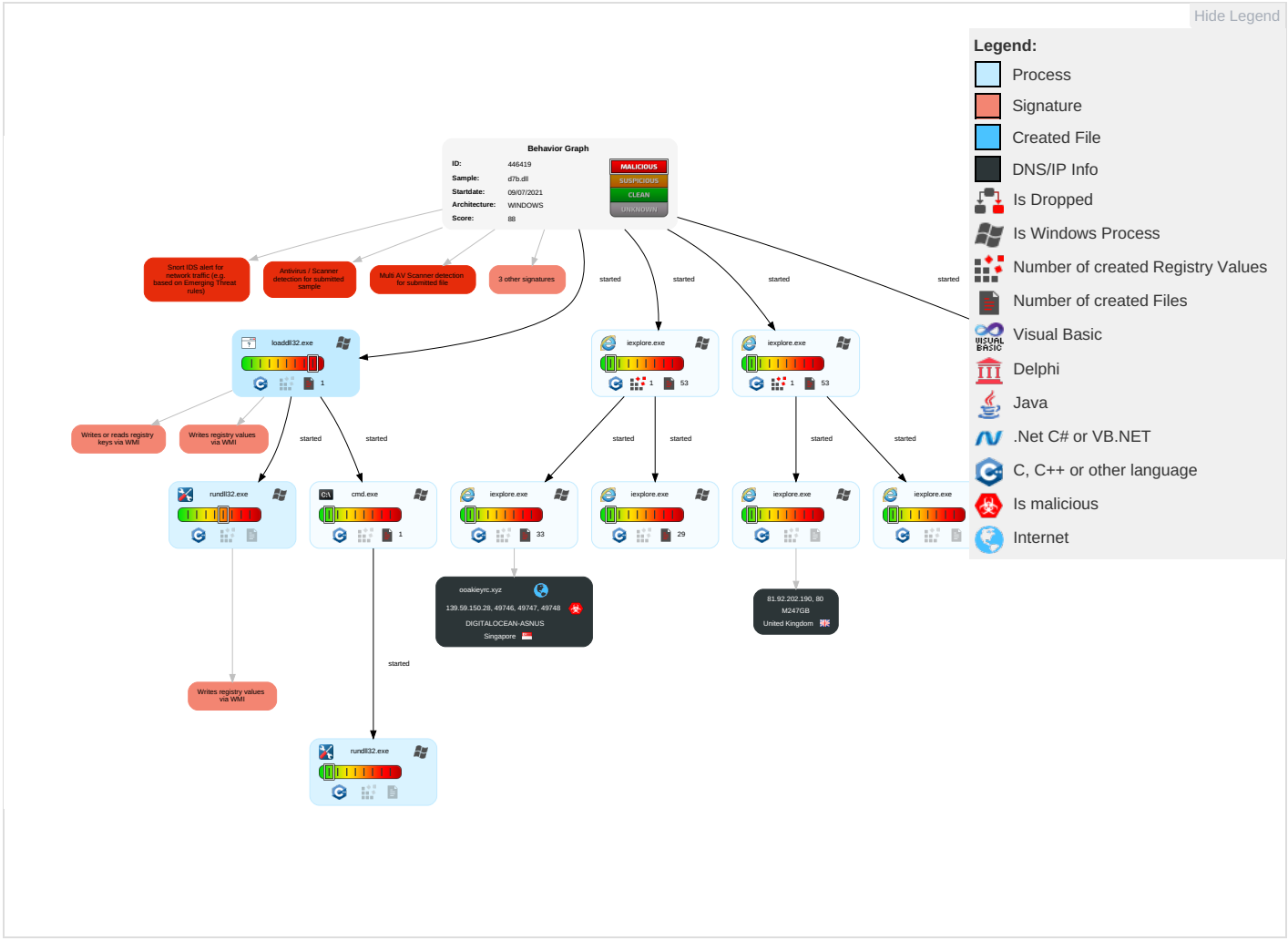


Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Eff
Valid Accounts	Windows Management Instrumentation 2	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Re Tra Wi Au
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Re Wi Wi Au
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	Security Software Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	Exploit SS7 to Track Device Location	Ob De Clo Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 2	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols	

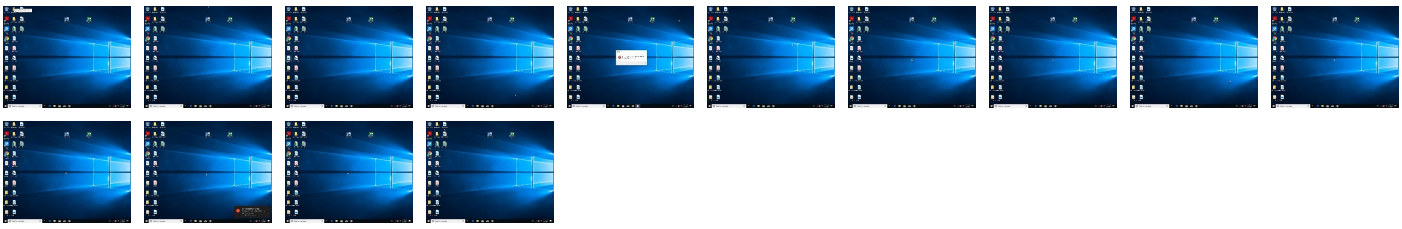
Behavior Graph



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
d7b.dll	40%	Metadefender		Browse
d7b.dll	62%	ReversingLabs	Win32.Trojan.Emotet	
d7b.dll	100%	Avira	TR/AD.Ursnif.wog	
d7b.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.6d970000.0.unpack	100%	Avira	HEUR/AGEN.1114221		Download File
4.2.rundll32.exe.6d970000.1.unpack	100%	Avira	HEUR/AGEN.1114221		Download File

Domains

Source	Detection	Scanner	Label	Link
ooakieyrc.xyz	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://ooakieyrc.xyz/images/X1oZp6Zj_2FwjdZ/GmHjDHWSzeA_2FTY8s/I0hYASmbJ/uk7yqg3FxgKimKg4iEaQ/oRj2iH	0%	Avira URL Cloud	safe	
http://ooakieyrc.xyz/images/7kc3AOalDAVrSC/miBJwAGiWQLur4VkluCOz/xRVn0UZ3CFv16_2B/wOU1EGTVWcgI78r/3l	0%	Avira URL Cloud	safe	
http://81.92.202.190/images/Rv8GrTLYptzSKPZ/L4_2FdPuwtqV2xQNJp/z_2FfwkAJ/Fv_2BGyCrahYt_2FNGpY/ghlbjT	0%	Avira URL Cloud	safe	
http://81.92.202.190/images/6_2Bfi3b1BN36VCLTJu/7xXAKaMrEwHuufQ0qCrZ8t/2MLMlwG9w9jdT/PNPs5keC/50Od9L	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ooakieyrc.xyz	139.59.150.28	true	true	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
81.92.202.190	unknown	United Kingdom		9009	M247GB	false
139.59.150.28	ooakieyrc.xyz	Singapore		14061	DIGITALOCEAN-ASNUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	446419
Start date:	09.07.2021
Start time:	15:22:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	d7b.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:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal88.troj.winDLL@22/43@4/2
EGA Information:	Failed

Copyright Joe Security LLC 2021

HDC Information:	• Successful, ratio: 7.5% (good quality ratio 7%) • Quality average: 78.8% • Quality standard deviation: 28.9%
HCA Information:	• Successful, ratio: 85% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:23:15	API Interceptor	2x Sleep call for process: rundll32.exe modified
15:23:18	API Interceptor	1x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DIGITALOCEAN-ASNUS	vbc.exe	Get hash	malicious	Browse	• 157.230.214.223
	FixKaseya.exe	Get hash	malicious	Browse	• 107.170.211.239
	fix.exe	Get hash	malicious	Browse	• 107.170.211.239
	update.exe	Get hash	malicious	Browse	• 107.170.211.239
	UpdateTool.exe	Get hash	malicious	Browse	• 107.170.211.239
	MuGnzsbhlG.exe	Get hash	malicious	Browse	• 157.230.214.223
	ew25132.xlsb	Get hash	malicious	Browse	• 134.122.57.157
	ew28031.xlsb	Get hash	malicious	Browse	• 134.122.57.157
	vbc.exe	Get hash	malicious	Browse	• 157.230.214.223
	ew28031.xlsb	Get hash	malicious	Browse	• 134.122.57.157
	Jhy2YPMShA.exe	Get hash	malicious	Browse	• 134.122.53.92
	7favAeMnIv.exe	Get hash	malicious	Browse	• 178.128.39.189
	NWMEaRqF7s.exe	Get hash	malicious	Browse	• 104.236.246.93
	Invoice-NBM01557.exe	Get hash	malicious	Browse	• 164.90.131.131
	RefdkUTxiF.exe	Get hash	malicious	Browse	• 167.99.117.21
	RFQ40110 (2).html	Get hash	malicious	Browse	• 159.65.84.127
	Enquiry#List For Order070621.exe	Get hash	malicious	Browse	• 206.189.50.215
	com.yanto.mo.codescan.apk	Get hash	malicious	Browse	• 161.35.218.92
	com.yanto.mo.codescan.apk	Get hash	malicious	Browse	• 46.101.121.244
	a.ps1	Get hash	malicious	Browse	• 206.189.69.35
M247GB	SecureMessageAtt.HTML	Get hash	malicious	Browse	• 45.141.152.18
	GCNJrvb044.exe	Get hash	malicious	Browse	• 185.156.175.51

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Reciept 7505704.xlsb	Get hash	malicious	Browse	• 37.120.222.56
	INOVICE -Reconciliation.exe	Get hash	malicious	Browse	• 193.29.104.186
	7GPtF4bk.php.exe	Get hash	malicious	Browse	• 37.120.222.56
	ONIu4vsKdI.exe	Get hash	malicious	Browse	• 37.221.121.20
	shippingnote (docs).jar	Get hash	malicious	Browse	• 193.142.58.20
	a8nAtkkusE.exe	Get hash	malicious	Browse	• 37.221.121.20
	taskhost.exe	Get hash	malicious	Browse	• 89.45.4.216
	4ouF4jBytp.exe	Get hash	malicious	Browse	• 89.45.4.101
	YaG4lqT080.exe	Get hash	malicious	Browse	• 89.45.4.101
	xK1IAFMiBO.exe	Get hash	malicious	Browse	• 89.45.6.74
	VFTGiBcSAf.exe	Get hash	malicious	Browse	• 193.29.104.98
	KO7UuzwSSQ.exe	Get hash	malicious	Browse	• 89.249.65.249
	MACHINE SPECIFICATIONS.exe	Get hash	malicious	Browse	• 46.243.140.12
	b4NByUUZ52.exe	Get hash	malicious	Browse	• 37.221.122.76
	NIMPOeli6U.exe	Get hash	malicious	Browse	• 89.45.6.74
	B2i1X1m7Mo.exe	Get hash	malicious	Browse	• 77.243.181.86
	dqVPlpmWYt.exe	Get hash	malicious	Browse	• 91.232.125.222
	47158.exe	Get hash	malicious	Browse	• 45.141.152.18

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{4867C43A-E104-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	50344
Entropy (8bit):	1.9974033292494315
Encrypted:	false
SSDEEP:	192:rRZGZ12eWetdf9FMasO6zFM4OEhTQxY2Qg:rXisVeV0asOSG4O1Yg
MD5:	28A7EAD9FEF0F8A1BEE33458A101203E
SHA1:	7372D71852AF2246FB4F42C90F608D0CA6A01E1C
SHA-256:	DACB9CD03A0E6447C93777143A7E60051FE92FB7286B2BAB8800D660C7AC3412
SHA-512:	87B1723921CABCD1BF4AD32CB22253841C3B939F394F37EBAA25B23BAC23815309F4DDE356E0A39BFB99526E00E6B081A9CB3656190222C8944DE28D8ABA560
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{6381B6AC-E104-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	50344
Entropy (8bit):	2.0083029787444335
Encrypted:	false
SSDEEP:	192:rhZ+Z42mWqtLf7umM4O69k6z27qM6TTD4fB4VnjyTiIonpog:rnqv9iL65fViem8
MD5:	B402D4DA42DB6AC7746B0C5EAB5AA449
SHA1:	BFF1BA3C5D8353B885F6A0DAF53EFA5ABA0D4F08
SHA-256:	CD68F120565EE340BA2783DDCB692871493A3EA95927E0EB8228CC99091B65E4
SHA-512:	435302DFA991BFC06DCD9DE332440BC1DB58CC8740F6187B441AD7F72927C860E92141F8B8C1E0745ED4DDF829582663329E27A3AA5066FB681A0DABA037EF8
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{6381B6AC-E104-11EB-90E5-ECF4BB2D2496}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{73AF066C-E104-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	50344
Entropy (8bit):	1.9937977853500815
Encrypted:	false
SSDEEP:	96:roZfZU2wW2tkAfPi+1MCmTOUxmRO6jq+O903UMOyy+X03a30Tx2ybyiv0Tz2ybyq:roZfZU2wW2tnfPBMfIhUM+yQxGMyIi0g
MD5:	39ADDC886722A39C458480580588A169
SHA1:	2EC5F8DCA103F5DE08020D951857FEFBBB0E5540
SHA-256:	1EDAC51AB67C28DFD2EB3E275202AAAD9EB4AF564B4D3B1CE6866F9F2D7F8D79
SHA-512:	3D140CAB801443FC7C08631F29622581F3078C4B875198F59F868BEA54C186DEEA9089E28925953DD965B7FAB56F4C8ACCCA57BD166E2A63D78798D7F62D883
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{4867C43C-E104-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27256
Entropy (8bit):	1.8057139501368606
Encrypted:	false
SSDEEP:	96:reZlQh6IBSJjJ21WsMwy+VzIbYR+VzIbwzIDA:reZlQh6IkJjJ21WsMwy+pIcR+plyIDA
MD5:	5A47016BD43BC6597414801E54A8B7E5
SHA1:	6F0E46FB00536DB43D59B5DD3C5969D72A014A00
SHA-256:	B72EA802E97334F829C08C7A24673BA39835D1841F047B442023EEEB50D5C949
SHA-512:	E32ABF314E0E734186E29BA1421D4648F91A2A58CA9D1E6854E89EE4FC3D758B20ED1517732CC0FE0F90D5FF00BEC3AE2E11D0E3632C6D6BA20483E6CD9C5E 1B
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{4867C43E-E104-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27248
Entropy (8bit):	1.8017088344250065
Encrypted:	false
SSDEEP:	192:rEYZ6ZQb0614kzjR25WDMn6vlXUxvlXcA:rEY6+bf1F/AoA6NXkNXX
MD5:	53D19F0802814ECB05CB126653E9E9FB
SHA1:	9736773A7DEF1E61627CC2FF034A245D0A93A0D3
SHA-256:	EF4E9E8108B9B4A86DFB184BD1402611B1F429957EF4A68C367CB76F5CE04C62
SHA-512:	4B55C6B497DBD50C9000236EAEBB1F1207DD6B56767F871CE11E4C8F17DC530AC23FC4F6CB79A92B21AA3EB10873C8C745D5E076453BB55B26D5A141626453
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{6381B6AE-E104-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27268

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{6381B6AE-E104-11EB-90E5-ECF4BB2D2496}.dat	
Entropy (8bit):	1.8124770775658368
Encrypted:	false
SSDEEP:	96:rNZCQr6RBSAjJ2FWyMimKt8quHRKt8qu2RA:rNZCQr6RkAjJ2FWyMimQ8BRQ8kRA
MD5:	982E7C8EBEE59300B32DABAA7E7A3BA3
SHA1:	329C11A1C3708568E9E3A80B16DB967DC94CE165
SHA-256:	05E59606F7508D66E16553464DEEDAFC107A112DA7FE829C59F45C2C0FC484F3
SHA-512:	33389C37A2A85C9D65B7D159077951D7A101A6CEE7E1D0A8293E354D2CDE9D069F6CF0B4E7AE4B33EBFB2AA6D9AB219AC5D34800445721CB9CE5A2F3BBD12CD
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{6381B6B0-E104-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27256
Entropy (8bit):	1.808470644144296
Encrypted:	false
SSDEEP:	192:rxZqVQi6TkIjB2lWfMLyGMLH5RGMLPMSA:r3qKNYKw8UuGUGu8
MD5:	8AB48EFC10317CEAA1FE2D0476A916E3
SHA1:	DAC3AB981176A5C155B3415D82A1FFF1B95DB430
SHA-256:	7FF5E0662A770619B57E9887E9D39E34FEDA289DC79354E6F4B5E2F134EBB908
SHA-512:	31336154D2015E64136F33601AD7AA6CB8411C9BBED9CB8C500C57CEE0429AD79D0D345A11F2C143816F96AA4DA018B905079AFEA7D5C531195125CC139B3B4
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{73AF066E-E104-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27264
Entropy (8bit):	1.8086331904448374
Encrypted:	false
SSDEEP:	48:Iw6GcprDGwpanG4pQrGrapbSUGQpB6GHHpc7TGUp8tGzYpmqgGopZmMkKCW3R9lG:r+ZdQJ6fBSMjB2VWTMDKdge28RdgeOfA
MD5:	7355D24494D7F9681275E40882D403F4
SHA1:	B5B61DAEC41A6957B14B256CAAF163EFFE2421D7
SHA-256:	02D6DD1797CA4FB30A5485D708CA54FD9F44DAF94A5CAAD939F8388C24A02A72
SHA-512:	A406F65B587BD3B4912CB66DECDEA3ACDD574C24D849173B8F779FEA2E7EF0A4463A9CC3C6D943DB0D8B39A35B6E796FFE6A07F53880B75A80B60A07D0FA626A
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{73AF0670-E104-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27312
Entropy (8bit):	1.8218355988501604
Encrypted:	false
SSDEEP:	96:rNZWQC6IBSqjp2BWFMxzmUAF3EdxUAF3EqF1A:rNZWQC6Ikqjp2BWFMx6bFUdxbFUqF1A
MD5:	F1179FACA6553E4D2ADFA8FE51BA41E4
SHA1:	F0ABCEA7A141C748996234D4BBA36DD70FB5E5F3
SHA-256:	8800F37EDE6C065D97F8FA4FEF848B4B847534F6270EB1B082E76F989D5A6B29
SHA-512:	10B95A14BF625ABEF92EF0B1926A0F8BD8AE531798EB2747FDC8ED69AE60017C9A4E08591FBB4190C3579AFF2B261C73B3434664BE3110975C50826319456C56
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{73AF0670-E104-11EB-90E5-ECF4BB2D2496}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
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
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: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....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\3Y2ADQKS\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet 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\3Y2ADQKS\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
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.su bstring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var pound Index = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	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
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\9QTQHWWN\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\googlelogo_color_150x54dp[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 150 x 54, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	3170
Entropy (8bit):	7.934630496764965
Encrypted:	false
SSDEEP:	96:c2ZEPhMXQnPkVrTEnGD9c4vnrmBYBaSfS18:c2/XQnPGroGD9vvnXVaq
MD5:	9D73B3AA30BCE9D8F166DE5178AE4338
SHA1:	D0CBC46850D8ED54625A3B2B01A2C31F37977E75
SHA-256:	DBEF5E5530003B7233E944856C23D1437902A2D3568CDFD2BEAF2166E9CA9139
SHA-512:	8E55D1677CDBFE9DB6700840041C815329A57DF69E303ADC1F994757C64100FE4A3A17E86EF4613F4243E29014517234DEBFBCEE58DAB9FC56C81DD147FDC05
Malicious:	false
IE Cache URL:	http://www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png
Preview:	.PNG.....IHDR.....6.....%.`....)IDATx..].pT..>.l.....b..(Hv7 D7.n.8....V..H_.R;S.hY`w.(..*.N_R."0`.-.A..|.*N..`....n..{.&..l.o..;.....a....d..$.....J.1.*.....7+.c...o..T/.~V.r.....D. .G.Ic.....E_.FUR.&..U%...X.4!!Q.H";.....e(Ic...$..."1..jR[.L..../Ek.}AH...W.L.V....Y..S..q...!._r.D....G,%...Hu.$q..\.j.x...G.....]....B.i.l.+B.....Hu.....Q...K;...J.q..._.....:_.x....A:.....j....:c ...^.....k=GIj..Y]B.V..m...Y.\....$..!....+.R%..U/;p.....R4.g.R...XH.3%..JHHby.eqOZdnS..$.. ....dn...$.w....E.o.8...b@.z.)5.L4|.F...9.....pP.8.|....-.M..:..ux...7.]...'..(q..~.....KQ.W...b. .L<.Y.].V+....t4.$.V.O.....D.5..v.j...Hd.M....z.....V..q.p.....;:.J.%2.G.;./.E...I.H. ..../Dk.8.T....+..%Vs4..DC.R.`..Z.....0.[)N!.....%.>&.b.$.M....P.!..!....'Kv..Nd...mvR.:.L.... w..y%.i..H..u....s.Se1.[.).".."..)%.I.....(.#M..4.@....#.....X..P<...k..g....O..I..>-...'._.Q..T.y.=Z.GR{]..&t}*.....>J..!,..X6.HC..$.:.}..z...._b.b.4.E.....;.Ha.?s.

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\NewErrorPageTemplate[1]	
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\G62TDH9B\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=9002
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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....#+....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\G62TDH9B\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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\G62TDH9B\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\OTUW0Q90\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\OTUW0Q90\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....l..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~}s8..&....IEND.B`.

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

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\robot[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 171 x 213, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	6327
Entropy (8bit):	7.917392761938663
Encrypted:	false
SSDEEP:	192:fqjwqVtaVHyEy9BWc2AwJ+3qg1f6WUBIT8mIKPNc93Y8Nm:Yk3WBkAkg1CWUCwmIKS93O
MD5:	4C9ACF280B47CEF7DEF3FC91A34C7FFE
SHA1:	C32BB847DAF52117AB93B723D7C57D8B1E75D36B
SHA-256:	5F9FC5B3FBDDF0E72C5C56CDCFC81C6E10C617D70B1B93FBE1E4679A8797BFF7
SHA-512:	369D5888E0D19B46CB998EA166D421F98703AEC7D82A02DC7AE10409AEC253A7CE099D208500B4E39779526219301C66C2FD59FE92170B324E70CF63CE2B429(
Malicious:	false
IE Cache URL:	http://www.google.com/images/errors/robot.png
Preview:	.PNG........IHDR..................WPLTE...z..z........2........W..{..V........z.....2..3.....V..2..................W.....>`......tRNS.............................Y..j....IDATx....BcI.@A.s..HX....k.0c...T.?n./. ~....b....GM.Gu.c...?.{5.5...4.'.o<...i.O.n<.f..?).g.&..8.E4..tl.4.G.o4.....'.....\......._ ...../.~..<......../.~^.}...?...~...Z../.~.]._ ...I. .Q.Y....YQu..i..4.._ |S...A.-.-h...9...o...k.....9o..?N .U,../+...Z.y...nbMu....4O.7>..Y.-L=J..q..`.B^{4~.p...bR.j.....Gq=..]&..7Y)G6.....A.h`i]...Pd.'.7....9.2...2x.........&..a0N..By.Y.C.*.S......nR.-..A[5.....|.p...+v...d\e..]Yq;.&q0..F.c..... p3.&.`..!q..}...k.g5n#........NG-.9...C..[.7.n.v..u......{o.C&n!.(.G7.JA.'6..{(<....p....:..!=..1.f..''..n.8....~o..N.3l..p.[....*......r..6..z...(.g1qA.[....q.v+..&...B{.I.\..-.....S.y&.......J.Wn!|D. ....+...y.....9.......> .j......{.....K\X.n!..e.I.+'...j...-pA.[..2...8g.DO.#.?p.. ....-.w5.d......4....n..!q..=..Gu.X..O.........sN.h.q..n!..qP

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

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Entropy (8bit):	4.45974266689267
Encrypted:	false
SSDEEP:	3:oVXUTXJ7EH8JOGXnETXJG7n:o9UbGHqEbg7
MD5:	C18CBA6ADE6711248CA5D7805B18FDA1
SHA1:	BD5235B5784ED6F6F3FF94C054B3EEF1D7FD25AB
SHA-256:	1A7EC4E2992080A33E6D7119B19C6E3096E605D52148E9EB953960866ECD0840
SHA-512:	53409E2A597E87C0192376368AE843380678D08B1E52D2D177118284EA70A561E1EAED3866EA675EE7D0891A7A5960F76E89DFA7DA97A213E8584F32E38C96F8
Malicious:	false
Preview:	[2021/07/09 15:24:42.296] Latest deploy version: ..[2021/07/09 15:24:42.296] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF2FCFC3BB466E5731.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39409
Entropy (8bit):	0.5242173715308606
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+xvdc/l+VzIbZ+VzIbl+VzIbK:kBqoxKAuqR+xvdc/l+pIF+pIx+pIW
MD5:	73329ED3AF6E87AAA47A37873CB490BA
SHA1:	179667E389BA5273E725EF23E9452016F0DB0CF7
SHA-256:	180D5D5452E7E9AD6AFCD4616E92A0F8C84DCFA5B03108C84615F7C3113B38E5
SHA-512:	062633C01A08E62A5B26B1BC614643869DA21C5FD2A5B0E90D6A1162CC8ED052C70EA75DB07EFADD2997FBC2A55B066570B9FF9E6E5E64D72C81E9D6834D64 2
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF37FF5ADB2A3C5C85.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39521
Entropy (8bit):	0.5462309734247927
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+357yZwmUAF3EWmUAF3EFUAF3EK:kBqoxKAuqR+357yZ7bFUxbFUFbFUK
MD5:	C425F6B267A0465BB17DCB3E571FF5A0
SHA1:	3C5898378E982C41A42C1101B3BC768EF3301399
SHA-256:	DA12B1C0B7D54A8503AAC76C311DEFFFB18561C34DFD7709D79808D260297283
SHA-512:	550F0C2043440002B74FEB023B6D072208FC27AB1EE47F9533355CB3FE81613D0144A4B9F1521C4ACAA9130D1F857075D210554A09E16781A4E3CE7D2D8A0860
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF3F9E1034F19351C0.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39433
Entropy (8bit):	0.5303714089486941
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+FrJ4btKt8qucKt8quQKt8qu5:kBqoxKAuqR+FrJ4btQ8uQ8CQ8z
MD5:	B5D386DF0BE0580FC2C231BFD46FD823
SHA1:	1D1F9C9477897FCAAD3CD92F080E32420C51815F
SHA-256:	29531CD8BB74AFF1110CD09AF7FE1413799733A2A22C03472DC7039FD31BBC9F
SHA-512:	5EA6B0BCADD5CD2809A4852FCE87CBE32D37FE96DB2B6B86EF2CD9CE3E0CE67897E1150828737CBDF3E52CDF4E76B18A293FE210ADCC0A92F682704C8B79E 525
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF5262AAEC80EEA271.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13237
Entropy (8bit):	0.5968208270390676
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loR9lox9lWmhH6hH6H08kVn9UhH0xNykKxNykN/:kBqoIakWqa/cn94qNylNys/
MD5:	CAE2D43708FDFEDC6701CE721A62C9A7
SHA1:	D4301490938CDB0596739B573553264774469817
SHA-256:	726162562205A89C0DD2CAA459FD1930589DD28BBFD76546AEF15AB819226E0B
SHA-512:	602458C8692AC9E65169AADC5339D6A947EB6F986B195C68E30A664B0C45E3AA6230C0EDF9EC2540399FD6DC8E6998C48E3F3C8E5A888F2C1B90D4FA6DFE8A4
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF7FBE38EED9F80135.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13237
Entropy (8bit):	0.5985413402485092
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loX9loX9lWE96+haPLuhanxan3P/:kBqoIYGcl5YEn
MD5:	9A85001A539F5FE426BE69F69B4C616C
SHA1:	B94ED00B0024057F33BB5D864423D2B2E74F5E90
SHA-256:	962BB0DB7476452650AFEB374A643195F565B9B86FA044121E7A71FF44F41167
SHA-512:	C0FA26451620662A1A940034824D186F833CEF8528FB5C140CE52641B676A854D908DC701F161309277F26C56CF2350522047C986C7C4ACAC111E8D0E4087023
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF9E247E5B8AC6418E.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39393
Entropy (8bit):	0.521014182505455
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+WQKjQevUKXOvUKXWvUKXv:kBqoxKAuqR+WQKjQevlXOvlXWvlXv
MD5:	E7571657C8E60647FFF6FC995A8E3F9D
SHA1:	CDBAF6E94ACEA9CB016BFF331E1B1C21262F6C54
SHA-256:	9358E491ACBC78F1CC55D0CAAABE406D5F25399E5AF634C4060411CC3E387FB3
SHA-512:	E9E3BB9D7B881635409C66F66DBB13867874CF97933F046CDAE3FA61E9267231FD766F1B7821E02D1D92E1CE611258CC30D9A6D9989A253D19F93A18DFD00D7
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFA7D5D08F02F08219.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39409
Entropy (8bit):	0.525703108618034
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+DdvmtHSlMqOWSlMqO2SlMqOv:kBqoxKAuqR+DdvmtHGMLWGML2GMLv
MD5:	EFE671830B139377402A1ED7E3CCF816
SHA1:	C0AED281E80F6E05E343B7A65AB27D414F2C7995
SHA-256:	EF07F596F23B2E8DC2543035AD6C58C354769DE7522A1429729AF49EF6329A30

Copyright Joe Security LLC 2021

C:\Users\user\AppData\Local\Temp\~DFA7D5D08F02F08219.TMP	
SHA-512:	68C72BACC80C6206C053CABBACDCE0CCBDDEC7721DA6ED2C1705DFA5CEDC455257BF5B34AD3150D772D29FC915620E1AAEC6E13CF9765D1BCCA9E35753A 71A3
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFCC73204E5D3290B9.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13237
Entropy (8bit):	0.5941164485926635
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loE9loU9lWXvQINcINyzINyiR:kBqoIv5/ZNDZ
MD5:	689F587B5BD42F0DF983C37DF23CA9CD
SHA1:	CBC78527AFABDBF6867C7D943387A9D0E0B50A5A
SHA-256:	537525993439B1C0E560E6079386A9B6EC99307899ABE68A8FDF425CD22D056C
SHA-512:	9E7B7F0F8AAEFF77B98D38F18B463B8FBC40AD99EB50314307B2A13CFB807A79B80DD695A91F82DF27D790B6E84758568F2A44A373314C15A61418934E528930
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFDCADCAD629B07705.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39425
Entropy (8bit):	0.52641825117157
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+g4l3eqIqnmMkKCW3R9luDIFmMkKCW3R9luDIkMkKCW3R9luDIV:kBqoxKAuvScS+rl3elHdgeBdgeldgeq
MD5:	B837B9544B6D62BBE35F348410004255
SHA1:	F7D0A81ED6E2CB03D00638F96EA4C588F41A5835
SHA-256:	2B33EDAA4C35443E7BFC32584198B915A020DCF85767B8EDD7009934F57904F1
SHA-512:	FA72E357720676FF4243D37977A5F6BEB4D35E9234848DF1670ABC1D28934D762A38C20DE6B94C6EC8AE4DC17C852635E940E77F330E2B9E73B31D5E65CEBCF
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.1671007952517
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	d7b.dll
File size:	177664
MD5:	d7b3fe9b94d3896df9d9f77b37adbf37
SHA1:	6b71978633aa2f91c15ef48eaf3cc4dd54ea7dd0
SHA256:	f7a1ecdd925fd1e03ff08f547b24a10e64a5996060feab65e77f6ca0339b6a00
SHA512:	cfa2df5ba9995cc4620394064a233a4def23184a1a01b9b22b0eaa0325fe6450e26a4a5fe7cf5e77f6608a60f8780f90bb87bf84f111645d38f4b66f22e731ff

Copyright Joe Security LLC 2021

General

SSDEEP:	3072:dCIks3iqbneE3yl7w51ftkvWpos24f8DauYpEwDSQ9pFq7mvY:3RSqb5201V60K4f8DanDSAFU
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5.....4.....1.....Rich.....PE..L.....x]...

File Icon



Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x41417a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5D78D3B5 [Wed Sep 11 11:00:05 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	ac619a5e9649fa4ff2fcaed7df41e611

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x17818	0x17a00	False	0.835400132275	data	6.99787070557	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x19000	0x9e4a	0xa000	False	0.692114257813	data	5.9333412859	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x23000	0x907a3c	0x4a00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x92b000	0x10	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x92c000	0x4ac4	0x4c00	False	0.105674342105	data	1.26252413606	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

Exports

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/09/21-15:23:30.291744	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49724	80	192.168.2.6	172.217.168.78

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 9, 2021 15:24:16.723835945 CEST	192.168.2.6	8.8.8.8	0x57f6	Standard query (0)	ooakieyrc.xyz	A (IP address)	IN (0x0001)
Jul 9, 2021 15:24:17.984766960 CEST	192.168.2.6	8.8.8.8	0xa1be	Standard query (0)	ooakieyrc.xyz	A (IP address)	IN (0x0001)
Jul 9, 2021 15:24:19.478872061 CEST	192.168.2.6	8.8.8.8	0x6acf	Standard query (0)	ooakieyrc.xyz	A (IP address)	IN (0x0001)
Jul 9, 2021 15:24:20.353898048 CEST	192.168.2.6	8.8.8.8	0x27e8	Standard query (0)	ooakieyrc.xyz	A (IP address)	IN (0x0001)

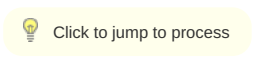
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 9, 2021 15:24:16.797673941 CEST	8.8.8.8	192.168.2.6	0x57f6	No error (0)	ooakieyrc.xyz		139.59.150.28	A (IP address)	IN (0x0001)
Jul 9, 2021 15:24:17.998545885 CEST	8.8.8.8	192.168.2.6	0xa1be	No error (0)	ooakieyrc.xyz		139.59.150.28	A (IP address)	IN (0x0001)
Jul 9, 2021 15:24:19.493341923 CEST	8.8.8.8	192.168.2.6	0x6acf	Server failure (2)	ooakieyrc.xyz	none	none	A (IP address)	IN (0x0001)
Jul 9, 2021 15:24:20.368391991 CEST	8.8.8.8	192.168.2.6	0x27e8	Server failure (2)	ooakieyrc.xyz	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 5604 Parent PID: 5764

General

Start time:	15:23:03
Start date:	09/07/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\d7b.dll'
Imagebase:	0x860000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
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: 00000000.00000003.386739440.0000000003458000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.386787805.0000000003458000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.386833228.0000000003458000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.386804155.0000000003458000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.386611964.0000000003458000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.594418378.0000000003458000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.386843346.0000000003458000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.386704666.0000000003458000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.386554114.0000000003458000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 3180 Parent PID: 5604

General

Start time:	15:23:04
Start date:	09/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\d7b.dll',#1
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 5672 Parent PID: 5604

General

Start time:	15:23:04
Start date:	09/07/2021

Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\d7b.dll,Moleculenotice
Imagebase:	0x13b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 6136 Parent PID: 3180

General

Start time:	15:23:04
Start date:	09/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\d7b.dll',#1
Imagebase:	0x13b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.384867126.0000000005308000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.384991598.0000000005308000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000002.596356802.0000000005308000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.384681414.0000000005308000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.385026148.0000000005308000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.385049727.0000000005308000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.385084591.0000000005308000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.384965086.0000000005308000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.385068995.0000000005308000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 5640 Parent PID: 792

General

Start time:	15:23:28
Start date:	09/07/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false

Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff721e20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 5532 Parent PID: 5640

General

Start time:	15:23:29
Start date:	09/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5640 CREDAT:17410 /prefetch:2
Imagebase:	0x1a0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 5548 Parent PID: 5640

General

Start time:	15:23:30
Start date:	09/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5640 CREDAT:17414 /prefetch:2
Imagebase:	0x1a0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 7080 Parent PID: 792

General

Start time:	15:24:12
Start date:	09/07/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff721e20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 5572 Parent PID: 7080

General

Start time:	15:24:14
Start date:	09/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7080 CREDAT:17410 /prefetch:2
Imagebase:	0x1a0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 6168 Parent PID: 7080

General

Start time:	15:24:16
Start date:	09/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7080 CREDAT:17414 /prefetch:2
Imagebase:	0x1a0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 5248 Parent PID: 792

General

Start time:	15:24:40
Start date:	09/07/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff721e20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 5392 Parent PID: 5248

General

Start time:	15:24:41
Start date:	09/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5248 CREDAT:17410 /prefetch:2
Imagebase:	0x1a0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 5468 Parent PID: 5248

General

Start time:	15:24:42
Start date:	09/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5248 CREDAT:17414 /prefetch:2
Imagebase:	0x1a0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Copyright Joe Security LLC 2021

Code Analysis